



Universidad
Norbert Wiener

Facultad de Ingeniería y Negocios
Escuela Académico Profesional de Ingenierías

ISO 27001 para mejorar la seguridad de la
información en una institución educativa, Lima
2022

**Tesis para optar el título profesional de Ingeniero de
Sistemas e Informática**

Presentado por:

Asqui Zevallos, Jhojan Alex

Código ORCID: 0000-0003-4984-9331

Torres Vásquez, Jean Pool

Código ORCID: 0000-0002-3177-6501

Asesor: Dr. Flores Zafra, David

Código ORCID: 0000-0001-5846-325X

Línea De Investigación General De La Universidad

Sociedad y transformación digital

Línea De Investigación Específica De La Universidad

Seguridad Digital

Lima - Perú

2023

 Universidad Norbert Wiener	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo, Jhojan Alex Asqui Zevallos y Jean Pool Torres Vasquez egresados de la Facultad de Ingeniería y Negocios Escuela Académica Profesional de Ingenierías privada Norbert Wiener declaro que el trabajo académico "ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022" Asesorado por el docente: Mg. Walter Amador Chávez Alvarado DNI 09731774 ORCID 0000-0001-8614-482X tiene un índice de similitud de 8 (ocho) % con código oid:14912:204659547, verificable en el reporte de originalidad del software Turnitin. Así mismo:

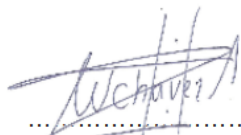
1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.



.....
Jhojan Alex Asqui Zevallos
 DNI: 73523107



.....
Jean Pool Torres Vasquez
 DNI: 76406517



.....
Walter Amador Chavez Alvarado
 DNI: 09731774

Lima, 3 de febrero de 2023

**ISO 27001 para mejorar la seguridad de la información en una
institución educativa, Lima 2022.**

Asesor temático:

Mg. Chávez Alvarado, Walter Amador (ORCID: 0000-0001-8614-482X)

Asesor metodólogo:

Dr. Flores Zafra, David (ORCID: 0000-0001-5846-325X)

Agradecimiento

Agradecemos primeramente a Dios por guiarnos en este camino muy difícil, y también agradecer enormemente a nuestros padres por darnos su apoyo incondicional en nuestra etapa universitaria y por último agradecer a nuestros amigos y docentes que en verdad se preocuparon por brindar una educación de calidad.

Índice general

	Pág.
Portada	i

Título	iii
Dedicatoria.....	iv
Agradecimiento	iv
Índice general	v
Índice de tablas	viii
Índice de figuras	ix
Resumen	x
Abstract.....	xi
Introducción.....	xii
CAPITULO I: EL PROBLEMA	13
1.1. Planteamiento del problema.....	13
1.2. Formulación del problema	16
1.2.1. Problema general	16
1.2.2. Problemas específicos.....	16
1.3. Objetivos de la investigación.....	16
1.3.1. Objetivo general	16
1.3.2. Objetivos específicos	16
1.4. Justificación de la investigación	17
1.4.1. Teórica	17
1.4.2. Metodológica.....	17
1.4.3. Práctica	17
1.5. Limitaciones de la investigación.....	18
CAPITULO II: MARCO TEÓRICO	19
2.1. Antecedentes de la investigación	19
2.2. Bases teóricas.....	22
2.3. Formulación de hipótesis	28
2.3.1. Hipótesis general	28
2.3.2. Hipótesis específicas.....	29
CAPITULO III: METODOLOGÍA	30
3.1. Método de investigación	30
3.2. Enfoque investigativo	30
3.3. Tipo de investigación.....	31
3.4. Diseño de la investigación	31
3.5. Población, muestra y muestreo	31

3.6.	Variables y operacionalización.....	32
3.7.	Técnicas e instrumentos de recolección de datos	33
3.7.1.	Técnica.....	33
3.7.2.	Descripción.....	33
3.7.3.	Validación.....	33
3.7.4.	Confiabilidad	34
3.8.	Plan de procesamiento y análisis de datos	34
3.9.	Aspectos éticos	35
CAPITULO IV: PRESENTACION Y DISCUSIÓN DE LOS RESULTADOS.....		36
4.1.	Resultados.....	36
4.1.1	Análisis descriptivo de resultados	36
4.1.2	Prueba de hipótesis.....	39
4.1.3	Discusión de resultados.....	48
CAPITULO V: CONCLUSIONES Y RECOMENDACIONES.....		51
5.1.	Conclusiones.....	51
5.2.	Recomendaciones	53
REFERENCIAS		54
ANEXOS		60
	Anexo 1: Matriz de consistencia	60
	Anexo 2: Instrumentos	62
	Anexo 3: Validez del instrumento.....	64
	Anexo 4: Confiabilidad del instrumento	73
	Anexo 5: Desarrollo de la ISO 27001	74
	Anexo 6: Informa del asesor de turnitin.....	1009

Índice de tablas

	Pág.
Tabla 1 Datos procesados	36
Tabla 2 Frecuencias Estadísticas	38
Tabla 3 Consolidación de los 3 indicadores	40
Tabla 4 Tasa de incidentes incremental de la confidencialidad	40
Tabla 5 Prueba de normalidad en hipótesis 1	41
Tabla 6 Prueba T-Student – indicador tasa de incidentes que afectan la confidencialidad.	41
Tabla 7 Prueba T-Student –incidentes en confidencialidad	42
Tabla 8 Tasa de incidentes incremental de la integridad.....	43
Tabla 9 Prueba de normalidad en hipótesis 2	43
Tabla 10 Prueba T-Student – indicador tasa de incidentes que afectan la integridad	44
Tabla 11 Prueba T-Student –incidentes en integridad.....	44
Tabla 12 Tasa de incidentes incremental de la disponibilidad	45
Tabla 13 Prueba de normalidad en hipótesis 3	46
Tabla 14 Prueba T-Student – indicador tasa de incidentes que afectan la disponibilidad ..	47
Tabla 15 Prueba T-Student – incidentes en disponibilidad	47

Índice de figuras

	Pág.
Figura 1 Árbol de problemas.....	15
Figura 2 Tasa de incidentes que afectan la confidencialidad	37
Figura 3 Tasa de incidentes que afectan la integridad.....	37
Figura 4 Tasa de incidentes que afectan la disponibilidad	38
Figura 5 Consistencia de la tasa de incidentes que afecta la confidencialidad.....	41
Figura 6 Reducción de la tasa de incidencia que afecta la confidencialidad.....	42
Figura 7 Consistencia de la tasa de incidentes que afecta la integridad	43
Figura 8 Reducción de la tasa de incidencia que afecta la integridad	45
Figura 9 Consistencia de la tasa de incidentes que afecta la disponibilidad	46
Figura 10 Reducción de la tasa de incidentes que afecta la disponibilidad.....	47

Resumen

El estudio tuvo por objetivo demostrar como la ISO 27001 mejora la confidencialidad, la integridad y la disponibilidad de la información en una institución educativa. El trabajo es de diseño experimental de enfoque cuantitativo y aplicada para el tipo de investigación, alineado a los métodos deductivo, hipotético y analítico.

La población estuvo constituida de 24 controles dentro de los parámetros de la ISO 27001, donde la muestra tuvo como resultado un aproximado de 20 controles a revisar. Además, se utilizó como técnica la observación y como instrumento se empleó la guía de observación. Para La implementación de la ISO 27001 se utilizó los controles del ANEXO A, también como guía de referencia se utilizó la ISO 27002 y por último se empleó el ciclo de Deming para mejora continua de las políticas de seguridad. En la parte estadística, se manejó la estadística inferencial utilizando la prueba de T-Student por presentar indicadores paramétricos. Los resultados evidenciaron que la ISO 27001 mejora la seguridad de la información, observando una reducción significativa en las tasas de incidentes del 61.38% en la confidencialidad, un 61.73% en la integridad y 61.83% en disponibilidad.

Palabras claves: ISO 27001, seguridad de la información, disponibilidad, confidencialidad e integridad.

Abstract

The objective of the study was to demonstrate how ISO 27001 improves the confidentiality, integrity, and availability of information in an educational institution. The work is of experimental design of quantitative and applied approach for the type of investigation, aligned to the deductive, hypothetical, and analytical methods.

The population consisted of 24 controls within the parameters of ISO 27001, where the sample resulted in approximately 20 controls to be reviewed. In addition, observation was used as a technique and the observation guide was used as an instrument. For the implementation of ISO 27001, the controls of ANNEX A were used, ISO 27002 was also used as a reference guide and finally the Deming cycle was used for continuous improvement of security policies. In the statistical part, the inferential statistics were handled using the T-Student test for presenting parametric indicators. The results showed that ISO 27001 improves information security, observing a significant reduction in incident rates of 61.38% in confidentiality, 61.73% in integrity and 61.83% in availability.

Key words: ISO 27001, information security, availability, confidentiality, and integrity.

Introducción

Actualmente, la tecnología ha ido avanzando y los ciberdelitos también han evolucionado, por ello, la ISO 27001 permitirá mejorar la seguridad de la información, de esta manera la parte administrativa de la institución tomaron decisiones basándose en la información obtenida al verificar la reducción de la tasa de incidentes al ser implementada. Seguidamente, se detalla los 5 capítulos.

Capítulo I: En el problema, se describe el planteamiento del problema del estudio. Asimismo, se formuló el problema y los objetivos de la investigación. De igual forma, se describe la justificación teórica, metodológica y práctica.

Capítulo II: Para el marco teórico, se observa los antecedentes nacionales e internacionales. Asimismo, en las bases teóricas se utilizó teorías que dan sustento a la investigación, así como conceptos para ambas variables. Por último, para la hipótesis se formularon hipótesis general y específicas.

Capítulo III: En la metodología, se describe enfoque, método, diseño, tipo, población y muestra de la investigación. Seguidamente, se procedió con la operacionalización de las variables. Por otra parte, para la validación y confiabilidad se utilizó técnicas e instrumentos. De igual forma, se realizó el procesamiento y análisis de datos. Por último, resaltamos los aspectos éticos que empleamos en la investigación.

Capítulo IV: Resultados y discusiones, se presentó el análisis descriptivo. Seguidamente, para las hipótesis se hicieron las pruebas de consistencia, normalidad y de contraste. Por último, se procedió a realizar la discusión donde se comparan los resultados obtenidos con la de los autores citados anteriormente.

Capítulo V: En las conclusiones y recomendaciones, se planteó 3 conclusiones por cada problema encontrado y 3 recomendaciones más allá de nuestra investigación al personal de la institución que puedan tomar decisiones.

CAPITULO I: EL PROBLEMA

1.1. Planteamiento del problema

Hoy en día, todo lo que se refiere a sistema, informática y tecnología, han dado un gran paso al siguiente nivel, pero esto conlleva a que la seguridad la información sea más vulnerable ante posibles amenazas, del mismo modo, existen buenas prácticas para mitigar estas amenazas sin embargo no hay sustento que lo respalde, por otro lado, la ISO 27001 cuenta con el reconocimiento internacional cuyo objetivo es proteger los 3 principios de la información.

En una revista de Estados Unidos indican que, el progreso de la sociedad ha ido evolucionando cada vez más gracias a los distintos equipos inteligentes, la vida de las personas ahora es más conveniente, pero que a la vez están expuestos a enormes riesgos de seguridad y privacidad (Lin *et al.*, 2022). Asimismo, en la India el robo datos es un tema preocupante debido a que las empresas en crecimiento han optado por economizar costos en el proceso de información y se han enfocado mucho más en la subcontratación en el extranjero (Tushar, 2011). Es decir, mientras la tecnología se extienda más en la vida humana, los delitos informáticos también incrementarán, por eso las empresas no deberían dejar en segundo plano la seguridad de la información.

En una noticia periodística en Londres, informaron que hackers norcoreanos habían robado casi \$1 millón de dólares en bitcoin a proveedores de salud, con una versión mejorada de ransomware para secuestrar datos informáticos (Tidy, 2022). También, en un informe realizado en la nación de Reino Unido se verificó que 4163 organizaciones, habrían sido víctimas de ataques cibernéticos en los años 2018 a 2019 (Fernandez *et al.*, 2022). En resumen, cada año los delitos informáticos van evolucionando a tal punto de que no existe una seguridad cien por ciento segura.

En un estudio realizado en Sudáfrica, se indicó que, para abordar esta deficiencia sobre la seguridad de la información, es fundamental tener éxito en las campañas de concientización sobre seguridad para transmitir el conocimiento de forma satisfactoria (Snyman y Kruger, 2022). Además, para transmitir este conocimiento sobre seguridad de la información es esencial que tanto formadores como alumnos trabajen en conjunto para que se realicen las mejoras de la seguridad (Spears y San Nicolas, 2015). Por ello, las campañas realizadas de la seguridad de la información casi nunca logran cumplir con sus objetivos porque no hay un trabajo en conjunto entre el ente realizador y las personas.

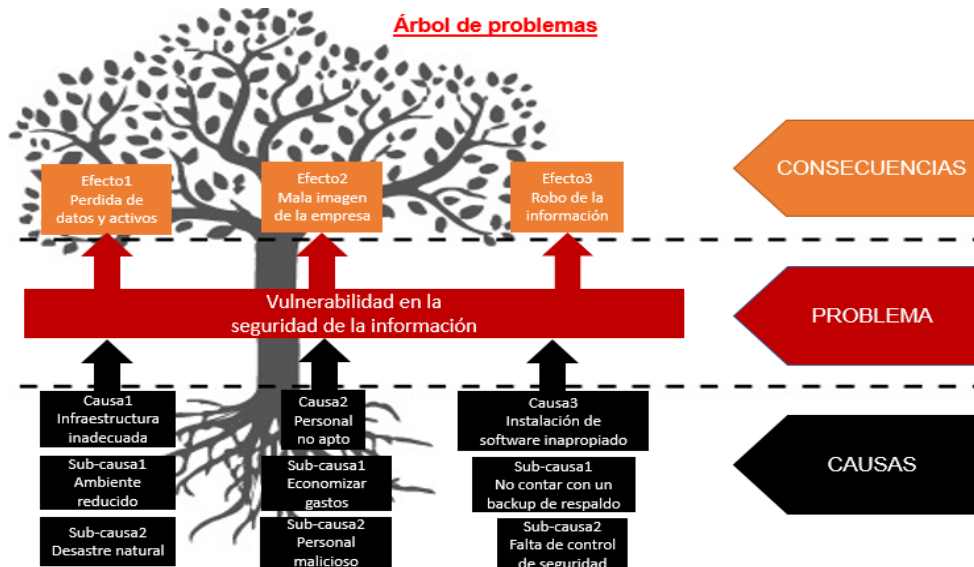
En Perú las pérdidas por ciberataque se estimaron en promedio a 5 mil millones de dólares, puesto que la gestión de riesgos cibernéticos debería tomarse como un tema comercial más serio (García *et al.*, 2018). A su vez, la gestión de seguridad es esencial en las organizaciones, ya que nos ayuda a proteger la información y con ella se busca la integridad y la confidencialidad de los atributos informáticos. Según Kaspersky (2022) nos dice que, en el año 2022, la nación peruana se encuentra en el ranking número 17 entre los países que más ataques cibernéticos ha sufrido, lo que nos da a entender que el Perú muestra signos de vulnerabilidad con respecto a países de primer mundo. De igual manera, Andina (2022) indicó que, el aumento de las amenazas y ataques donde se recopila información de sistemas vulnerables haciendo así su selección de objetivos de acuerdo con su descubrimiento se debe al trabajo remoto. En resumen, los ataques informáticos se dan de la misma manera dentro o fuera del Perú, siendo uno de los países con mayor tasa de ataques en los últimos años.

En la figura 1, se utilizó la herramienta de análisis “árbol de problemas” en donde se identificó diversas causas y consecuencias como: (a) infraestructura inadecuada: debido al ambiente reducido y ante un desastre natural tendría como efecto la pérdida de los datos y activos en la institución superior; (b) personal no apto: debido a economizar gastos se

contratan personal sin conocimientos básicos y maliciosos, lo que en efecto ocasiona una mala imagen de la empresa y (c) instalación de software inapropiado: debido a no tener un control de seguridad y no contar con una copia de seguridad, tendría como consecuencia el robo de la información en contra de la institución educativa. En general, la institución no cuenta con políticas para proteger la información, por ello, no existe un procedimiento ante un posible ataque o fuga en la información. Además, no se realiza encriptación en la información, por ende, la información es vulnerable al caer en el poder de personas no autorizadas, Por último, los activos críticos no están bien definidos y clasificados, por lo cual, no hay conocimiento claro de que activos guardan información importante. En consecuencia, al no presentar políticas y procedimientos ante un ataque en la seguridad de la información, todo sistema, archivo, datos relacionados a la información estarían expuestos al atacante para su propio beneficio, pudiendo extorsionar a la víctima, con hacer público datos sensibles.

Figura 1

Árbol de problemas.



1.2. Formulación del problema

1.2.1. Problema general

“¿De qué manera la ISO 27001 mejora la seguridad de la información en una institución educativa, Lima 2022?”

1.2.2. Problemas específicos

PE1: “¿De qué manera la ISO 27001 mejora la confidencialidad de la información en una institución educativa, Lima 2022?”

PE2: “¿De qué manera la ISO 27001 mejora la integridad de la información en una institución educativa, Lima 2022?”

PE3: “¿De qué manera la ISO 27001 mejoran la disponibilidad de la información en una institución educativa, Lima 2022?”

1.3. Objetivos de la investigación

1.3.1. Objetivo general

“Demostrar cómo la ISO 27001 mejora la seguridad de la información en una institución educativa, Lima 2022.”

1.3.2. Objetivos específicos

OE1: “Demostrar cómo la ISO 27001 mejora la confidencialidad de la información una institución educativa, Lima 2022.”

OE2: “Demostrar cómo la ISO 27001 mejora la integridad de la información una institución educativa, Lima 2022.”

OE3: “Demostrar cómo la ISO 27001 mejora la disponibilidad de la información una institución educativa, Lima 2022.”

1.4. Justificación de la investigación

1.4.1. Teórica

Como parte del respaldo teórico, se plasmaron 3 teorías que sirven como soporte para las variables. Estas son: (a) la teoría de la información, de modo que, si la información es alterada durante el proceso ambas variables tratan de analizar el impacto para minimizar los riesgos que puedan surgir; (b) la teoría de la mejora continua, dado que, ambas variables tienen la mejora continua implícita dentro de sus argumentos es perfecta para abordar los temas derivados a ellas y (c) la teoría de sistemas, de modo que, ambas variables en sí son un conjunto de elementos que forman un tema en particular.

1.4.2. Metodológica

Para la justificación metodológica se usó enfoque cuantitativo, además, se utilizó un diseño experimental porque se realiza un pre experimento entre las variables de la ISO 27001 para mejorar la seguridad de la información. Con el propósito de, mitigar las vulnerabilidades en la institución educativa. Asimismo, la investigación ayudará a futuros investigadores a tener una perspectiva del uso de estadísticas e instrumentos para determinar los riesgos y amenazas que tiene dejar de lado la seguridad de la información.

1.4.3. Práctica

El trabajo tiene como finalidad mejorar la seguridad de información y así asegurar la accesibilidad a los datos, facilitando una serie de políticas en cuanto a la aplicación y las maneras en las que se utilizará, además, la institución contará con la implementación de 20 controles de la ISO 27001, las cuales se enfocan en: seguridad de las comunicación, para mitigar los incidentes de la confidencialidad, criptografía, para mitigar los incidentes de la integridad y por último, la gestión de los activos, para mitigar los incidentes de la disponibilidad. Asimismo, la institución obtendrá una aseguración de activos importantes

información e imagen corporativa. Las mejoras se verán afectadas en todas las siguientes dimensiones: (a) disponibilidad, (b) confidencialidad y (c) la integridad.

1.5. Limitaciones de la investigación

1.5.1. Temporal

El estudio se realizó en noviembre y diciembre de 2022.

1.5.2. Espacial

El estudio fue realizado en una institución educativa ubicada en Lima, Perú.

1.5.3. Recursos

En el estudio se estimó un valor de S/ 3050, el cual fue financiado con un 80% por la parte interesada y un 20% por los investigadores.

CAPITULO II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

Chávarry (2021), presentó un estudio que tuvo por objetivo general implementar la norma “ISO 27001” Y “27002” adaptada a la gestión de seguridad de información. La metodología tuvo un diseño cuasi experimental aplicada, como resultado se obtuvo que el tiempo para responder incidencias de seguridad de información se redujeron de 36.5 a 9.8 minutos. Como conclusión después de haber implementado las ISO 27001 y 27002 adaptada a gestión de seguridad se aceptaron las hipótesis, mejorando el tiempo de respuesta para la atención de incidencias un 27% en la secretaria ejecutiva.

Silva (2022), presentó un estudio que tuvo como objetivo general mejorar la seguridad de la información a través de un sistema. Cuyo diseño de investigación fue experimental de tipo aplicada, asimismo con un enfoque mixto. Como resultado obtuvieron una mejora en la variable dependiente al implantar un SGSI fundamentado en la norma ISO 27001. Como conclusión después de haber implantado el SGSI se aceptaron las hipótesis, garantizando la continuidad de las operaciones, incrementa la productividad del talento humano con relación a la reducción de incidentes, que se generaban por su poca seguridad información.

Porras (2020), en una de sus investigaciones realizadas, tuvo como objetivo general analizar los resultados de la implementación de una gestión de riesgos en servicios de la información. De igual manera la metodología empleada en la investigación fue del tipo aplicada, de nivel explicativo, con diseño de investigación experimental. Además, se tomó en cuenta 114 controles del anexo A de la ISO 27001 como población y parte de la muestra fueron 70 controles. En cuanto a los resultados el valor promedio subió de 3.65 a 5.22 teniendo como mejora la gestión de los riesgos en los activos informáticos. Finalmente

concluyeron que al implementar un SGSI se obtuvieron resultados óptimos en la gestión de riesgos de activos informáticos.

Huacasi (2018), desempeñó un estudio cuyo objetivo fue incrementar el proceso de seguridad de la información considerando insertar un sistema. Además, el diseño fue pre experimento de nivel explicativo de enfoque cuantitativo aplicado. Con respecto a los resultados de la aplicación de una SGSI permitió identificar activos críticos relacionado a la seguridad de la información, como también identificar las vulnerabilidades y amenazas hechas con la gestión de riesgos que presenta la dirección con seguridad de información.

