FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO

PARA OPTAR EL TÍTULO PROFESIONAL

DE INGENIERO DE SISTEMAS

Autor (es)

Bach. Farroñan Teran Nixon Paul

ORCID: https://orcid.org/0000-0003-3880-0487

Asesor(a)

Dr. Tuesta Monteza Víctor Alexci

ORCID: https://orcid.org/0000-0002-5913-990X

Línea de Investigación

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2024

APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO

Aprobación del jurado

_____

Dr. Carlos William Atalaya Urrutia

Presidente del Jurado de Tesis

_____

MG. David Enrique Bances Saavedra

Secretario del Jurado de Tesis

_____

Mg. Hermes Marino Quinteros Gonzáles

Vocal del Jurado de Tesis

Universidad
Señor de Sipán

Reporte de similitud

NOMBRE DEL TRABAJO

Nixon Paul Farroñan Teran - NIXON PAU L FARROÑAN TERAN-turnitin.docx

RECUENTO DE PALABRAS

14123 Words

RECUENTO DE CARACTERES

76911 Characters

RECUENTO DE PÁGINAS

74 Pages

TAMAÑO DEL ARCHIVO

629.9KB

FECHA DE ENTREGA

Oct 7, 2024 10:46 AM GMT-5

FECHA DEL INFORME

Oct 7, 2024 10:47 AM GMT-5

20% de similitud general

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

- 18% Base de datos de Internet
- 3% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 16% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien(es) suscribe(imos) la **DECLARACIÓN JURADA**, soy(somos) egresado. del Programa de Estudios de Ingeniería de Sistemas. de la Universidad Señor de Sipán S.A.C, declaro (amos) bajo juramento que soy (somos) autor(es) del trabajo titulado:

APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO.

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán (CIEI USS) conforme a los principios y lineamientos detallados en dicho documento, en relación a las citas y referencias bibliográficas, respetando al derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

Farroñan Teran Nixon Paul	DNI: 70070528	

Pimentel, 09 de setiembre de 2024

Dedicatorias

Agradecimientos

A Dios, por su magna bendición en mi vida,
A mis padres, por buscar en todo momento mi bienestar y protección,
A mis docentes, por su calidad humana y vocación de enseñanza latente

Índice

Índice de Tablas y Figuras

Índice de Tablas

Índice de Figuras

Resumen

Actualmente, en el Perú se estima aproximadamente de 2.8 millones de empresas activas registradas, siendo entre enero y marzo del 2021 donde hubo un ascenso notorio de casi 70 mil empresas constituidas, dicho de otra forma, algunas MYPES del sector público experimentaron una sobresaliente recuperación económica en comparación con el 2020.Dado que, en la actualidad cada vez más los institutos tecnológicos públicos peruanos tienen un alto consumo de información digitalizada, la cual influye en el momento realizar decisiones la alta gerencia, debe estar salvaguardada frente a diversos tipos de amenazas que valiéndose de cualquier vulnerabilidad existente tanto interna (personas) como externa (entorno), pueden llegar a doblegar los activos críticos de información por diferentes maneras: manipulación de software, robo de equipos, accesos no autorizados, espionaje, desastres naturales, revelación y alteración de información, entre otros. Es por ello que, en los últimos años se han estado probando distintos tipos de modelos de gestión de riesgos TI en institutos tecnológicos públicos peruanos, que puedan adaptarse al contexto, realidad económica, situación actual y demás factores, a los que pueda estar relacionado dicha organización, y es donde el objetivo de este estudio se centra en crear un modelo basado en el estándar ISO/IEC 27001:2017 para perfeccionar el desarrollo de la gestión de inseguridad informática en un instituto tecnológico público peruano. Se realizó una valoración de la condición actual de la entidad en gestión de inseguridad de TI bajo 07 subactividades, las cuales fueron: análisis del instituto tecnológico publico peruano, definición del proceso TI actual de instituto, realización de conteo de activos de datos, orden y valuación de activos de información. Las respuestas obtenidas evidenciaron que, el presente modelo de gestión para mejorar el proceso TI de un instituto tecnológico público peruano fundamentado en el estándar ISO 27001:2017 obtuvo un promedio final de 85,00/100 en cuanto a criterios aceptación de modelo, pertinencia, consistencia, coherencia, objetividad, metodología, organización, suficiencia, intencionalidad, actualidad y claridad.

Palabras Clave:

Modelo de gestión de riesgos, Riesgo de seguridad, Iso 27001, Mejora de procesos, Seguridad de la información.

Abstract

Currently, in Peru it is estimated that there are approximately 2.8 million active companies registered, being between January and March 2021 where there was a notorious increase of almost 70 thousand companies incorporated, in other words, some MYPES of the public sector experienced an outstanding economic recovery compared to 2020. Given that, currently more and more Peruvian public technological institutes have a high consumption of digitized information, which influences when making decisions, the top management must be safeguarded against various types of threats that using any existing vulnerability both internal (people) and external (