Vásquez (2018), presentó un trabajo lo cual tuvo como objetivo proteger la información mediante la implantación de una metodología de riesgos. El trabajo tiene como diseño experimental de tipo descriptiva aplicada. Como resultado después de identificar, analizar, evaluar y tratar el riesgo, identificó que la implementación de controles para minimizar esas brechas trajo una mejora significativa para el desarrollo de las políticas de 14% al 81% y de 52% al 91% en controles del anexo A. El trabajo concluye que la SGSI ISO27001:2013 permitió defender la información de distintas amenazas.

Ortiz (2018), efectuó un estudio donde tuvo como objetivo general mejorar la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva implementando de forma progresiva la norma ISO 27002:2013. Con respecto a la metodología se utilizó el diseño cuasi experimental de tipo aplicada. Para los resultados se manifestaron diez indicadores de la gestión de seguridad con respecto al antes y después de los riesgos disminuyeron en un promedio del 11%. En conclusión, se afirma con una confianza del 95 % al implementar los controles de seguridad de la información de la Norma ISO 27002 existe una mejora positiva como mínimo al 5% en la gestión de seguridad de la información.

Con temas relacionados internacionalmente tenemos a Prada y Ortiz (2022), que presento una tesis que tuvo como objetivo diseñar un SGSI lo cual permitirá gestionar la seguridad de información en el campo de TI. En la cual, presento una metodología de diseño experimental con enfoque cualitativo aplicado. Como resultado, se implantaron políticas de seguridad para el área de tecnología y comunicación. Por lo tanto, concluyeron que el desarrollo del SGSI tendrá una mejora en cuanto a protección de los activos de información, agilizando también el tiempo en que responde el sistema que tiene una red de datos.

Peñañiel (2019) realizó su tesis en Ecuador, donde su objetivo fue diseñar un modelo de los procedimientos de seguridad de información, en miras de implementar un sistema de gestión de seguridad de la información de la norma ISO 270001:2013 dentro de un ambiente “cloud computing”. Donde la metodología utilizada es del tipo descriptivo de diseño simple con enfoque cualitativo. Los resultados obtenidos al hacer uso de la norma ISO 27001 fueron factibles en el ambiente cloud computing. En conclusión, la norma ISO 27001 brinda al proveedor la opción de manejar los recursos sin dejar que la información se encuentre expuesta.

Moreira (2019), ejecutó su trabajo de investigación en Calceta Ecuador, donde tuvo como objetivo desarrollar un plan de gestión basado en la norma ISO/IEC 27001 para mejorar la seguridad de la información de la infraestructura técnica y sistemas informáticos del Municipio Autónomo Descentralizado del Estado de Chone. Para el trabajo utilizó la metodología de diseño experimental de tipo aplicada con enfoque cuantitativo. Cuyo resultado fue elaborar un plan de gestión de seguridad de la información donde plantea varias soluciones al departamento tecnológico. En conclusión, la propuesta permite mejorar todo aspecto de seguridad de TI para salvaguardar la integridad de sus datos.

Rajab (2018), en su investigación en Michigan su objetivo primordial fue el estudio de la intención de los empleados de cumplir con las políticas de seguridad de información

en la educación superior. La metodología de la investigación fue de enfoque mixto secuencial explicativo. Asimismo, en los resultados sobre la recogida y el análisis de datos beneficia a los colegios y universidades para diseñar mejor las soluciones preventivas, ahorrando así posibles pérdidas financieras y de reputación. En conclusión, los futuros estudios sobre la intención de cumplimiento de la seguridad de la información (PSI) deberían incluir la vulnerabilidad y eficacia en respuesta a elementos principales de sus modelos.

En el ámbito internacional Haz y Cervantes (2017), en su presente trabajo tuvieron como objetivo desarrollar un proceso para identificar, medir y manejar los riesgos de información al aplicar normas y estándares nacionales e internacionales. Para ello, utilizaron el enfoque mixto, con método analítico, deductivo e inductivo. Como resultados se obtuvo que la inserción de un SGSI mejoró la mitigación de riesgos y que estas sean procesos sostenibles en el tiempo y ejecutados por los personales capacitados. En conclusión, crear y aprobar procesos formales de seguridad en áreas tecnológicas y de información son un factor fundamental para la realización y cumplimiento de estas, más aún si estas son creadas por estándares y normas internacionales aceptadas mundialmente lo que facilita la inserción y aceptación por la parte involucrada.

2.2. Bases teóricas

El estudio comprende 3 teorías que son la base de las variables: Entre ellas tenemos: (a) la teoría de la información, según Shannon y Weaver (1949) indican que, tiene como base la transmisión de un mensaje de emisor a receptor, y que parte del mensaje puede ser alterado o barrado por un agente externo, por lo tanto, guarda relación con la variable ISO 27001, ya que reduce la complejidad a la hora de evaluar riesgos en seguridad de la información (Calder, 2017); y también relaciona con seguridad de la información, debido a que tiene como uno de sus objetivos la no alteración de la información (Godoy, 2014). Es decir, si la información es alterada durante el proceso ambas variables tratan de analizar el impacto; (b)

la teoría de la mejora continua, según Deming (1989), la calidad total se alcanza mediante un mejoramiento continuo, donde nunca se llega a perfección, pero se busca. Por lo tanto, se relaciona la norma ISO 27001 en uno de los puntos de su apartado menciona que debe haber una mejora continua al implementar un SGSI (Gómez y Fernández, 2018), a su vez, se relaciona con la seguridad de la información, debido a la insuficiencia de manejar un SGSI, si no hay un control y superación en la seguridad (ISOTools, 2018). Es decir, que ambas variables tienen la mejora continua implícita dentro de sus argumentos y (c) teoría de sistemas, donde Von Bertalanffy (1976) afirma que, el sistema es la suma total de los factores y pueden ser estudiado componente por componente, por consiguiente, guarda relación con la variable ISO 27001 que consta de 11 secciones más un anexo que son requerimientos básicos para cumplir con la norma (Calder, 2017), a su vez, la doctrina de sistemas está conectada con seguridad de la información, ya que lo componen tres elementos claves para asegurar la seguridad de la información (Azurza, 2020). Es decir, que ambas variables en sí son un conjunto de elementos que forman que un tema en particular.

Variable independiente: ISO 27001

Existen diversidad de guías, libros e incluso opiniones de expertos que sugieren como implementar, pero la única que define los requisitos y paso que hay que seguir para desarrollar e implementar un SGSI capaz de ser acreditada con la certificación es la propia ISO 27001 (Calder y Watkins, 2019). Es decir, se puede utilizar otras fuentes de información, pero se debe consultar la guía de la propia ISO, porque es la única fuente verídica que muestra como ser implementado.

Historia de la Norma ISO 27001

A lo largo del tiempo la Norma ISO 27001 ha ido evolucionando (Calder, 2017). Es decir, ha pasado por grandes cambios hasta establecerse como norma internacional.

BS7799-1:1999: Se publicó en Reino Unido como una norma de dos partes. BS7799-1:1999: Código de prácticas (Calder, 2017). Es decir, esta norma fue la primera versión de dos partes.

BS7799-2:1999: Es la especificación para un SGSI que hace uso del código prácticas. En el mismo ámbito, en el 2005 la ISO 17799 se mejoró y actualizó y cambió el número a la serie de LA ISO 27000 (Calder, 2017). Es decir, se añadió la segunda versión de la norma, completándola en su totalidad.

BS7799-2:2002: Se volvió a revisar y publicar como BS7799-2:2002. Sucedieron cambios importantes como: El alineamiento de la numeración de la cláusula en ambas partes de la norma. La adición del modelo de PDCA a la norma. La adición de un requisito para mejorar continuamente el SGSI (Calder, 2017). Es decir, después de 3 años de su publicación, la norma tuvo cambios y adiciones en sus cláusulas.

ISO 27001:2005: Varios países habían adoptado la BS7799-2 aunque solo era una norma británica, y para realizar el proceso de internalización se publicó el borrador final como la BS7799-2:2005 (ISO/IEC 27001:2005) en octubre de 2005 (Calder, 2017). Es decir, la norma era empleada en diversos países, pero para ser conocida internacionalmente tuvieron que pasar 6 años.

ISO 27001:2013: En la última reunión con las organizaciones los miembros del ISO/IEC, publicaron la última edición de la ISO 27001 en octubre de 2013. El cambio fue en la atención hacia crear un SGSI que complemente la organización y sus procesos, y una reducción de la redundancia en la especificación y los controles (Calder, 2017). Es decir, en este año se publica la versión más completa, subsanando redundancias y añadiendo mejoras.

ISO 27001:2022: Esta sería la última versión publicada en la que se realizaron algunas modificaciones en la cláusula 4.4, 8.1, 5.3, 7.4, 9.2, 9.3, 10.1 y 10.2. También, hubo ciertos cambios creando un nuevo anexo A, en la cual se redujeron de 14 cláusulas a solo 4,

además se añadieron 11 controles nuevos quedando 93 controles (Jegelka, 2022). Es decir, los objetivos de control el Anexo A se han revisado, actualizado, complementado y reorganizado con algunos controles nuevos.

Como punto a recalcar, hoy en día hay confusión en cómo se escribe ISO/IEC 27001:2013 o ISO/IEC 27001:2017, el IEC muchas veces ni siquiera se menciona. Pero ciertos organismos de normalizadores le colocan la fecha como 2017 o 2022 debido a las enmiendas que le efectúan al estándar (Araujo, 2020). Es decir, la norma publicada en el 2013 es la norma oficial que se toma como base y de esta surgen correcciones que se abordan con el pasar de los años.

Controles del Anexo A ISO 27002

Es un estándar que proporciona distintas recomendaciones de prácticas en la gestión de la seguridad de la información para responsables e interesados, que estén listos para desarrollar o preservar sistemas de gestión de seguridad enfocado a todo tipo de empresa, además se encuentra organizado en 14 dominios, 35 objetivos y 114 controles (Toro, 2022). Es decir, la ISO 27001 te nombra los controles del anexo A, pero en esta ISO habla más a detalle de como implementar cada control.

Ciclo de Deming

El ciclo de Deming es el estudio continuo que toma parte del ciclo PEVA: planificar (definir objetivos y medidas), ejecutar (preparación y proceder a la acción), verificar (los resultados, objetivos y efectos) y actuar (poner en acción las mejoras obtenidas). El principio de la mejora continua es de nunca parar (Vasquez, 2018). Es decir, una acción ejecutada en una operación más adelante puede ser mejorada o cambiada por una acción más eficiente.

Modelo PDCA enfocado a la Norma ISO 27001

El ciclo de Deming o de mejora continua, también conocido por sus siglas en inglés como modelo PDCA los cuales son: (a) plan, (b) do, (c) check y (d) act. Además, una de las novedades más relevantes con versiones anteriores es que el ISO 27001 de la versión 2013 elimina al modelo PDCA del marco obligatorio en la gestión para mejora continua. El apartado 10.2 indica como mejorar el SGSI de acuerdo con la conveniencia de la organización. Sin embargo, aunque no se mencione el modelo PDCA está sobreentendido en la estructura (Gómez y Fernández, 2018). Por ello, se detalla lo que se necesita saber.

Planificar: Es la etapa de planificación del SGSI, para determinar las metas y las políticas de la organización (Gómez y Fernández, 2018). Es decir, es la etapa inicial en la cual se plasman las actividades a futuro.

Hacer: Es la etapa donde se implementa y ejecuta el SGSI. Con la cual, las políticas y controles van de acuerdo con el análisis de riesgo, que fueron definidas de acuerdo con las tareas y capacitaciones asignadas al personal (Gómez y Fernández, 2018). Es decir, que en esta etapa las tareas planificadas son realizadas.

Verificar: Es la etapa donde se monitorea y se revisa el SGSI. Además, los procesos son controlados de forma eficiente para cumplir las metas (Gómez y Fernández, 2018). En otras palabras, en esta etapa se monitorean las actividades, para medir su desempeño.

Actuar: Es la etapa donde se mejora y mantiene el SGSI. Además, se ejecutan las revisiones para detectar anomalías de la etapa anterior (Gómez y Fernández, 2018). Es decir, en esta esta se detecta los errores y se procede a realizar las mejoras.

Variable dependiente: Seguridad de la información

Se determina como procedimientos que dificultan las ejecuciones no autorizadas en las operaciones de un sistema o red, cuyas consecuencias dañan la: (a) confidencialidad, (b) integridad y (c) disponibilidad. A su vez, impacta en el funcionamiento de los equipos y

deniega a usuarios autorizado el acceso al sistema (Gómez, 2011). Es decir, son medidas que impiden que el atacante ejecute tareas no autorizadas.

En otro punto, La seguridad de la información no debe confundirse con la seguridad informática, ya que solo es responsable de la seguridad del entorno informático, mientras que la información se encuentra en diferentes áreas o aspectos del entorno informático (Godoy, 2014). Es decir, la seguridad informática se refiere más a la parte lógica, mientras que, seguridad de la información es tanto lógica como física.

Objetivos de la seguridad de la información.

Es una ciencia en continua evolución, que tiene como finalidad satisfacer los objetivos de la organización, implementando sistemas que tiene como consideración los riesgos relativos a las TIC (Areitio, 2008). Como objetivos principales tenemos:

Confidencialidad: Es el atributo que obstruye la difusión de información a agentes o sistemas no permitidos (Godoy, 2014). Es decir, la información solo podrá ser vista y manipulada por el personal autorizado.

Integridad: Es la característica que mantiene la información libre de acciones no consensuadas (Godoy, 2014). Es decir, que mientras la información viaje esta no será alterada o modificada.

Disponibilidad: Es la propiedad, cualidad o condición que debe encontrarse a disposición a la persona, proceso o aplicación autorizada (Godoy, 2014). Es decir, que la información debe estar disponible cuando el personal requiera de su uso.

Responsabilidad: Es el requerimiento que obliga a entidades trazar acciones de manera única (Areitio, 2008). Es decir, que las partes implicadas tengan un plan de respaldo que permitan asegurar la información.

Confiabilidad: Es el respaldo que los cuatro objetivos anteriores se cumplan de manera adecuada (Areito, 2008). Es decir, para alcanzar el objetivo de la seguridad en su máxima expresión, se debe cumplir con los 4 objetivos anteriores.

Amenazas, vulnerabilidades, riesgos e impacto

Cuando se observa que hay posibilidades de que un ataque en particular nos afecte podemos hablar de él en términos de amenazas, vulnerabilidades, riesgo e impacto (Vega, 2021). Es decir, se tiene que estar preparados ante cualquier signo de hostilidad, debido a que, esto puede traer consecuencia y formar parte de los siguientes términos:

Amenaza: Tiene la capacidad de causar daños, puede ser específica especialmente en el universo de la seguridad de la información (Vega, 2021). Es decir, son acciones que buscan debilidades en el sistema con el fin de causar daño.

Vulnerabilidades: Es una debilidad que se encuentra en los sistemas operativos y pueden ser explotados para causar daño (Vega, 2021). Es decir, son áreas desprotegidas o con poca seguridad que son aprovechadas por los atacantes.

Riesgos: Probabilidad de que algo malo suceda, para ello se necesita tener una amenaza y un cierto grado de vulnerabilidad para que pueda explotar la amenaza específica. (Vega, 2021). Es decir, los riesgos se determinan mediante vulnerabilidades específicas que pueden ser amenazadas con una alta tasa de probabilidad.

Impacto: En forma de impacto. Si consideramos que el valor del activo amenazado es un factor. esto puede cambiar si vemos un riesgo presente o no (Vega, 2021). Es decir, el impacto en un activo es diferente, debido a que, cada activo tiene su propio valor.

2.3. Formulación de hipótesis

2.3.1. Hipótesis general

“La ISO 27001 mejora la seguridad de la información en una institución educativa, Lima 2022.”

2.3.2. Hipótesis específicas

HE1: “La ISO 27001 mejora la confidencialidad de la información en una institución educativa, Lima 2022.”

HE2: “La ISO 27001 mejora la integridad de la información en una institución educativa, Lima 2022.”

HE3: “La ISO 27001 mejora la disponibilidad de la información en una institución educativa, Lima 2022.”

CAPITULO III:METODOLOGÍA

3.1. Método de investigación

El presente trabajo sobre la “ISO 27001” para mejorar la “seguridad de la información” emplearon los método hipotético, deductivo y analítico.

Hipotético, porque se contrastará hipótesis de la variable dependiente. El método hipotético deductivo es una teoría que no se considera verdadera sino como no refutada donde se plantea hipótesis con base a datos recopilados y que a través de la deducción se llega a la conclusión previo a una experimentación (Puebla, 2010).

El deductivo, porque se conocerá la problemática general partiendo de unos problemas específicos, para poder determinar el incremento de: (a) confidencialidad, (b) integridad y (c) disponibilidad. Asimismo, con el método deductivo se asume que en la premisa está incluida la conclusión, esto quiere decir si la premisa es verdadera el razonamiento deductivo es correcto, en caso contrario la conclusión no puede ser verdadera (Carvajal, 2013).

Analítico, porque se interpretarán diferentes gráficos y tablas para identificar la aseveración de las hipótesis planteadas. El método analítico es un método que descompone en sus partes el todo, con el fin de analizar su naturaleza, que además da paso a nuevas teorías (Gómez, 2012).

3.2. Enfoque investigativo

El enfoque aplicado es cuantitativo porque se manipuló la variable “seguridad de la información”, y afectada por la variable independiente “ISO 27001” para la mejora de la seguridad de la información en la institución educativa. Una investigación de enfoque cuantitativa debe presentar ciertas características como ser objetiva, contrastar las hipótesis, utilizar estadística inferencial, tener el control de las variables y utilizar el método deductivo (Flores y Gardi, 2020).

3.3. Tipo de investigación

La investigación aplicada consta de una base teórica donde los investigadores funden la teoría en resultados concretos (Ulin *et al.*, 2005). Por ende, la investigación realizada es de tipo aplicada.

3.4. Diseño de la investigación

En un análisis experimental, la variable independiente se manipula deliberadamente con una o muchas variables dependientes en un escenario controlado por el investigador (Hernández *et al.*, 2014). De modo que, se empleó el diseño experimental de tipo pre experimental, porque afecta la variable dependiente que es “seguridad de la información”, donde se reflejó la mejora al implantar la “ISO 27001”.

3.5. Población, muestra y muestreo

Población

Según Carrillo (2015) argumenta que, la población es un grupo de individuos, elementos u objetos con características especiales para ser estudiadas. Es decir, que no solo las personas conforman una población sino todo aquello que presente características que llamen la atención para ser objeto de estudio. En este caso la población comprende de un total de 22 controles de anexo A, en donde se emplearán guías de observación antes, durante y después de la mejora con la Norma ISO 27001. Estos 20 controles fueron categorizados para cada dimensión donde la dimensión confidencialidad tuvo como control la seguridad de las comunicaciones, la dimensión integridad tuvo como control la criptografía y un sub-control de la seguridad física y la dimensión disponibilidad tuvo como control gestión de activos donde todo esto hace referente al anexo A de la ISO 27001.

Muestra

Como menciona Toledo (2016), para seleccionar la muestra primero se debe ver ciertas características que mi población debe presentar para poder ser estudiada. Es decir, que la

muestra tiene que cumplir con los parámetros del estudio para ser seleccionada. Por lo tanto, al realizar el tamaño muestral se obtiene 20.86, que al redondearlo sería 20. En donde, se opta por utilizar como muestra a 20 controles de seguridad.

Muestreo

Como señala Otzen y Manterola (2017), el principio del muestreo es estudiar la distribución de una variable dentro de una población y esta misma variable dentro de la muestra de estudio. Para ello, es importante definir pautas de agrupamiento a la población y muestra que van a ser parte del estudio (Arias *et al.*, 2016). En resumen, en este caso por tener 20 controles de seguridad se descarta el uso del muestreo al ser significativo.

3.6. Variables y operacionalización

El trabajo busca mejorar la “seguridad de información” a través de los controles de la “ISO 27001”.

La variable independiente es la “ISO 27001” y la variable dependiente es la “seguridad de la información” aplicando los controles del ANEXO A.

Variable independiente: ISO 27001

La **definición conceptual** de la metodología ISO 27001 según ISOTools (2022), es un estándar internacional que garantiza la seguridad, confidencialidad e integridad de los datos y la información y los sistemas que los procesan.

La **definición operacional** de la ISO 27001 permite a las organizaciones evaluar los riesgos y aplicar las políticas necesarias para mitigarlos o prevenirlos. Los indicadores son los controles aplicados a la variable dependiente en la institución educativa.

Variable dependiente: seguridad de la información

Como **definición conceptual** de seguridad de la información según Toro (2021) nos dice que, es la suma de técnicas y medidas utilizadas para manejar y proteger la totalidad de los

datos procesados en una sociedad empresarial para garantizar que no se filtre ningún dato del sistema establecido.

La **definición operacional** de seguridad de información consiste en proteger la confidencialidad, integridad y disponibilidad de la información. Cuyos indicadores miden las características de estos 3 pilares.

3.7. Técnicas e instrumentos de recolección de datos

3.7.1. Técnica

Según Rodríguez (2008) las técnicas, son recursos que se utiliza para recopilar información, entre las más comunes tenemos la observación, entrevistas, encuestas, análisis documental y contenido. Asimismo, como técnica de investigación se utiliza la observación de la variable dependiente para la seguridad de la información mediante la ISO 27001 que es la variable independiente. Es decir, que con la observación en la variable dependiente se compara el antes y un después de aplicar la herramienta.

3.7.2. Descripción

El instrumento empleado fueron las guías de observación por ser de diseño experimental de tipo pre experimental, en donde los datos recopilados son cuantitativos y que se medirán en un antes y después de aplicar la herramienta de la norma ISO 27001 (ver anexo 2). En un tema para desmembrar la información, es necesario, que el investigador se ayude de instrumentos como ficha de trabajo en la que se encuentra contenida un resumen de la información importante, que se obtiene a través de un reconocimiento preliminar de un estudio en campo, mediante guías o entrevistas a informante claves (Rojas, 2006).

3.7.3. Validación

Con respecto a la validación no se utilizará el juicio de expertos debido a que el instrumento no lo requiere, debido a que son guías de observación, pero de igual forma serán verificados

por 3 expertos para un mejor nivel de confiabilidad (ver anexo 3). Estas guías de observación permiten al investigador enfocarse en aquello que considere objeto de estudio con el fin de recolectar datos o información de un hecho o fenómeno (Campos y Lule, 2012).

3.7.4. Confiabilidad

Se aplicará el análisis de doble masas donde se evidenció la confiabilidad del antes y después de las pruebas. El análisis de doble de masas te permite comparar una información con distintas fuentes confiables, y detectar si hay errores que luego pueden ser corregidos (Arias O. , 2001).

3.8. Plan de procesamiento y análisis de datos

Como parte del procesamiento, al tener un diseño experimental de enfoque cuantitativo, se construyó el instrumento guías de observación basados en la “seguridad de la información”, la cual fue manipulada por la variable independiente “ISO 27001”. En este caso no será necesaria la validación de expertos, debido a que, dichos instrumentos son las fichas de observación, pero para una mejor confiabilidad se contara con el juicio de expertos. Luego se procederá a aplicar la técnica de la observación en un antes y después de emplear la norma ISO 27001 en la institución educativa. Asimismo, con los datos obtenidos del antes y después de la prueba, estas se consolidan en el Excel para luego ser trabajadas en el SPSS y con la prueba de doble masas perder aplicar la consistencia a los datos, con la finalidad de que los niveles de aceptación y consistencia sean cumplidos por los datos ingresados. Asimismo, para la obtención de la suma, promedio, varianza y media de los datos del antes y después de aplicar la norma ISO 27001 mediante la prueba descriptiva. Para finalizar, con la estadística inferencial se procederá a realizar la consistencia para verificar la confiabilidad de los datos, y con respecto a la población se realizará la prueba de normalidad, por último, para verificar las hipótesis se hará la prueba de contraste y proponer resultados.

Como parte del análisis de datos, estos serán recopilados mediante las fichas de observación. Para luego emplear la prueba de doble masas para verificar el nivel de confiabilidad de la pre y post prueba. Seguidamente, se realizó la prueba de Shapiro, la cual demostrará si serán o no paramétricos. En última instancia se empleará la prueba de comparación basada en la normalidad para analizar los resultados obtenidos. En resumen, se usa la prueba de T-Student o Z-test si los valores son paramétricos, caso contrario se usa la prueba de T-Wilcoxon o U de Mann-Whitney.

3.9. Aspectos éticos

El trabajo utilizó la séptima edición de la norma APA y Turnitin (ver anexo 9), además se aplicará la ética profesional de tal manera que a los involucrado se le informo de manera clara y precisa de esta investigación por lo que se garantiza la protección y confidencialidad de acuerdo con la ley Número 29733 del Decreto Supremo Número 003-2013-JUS.

CAPITULO IV:PRESENTACION Y DISCUSIÓN DE LOS RESULTADOS

4.1. Resultados

Por tener un diseño experimental de nivel pre experimental, se utilizó la ISO 27001 para la seguridad de la. Los datos se obtuvieron mediante la observación, en la cual contamos con el apoyo del comité educativo donde se recopilaron los datos con las guías de observación que se encuentran en el anexo 2.

4.1.1 Análisis descriptivo de resultados

En la tabla 1, se procesó los datos de los 3 indicadores del objetivo principal, estos datos se obtuvieron de SPSS v.25.

Tabla 1

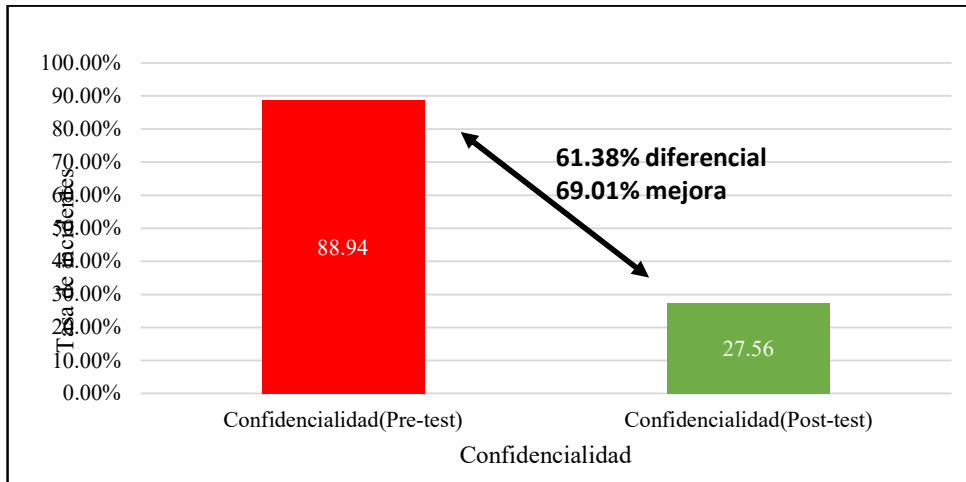
Procesamiento de datos

	N	Rango	Mínimo	Máximo	Suma	Media	Desv. Desviación
Confidencialidad_pre-test	7	33,33	66,67	100,00	622,61	88,9443	11,85012
Confidencialidad_post-test	7	35,71	14,29	50,00	192,92	27,5600	11,36246
Integridad_pre-test	3	27,08	66,67	93,75	229,65	76,5500	14,95053
Integridad_post-test	3	8,89	11,11	20,00	44,44	14,8133	4,62690
Disponibilidad_pre-test	10	31,25	62,50	93,75	775,00	77,5000	9,95520
Disponibilidad_post-test	10	24,10	6,67	30,77	156,73	15,6730	7,87833

En la figura 2, evidenciamos que existe un diferencial del 61.38 % para la tasa de incidentes que afectan la confidencialidad entre la media estadística del pre-test y post-test. Es decir, la tasa de incidentes para el pre-test se evidencia un promedio estadístico del 88.94% y para el post-test un promedio del 27.56% que afectan la confidencialidad. En resumen, como parte análisis investigador, corroboramos que la tasa de incidentes ha mejorado un 69.01% en general, para asegurar lo indicado, se siguió con la prueba de normalidad y de contraste para evaluar la HE1.

Figura 2

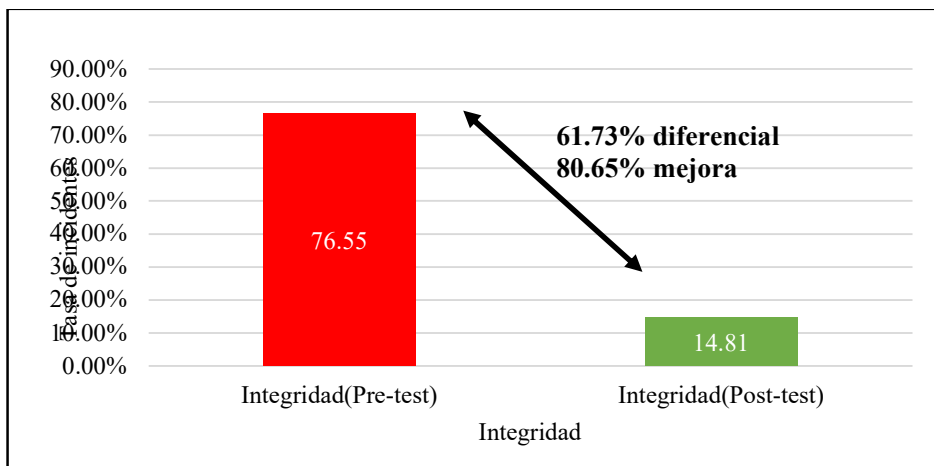
Tasa de incidentes que afectan la confidencialidad



En la figura 3, evidenciamos que existe un diferencial del 61.73 % para la tasa de incidentes que afectan la integridad entre la media estadística del pre-test y post-test. Es decir, la tasa de incidentes para el pre-test se evidencia un promedio estadístico del 76.55% y para el post-test un promedio del 14.81% que afectan la integridad. En resumen, como parte análisis investigador, corroboramos que la tasa de incidentes ha mejorado un 80.65% en general, para asegurar lo indicado, se procedió con la prueba de normalidad y de contraste para evaluar la HE2,

Figura 3

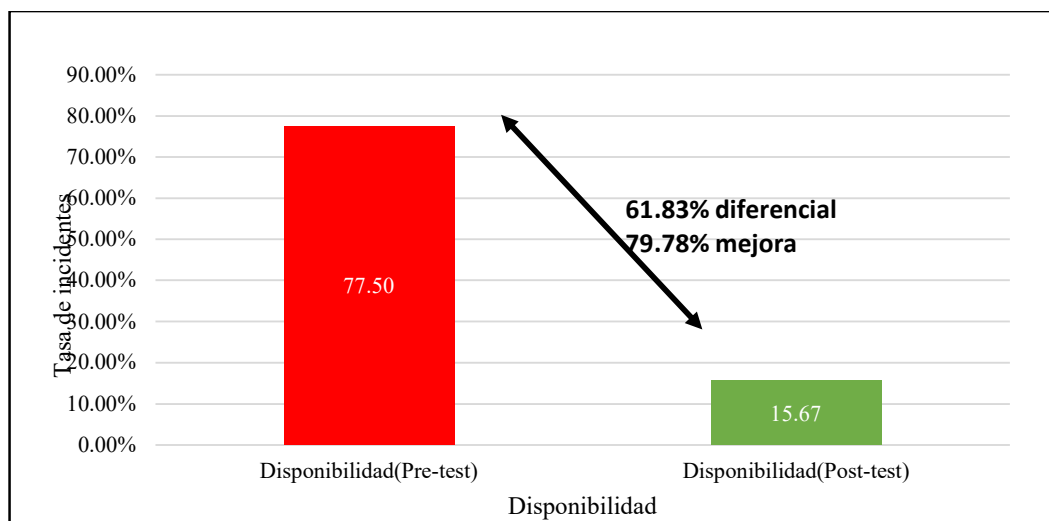
Tasa de incidentes que afectan la integridad



En la figura 4, evidenciamos que existe un diferencial del 61.83 % para la tasa de incidentes que afectan la disponibilidad entre la media estadística del pre-test y post-test. Es decir, la tasa de incidentes para el pre-test se evidencia un promedio estadístico del 77.50% y para el post-test un promedio del 15.67% que afectan la disponibilidad. En resumen, como parte análisis investigador, corroboramos que la tasa de incidentes ha mejorado un 79.78% en general, para asegurar lo indicado, se procedió con la prueba de normalidad y de contraste para evaluar la HE3.

Figura 4

Tasa de incidentes que afectan la disponibilidad



En la tabla 2, observamos la obtención de las frecuencias de los indicadores. Respecto a la confidencialidad se corrobora el 100% del máximo valor en la tasa de incidentes Pre-test, seguido del 50% en la tasa de incidentes Post-test. Además, en la integridad se confirma el valor máximo del 93,75% en la tasa incidentes Pre-test, seguido del 20% en la tasa de incidentes Post-test. Por último, en la disponibilidad se confirma el valor máximo del 93,75% en la tasa incidentes Pre-test, seguido del 30,77% en la tasa de incidentes Post-test.

Tabla 2*Frecuencias Estadísticas*

		Estadísticos					
		Confidenciali dad_pre-test	Confidenciali dad_post-test	Integridad_pr e-test	Integridad_p ost-test	Disponibilid ad_pre-test	Disponibilid ad_post-test
N	Válido	7	7	3	10	10	10
	Perdidos	4	4	8	0	0	0
Media		88,9443	27,5600	76,5500	14,8133	77.5000	15.6730
Mediana		93,3300	25,0000	69,2300	13,3300	75.0000	15.4800
Moda		100,00	25,00	66,67 ^a	11,11 ^a	75.00	8,33 ^a
Desv. Desviación		11,85012	11,36246	14,95053	4,62690	9.95520	7.87833
Varianza		140,425	129,105	223,518	21,408	99.106	62.068
Rango		33,33	35,71	27,08	8,89	31.25	24.10
Mínimo		66,67	14,29	66,67	11,11	62.50	6.67
Máximo		100,00	50,00	93,75	20,00	93.75	30.77
Suma		622,61	192,92	229,65	44,44	775.00	156.73

4.1.2 Prueba de hipótesis

Peña (2017) indica que, la consistencia de datos es la clasificación, donde los datos presentan un patrón de selección de uniformidad y periodicidad. Es decir, los datos serán clasificados según su similitud que en este caso serían los incidentes que afectan la seguridad de la información, teniendo en cuenta un periodo de 15 días para pre-test y 15 días para post-test.

En la tabla 3, evidenciamos el consolidado para los indicadores. Para la tasa de incidentes que afectan la confidencialidad en el pre-test se obtuvieron porcentajes del 66% al 100% y para el post-test se obtuvieron porcentajes del 25% al 50%. Además, en la tasa de incidentes que afectan la integridad en el pre-test se obtuvieron porcentajes del 60% al 94% y para el post-test se obtuvieron porcentajes del 13% al 20%. Por último, para la tasa de incidentes que afectan la disponibilidad en pre-test se obtuvieron porcentajes del 75% al 94% como y para el post-test los porcentajes eran del 8% al 20%.

Tabla 3*Consolidación de los 3 indicadores*

Confidencialidad "Pre-test"	Confidencialidad "Post-test"	Integridad "Pre-test"	Integridad "Post-test"	Disponibilidad "Pre-test"	Disponibilidad "Post-test"
66.67	25.00	66.67	20.00	93.75	20.00
86.67	23.08	69.23	11.11	82.35	14.29
81.82	22.22	93.75	13.33	62.50	10.00
94.12	25.00			76.47	30.77
93.33	14.29			93.75	6.67
100.00	33.33			70.59	8.33
100.00	50.00			75.00	16.67
				70.59	25.00
				75.00	16.67
				70.59	8.33
				75.00	8.33

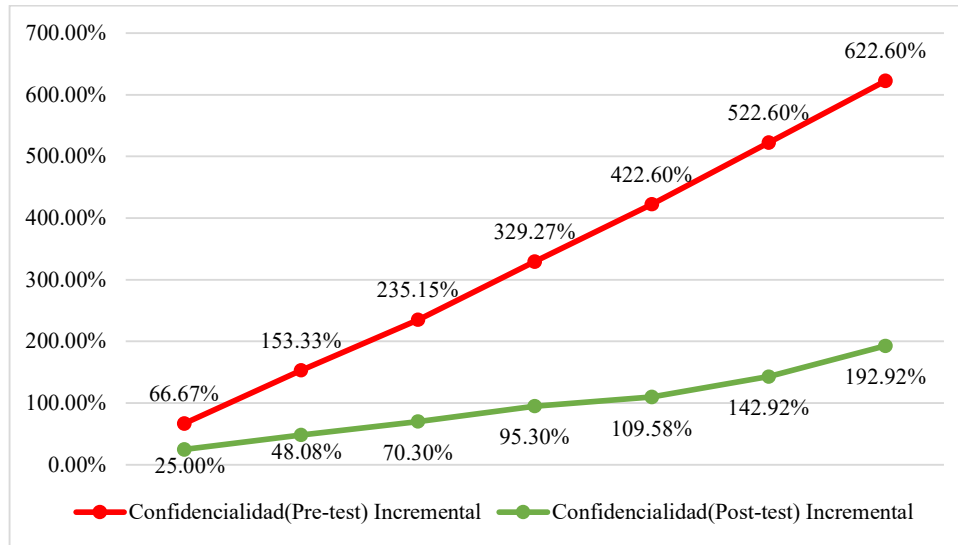
Hipótesis específica 1**a. Consistencia****Tabla 4***Tasa de incidentes incremental de la confidencialidad*

Confidencialidad (Pre-test) Incremental	Confidencialidad (Post-test) Incremental
66.67	25.00
153.33	48.08
235.15	70.30
329.27	95.30
422.60	109.58
522.60	142.92
622.60	192.92

En la figura 5, se evidencia que los valores consolidados de la tasa de incidentes en la confidencialidad, se dibuja una recta creciente, lo que demuestra que los datos son consistentes. En resumen, la prueba doble masas nos afirma que los datos acumulados son confiables, es decir, no habrá ningún problema al realizar la prueba de normalidad y de contraste en la hipótesis específica 1.

Figura 5

Consistencia de la tasa de incidentes que afecta la confidencialidad



b. Normalidad

Tabla 5

Prueba de normalidad en hipótesis 1

Confidencialidad	"Shapiro-Wilk"		
	"Estadístico"	"gl"	"Sig."
Confidencialidad_pre-test	0.919	3	0.448
Confidencialidad_post-test	0.954	3	0.586

En la tabla 5, se evidencia que la tasa de incidentes que afectan la confidencialidad tanto para pre-test como post-test comprende datos paramétricos, según el estadígrafo para la prueba de Shapiro-Wilk, el valor Sig. supera 0.05.

c. Contraste (Prueba de hipótesis)

Tabla 6

Prueba T-Student – indicador tasa de incidentes que afectan la confidencialidad

Estadísticas emparejadas - confidencialidad				
	"Media"	"N"	"Desv. Desviación"	"Desv. Error promedio"
Par 1 Confidencialidad_pre-test	88.9443	7	11.85012	4.47892
Confidencialidad_post-test	27.5600	7	11.36246	4.29461

Tabla 7

Prueba T-Student –incidentes en confidencialidad

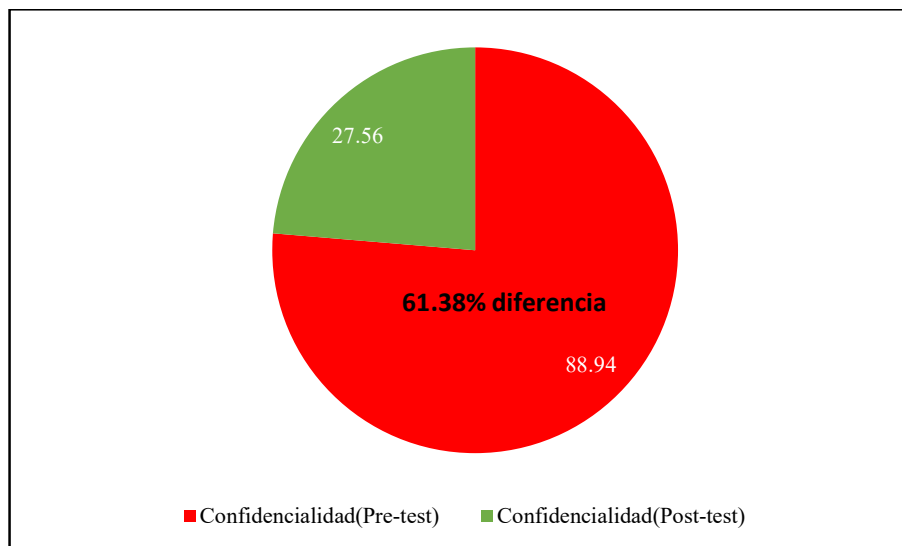
Muestras emparejadas - Confidencialidad									
Par 1	"Media"	Diferencias emparejadas						Sig.	
		"Desv. Error"	"Desv. Error"	95% de intervalo de confianza de la diferencia		"t"	"gl"		
	"Mediación"	"Desviación"	"Error promedio"	"Inferior"	"Superior"			"bilateral"	
Confidencialidad_pre-test-	61.3842	12.4218	4.6950	49.89603	72.8725	13.07	6	0.000	
Confidencialidad_post-test							4		

En la tabla 6 y 7, se verifica que el promedio de las 2 tasas de incidentes de confidencialidad es relevante, al mostrar 88.94% de promedio en el pre-test y del 27.56% en post-test. Asimismo, se emparejo la muestra en la prueba de T-Student, donde se apreció que el valor "Sig." es menor que 0.05 en la tasa de incidentes que afecta la confidencialidad, por lo que, se acepta que los controles de la ISO 27001 mejoran la confidencialidad de la información en una institución educativa, Lima 2022, rechazando la hipótesis nula.

Para la figura 6, se evidencia la reducción exponencial del 61.38% aproximadamente de la tasa de incidentes que afectan la confidencialidad aplicando los controles de la norma ISO 27001.

Figura 6

Reducción de la tasa de incidencia que afecta la confidencialidad



Hipótesis específica 2

a. Consistencia

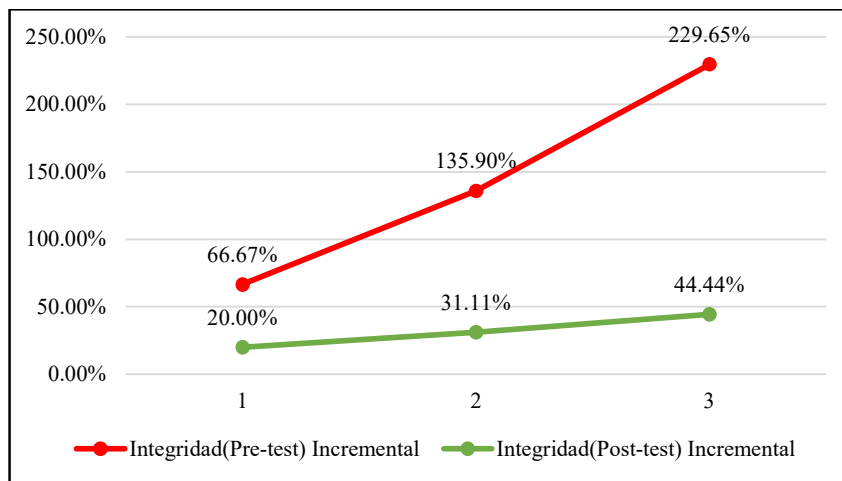
Tabla 8

Tasa de incidentes incremental de la integridad

Integridad (Pre-test)	Integridad (Post-test)
Incremental	Incremental
66.67	20.00
135.90	31.11
229.65	44.44

Figura 7

Consistencia de la tasa de incidentes que afecta la integridad



En la figura 7, se evidencia que los valores consolidados de la tasa de incidentes en la integridad, se dibuja una recta creciente, lo que demuestra que los datos son consistentes. En resumen, la prueba doble masas nos afirma que los datos acumulados son confiables, es decir, no habrá ningún problema al realizar la prueba de normalidad y de contraste en la hipótesis específica 2.

b. Normalidad

En la tabla 9, se evidencia que la tasa de incidentes que afectan la integridad tanto para pre-test como post-test comprende datos paramétricos, según el estadígrafo para la prueba de Shapiro-Wilk, el valor Sig. supera 0.05.

Tabla 9*Prueba de normalidad en hipótesis 2*

Integridad			
	"Shapiro-Wilk"		
	"Estadístico"	"gl"	"Sig."
Integridad_pre-test	0.820	3	0.164
Integridad_post-test	0.923	3	0.463

c. Contraste

En la tabla 10 y 11, se verifica que el promedio de las 2 tasas de incidentes de integridad es relevante, al mostrar 76.55% de promedio en el pre-test y del 14.81% en post-test. Asimismo, se emparejo la muestra en la prueba de T-Student, donde se apreció que el valor "Sig." es menor que 0.05 en la tasa de incidentes que afecta la integridad, por lo que, se acepta que los controles de la ISO 27001 mejoran la integridad de la información en una institución educativa, Lima 2022, rechazando la hipótesis nula.

Tabla 10*Prueba T-Student – indicador tasa de incidentes que afectan la integridad*

Estadísticas emparejadas - Integridad					
		"Media"	"N"	"Desv. Desviación"	"Desv. Error promedio"
Par 1	Integridad_pre-test	76.5500	3	14.95053	8.63169
	Integridad_post-test	14.8133	3	4.62690	2.67134

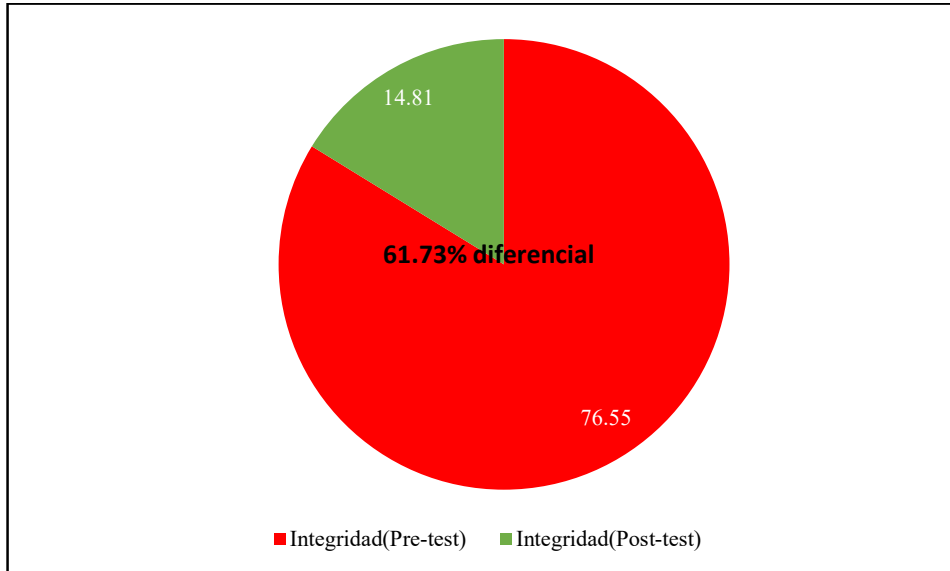
Tabla 11*Prueba T-Student – incidentes en integridad*

Muestras emparejadas - Integridad									
"Diferencias emparejadas"									
95% de intervalo de confianza de la diferencia									
		"Desv. Desviación"	"Desv. Error promedio"	95% de intervalo de confianza de la diferencia		"t"	"gl"	Sig.	
Par 1	"Media"	"Desv. Desviación"	"Desv. Error promedio"	"Inferior"	"Superior"	"t"	"gl"	"bilateral"	
Integridad_pre-test -	61.73667	17.16321	9.90918	19.10089	104.37245	6.230	2	0.025	
Integridad_post-test									

Para la figura 8, se evidencia la reducción exponencial del 61.73% aproximadamente de la tasa de incidentes que afectan la integridad aplicando los controles de la norma ISO 27001

Figura 8

Reducción de la tasa de incidencia que afecta la integridad



Hipótesis específica 3

a. Consistencia

Tabla 12

Tasa de incidentes incremental de la disponibilidad

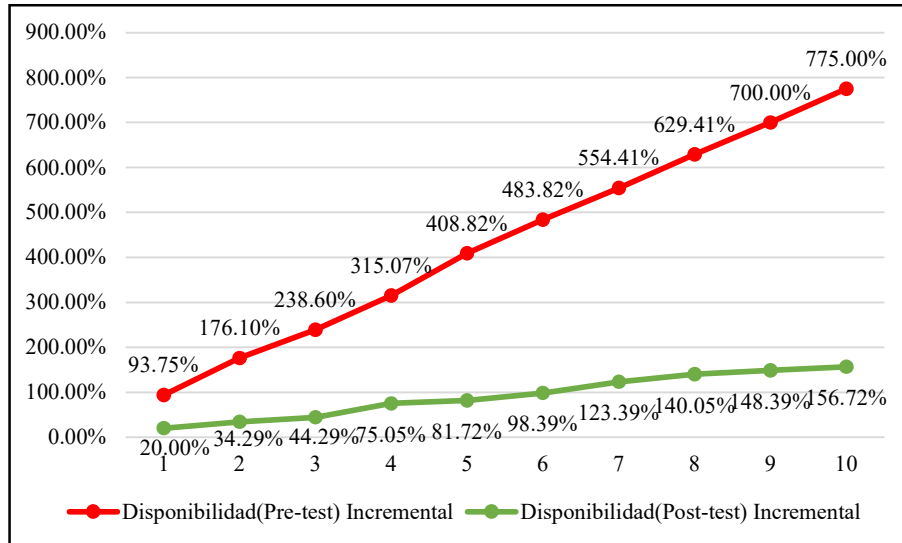
Disponibilidad (pre-test)	Disponibilidad (post-test)
Incremental	Incremental
93.75%	20.00%
176.10%	34.29%
238.60%	44.29%
315.07%	75.05%
408.82%	81.72%
483.82%	98.39%
554.41%	123.39%
629.41%	140.05%
700.00%	148.39%
775.00%	156.72%

En la figura 9, se evidencia que los valores consolidados de la tasa de incidentes en la disponibilidad, se dibuja una recta creciente, lo que demuestra que los datos son consistentes. En resumen, la prueba doble masas nos afirma que los datos acumulados son

confiables, es decir, no habrá ningún problema al realizar la prueba de normalidad y de contraste en la hipótesis específica 3.

Figura 9

Consistencia de la tasa de incidentes que afecta la disponibilidad



b. Normalidad

Tabla 13

Prueba de normalidad en hipótesis 3

	Disponibilidad		
	“Estadístico”	“Shapiro-Wilk” “gl”	“Sig.”
Disponibilidad_pre-test	0.976	3	0.704
Disponibilidad_post-test	0.993	3	0.844

En la tabla 13, se evidencia que la tasa de incidentes que afectan la disponibilidad tanto para pre-test como post-test comprende datos paramétricos, según el estadígrafo para la prueba de Shapiro-Wilk, el valor Sig. supera 0.05.

c. Contraste

En la tabla 14 y 15, se verifica que el promedio de las 2 tasas de incidentes de disponibilidad es relevante, al mostrar 77.50 % de promedio en el pre-test y del 15.67% en post-test. Asimismo, se emparejo la muestra en la prueba de T-Student, donde se apreció que el valor "Sig." es menor que 0.05 en la tasa de incidentes que afecta la disponibilidad, por lo que, se

acepta que los controles de la ISO 27001 mejoran la disponibilidad de la información en una institución educativa, Lima 2022, rechazando la hipótesis nula.

Tabla 14

Prueba T-Student – indicador tasa de incidentes que afectan la disponibilidad

Estadísticas emparejadas - Disponibilidad					
		“Media”	“N”	“Desv. Desviación”	“Desv. Error promedio”
Par 1	Disponibilidad_pre-test	77.5000	10	9.95520	3.14811
	Disponibilidad_post-test	15.6730	10	7.87833	2.49135

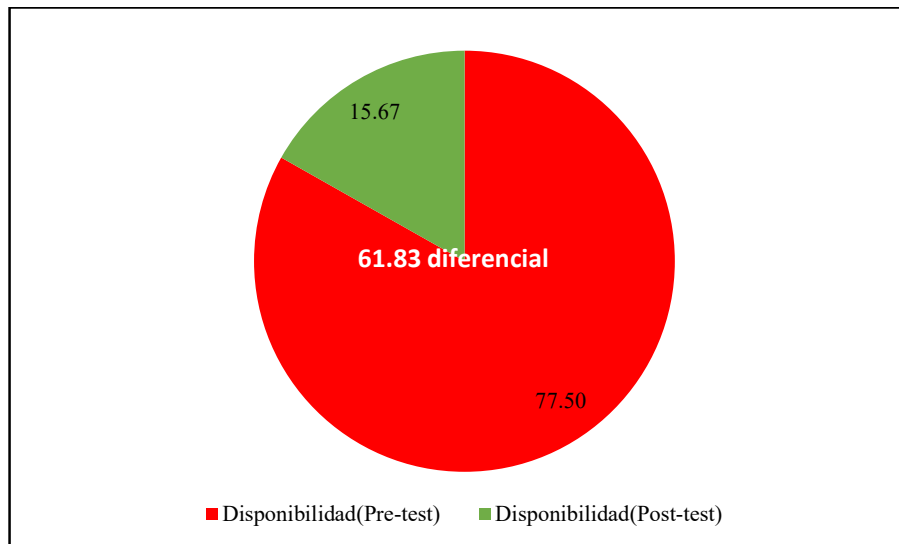
Tabla 15

Prueba T-Student – incidentes en disponibilidad

Muestras emparejadas - Disponibilidad									
“Diferencias emparejadas”									
		“Desv. Desviación”		“Desv. Error promedio”	95% de intervalo de confianza de la diferencia		“t”	“gl”	Sig. “bilateral”
Par 1	“Media”	Desviación”	“Desv. Error promedio”	“Inferior”	“Superior”	“t”	“gl”	Sig. “bilateral”	
Disponibilidad_pre-test – Disponibilidad_post-test	61.82700	12.81291	4.05180	52.66120	70.99280	15.259	9	0.000	

Figura 10

Reducción de la tasa de incidentes que afecta la disponibilidad



Para la figura 10, se evidencia la reducción exponencial del 61.83% aproximadamente de la tasa de incidentes que afectan la disponibilidad aplicando los controles de la norma ISO 27001.

4.1.3 Discusión de resultados

En referencia a lo evidenciado en las bases teóricas y los antecedentes de estudio. Se confirma la aceptación de la hipótesis donde se indica que en la institución educativa la “ISO 27001” mejoro la “seguridad de la información”. Cabe señalar que la seguridad sin aplicar la ISO 27001 no eran suficiente para la institución, debido a que se generaban varios incidentes cada día. Con la implementación de la “ISO 27001”, la seguridad de la información mejoro un 76.48% en promedio reduciendo en un 61.65% los incidentes. Es decir, existe una mejora reduciendo la tasa de incidentes que afectan la seguridad de información. Asimismo, dichos resultados críticos. Guarda relación con lo evidenciado por Huacasi (2018), donde su investigación sobre implementar un sistema de seguridad aplicando la NTP ISO 27001 para mejorar los procesos de seguridad de información. Los resultados obtenidos estuvieron alineados al nivel del conocimiento de los usuarios, el cual tuvo un incremento del 68.4% en general. Del mismo modo, se validó el avance que corresponde a un 68.4%. Por último, se relaciona con Calder (2017), donde aporta que, para asegurar la información se deberá proporcionar un enfoque sistemático conforme a la ISO27001.

En el mismo contexto, se confirma que la aceptación de la hipótesis del objetivo específico número 1 donde se indica que la ISO 27001 mejora la confidencialidad en la institución educativa. Cabe manifestar que la tasa de incidentes que afectan la confidencialidad sin aplicar los controles de la ISO 27001, tiene un promedio del 88.94% de incidentes, y luego de la implementación de los controles se obtuvo un promedio del 27.56% de incidentes, lo que significa que existe una reducción del 61.38%. Es decir, existe una

mejora en la confidencialidad de la información en la institución educativa. Asimismo, con lo indicado por Silva (2022), donde tuvo como objetivo implementar un sistema de seguridad de información para mejorar la confidencialidad. Los resultados evidenciaron que antes de la ejecución de los controles del SGSI, la confidencialidad era de un 10% y luego de la implementación aumento en 80%, obteniendo una mejora del 70% en preservar la confidencialidad, por ende, los incidentes que afectan la confidencialidad han disminuido. En términos generales se confirma que la “ISO 27001” mejora la confidencialidad en la institución educativa. Por último, se relaciona con Gómez y Fernandez (2018), en su aporte sobre la ISO 27001, donde los controles de seguridad permiten proteger la información frente a pérdidas de confidencialidad.

En el mismo contexto, se confirma que la aceptación de la hipótesis del objetivo específico número 2 donde se indica que la “ISO 27001” mejora la integridad de la información en la institución educativa. Cabe manifestar que la tasa de incidentes que afectan la integridad sin aplicar los controles de la ISO 27001, tiene un promedio del 76.55% de incidentes, y luego de la implementación de los controles se obtuvo un promedio del 14.81% de incidentes, lo que significa que existe una reducción del 61.73%. Es decir, existe una mejora en la integridad de la información en la institución educativa. Asimismo, con lo indicado con Chavarri (2021), donde tuvo que implementar las ISO 27001 Y 27002 para identificar las consecuencias en la integridad de la información. Los resultados evidenciaron que la implementación de las ISO 27001 y 27002 contribuye en la integridad de estar en 48% elevándolo a 94% obteniendo así una mejora del 46%. En términos generales se confirma que la implementación de la “ISO 27001” mejora la integridad de la información en la institución educativa. Por último, se relación con AENOR (2023), en su aporte sobre la ISO 27001, al mencionar que garantiza métodos de procesos exactos y completos, para asegurar la integridad de la información.

Por último, se confirma el cumplimiento de la hipótesis del objetivo específico número 3 donde se indica que la “ISO 27001” mejora la disponibilidad de la información en la institución educativa. Cabe manifestar que la tasa de incidentes que afectan la disponibilidad sin aplicar los controles de la “ISO 27001”, tiene un promedio del 77.50% de incidentes, y luego de la implementación de los controles se obtuvo un promedio del 15.67% de incidentes, lo que significa que existe una reducción del 61.83%. Es decir, existe una mejora en la disponibilidad de la información en la institución educativa. Asimismo, con lo indicado por Vasquez (2018), el cual tuvo como objetivo implementar un sistema de gestión “ISO 27001” para brindar una política que esté disponible a todo el personal. Los resultados evidenciaron que la aplicación del sistema del “ISO 27001” contribuye en la disponibilidad de las políticas al aumentar de 4% al 100%, mejorando la disponibilidad en un 96%. En términos generales se confirma que la implantación de la “ISO 27001” asegura la disponibilidad de la información en la institución educativa. Por último, se relaciona con Calder y Watkins (2019), en su aporte sobre la ISO 27001, para garantizar la disponibilidad, menciona que, todo activo y dato debe estar identificado.

Finalmente, las pruebas de evidencias de la implementación de la ISO 27001 se verifican en el siguiente anexo (ver anexo 10).

CAPITULO V:CONCLUSIONES Y RECOMENDACIONES.

5.1. Conclusiones

Primera: Se demostró que al implementar la ISO 27001, mejoro la seguridad de la información en la institución educativa; el cual mejoró en promedio un 61.64% en reducir la tasa de incidentes que afectan la seguridad de la información, que corresponde a un umbral promedio de 19.35% en general. Por lo tanto, la institución educativa mejora la seguridad de la información, debido a que antes había un aproximado de 290 incidentes, donde de manera eficiente y con la implementación de la ISO 27001 se redujo a 39 incidentes, lo cual beneficia a la institución.

Segunda: Se demostró que al implementar la ISO 27001, mejoró la confidencialidad de la información en la institución educativa; el cual mejoro un 61.38% en reducir la tasa de incidentes que afectan la confidencialidad, que corresponde a un umbral promedio de 27.56% en general. Por lo tanto, la institución educativa mejora la confidencialidad, debido a que antes había un promedio de 70 incidentes, donde de manera eficiente y con la implementación de la ISO 27001 se redujo a 14 incidentes, lo cual beneficia a la institución.

Tercera: Se demostró que la implementación de la ISO 27001, mejoró la integridad de la información en la institución educativa; el cual mejoro un 61.73% en reducción de la tasa de incidentes que afectan la integridad, que corresponde a un umbral promedio de 14.81% en general. Por lo tanto, la institución educativa mejora la integridad, debido a que antes había un promedio de 40 incidentes, donde de manera eficiente y con la implementación de la ISO 27001 se redujo a 5 incidentes, lo cual beneficia a la institución.

Cuarta: Se demostró que la implementación de la ISO 27001, mejoró la disponibilidad de la información en la institución educativa; el cual mejoro un 61.83% en reducción de la tasa de incidentes que afectan la disponibilidad, que corresponde a un umbral promedio de 15.67% en general. Por lo tanto, la institución educativa mejora la disponibilidad, debido a que antes había un promedio de 130 incidentes, donde de manera eficiente y con la implementación de la ISO 27001 se redujo a 20 incidentes, lo cual beneficia a la institución.

5.2. Recomendaciones

- Primera:** Se recomienda al director, hacer cumplir las políticas a todo el personal de la institución, y con ello reducir en un 100% los incidentes que afecta la seguridad de la información.
- Segunda:** Se recomienda al director, programar charlas de concientización sobre las vulnerabilidades y amenazas que pueden afectar los activos de información al no seguir las normas o políticas que establece la ISO 27001, y con ello disminuir en un 99% la tasa de incidentes que afectan la integridad, confidencialidad y disponibilidad.
- Tercera:** Se recomienda al encargado de TI, mejorar las políticas y controles que se basan en la norma ISO 27001 utilizando la mejora continua, con ello reducir en un 99% los incidentes que afectan la seguridad de la información, así mismo, llegar al máximo nivel de madurez.
- Cuarta:** Se recomienda a la propietaria de la institución, implementar al 100% la norma “ISO 27001” en todo el ámbito institucional, con ello optar por la certificación y ser reconocida internacionalmente.

REFERENCIAS

1. AENOR. (15 de enero de 2023). <https://www.aenor.com>. [https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion](https://www.aenor.com:https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion)
2. Andina. (17 de febrero de 2022). <https://andina.pe>. [https://andina.pe/agencia/noticia-peru-sufrio-mas-115-mil-millones-intentos-ciberataques-2021-881221.aspx](https://andina.pe:https://andina.pe/agencia/noticia-peru-sufrio-mas-115-mil-millones-intentos-ciberataques-2021-881221.aspx)
3. Araujo, G. (18 de julio de 2020). <https://www.linkedin.com/>. [https://www.linkedin.com/pulse/confusi%C3%B3n-usual-la-isoiec-27001-vigente-es-del-2013-%C3%B3-gilberth-araujo/?originalSubdomain=es](https://www.linkedin.com:https://www.linkedin.com/pulse/confusi%C3%B3n-usual-la-isoiec-27001-vigente-es-del-2013-%C3%B3-gilberth-araujo/?originalSubdomain=es)
4. Areito, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Paraninfo.
5. Arias, J., Villasís, M., & Miranda, M. (2016). The research protocol III. Study population. *Revista Alergia México*, 63(2), 201-206.
6. Arias, O. (2001). *Estudio hidrometeorológico de la cuenca*. Instituto Tecnológico de Costa Rica.
7. Azurza, W. (20 de octubre de 2020). <https://www.linkedin.com>. [https://www.linkedin.com/pulse/principales-aspectos-de-seguridad-en-los-sistemas-el-azurza-neyra/?originalSubdomain=es](https://www.linkedin.com:https://www.linkedin.com/pulse/principales-aspectos-de-seguridad-en-los-sistemas-el-azurza-neyra/?originalSubdomain=es)
8. Calder, A. (2017). *Una guía de bolsillo*. IT Governance Publishing.
9. Calder, A., & Watkins, S. (2019). *Information Security Risk Management for ISO 27001/ISO 27002, third edition*. IT Governance Ltd.

10. Campos, G., & Lule, N. (2012). La observación, un método para el estudio de la realidad. *Revista Xihmai*, VII(13), 45-60.
<https://dialnet.unirioja.es/servlet/articulo?codigo=3979972>
11. Carrillo, A. (2015). *Métodos de la investigación*. Universidad Autónoma de la Ciudad de Mexico.
12. Carvajal, L. (2013). *El método deductivo de investigación*. Mexico Editores.
13. Chávarry, S. (2021). *implementación de iso 27001 y 27002 adaptadas para gestión de seguridad de información en secretaría ejecutiva de Policía Nacional del Perú*. Universidad César Vallejo.
14. Deming, W. (1989). *Calidad, productividad y competitividad: la salida de la crisis*. Ediciones Díaz de Santos.
15. Fernandez, I., A., C., Fernandez, M., & Fernandez, J. (2022). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security*, 22, 1-43.
<https://doi.org/10.1016/j.cose.2022.102954>
16. Flores, D., & Gardi, V. (2020). Sistema experto para la SGTI en la empresa Sion Global Solutions. *INNOVA Research Journal*, 5(3.2), 235-248.
<https://doi.org/10.33890/innova.v5.n3.2.2020.1568>
17. García, J., Huamani, S., & Lomparte, R. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista peruana de computación y sistemas*, 47-56.
<https://doi.org/https://doi.org/https://doi.org/10.15381/rpcs.v1i1.14856>
18. Godoy, R. (2014). *Seguridad de la Información*. Revista dela Segunda Cohorte del Doctorado en Seguridad Estratégica.
19. Gómez, Á. (2011). *Enciclopedia de la Seguridad Informática. 2ª edición*. RA-MA.

20. Gómez, L., & Fernández, P. (2018). *Cómo implantar un SGSI según UNE-ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad*. AENOR.
21. Gómez, S. (2012). *Metodología de la investigación*. Red Tercer Milenio. <http://up-rid2.up.ac.pa:8080/xmlui/handle/123456789/2019>
22. Haz, L., & Cervantes, J. (2017). *Implementación del proceso de gestión de riesgos tecnológicos y de Seguridad de la Información a la plataforma de gestión académica de una Institución de Educación Superior del Ecuador*. Escuela Superior PolitÉcnica del Litoral.
23. Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación*. Mc Graw Hill Education.
24. Huacasi, J. (2018). *Implementación de un Sistema de Gestión de Seguridad de la Información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de seguridad de información en el Ejército del Perú*. Universidad Privada Telesup.
25. ISOTools. (27 de septiembre de 2018). <https://www.pmg-ssi.com/>. <https://www.pmg-ssi.com/>: <https://www.pmg-ssi.com/2018/09/que-importancia-tiene-la-mejora-continua-en-la-seguridad-de-la-informacion/>
26. ISOTools. (16 de noviembre de 2022). <https://www.isotools.org>. <https://www.isotools.org>: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>
27. Jegelka, M. (25 de Octubre de 2022). <https://www.dqsglobal.com/>. <https://www.dqsglobal.com/>: <https://www.dqsglobal.com/es-ar/blog/new-iso-27001-2022-key-changes#normative-aenderungen-chapter03>
28. Kaspersky. (24 de octubre de 2022). <https://cybermap.kaspersky.com>. <https://cybermap.kaspersky.com>: <https://cybermap.kaspersky.com/es>

29. Lin, T., Wu, P., & Gao, F. (2022). Information security of flowmeter communication network based on multi-sensor data fusion. *Energy Reports*, 8, 12643-12652. <https://doi.org/10.1016/j.egy.2022.09.072>
30. Monteza, L. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino*. Universidad Peruana de Ciencias Aplicadas.
31. Moreira, J. (2019). *Seguridad de la información de infraestructura tecnológica y sistemas informáticos del GADM del cantón Chone basado en la norma ISO/IEC 27001*. Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix Lopez.
32. Ortiz, E. (2018). *Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva*. Universidad Nacional Agraria de la Selva.
33. Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, 35(1), 227-232. <https://doi.org/10.4067/S0717-95022017000100037>
34. Peña, S. (2017). *Análisis de Datos*. Bogota DC: Fondo Editorial Areandino.
35. Peñafiel, C. (2019). *Diseño de un modelo para establecer un sistema de gestión*. Pontificia Universidad Católica del Ecuador.
36. Porras, M. (2020). *Sistema de Gestión de Seguridad de la Información para la Gestión de Riesgos en Activos de Información*. Universidad Peruana Los Andes.
37. Prada, G., & Ortiz, R. (2022). *Diseño de un Sistema de Gestión de Seguridad de la Información (sgsi) para el área de Tecnologías de la Información y la Comunicación del hospital San Vicente de Paúl de Fresno*. Universidad Nacional Abierta y a Distancia - UNAD.
38. Puebla, C. (2010). *Método hipotético deductivo*. Universidad de Valparaíso Chile.

39. Rajab, M. (2018). *The Relevance of Social and Behavioral Models in Determining Intention to Comply with Information Security Policy in Higher Education Environments*. Eastern Michigan University.
40. Rodríguez, P. (2008). *Material de Seminario de Tesis*. UAS.
41. Rojas, R. (2006). *Guía para realizar investigaciones sociales*. Plaza y Valdés Editores.
42. Shannon, C., & Warren, W. (1949). *The Mathematical Theory of Communication*. University of Illinois Press.
43. Silva, A. (2022). *Implementación de un sistema de gestión de seguridad de la información para mejorar la seguridad de la información en una empresa MyPE, 2021*. Universidad Tecnológica del Perú.
44. Snyman, D., & Kruger, H. (2022). The Role of Information Deserts in Information Security Awareness and Behaviour. *Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP*, 613-620. <https://doi.org/10.5220/0010984200003120>
45. Spears, J., & San Nicolas, T. (2015). Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations. *International Journal of Knowledge Management (IJKM)*, 11(4), 52-69. <https://doi.org/10.4018/IJKM.2015100104>
46. Tidy, J. (21 de julio de 2022). <https://www.bbc.com/>. <https://www.bbc.com/:https://www.bbc.com/mundo/noticias-internacional-62246974>
47. Toledo, N. (2016). *Población y Muestra*. Universidad Autónoma de Ciudad de México.

48. Toro, R. (5 de Noviembre de 2022). <https://www.pmg-ssi.com>. <https://www.pmg-ssi.com>: <https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/>
49. Toro, R. (20 de Diciembre de 2022). <https://www.pmg-ssi.com/>. <https://www.pmg-ssi.com/>: <https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/>
50. Tushar , B. (2011). Data and information theft in e-commerce, jurisdictional challenges, related issues and response of Indian laws. *Computer Law & Security Review*, 27(4), 385-393. <https://doi.org/10.1016/j.clsr.2011.05.009>
51. Ulin, P., Robinson, E., & Tolley, E. (2005). *Investigación aplicada en salud pública*. Family Health Internacional.
52. Vásquez, J. (2018). *Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI*. Universidad Nacional Mayor de San Marcos.
53. Vega, E. (2021). *Seguridad de la información*. Editorial Área de Innovación y Desarrollo,S.L.
54. Von Bertalanffy, L. (1976). *Teoría general de los sistemas. Fundamentos, desarrollo, aplicaciones*. Fondo de Cultura Económica.

ANEXOS


Anexo 1: Matriz de consistencia

Título: ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022. Autor(es): Asqui Zevallos, Jhojan Alex - Torres Vasquez, Jean Pool							
PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES				
Problema general ¿De qué manera la norma ISO 27001 mejora la seguridad de la información en los procesos de TI en instituciones de educación, Lima 2022?	Objetivo general: Demostrar como la norma ISO 27001 mejora la seguridad de la información en los procesos de TI en instituciones de educación, Lima 2022.	Hipótesis general: La norma ISO 27001 mejora la seguridad de la información en los procesos de TI en instituciones de educación, Lima 2022	Variable Independiente: Metodología del ISO 27001				
			Dimensiones	Indicadores	Ítems	Niveles o rangos	
			Ciclo de Deming				
Problemas específicos	Objetivos específicos	Hipótesis específicas	Variable Dependiente: Seguridad de la información				
			Dimensiones	Indicadores	Ítems	Niveles o rangos	
PE1: ¿De qué manera la norma ISO 27001 mejora la confidencialidad de la información en los procesos de TI en instituciones de educación, Lima 2022?	OE1: Demostrar como la norma ISO 27001 mejora la confidencialidad de la información en los procesos de TI en instituciones de educación, Lima 2022.	HE1: La norma ISO 27001 mejora la confidencialidad de la información en los procesos de TI en instituciones de educación, Lima 2022.	Confidencialidad	Tasa de incidentes que afectan la confidencialidad de la información.	Porcentaje	Razón	

PE2: ¿De qué manera la norma ISO 27001 mejora la integridad de la información en los procesos de TI en instituciones de educación, Lima 2022?	OE1: Demostrar como la norma ISO 27001 mejora la integridad de la información en los procesos de TI en instituciones de educación, Lima 2022.	HE2: La norma ISO 27001 mejora la integridad de la información en los procesos de TI en instituciones de educación, Lima 2022.	Integridad	Tasa de incidentes que afectan la integridad de la información.	Porcentaje	Razón
PE3: ¿De qué manera la norma ISO 27001 mejora la disponibilidad de la información en los procesos de TI en instituciones de educación, Lima 2022?	OE1: Demostrar como la norma ISO 27001 mejora la disponibilidad de la información en los procesos de TI en instituciones de educación, Lima 2022.	HE3: La norma ISO 27001 mejora la disponibilidad de la información en los procesos de TI en instituciones de educación, Lima 2022.	Disponibilidad	Tasa de incidentes que afectan la disponibilidad de la información.	Porcentaje	Razón

Anexo 2: Instrumentos


Instrumento para medir la tasa de incidentes que afectan la confidencialidad

 Universidad Norbert Wiener			
FACULTAD DE INGENIERÍA Y NEGOCIOS ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD "ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"			
Guía de Observación			
Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)		Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)	
Formula->TIAC=(CIC/ITC) *100		Autor: José A. Tapia Granados	
TIAC: Tasa de incidentes que afectan la confidencialidad		Libro: Incidencia: concepto, terminología y análisis dimensional - 1994	
CIC: Cantidad de incidentes de confidencialidad		Variable: Seguridad de la información	
ITC: Incidentes totales de confidencialidad		Dimensión: Confidencialidad	
Pre-test			
Controles	CIC	ITC	TIAC
Controles de redes			
Seguridad de los servicios de red			
Segregación en redes			
Políticas y procedimientos de intercambio de información			
Acuerdos de intercambio de información			
Mensajería electrónica			
Acuerdos de confidencialidad o no revelación			
		Promedio	

Instrumento para medir la tasa de incidentes que afectan la integridad

 Universidad Norbert Wiener			
FACULTAD DE INGENIERÍA Y NEGOCIOS ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD "ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"			
Guía de Observación			
Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)		Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)	
Formula->TIAI=(CII/ITI) *100		Autor: José A. Tapia Granados	
TIAI: Tasa de incidentes que afectan la integridad		Libro: Incidencia: concepto, terminología y análisis dimensional - 1994	
CII: Cantidad de incidentes de integridad		Variable: Seguridad de la información	
ITI: Incidentes totales de integridad		Dimensión: Integridad	
Pre-test			
Controles	CII	ITI	TIAI
Política sobre el uso de controles criptográficos			
Gestión de claves			
Controles físicos de entrada			
		Promedio	


Instrumento para medir la tasa de incidentes que afectan la disponibilidad

 Universidad Norbert Wiener			
FACULTAD DE INGENIERÍA Y NEGOCIOS ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD "ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"			
Guía de Observación			
Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)		Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)	
Formula->TIAD=(CID/ITD)*100		Autor: José A. Tapia Granados	
TIAD: Tasa de incidentes que afectan la disponibilidad		Libro: Incidencia: concepto, terminología y análisis dimensional - 1994	
CID: Cantidad de incidentes de disponibilidad		Variable: Seguridad de la información	
ITD: Incidentes totales de disponibilidad		Dimensión: Disponibilidad	
Pre-test			
Controles	CID	ITD	TIAD
Inventario de activos			
Propiedad de los activos			
Uso aceptable de los activos			
Retorno de activos			
Clasificación de la información			
Etiquetado de la información			
Manejo de activos			
Gestión de medios removibles			
Disposición de medios			
Transferencia de medios físicos			
		Promedio	

Anexo 3: Validez del instrumento

Guías de observación validadas por los expertos

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENTES QUE AFECTAN LA CONFIDENCIALIDAD DE LA INFORMACIÓN

 Universidad Norbert Wiener FACULTAD DE INGENIERÍA Y NEGOCIOS ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD "ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"			
Guía de Observación			
Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)	Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)		
Formula->TIAC=(CINC/ITC) *100	Autor: José A. Tapia Granados		
TIAC: Tasa de incidentes que afectan la confidencialidad	Libro: Incidencias: concepto, terminología y análisis dimensional - 1994		
CIC: Cantidad de incidentes de confidencialidad	Variable: Seguridad de la información		
ITC: Incidentes totales de confidencialidad	Dimensión: Confidencialidad		
Pre-test			
Controles	CIC	ITC	TIAC
Controles de redes			
Seguridad de los servicios de red			
Segregación en redes			
Políticas y procedimientos de intercambio de información			
Acuerdos de intercambio de información			
Mensajería electrónica			
Acuerdos de confidencialidad o no revelación			
		Promedio	

Observaciones (precisar si hay suficiencia): Es conciso, exacto y directo

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir []** **No aplicable []**

Apellidos y nombres del juez validador: Chávez Alvarado, Walter Amador DNI: 09731774

Especialidad del validador: Ingeniero de sistemas / Proyecto de IT Ingeniero de Sistemas e informática

Colegiado: Si

28 de diciembre del 2022



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENTES QUE AFECTAN LA INTEGRIDAD DE LA INFORMACIÓN



**Universidad
Norbert Wiener**

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"

Guía de Observación

Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)	Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)		
Formula->TIAI=(CINI/ITI) *100	Autor: José A. Tapia Granados		
TIAI: Tasa de incidentes que afectan la integridad	Libro: Incidencias: concepto, terminología y análisis dimensional - 1994		
CII: Cantidad de incidentes de integridad	Variable: Seguridad de la información		
ITI: Incidentes totales de integridad	Dimensión: Integridad		
Pre-test			
Controles	CII	ITI	TIAI
Política sobre el uso de controles criptográficos			
Gestión de claves			
Controles físicos de entrada			
		Promedio	

Observaciones (precisar si hay suficiencia): Es conciso, exacto y directo

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir []** **No aplicable []**

Apellidos. y nombres del juez validador: **Chávez Alvarado, Walter Amador** **DNI: 09731774**

Especialidad del validador: **Ingeniero de sistemas / Proyecto de IT Ingeniero de Sistemas**

Colegiado: **Si**

28 de diciembre del 2022

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENTES QUE AFECTAN LA DISPONIBILIDAD DE LA INFORMACIÓN



**Universidad
Norbert Wiener**

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"

Guía de Observación			
Fecha Inicio: 01/12/2022	Fecha Fin: 15/12/2022		
Formula->TIAD=(CIND/ITD) *100	Autor: José A. Tapia Granados		
TIAD: Tasa de incidentes que afectan la disponibilidad	Libro: Incidencia: concepto, terminología y análisis dimensional - 1994		
CID: Cantidad de incidentes de disponibilidad	Variable: Seguridad de la información		
ITD: Incidentes totales de disponibilidad	Dimensión: Disponibilidad		
Pre-test			
Controles	CID	ITD	TIAD
Inventario de activos			
Propiedad de los activos			
Uso aceptable de los activos			
Retorno de activos			
Clasificación de la información			
Etiquetado de la información			
Manejo de activos			
Gestión de medios removibles			
Disposición de medios			
Transferencia de medios físicos			
		Promedio	

Observaciones (precisar si hay suficiencia): Es conciso, exacto y directo

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir []** **No aplicable []**

Apellidos. y nombres del juez validador: **Chávez Alvarado, Walter Amador** **DNI:**

Especialidad del validador: **Ingeniero de sistemas / Proyecto de IT. Ingeniero de Sistemas**
Colegiado: **Si**

28 de diciembre del 2022

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENTES QUE AFECTAN LA CONFIDENCIALIDAD DE LA INFORMACIÓN



**Universidad
Norbert Wiener**

**FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD**

"ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"

Guía de Observación

Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)	Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)		
Formula->TIAC=(CINC/ITC) *100	Autor: José A. Tapia Granados		
TIAC: Tasa de incidentes que afectan la confidencialidad	Libro: Incidencias: concepto, terminología y análisis dimensional - 1994		
CIC: Cantidad de incidentes de confidencialidad	Variable: Seguridad de la información		
ITC: Incidentes totales de confidencialidad	Dimensión: Confidencialidad		
Pre-test			
Controles	CIC	ITC	TIAC
Controles de redes			
Seguridad de los servicios de red			
Segregación en redes			
Políticas y procedimientos de intercambio de información			
Acuerdos de intercambio de información			
Mensajería electrónica			
Acuerdos de confidencialidad o no revelación			
		Promedio	

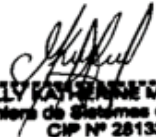
Observaciones (precisar si hay suficiencia): Es conciso, exacto y directo

Opinión de aplicabilidad: Aplicable Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador: Mera Jara, Kelly Katherine DNI: 47116235

Especialidad del validador: Ingeniero de sistemas / Proyecto de IT Ingeniera de Sistemas e informática
Colegiada:281325

28 de diciembre del 2022


KELLY KATHERINE MERA JARA
 Ingeniera de Sistemas e Informática
 CIP N° 281325

 Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENCIAS QUE AFECTAN LA INTEGRIDAD DE LA INFORMACIÓN

 Universidad Norbert Wiener FACULTAD DE INGENIERÍA Y NEGOCIOS ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD "ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"			
Guía de Observación			
Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)	Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)		
Formula->TIAI=(CINI/ITI) *100	Autor: José A. Tapia Granados		
TIAI: Tasa de incidentes que afectan la integridad	Libro: Incidencias: concepto, terminología y análisis dimensional - 1994		
CII: Cantidad de incidentes de integridad	Variable: Seguridad de la información		
ITI: Incidentes totales de integridad	Dimensión: Integridad		
Pre-test			
Controles	CII	ITI	TIAI
Política sobre el uso de controles criptográficos			
Gestión de claves			
Controles físicos de entrada			
		Promedio	

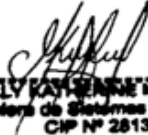
Observaciones (precisar si hay suficiencia): Es conciso, exacto y directo

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

Apellidos. y nombres del juez validador: Mera Jara, Kelly Katherine DNI: 47116235

Especialidad del validador: Ingeniero de sistemas / Proyecto de IT Ingeniera de Sistemas e informática
 Colegiada:281325

28 de diciembre del 2022



 KELLY KATHERINE MERA JARA
 Ingeniera de Sistemas e Informática
 CIP Nº 281325

 Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENTES QUE AFECTAN LA DISPONIBILIDAD DE LA INFORMACIÓN



FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"

Guía de Observación			
Fecha Inicio: 01/12/2022	Fecha Fin: 15/12/2022		
Formula->TIAD=(CIND/ITD) *100	Autor: José A. Tapia Granados		
TIAD: Tasa de incidentes que afectan la disponibilidad	Libro: Incidencia: concepto, terminología y análisis dimensional - 1994		
CID: Cantidad de incidentes de disponibilidad	Variable: Seguridad de la información		
ITD: Incidentes totales de disponibilidad	Dimensión: Disponibilidad		
Pre-test			
Controles	CID	ITD	TIAD
Inventario de activos			
Propiedad de los activos			
Uso aceptable de los activos			
Retorno de activos			
Clasificación de la información			
Etiquetado de la información			
Manejo de activos			
Gestión de medios removibles			
Disposición de medios			
Transferencia de medios físicos			
		Promedio	

Observaciones (precisar si hay suficiencia): Es conciso, exacto y directo

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

Apellidos. y nombres del juez validador: Mera Jara, Kelly Katherine DNI: 47116235

Especialidad del validador: Ingeniero de sistemas / Proyecto de IT. Ingeniera de Sistemas e informática
Colegiada:281325

28 de diciembre del 2022


"KELLY KATHERINE MERA JARA"
Ingeniera de Sistemas e Informática
CIP Nº 281325

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENCIAS QUE AFECTAN LA CONFIDENCIALIDAD DE LA INFORMACIÓN



**Universidad
Norbert Wiener**
FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD
"ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"

Guía de Observación			
Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)		Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)	
Formula->TIAC=(CIC/ITC) *100		Autor: José A. Tapia Granados	
TIAC: Tasa de incidentes que afectan la confidencialidad		Libro: Incidencia: concepto, terminología y análisis dimensional - 1994	
CIC: Cantidad de incidentes de confidencialidad		Variable: Seguridad de la información	
ITC: Incidentes totales de confidencialidad		Dimensión: Confidencialidad	
Pre-test			
Controles	CIC	ITC	TIAC
Controles de redes			
Seguridad de los servicios de red			
Segregación en redes			
Políticas y procedimientos de intercambio de información			
Acuerdos de intercambio de información			
Mensajería electrónica			
Acuerdos de confidencialidad o no revelación			
Promedio			

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

Mg Menacho Navarrete Kareem. DNI: 24002602

Especialidad del validador: Ingeniero de sistemas / Proyecto de IT / Transformación Digital
Colegiado: Si

28 de diciembre del 2022

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENCIAS QUE AFECTAN LA INTEGRIDAD DE LA INFORMACIÓN



**Universidad
Norbert Wiener**

**FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD**

"ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"

Guía de Observación

Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)	Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)		
Formula->TIAI=(CII/ITI) *100	Autor: José A. Tapia Granados		
TIAI: Tasa de incidentes que afectan la integridad	Libro: Incidencia: concepto, terminología y análisis dimensional - 1994		
CII: Cantidad de incidentes de integridad	Variable: Seguridad de la información		
ITI: Incidentes totales de integridad	Dimensión: Integridad		
Pre-test			
Controles	CII	ITI	TIAI
Política sobre el uso de controles criptográficos			
Gestión de claves			
Controles físicos de entrada			
		Promedio	

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

Mg Menacho Navarrete Karem. **DNI: 24002602**

Especialidad del validador: Ingeniero de sistemas / Proyecto de IT / Transformación Digital
Colegiado: Si

28 de diciembre del 2022

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE TASA DE INCIDENCIAS AFECTAN LA DISPONIBILIDAD DE LA INFORMACIÓN



**Universidad
Norbert Wiener**

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022"

Guía de Observación

Fecha Pre-test: 01/12/2022-15/12/2022(Dic vs Nov)	Fecha Post-test: 01/01/2023-15/01/2023(Ene vs Dic)
Formula->TIAD=(CID/ITD) *100	Autor: José A. Tapia Granados
TIAD: Tasa de incidentes que afectan la disponibilidad	Libro: Incidencia: concepto, terminología y análisis dimensional - 1994
CID: Cantidad de incidentes de disponibilidad	Variable: Seguridad de la información
ITD: Incidentes totales de disponibilidad	Dimensión: Disponibilidad

Pre-test

Controles	CID	ITD	TIAD
Inventario de activos			
Propiedad de los activos			
Uso aceptable de los activos			
Retorno de activos			
Clasificación de la información			
Etiquetado de la información			
Manejo de activos			
Gestión de medios removibles			
Disposición de medios			
Transferencia de medios físicos			
		Promedio	

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad: Aplicable [] Aplicable después de corregir [] No aplicable []

Mg Menacho Navarrete Karem. DNI: 24002602

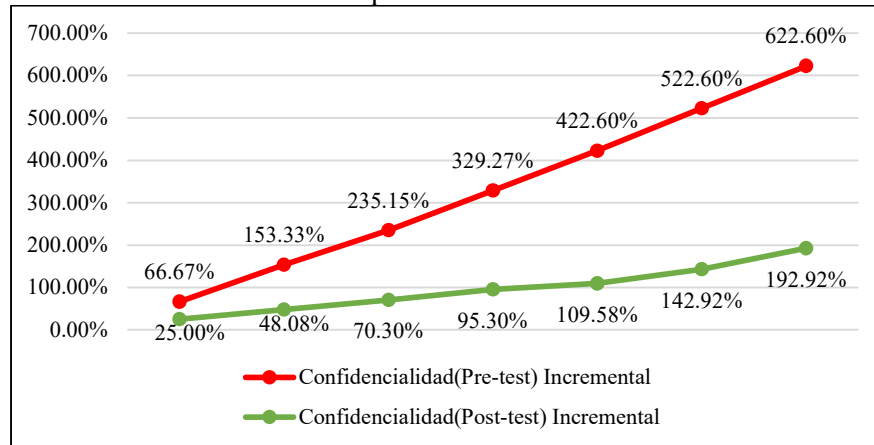
Especialidad del validador: Ingeniero de sistemas / Proyecto de IT / Transformación Digital
Colegiado: Si

28 de diciembre del 2022

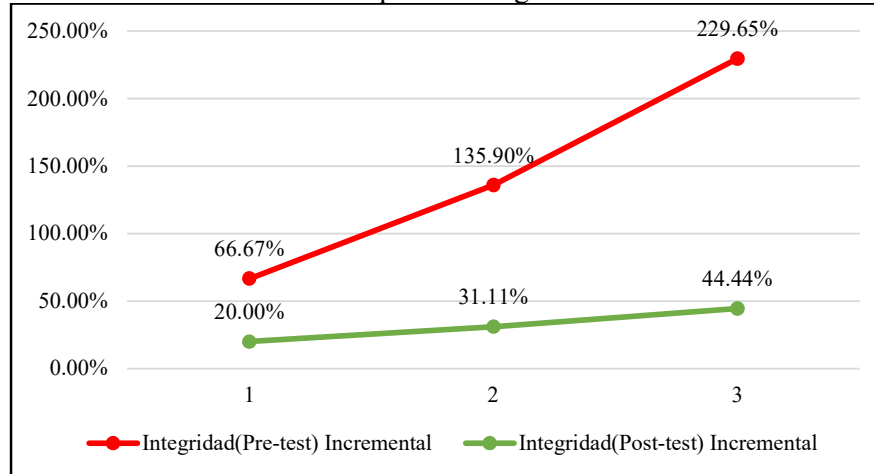
Firma del Experto Informante

Anexo 4: Confiabilidad del instrumento

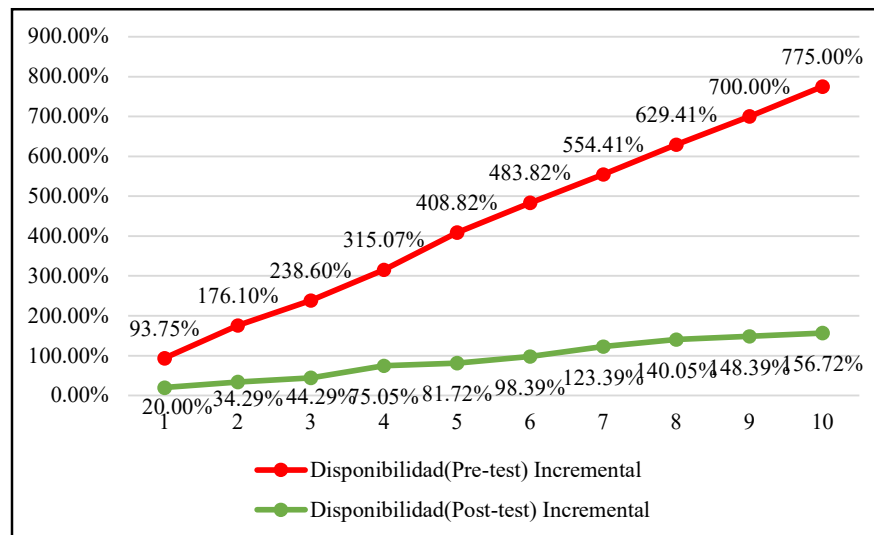
Confiabilidad de instrumento para la Confidencialidad



Confiabilidad del instrumento para la Integridad



Confiabilidad del instrumento para la Disponibilidad



Anexo 5: Desarrollo de la ISO 27001

DESARROLLO DE LA ISO 27001

1. Introducción

En la institución educativa fueron conscientes de la importancia de la información y el valor que aporta al negocio. Por ello, fue conveniente implementar la ISO 27001, Sistema de gestión de seguridad de la información, con el fin de ser protegido de los incidentes que está expuesta la información. A continuación, se menciona los 11 puntos del desarrollo de la ISO 27001:

Punto 1: La introducción: En este punto, se detalla cada punto del desarrollo de la ISO 27001.

Punto 2: Las políticas de seguridad de la información: En este punto, se describe las políticas consideradas en la institución educativa.

Punto 3: El plan de seguridad de la información: En este punto, se detalla el proceso que se ha seguido para la implementación de cada control.

Punto 4: GAP análisis: En este punto, se analiza el nivel de madurez actual de la institución educativa.

Punto 5: El resumen: En este punto, se describe una breve representación del contenido de todo el documento.

Punto 6: Los objetivos: En este punto, se menciona el logro que se quiere alcanzar con la implantación de la ISO 27001.

Punto 7: El alcance: En este punto, se detalla hasta donde se llegará y lo que se va a realizar.

Punto 8: Las generalidades: En este punto, se detalla los capítulos, objetivos y controles utilizados en cada pilar de la seguridad de la información.

Punto 9: La aplicación de los controles: En este punto, se muestra la evidencia que se aplicó por cada control.

Punto 10: La verificación de la efectividad de los controles: En este punto, se detalla efectividad que tienen los controles al ser implementados.

Punto 11: El actuar: En este punto, se describe la última fase del ciclo de Deming.

2. Políticas de seguridad de la información.

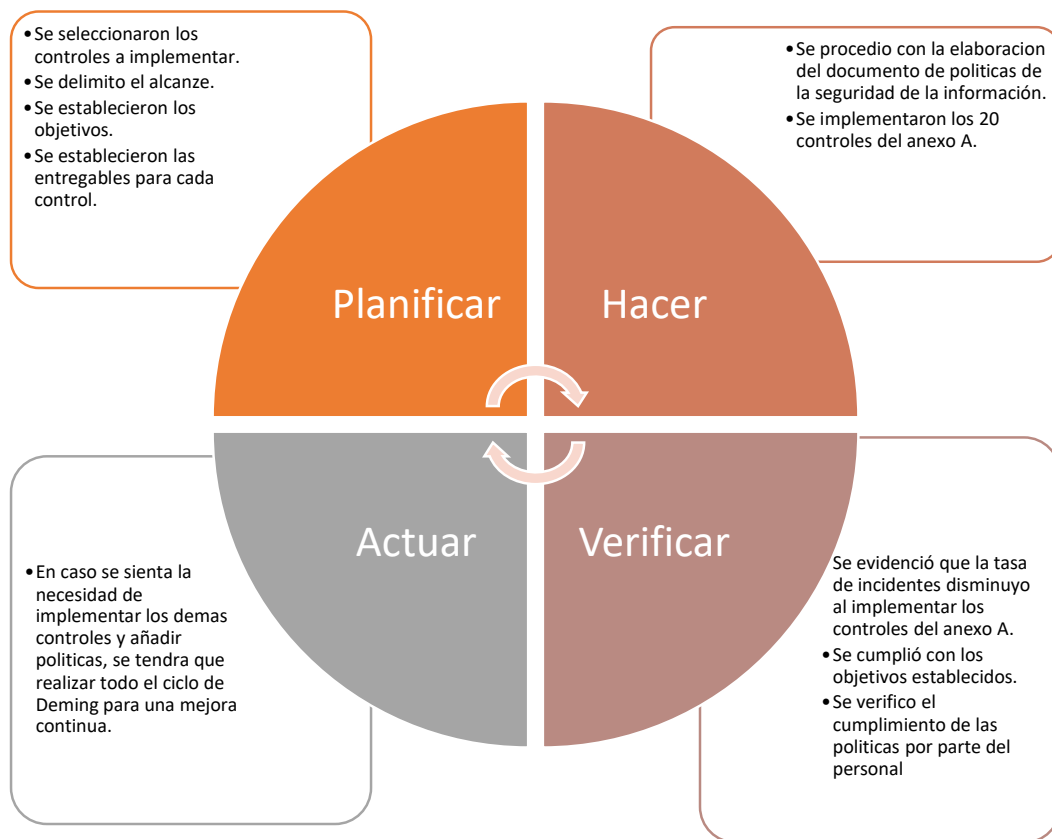
A continuación, se consideran las siguientes políticas de seguridad de la información:

1. Se deberá contar con un permiso especial para acceder a la red.
2. Las conexiones de red y servicios de red deberán ser bloqueado para no interferir en el proceso de enseñanza.

3. La red deberá estar segmentada de acuerdo con los niveles de la institución.
4. Contar con filtros de bloqueo de páginas no deseadas.
5. La institución estipular en su contrato con su proveedor donde apruebe el manejo responsable de la información para una mayor seguridad.
6. Todo correo enviado deberá estar firmado en el pie de página y libre de virus y además encriptado.
7. Estipular procedimientos en caso haya fuga de información en la institución educativa.
8. La información será clasificada según nivel, tipo y calidad, luego debe ser transportada a través de un medio lógico o físico, dicha información deberá estar encriptada por los propios responsables.
9. Las claves que se utilizaron deberán ser distribuidas al personal autorizado, dichas claves deberán estar almacenadas en un gestor de contraseñas.
10. Para el ingreso en la institución o a cualquier otra ares, el agente desconocido se deberá identificar.
11. Identificar los activos que dan soporte a la institución, cada activo deberá ser clasificado según su importancia, nivel y tipo que ocupa en la institución, para luego seleccionar a un responsable de cada activo.
12. Garantizar que los activos sean inventariados, clasificados, etiquetados y almacenados en una base de datos.
13. Concientizar a toda la institución sobre el uso responsable de los activos.
14. Crear procedimientos para la devolución de los activos.
15. Clasificar la información de la institución educativa según: valor, requisito y nivel de protección.
16. Realizar el etiquetado periódicamente por cada equipo y material educativo para luego trasladarlo a una base de datos.
17. Etiquetar y clasificar los medios removibles según la información que contiene.
18. Copiar la información necesaria, y eliminar la información obsoleta que no se requiera.
19. Tener el máximo cuidado al momento de transportar cualquier tipo de medio físico.

3. Plan de Seguridad de la información.

Esta implementación se ha realizado utilizando el ciclo de Deming:



4. GAP de análisis.

Los niveles de madurez se miden en 6 estados los cuales estan descritos en la siguiente tabla:

Nº	Nivel de implementación	% de cumplimiento	Descripción
5	Gestionado	100%	Los procesos, controles, procedimientos, acciones y políticas han sido llevados al nivel de la mejora continua en relación con su resultado.
4	Medible	80%	Es posible hacer seguimiento y medir la efectividad de los controles, procedimientos, acciones y políticas.
3	Definido	60%	Los controles, procedimientos, acciones y políticas se encuentran totalmente documentadas y aprobadas, pero la responsabilidad recae en cada individuo.
2	Repetible	40%	Se ha identificado procesos y acciones de implementación, pero la documentación no está totalmente aprobada.
1	Inicial	20%	Se ha identificado acciones de implementación, pero no hay un proceso de documentación relacionada a la acción.
0	Inexistente	0%	No se ha identificado controles, procedimientos, acciones y políticas en la institución educativa.

Nivel de madurez actual para confidencialidad

Capitulo	Objetivos	Control	Situación actual	Situación ideal
“ Seguridad de las comunicaciones”	“ 13.1. Gestión de la seguridad de redes”	“13.1.1. Controles de red”	0	≥3
		“13.1.2. Seguridad de servicios de red”	1	≥3
		“13.1.3 Segmentación en redes”	0	≥3
	“ 13.2. Intercambio de información”	“13.2.1. Políticas y procedimientos de intercambio de información”	0	≥3
		“13.2.2. Acuerdos de intercambio de información”	0	≥3
		“13.2.3. Mensajería electrónica”	0	≥3
		“13.2.4. Acuerdos de confidencialidad o no revelación”	2	≥3
	Nivel de madurez actual			0,42 = 0

Nivel de madurez actual para integridad

Capitulo	Objetivos	Control	Situación actual	Situación ideal
“ Criptografía”	“ 10.1. Controles Criptográficos”	“10.1.1. Políticas de uso”	0	≥3
		“10.1.2. Gestión de Claves”	2	≥3
“ Seguridad física y ambiental”	“ 11.1 Áreas seguras”	“11.1.2. Controles físicos de entrada”	1	≥3
Nivel de madurez actual			1	≥3

Nivel de madurez actual para disponibilidad

Capítulo	Objetivos	Control	Inicio	Esperado
“ Gestión de activos”	“ 8.1.1. Responsabilidad sobre los activos”	“8.1.1. Inventario de activos”	1	≥3
		“8.1.2. Propiedad de los activos”	0	≥3
		“8.1.3. Uso aceptable de los activos”	2	≥3
		“8.1.4 Retorno de activos”	1	≥3
	“ 8.2. Clasificación de la información”	“8.2.1. Clasificación de la información”	1	≥3
		“8.2.2. Etiquetado de la información”	0	≥3
		“8.2.3. Manejo de activos”	2	≥3
	“ 8.3. Manejo de los medios”	“8.3.1. Gestión de medios removibles”	1	≥3
		“8.3.2. Disposición de medios”	0	≥3
		“8.3.3. Transferencia de medios físicos”	1	≥3
Nivel de madurez actual			0.9 = 1	≥3

5. Resumen.

El presente documento se elaboró como parte del estudio, para mejorar la confidencialidad, integridad y disponibilidad de la información, haciendo uso de la ISO 27001, de la cual se empleó los controles, procedimiento y políticas. Además, del plan de seguridad de la información aplica el ciclo de Deming como parte de la metodología de desarrollo, con el fin de realizar una mejora continua en todo lo aplicado con el estudio.

6. Objetivos.

La implementación tiene como objetivo establecer políticas para la seguridad de la información, procedimientos y el desarrollo de los controles del anexo A, para garantizar la integridad, confidencialidad y disponibilidad de información de la institución educativa.

7. Alcance.

Estas políticas se aplican a toda la institución educativa la cual cuenta con equipos informativos, documentos sensibles e información clasificada. Debido a la auditoría realizada se planteó utilizar 4 de los 14 capítulos, donde se verificó que eran los capítulos más vulnerables en la institución educativa. Estos capítulos son: A8, A10, A11 y A13, dentro de las cuales se implementó un total de 20 controles entre todos los capítulos.

8. Generalidades.

En este punto se detalla los capítulos, objetivos de control y controles alineados a las especificaciones del anexo A de la ISO 27001, las mismas que están categorizadas por los “3 pilares de la seguridad de la información”.

A. Confidencialidad

Es la propiedad en que debe tener la información, para que solo los agentes autorizados, puedan visualizarlo.

Capítulo	“A13. Seguridad de las comunicaciones”
	Consiste en que ninguna entidad, y persona no autoriza pueda acceder de forma sencilla a la información.
Objetivo	“A13.1. Gestión de seguridad de la red”
	Mantener la protección de la información en las redes y en el procesamiento de la información.
Controles	“A13.1.1. Controles de la red” El encargado de TI deberá tener el permiso para acceder a los servicios de red cuando sea necesario, dicho permiso deberá ser solicitado por el encargado de TI a través de un correo o llenado de un formulario. (ver evidencia 1)
	“A13.1.2. Seguridad de servicios de red” Las conexiones de red y servicios de red están configuradas para el uso adecuado de los estudiantes y profesores bloqueando paginas no educativas como: <ul style="list-style-type: none">• páginas de videojuegos.• contenido para mayores de edad.• redes sociales, etc. (ver evidencia 2)
	“A13.1.3. Segregación en redes” La red esta segmentada por los distintos niveles que hay en la institución: <ul style="list-style-type: none">• Alumno• Profesor• Área administrativa: director, subdirector, coordinador y auxiliares. (ver evidencia 3)
Objetivo	“A13.2 Transferencia de la información”
	Mantener la seguridad en la transferencia de la información dentro y fuera de la organización.

Controles	<p>“A13.2.1. Políticas y procedimientos de la transferencia de la información”</p> <p>Se deberá contar con los siguientes procedimientos:</p> <ul style="list-style-type: none"> • Filtro de navegación. • Registro de bloqueo de sitio web. • Registro de conexiones denegadas. (ver evidencia 4)
	<p>“A13.2.2. Acuerdo sobre transferencia de información”</p> <p>Para que el proveedor de internet otorgue un servicio de forma segura, los reportes y registros son solicitados a través de un contrato, o bien solicitado por la misma institución educativa, tales como los registros de sitios web o el monitoreo de la red. Por motivos de confidencialidad no se evidenciará este reporte. (véase el punto 13.2.1). (ver evidencia 5)</p>
	<p>“A13.2.3. Mensajes electrónicos”</p> <p>Se debe utilizar el estándar institucional de pie de firma para los correos. En caso de que la comunicación lo amerite, por su contenido o por el cargo de los participantes, el correo electrónico debiese generarse firmado digitalmente y cifrado.</p> <p>Es responsabilidad del usuario revisar y eliminar mensajes de correo detectados como SPAM.</p> <p>Deben existir mecanismos de protección de dichas comunicaciones: (a) sistemas antivirus y antimalware para correo electrónico. (b) uso de cifrado del propio Google para transacciones que lo ameriten. (ver evidencia 6)</p>
	<p>“A13.2.4. Acuerdos de confidencialidad o no divulgación.”</p> <p>Verificar y definir la información que se protege.</p> <p>Responsabilidades y acciones de los firmantes para evitar la divulgación de las notas.</p> <p>El uso permitido de la información confidencial del alumno y los derechos del firmante para que dicha información sea utilizada por la institución para tramites estudiantiles.</p> <p>Notificar en caso haya una fuga o pérdida de información confidencial.</p> <p>Medidas esperadas que se toman en caso un personal no llega a informa sobre el incumplimiento del acuerdo confidencial.</p> <p>Revisión y medición.</p> <p>La presente política debe ser revisada al menos cada 2 años o cuando ocurra cambios significativos, para asegurar su continua idoneidad, eficiencia y efectividad. (ver evidencia 7)</p>

B. Integridad

Es la propiedad donde la información no pueda ser modificada, eliminada y usada por un agente no autorizado.

Capítulo	“A10. Criptografía”
Consiste en un conjunto de técnicas que permite cifrar información para no ser expuestos a personas no autorizadas y no ser leído sin su clave correspondiente.	
Objetivo	“A10.1 Controles criptográficos”
Aseguran el uso apropiado y efecto de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.	

Controles	“A10.1.1 Políticas sobre el uso de controles criptográficos.” Se clasifico la información del negocio, el cual será transportado en un medio extraíble o por correo, esta información o archivo será encripto por un software (AES Encrypt o WinRAR) que el personal responsable selecciono. (ver evidencia 8)
	“A10.1.2 Gestión de claves” Las claves o contraseña ya sea de WinRAR o AES Encrypt será distribuido al personal autorizado, dichas claves serán almacenadas en un gestor de contraseñas, para ello, se utilizará el software Lastpass. (ver evidencia 9)
Capítulo	“A11. Seguridad física y ambiental”
Consiste en utilizar medidas para proteger la infraestructura, sistemas e información en relación con los riesgos del ambiente físico.	
Objetivo	“A11.1 Áreas seguras”
Consiste en utilizar medidas para proteger la infraestructura, sistemas e información en relación con los riesgos del ambiente físico.	
Control	“A11.1.2 Controles de ingreso físico” Al momento de ingresar el agente deberá de rellenar un formulario el cual ha sido establecido por la institución. (ver evidencia 10)

C. Disponibilidad

Es la propiedad que permite a la información estar disponible, pero solo al agente autorizado.

Capítulo	“A8. Gestión de activos”
Consiste en organización los bienes y servicios que tengan valor para la organización.	
Objetivo	“A8.1. Responsabilidad por los activos”
Identificar los activos y definir los responsables de protección apropiada.	
Controles	“A8.1.1. Inventario de activos” Para el inventario de activo se procedió a registrar en una base de datos los activos que aporten valor a la institución en una base de datos. Asimismo, se especifica una breve descripción del activo, el sistema que utiliza, tipo, nivel y valor del activo. (ver evidencia 11)
	“A8.1.2. Propiedad de los activos” Se ha etiquetado los activos en físico y luego fueron almacenos en una base con todas las especificaciones del activo. (ver evidencia 12)
	“A8.1.3. Uso aceptable de los activos” Impartir charlas cada 3 meses sobre los riesgos que implican el mal uso de los activos. (ver evidencia 13)
	“A8.1.4. Retorno de activos” Todo activo prestado deberá ser devuelto en perfectas condiciones por el responsable que lo solicito. Caso contrario, haya una pérdida o daño del activo, se sancionará al responsable, en cambio sí, solo se daña se le llamara la atención. (ver evidencia 14)
Objetivo	“A8.2. Clasificación de la información”
La información debe ser clasificado según su nivel e importancia para la organización.	

Controles	<p>“A8.2.1. Clasificación de la información” Clasificar la información de la institución educativa según: valor (dato numérico), Tipos (lógico, físico, información, servicio, etc.) y nivel (según los siguientes criterios confidencialidad, disponibilidad e integridad). (ver evidencia 15)</p>
	<p>“A8.2.2. Etiquetado de la información” Se realizó el etiquetado de todos los equipos TI de forma física y digital. Y este etiquetado se debería actualizar cada 2 o 3 meses. (ver evidencia 16)</p>
	<p>“A8.2.3. Manejo de activos” Para un adecuado manejo se tendrá que cumplir con los puntos anteriores a este control los cuales hacen mención del inventario, etiquetado, clasificación y el retorno de los activos los cuales hacen referencia a la categoría de los controles 8.1 y 8.2 de gestión de activos. (ver evidencia 17)</p>
Objetivo	“A8.3. Manejo de los medios”
Prevenir la remoción, divulgación, modificación y destrucción no autorizada en medios.	
Controles	<p>“A8.3.1. Gestión de medios removibles” Cada medio removible como USB, CD-DVD, fueron etiquetados y clasificados según su información. (ver evidencia 18)</p>
Controles	<p>“A8.3.2. Disposición de medios” Se procedió a eliminar la información innecesaria a través de un borrado o destrucción del medio extraíble. En caso, de que el medio aun contenga datos necesarios se procederá a hacer una copia a otro medio de almacenamiento y se verificara antes de su destrucción. Y para este procedimiento se debe contar con la aprobación del director. (ver evidencia 19)</p>
	<p>“A8.3.3. Transferencia de medios” Como los medios de transferencia es interna en la institución, el personal a cargo trasladará de manera adecuada los medios de información. (por ejemplo: el transporte de los activos deberá ser entregado en un sobre manila sellado). (ver evidencia 20)</p>

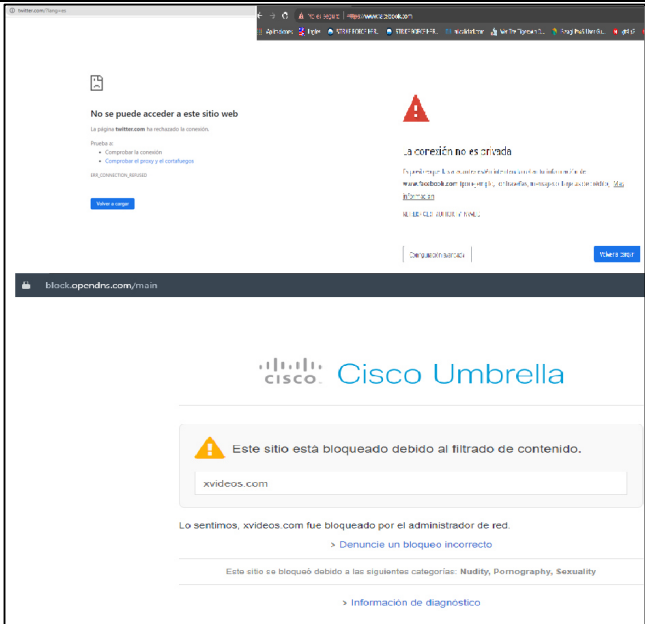
9. Aplicación de los controles

Se implementaron los 4 capítulos establecidos con las siguientes evidencias:

Evidencia 1:

"A13.1.1. Controles de la red"			
Formato de correo de permiso o llenado de formulario.			
Explicación: Se elaboró un formato de solicitud, con el fin de mantener un registro de quienes hacen uso del área de TI y configuraciones de los equipos de TI.			
Formato de solicitud			
Datos del solicitante			
Apellidos y Nombres:			
Tipo de Identificación:	DNI	Numero de Identificación:	
Area:	Sala computo	Cargo:	Encargado TI
Motivo del permiso:			
Configuración de red: LAN, VLAN, Accesos remotos al router, contraseñas.			
Horario			
Inicio		Fin	
Fecha	5/01/2023	Fecha	5/01/2023
Hora	8:30 a. m.	Hora	10:00am

Evidencia 2:

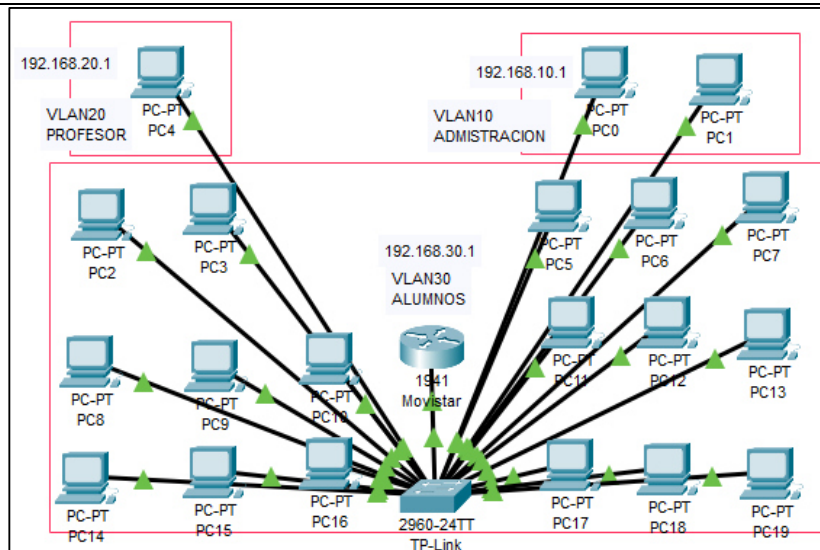
"A13.1.2. Seguridad de servicios de red"	
Páginas no autorizas	
Explicación: Se utilizo la herramienta OpenDNS y como medida alterna System32 para el bloqueo de la paginas no autorizadas.	
	

Evidencia 3:

“A13.1.3. Segregación en redes”

Redes segmentadas.

Explicación: Se realizó un modelo de segmentación de redes que fue aceptado por la institución, con la finalidad de mantener privacidad de datos entre los distintos roles de la institución.



VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10 Administracion	active	Fa0/2, Fa0/3
20 Profesor	active	Fa0/4
30 Alumnos	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21

Evidencia 4:

“A13.2.1. Políticas y procedimientos de la transferencia de la información”

Página y Registros de bloqueo.

Explicación: Se bloqueo la paginas con OpenDNS, que permitía bloquear las páginas de forma manual y automática. Además, se bloqueó desde System32 en el propio Windows , donde solo permite el bloqueo de manera manual ingresando el dominio de la página.

The screenshot displays the OpenDNS configuration interface. On the left, the 'Customization' tab is active, showing 'Choose your filtering level' with 'High' selected. Below this, the 'Manage individual domains' section lists domains to be blocked, with 'twitter.com' and 'facebook.com' highlighted in red. The main content area shows a browser window with a red warning triangle and the message 'La conexión no es privada' (The connection is not private) for 'https://www.facebook.com'. Below this, another browser window shows a 'No se puede acceder a este sitio web' (Cannot access this website) error for 'twitter.com', with the message 'La página twitter.com ha rechazado la conexión.' (The page twitter.com has rejected the connection.) and the error code 'ERR_CONNECTION_REFUSED'.

```
hosts file de notas
Archivo Edición Formato Ver Ayuda
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 182.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host

# localhost name resolution is handled within DNS itself.
#
127.0.0.1 localhost
#
::1 localhost
127.0.0.1 activate.adobe.com
127.0.0.1 praivate.adobe.com
127.0.0.1 lm.licenses.adobe.com
127.0.0.1 twitter.com
127.0.0.1 facebook.com
127.0.0.1 xvideos.com
127.0.0.1 frivsonline.com
```

Evidencia 5:

“A13.2.2. Acuerdo sobre transferencia de información”

Contrato con el proveedor de internet.

Explicación: Se detalla la cláusula de confidencialidad con la empresa Movistar, con la finalidad de autorizar el correcto uso de la información de la institución educativa, para mantener la confidencialidad segura.

Privacidad y Protección de Datos Personales de Movistar

Telefónica del Perú S.A.A., Telefónica Móviles S.A., Telefónica Multimedia S.A.C (en adelante, "Movistar") garantiza la confidencialidad en el tratamiento de los datos de carácter personal facilitados por sus clientes, de conformidad con la legislación peruana. En ningún caso Movistar proporciona información que identifique al CLIENTE, sin previa autorización de éstos, salvo para el estricto y único fin de atenderlos de la mejor forma.

El Cliente otorga autorización expresa a Movistar para hacer uso y realizar tratamiento de la información personal que éste proporcione a Movistar en virtud de la contratación de servicios, además de la información que se derive del uso de los mismos y de cualquier información pública o que pudiera recoger a través de fuentes de acceso público, incluyendo aquella a la que Movistar tenga acceso como consecuencia de su navegación en su página web (www.movistar.com.pe) (en adelante, la "Información") con la finalidad de enviarle comunicaciones comerciales, comercializar productos y servicios, mantenimiento de su relación contractual y de gestión con Movistar, creación de perfiles personalizados del Cliente y adecuar nuestras ofertas comerciales a sus características particulares. El Cliente reconoce y acepta que Movistar podrá ceder sus datos personales a cualquier tercero, siempre que sea necesaria su participación para cumplir con la prestación de servicios y comercialización de productos y servicios.

Movistar podrá ceder, en su caso, la Información a las sociedades del Grupo de empresas del que forma parte (http://www.telefonica.com.pe/telefonica_worldwide.shtml), con las mismas finalidades que se han indicado para la recogida de la Información por parte de Movistar, Movistar garantiza el mantenimiento de la confidencialidad y el tratamiento seguro de la Información en las transferencias internacionales que se realicen. El uso de la Información por las empresas antes indicadas se circunscribirá a los fines contenidos en esta cláusula.

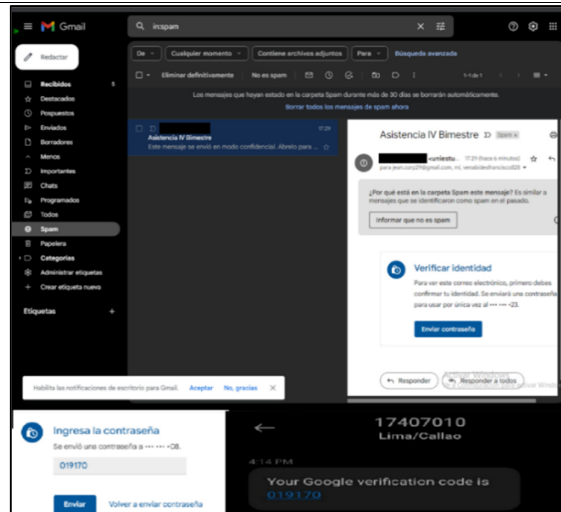
Movistar le informa que puede ejercer, de acuerdo a la legislación vigente, los derechos de información, acceso, actualización, inclusión, rectificación, supresión y oposición sobre sus datos personales, enviando una comunicación a cualquier centro de Atención al Cliente de Movistar a o al correo electrónico: protecciondedatos@movistar.com.pe

Evidencia 6:

“A13.2.3. Mensajes electrónicos”

Correo cifrado.

Explicación: Se realizó el cifrado de envío de correo mediante el propio Gmail, con la finalidad, que ante un descuido de dejar el correo abierto o enviar al destinatario equivocado, estos no puedan acceder a los archivos, ya que se pedirá un código de confirmación que ha sido vinculado mediante el número telefónico.



Evidencia 7:

“A13.2.4. Acuerdos de confidencialidad o no divulgación”

Documento de políticas, procedimientos y controles sobre la confidencialidad.

Explicación: Se elaboró un conjunto de políticas, con la finalidad de que el personal cumpla con cada una de ellas, para asegurar la información y salvaguardar los activos de la institución.

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION

1. Introducción

En la institución educativa fueron conscientes de la importancia de la información y el valor que aporta al negocio. Por ello, fue conveniente implementar la ISO 27001, Sistema de gestión de seguridad de la información, con el fin de ser protegido de los incidentes que está expuesta la información.

2. Políticas de Seguridad de la información.

- Se deberá contar con un permiso especial para acceder a la red.
- Las conexiones de red y servicios de red deberán ser bloqueado para no interferir en el proceso de enseñanza.
- La red deberá estar segmentada de acuerdo con los niveles de la institución.
- Contar con filtros de bloqueo de páginas no deseadas.
- La institución estipular en su contrato con su proveedor donde apruebe el manejo responsable de la información para una mayor seguridad.
- Todo correo enviado deberá estar firmado en el pie de página y libre de virus y además encriptado.
- Estipular procedimientos en caso haya fuga de información en la institución educativa.
- Las claves que se utilizaron deberán ser distribuidas al personal autorizado, dichas deberán estar almacenadas en un gestor de contraseñas.

Confidencialidad

Es la propiedad en que debe tener la información, para que solo los agentes autorizados, puedan visualizarlo.

Capítulo	A13. Seguridad de las comunicaciones
Consiste en que ninguna entidad, y persona no autoriza pueda acceder de forma sencilla a la información.	
Objetivo	A13.1. Gestión de seguridad de la red
Mantener la protección de la información en las redes y en el procesamiento de la información.	
Controles	A13.1.1. Controles de la red Los profesores y alumnos deberán pedir permiso para acceder a los servicios de red cuando sea necesario para la clase o cualquier uso recreativo, dicho permiso deberá ser solicitado por el profesor a través de un correo o llenado de un formulario.(ver evidencia 1)
	A13.1.2. Seguridad de servicios de red Las conexiones de red y servicios de red están configuradas para el uso adecuado de los estudiantes y profesores bloqueando paginas no educativas como: <ul style="list-style-type: none"> • páginas de videojuegos. • contenido para mayores de edad. • redes sociales, etc. (ver evidencia 2)
	A13.1.3. Segregación en redes La red esta segmentada por los distintos niveles que hay en la institución: <ul style="list-style-type: none"> • Alumno • Profesor • Área administrativa: director, subdirector, coordinador y auxiliares. (ver evidencia 3)

Evidencia 8:

“A10.1.1 Políticas sobre el uso de controles criptográficos”

Uso de las aplicaciones criptográficas.

Explicación: Se utilizó el AES Encrypt y el WinRAR, con la finalidad de encriptar documentos al momento de la transferencia de archivos, y no pueda ser legible ante agentes no autorizados.

The screenshot shows a file explorer window with the following table:

Nombre	Tipo	Tamaño
ASISTENCIA IV BIMESTRE 2022.xlsx.aes	AES Crypt Encrypt...	163 KB

Below the file explorer is a dialog box titled "AES Crypt Password" with the text "Enter password:" and a password input field filled with dots. There are "OK" and "Cancel" buttons.

The screenshot shows a WinRAR window with the following table:

Nombre	Fecha de modifica...	Tipo	Tamaño
ASISTENCIA IV BIMESTRE 2022	4/01/2023 17:22	Archivo WinRAR	121 KB

Below the file explorer is a dialog box titled "Introducir contraseña" (Introduce password) with the text "Introduzca contraseña para el archivo cifrado ASISTENCIA IV BIMESTRE 2022.rar". It includes a password input field, a "Mostrar contraseña" checkbox, and "Aceptar", "Cancelar", and "Ayuda" buttons.

At the bottom, the WinRAR interface shows a file list with the following table:

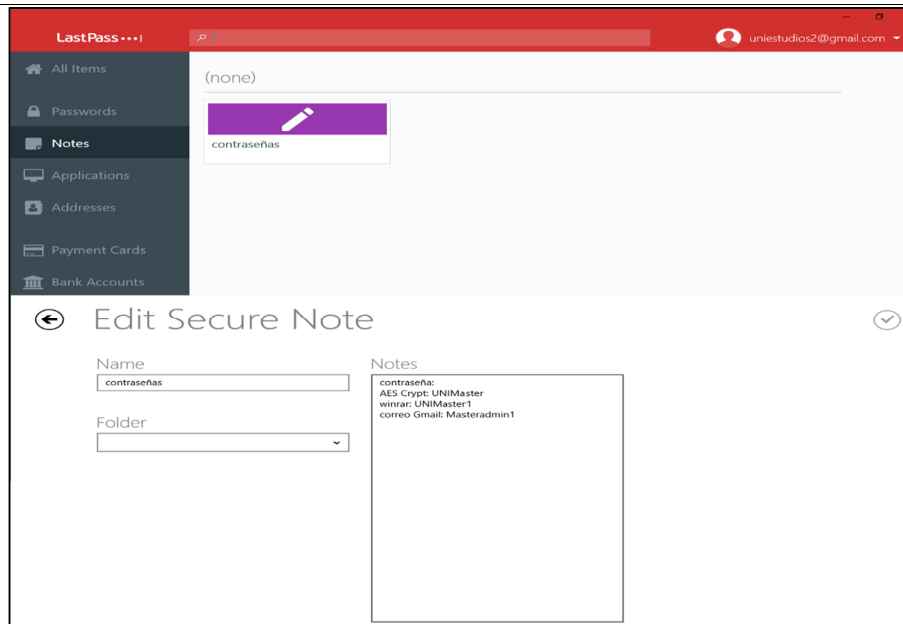
Nombre	Tamaño	Comprimido	Tipo	Modificado	CRC32
ASISTENCIA IV B...	165,859	122,976	Hoja de cálculo de...	16/12/2019 09:25	7B266333

Evidencia 9:

“A10.1.2 Gestión de claves”

Gestión de claves.

Explicación: Se utilizó la herramienta Lastpass, con la finalidad de almacenar las diferentes contraseñas con las que cuenta la institución. Además, se puede agregar como recordatorios claves que no se puedan sincronizar en Google.



Evidencia 10:

“A11.1.2 Controles de ingreso físico”

Formulario de acceso.

Explicación: Se elaboró un formulario de ingreso general, con la finalidad de contar con un registro, para identificar quienes ingresan al ambiente de TI.

FORMULARIO DE INGRESO						
Nombre del encargado	Francisco	Cargo	Supervisor			
Apellidos	Nombres	Fecha	Hora Entrada	Hora Salida	Nota	
1	torres vasquez	jean pool	21/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
2	Asqui Zevallos	Jhojan Alex	21/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
3	Benavides	Francisco	21/12/2022	08:00am	5:00pm	Supervisión
4	torres vasquez	jean pool	22/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
5	Asqui Zevallos	Jhojan Alex	22/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
6	Benavides	Francisco	22/12/2022	08:00am	5:00pm	Supervisión
7	torres vasquez	jean pool	23/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
8	Asqui Zevallos	Jhojan Alex	23/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
9	Benavides	Francisco	23/12/2022	08:00am	5:00pm	Supervisión
10	torres vasquez	jean pool	27/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
11	Asqui Zevallos	Jhojan Alex	27/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
12	Benavides	Francisco	27/12/2022	08:00am	5:00pm	Supervisión
13	torres vasquez	jean pool	28/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
14	Asqui Zevallos	Jhojan Alex	28/12/2022	08:00am	5:00pm	Implementacion de ISO 27001
15	Benavides	Francisco	28/12/2022	08:00am	5:00pm	Supervisión
16						
17						

Evidencia 11:

“A8.1.1. Inventario de activos”

Clasificación de los activos en excel.

Explicación: Se realizó la clasificación de los activos, con la finalidad de saber el tipo, nivel y valor que aportan a la institución educativa.

INVENTARIO							Nivel			Nivel de tasación	
Nombre de activo	Descripción del activo	Sistema involucrado	Tipo de activo	Tipo de ubicación	Nivel de confidencialidad	Propietario del activo	Confidencialidad	Integridad	Disponibilidad		Valor
Contrato de prestación de servicio de personal	Documento que regula la prestación de servicios de un personal con la institución.	Google Drive / DocuSign	Información	Lógica	Confidencial de la compañía	Responsable de RR.HH.	5	5	5	5.00	Muy Alto
PC Marca XXX-XXXX	Computadoras asignadas en la institución educativa.	N/A	Físico	Física	Confidencial de la compañía	Encargado de computo	3	4	2	3.00	Medio
Gestion de notas	Registro y almacenamiento de las notas del alumno.	Excel	Información	Lógica	Confidencial de la compañía	Encargado de computo	5	5	3	4.33	Muy Alto
Repositorio de libros,examen,mat.	Materiales para el aprendizaje	Google Drive	Información	Física-Lógica	Confidencial de la compañía	Encargado de computo	3	4	4	3.67	Alto
Servicio de internet	Servicio prestado por otra entidad	N/A	Servicios	Física-Lógica	No clasificado	Tercero	1	5	5	3.67	Alto
Imagen de marca	Documento que contiene la identidad visual de la empresa.	Figma	Intangibles	Lógica	No clasificado	Responsable de Marketing	1	3	2	2	Bajo
Switch Tp-link	Dispositivo para la segmentación de redes	N/A	Físico	Física-Lógica	Confidencial de la compañía	Encargado de computo	5	4	5	4.667	Muy Alto

Evidencia 12:

“A8.1.2. Propiedad de los activos”

Etiquetado de activo.

Explicación: Se etiqueto los activos, con la finalidad de saber las características de cada activo TI, y tener la información disponible, para futuras mejoras o reposiciones.

INVENTARIO PC'S						
Nombre de activo	Sistema Operativo	Procesador	Memoria RAM	Disco Duro	Area	Responsable
PC1	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC2	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC3	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC4	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC5	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC6	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC7	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC8	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC9	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC10	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC11	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo

Evidencia 13:

“A8.1.3. Uso aceptable de los activos”

Documento de políticas sobre la disponibilidad.

Explicación: Se elaboró un conjunto de políticas, con la finalidad de que el personal cumpla con cada una de ellas, para asegurar la información y disponer de los activos.

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION	
1. Introducción	En la institución educativa fueron conscientes de la importancia de la información y el valor que aporta al negocio. Por ello, fue conveniente implementar la ISO 27001, Sistema de gestión de seguridad de la información, con el fin de ser protegido de los incidentes que está expuesta la información.
2. Políticas de Seguridad de la información.	<ul style="list-style-type: none"> • Se deberá contar con un permiso especial para acceder a la red. • Las conexiones de red y servicios de red deberán ser bloqueado para no interferir en el proceso de enseñanza. • La red deberá estar segmentada de acuerdo con los niveles de la institución. • Contar con filtros de bloqueo de páginas no deseadas. • La institución estipular en su contrato con su proveedor donde apruebe el manejo responsable de la información para una mayor seguridad. • Todo correo enviado deberá estar firmado en el pie de página y libre de virus y además encriptado. • Estipular procedimientos en caso haya fuga de información en la institución educativa.

Disponibilidad									
Es la propiedad que permite a la información estar disponible, pero solo al agente autorizado.									
Capítulo	A8. Gestión de activos								
Consiste en organización los bienes y servicios que tengan valor para la organización.									
Objetivo	A8.1. Responsabilidad por los activos								
Identificar los activos y definir los responsables de protección apropiada.									
Controles	<table border="1"> <tr> <td style="vertical-align: top;">A8.1.1. Inventario de activos</td> <td>Para el inventario de activo se procedió a registrar en una base de datos los activos que aporten valor a la institución en una base de datos. Asimismo, en la base de datos se especifica una breve descripción del activo, el sistema que utiliza, tipo, nivel y valor del activo. (ver evidencia 11)</td> </tr> <tr> <td style="vertical-align: top;">A8.1.2. Propiedad de los activos</td> <td>Se ha etiqueto los activos de forma fisica y luego fueron almacenos en una base con todas las especificaciones del activo. (ver evidencia 12)</td> </tr> <tr> <td style="vertical-align: top;">A8.1.3. Uso aceptable de los activos</td> <td>Impartir charlas cada 3 meses sobre los riesgos que implican el mal uso de los activos. (ver evidencia 13)</td> </tr> <tr> <td style="vertical-align: top;">A8.1.4. Retorno de activos</td> <td>Todo activo prestado deberá ser devuelto en perfectas condiciones por el responsable que lo solicito. Caso contrario, haya una pérdida o daño del activo, se sancionará al responsable, en cambio sí, solo se dañe se le llamara la atención. (ver evidencia 14)</td> </tr> </table>	A8.1.1. Inventario de activos	Para el inventario de activo se procedió a registrar en una base de datos los activos que aporten valor a la institución en una base de datos. Asimismo, en la base de datos se especifica una breve descripción del activo, el sistema que utiliza, tipo, nivel y valor del activo. (ver evidencia 11)	A8.1.2. Propiedad de los activos	Se ha etiqueto los activos de forma fisica y luego fueron almacenos en una base con todas las especificaciones del activo. (ver evidencia 12)	A8.1.3. Uso aceptable de los activos	Impartir charlas cada 3 meses sobre los riesgos que implican el mal uso de los activos. (ver evidencia 13)	A8.1.4. Retorno de activos	Todo activo prestado deberá ser devuelto en perfectas condiciones por el responsable que lo solicito. Caso contrario, haya una pérdida o daño del activo, se sancionará al responsable, en cambio sí, solo se dañe se le llamara la atención. (ver evidencia 14)
A8.1.1. Inventario de activos	Para el inventario de activo se procedió a registrar en una base de datos los activos que aporten valor a la institución en una base de datos. Asimismo, en la base de datos se especifica una breve descripción del activo, el sistema que utiliza, tipo, nivel y valor del activo. (ver evidencia 11)								
A8.1.2. Propiedad de los activos	Se ha etiqueto los activos de forma fisica y luego fueron almacenos en una base con todas las especificaciones del activo. (ver evidencia 12)								
A8.1.3. Uso aceptable de los activos	Impartir charlas cada 3 meses sobre los riesgos que implican el mal uso de los activos. (ver evidencia 13)								
A8.1.4. Retorno de activos	Todo activo prestado deberá ser devuelto en perfectas condiciones por el responsable que lo solicito. Caso contrario, haya una pérdida o daño del activo, se sancionará al responsable, en cambio sí, solo se dañe se le llamara la atención. (ver evidencia 14)								

Evidencia 14:

“A8.1.4. Retorno de activos”

Formato de sanción o amonestación.

Explicación: Se diseñó un formato para la sanción y amonestación, con la finalidad de sancionar al responsable al no devolver un activo en perfectas condiciones

MEMORÁNDUM 1 – 2023

De: Nombre de director
A: Trabajador a sancionar

Asunto: Llamado de atención por irresponsabilidad del uso de las TIC.

Fecha: 14 de enero del 2023

Reciba un cordial saludo, a través de la presente hacemos expresa el llamado de atención severa hacia usted con respecto al incumplimiento por al entregar entregar un monitor en mal estado (pintado con plumón indeleble).

Sirva la presente como un precedente en caso de que las conductas continúen y afecte la productividad laboral de la compañía. Si fuese este el caso se dará inicio a un procedimiento laboral para sancionarle. Entiéndase esta como una llamada de atención y no una sanción.

Atentamente,

Nombre del director

Firma

[Sello]

Evidencia 15:

“A8.2.1. Clasificación de la información”

Clasificación de la información.

Explicación: Se clasifica la información, con la finalidad de mantener un orden, organizándolo según el tipo, nivel y valor, además, se añadió la propiedad de cada uno.

INVENTARIO						Nivel			Nivel de sanción		
Nombre de activo	Descripción del activo	Sistema involucrado	Tipo de activo	Tipo de ubicación	Propietario del activo	Confidencialidad	Integridad	Disponibilidad			
Contrato de prestación de servicio de personal	Documento que regula la prestación de servicios de un personal con la institución.	Google Drive / Docusign	Información	Lógica	Confidencial de la compañía	Responsable de RR.HH.	5	5	5	5.00	Muy Alto
PC Marca XXX-XXXX	Computadoras asignadas en la institución educativa.	N/A	Físico	Física	Confidencial de la compañía	Encargado de computo	3	4	2	3.00	Medio
Destin de notas	Registro y almacenamiento de las notas del alumno.	Excel	Información	Lógica	Confidencial de la compañía	Encargado de computo	5	5	3	4.33	Muy Alto
Repositorio de libros.examen.mat	Materiales para el aprendizaje	Google Drive	Información	Física-Lógica	Confidencial de la compañía	Encargado de computo	3	4	4	3.67	Alto
Servicio de internet	Servicio prestado por otra entidad	N/A	Servicios	Física-Lógica	No clasificado	Tercero	1	5	5	3.67	Alto
Tipo de activos	Información: bases de datos, archivos, documentación del sistema, manuales, material de capacitación, procedimientos de contingencia, etc. Físico: aplicaciones, desarrollos, utilitarios, herramientas de desarrollo, etc. Intangibles: equipos de comunicaciones, equipo de cómputo, gabinetes, ups, dispositivos, etc. Personas: reputación, imagen Servicios: capital humano, habilidades, experiencia Otros: servicios de comunicaciones, servicios necesarios para la ejecución del negocio										
Nivel de confidencialidad	No clasificado: Es información que se puede hacer pública, sin que implique consecuencias negativas para la empresa, como es la información que es de conocimiento público. Confidencial de los empleados: Esto incluye información como, registros médicos, salarios, entre otros. Confidencial de la compañía: Como contratos, códigos fuente, contraseñas para sistemas críticos de TI, contratos de clientes, cuentas, etc. Confidencial de cliente: Esto incluye información de identificación como nombre, dirección, claves de acceso al sistema de clientes, planes de negocio, información de nuevos productos, información sensible del mercado, etc.										
Tipo de ubicación	Físico Lógica Física-Lógica										
Criticidad	Muy Alto: El activo es esencial para el proceso del negocio. Si se detiene el riesgo de imagen reputacional y seguridad de los asociados. Alto: El activo se requiere para el proceso del negocio. Puede no estar disponible el activo o el proceso, pero solo por un corto tiempo. Puede ser en pérdida reputacional. Medio: El activo es importante para el proceso del negocio. Su falta no interrumpe proceso, así como tampoco la continuidad de negocio. El tiempo es operacional. Bajo: El activo tiene poca importancia en el proceso. La disponibilidad no es crítica, podrá estar ausente y no afecta a la calidad y continuidad del proceso. Muy Bajo: El activo tiene importancia muy baja en el proceso. No necesita cuidados especiales y protección.										

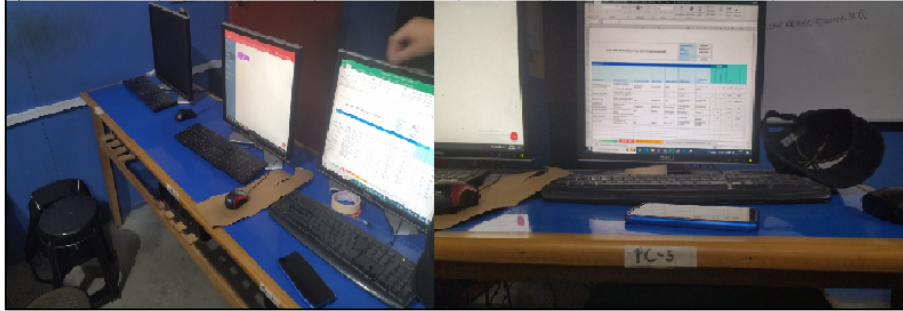
Evidencia 16:

“A8.2.2. Etiquetado de la información”

Etiquetado de información en excel y físico.

Explicación: Se realizó el etiquetado tanto físico como digital, con la finalidad de disponer las características detallada y facilitar la ubicación de cada activo.

INVENTARIO PC'S						
Nombre de activo	Sistema Operativo	Procesador	Memoria RAM	Disco Duro	Area	Responsable
1 PC1	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
2 PC2	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
3 PC3	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
4 PC4	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
5 PC5	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
6 PC6	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
7 PC7	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo



Evidencia 17:

“A8.2.3. Manejo de activos”

Adecuado manejo de los activos.

Explicación: Se implementó los controles de la gestión de activos, con la finalidad de disponer con la información necesaria, para darle el uso adecuado a los activos.

A8.1.1

Nombre de activo	Sistema Operativo	Procesador	Memoria RAM	Disco Duro	Area	Responsable
PC1	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC2	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC3	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC4	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC5	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC6	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC7	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC8	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC9	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC10	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC11	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo

A8.2.1

INVENTARIO PC'S

Nombre de activo	Sistema Operativo	Procesador	Memoria RAM	Disco Duro	Area	Responsable
PC1	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC2	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC3	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC4	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC5	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC6	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC7	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC8	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC9	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC10	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo
PC11	Windows 10	Intel Core i5 3.20 Ghz	4 Ram	500 Gb	Sala de computo	Encargado de sala de computo

A8.1.3

MEMORANDUM - 2023

De: Titular de director
A: Titular de subdirector

Asunto: Listado de atención por responsabilidad del uso de TIC.

Fecha: 14 de enero del 2023

Resalta un control actual, a través de la presente herramienta empresa del Titular de atención entre las actividades con respecto al etiquetado para el manejo adecuado de los activos en su estado (entendido con planillas adjuntas).

Es de la presente como un procedimiento en caso de que los resultados continúan y afectan la productividad laboral de la compañía. Se tiene en el caso de ser así iniciar un procedimiento laboral para su sanción. Entendidos así como una muestra de atención y de sus acciones.

Atentamente,

Titular del Director

Evidencia 18:

“A8.3.1. Gestión de medios removibles”

Etiquetado en Excel y físico.

Explicación: Se etiqueto tanto físico como en excel los medios de información removibles, con la finalidad de disponer con las características necesarias, y facilitar el contenido que almacena cada medio extraíble.

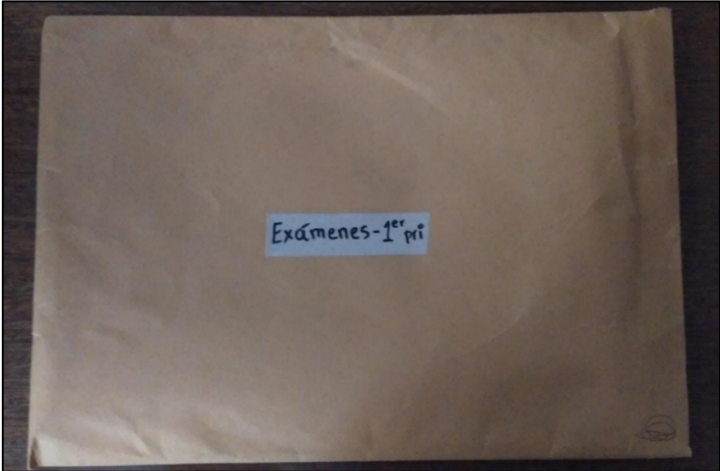
INVENTARIO MEDIOS						
	Nombre de activo	Marca	Capacidad	Contenido	Area	Responsable
1	USB 1	Kingston	32 Gb	Programas	Sala de computo	Encargado de sala de computo
2	USB 2	Kingston	32 Gb	Formatos	Sala de computo	Encargado de sala de computo
3	Disco Duro 1	Kingston	500 Gb	Default	Sala de computo	Encargado de sala de computo
4	Disco Duro 2	Kingston	501 Gb	Default	Sala de computo	Encargado de sala de computo
5	Disco Duro 3	Kingston	502 Gb	Default	Sala de computo	Encargado de sala de computo
6	Disco Duro 4	Wester Digital	500 Gb	Default	Sala de computo	Encargado de sala de computo
7	Disco Duro 5	Wester Digital	500 Gb	Default	Sala de computo	Encargado de sala de computo
8	Disco Duro 6	Wester Digital	500 Gb	Default	Sala de computo	Encargado de sala de computo



Evidencia 19:

“A8.3.2. Disposición de medios”	
Documento de aprobación para la destrucción de activos.	
Explicación: Se diseñó un formato de aprobación para la destrucción de activos, con la finalidad de dar a conocer que la información o contenido no es requerida por la institución educativa.	
	<p style="text-align: center;">Documento de aprobación</p> <p>Yo (nombre del director)</p> <p>Doy mi consentimiento a (nombre del encargado)</p> <p>De proceder con la destrucción y eliminación de información del (medio físico). Sin antes haber copiado primero la información y haberlo guardado.</p> <p>El motivo de la destrucción se ha dado debido a que el medio físico ha cumplido su vida útil.</p> <p>El copiado de información se dará en una unidad similar o se guardará en una computadora temporalmente.</p> <p>Gracias,</p> <p style="text-align: right;">_____</p> <p style="text-align: right;">Firma del director</p>

Evidencia 20:

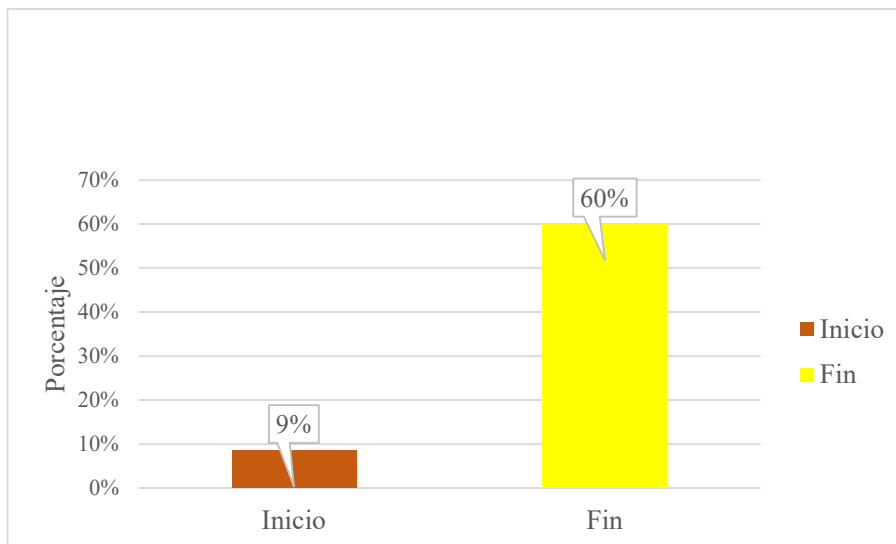
“A8.3.3. Transferencia de medios”	
Protección de transferencia de activos.	
Explicación: Se implementó la protección de transferencia de activos físicos, con la finalidad de que al momento de ser traslado estén debidamente protegidos y disponibles a la hora de solicitarlo.	
	

10. Verificación de los controles

Nivel de madurez de los controles de confidencialidad

Al inicio, los controles tenían un cumplimiento del 9% estando nivel de madurez inicial, luego con el desarrollo de la investigación el cumplimiento fue del 60% llegando al nivel de madurez definido. Es decir, al inicio se identificaron acciones mínimas de implementación, pero no estaban documentadas, luego del desarrollo y aprobó la implementación de la ISO 27001. Por lo tanto, se recomienda llegar al nivel de madurez gestionado que vendría a ser el 100% del cumplimiento.

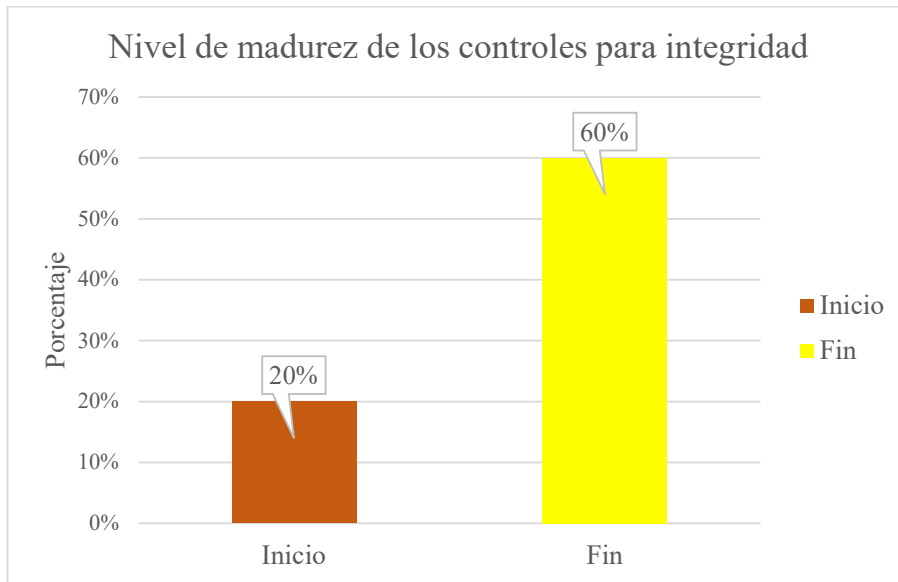
Capítulo	Objetivos	Control	Pre	Post	Ideal
“ Seguridad de las comunicaciones”	“ 13.1. Gestión de la seguridad de redes”	“13.1.1. Controles de red”	0	3	5
		“13.1.2. Seguridad de servicios de red”	1	3	5
		“13.1.3 Segmentación en redes”	0	3	5
	“ 13.2. Intercambio de información”	“13.2.1. Políticas y procedimientos de intercambio de información”	0	3	5
		“13.2.2. Acuerdos de intercambio de información”	0	3	5
		“13.2.3. Mensajería electrónica”	0	3	5
		“13.2.4. Acuerdos de confidencialidad o no revelación”	2	3	5
	Nivel de madurez			0.42 = 0	3
			9%	60%	100%



Nivel de madurez de los controles de integridad

Al inicio, los controles tenían un cumplimiento del 20% estando nivel de madurez inicial, luego con el desarrollo de la investigación el cumplimiento fue del 60% llegando al nivel de madurez definido. Es decir, al inicio se identificaron acciones mínimas de implementación, pero no estaban documentadas, luego del desarrollo y aprobó la implementación de la ISO 27001. Por lo tanto, se recomienda llegar al nivel de madurez gestionado que vendría a ser el 100% del cumplimiento.

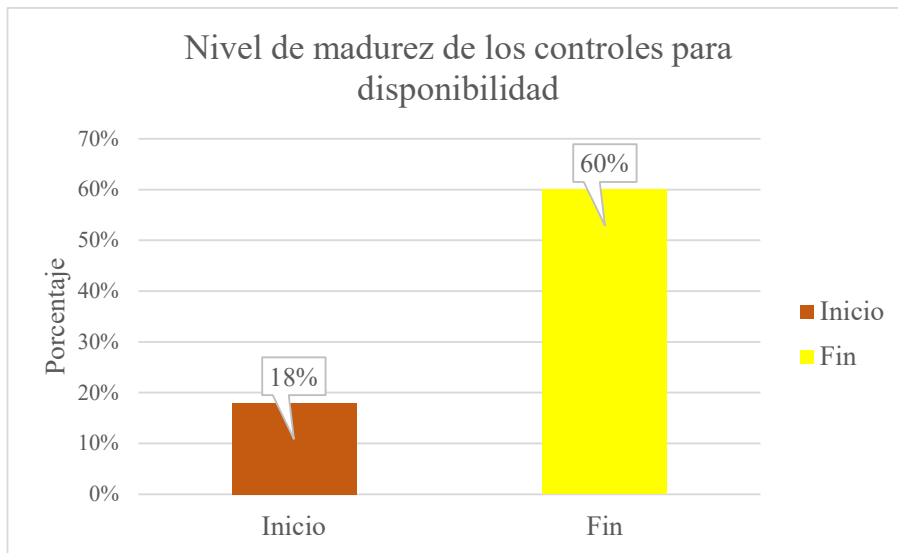
Capítulo	Objetivos	Control	Pre	Post	Ideal
" Criptografía"	" 10.1. Controles Criptográficos"	"10.1.1. Políticas de uso"	0	3	5
		"10.1.2. Gestión de Claves"	2	3	5
" Seguridad física y ambiental"	" 11.1 Áreas seguras"	"11.1.2. Controles físicos de entrada"	1	3	5
Nivel de madurez			1	3	5
			20%	60%	100%



Nivel de madurez de los controles de disponibilidad

Al inicio, los controles tenían un cumplimiento del 18% estando nivel de madurez inicial, luego con el desarrollo de la investigación el cumplimiento fue del 60% llegando al nivel de madurez definido. Es decir, al inicio se identificaron acciones mínimas de implementación, pero no estaban documentadas, luego del desarrollo y aprobó la implementación de la ISO 27001. Por lo tanto, se recomienda llegar al nivel de madurez gestionado que vendría a ser el 100% del cumplimiento.

Capítulo	Objetivos	Control	Pre	Post	Ideal	
"Gestión de activos"	"8.1. Responsabilidad sobre los activos"	"8.1.1. Inventario de activos"	1	3	5	
		"8.1.2. Propiedad de los activos"	0	3	5	
		"8.1.3. Uso aceptable de los activos"	2	3	5	
		"8.1.4 Retorno de activos"	1	3	5	
	"8.2. Clasificación de la información"	"8.2.1. Clasificación de la información"	1	3	5	
		"8.2.2. Etiquetado de la información"	0	3	5	
		"8.2.3. Manejo de activos"	2	3	5	
	"8.3. Manejo de los medios"	"8.3.1. Gestión de medios removibles"	1	3	5	
		"8.3.2. Disposición de medios"	0	3	5	
		"8.3.3. Transferencia de medios físicos"	1	3	5	
		Nivel de madurez actual		0.9 = 1	3	5
				18%	60%	100%



11. Actuar

En esta etapa que corresponde a la mejora continua, se plantea en un futuro mejorar e implementar los controles que no sido utilizados, volviendo a realizar todo el proceso del ciclo de Deming. Además, de llegar al nivel de madurez más alto en todos los capítulos del anexo A de la ISO 27001.

Anexo 6: Informa del asesor de turnitin

NOMBRE DEL TRABAJO

ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022-3.docx

AUTOR

Jean Pool / Alex / Torres / Asqui

RECuento DE PALABRAS

16174 Words

RECuento DE CARACTERES

89342 Characters

RECuento DE PÁGINAS

99 Pages

TAMAÑO DEL ARCHIVO

4.0MB

FECHA DE ENTREGA

Feb 11, 2023 10:22?AM GMT-5

FECHA DEL INFORME

Feb 11, 2023 10:24?AM GMT-5

● 8% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos

- 7% Base de datos de Internet
- Base de datos de Crossref
- 4% Base de datos de trabajos entregados
- 2% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref

● Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)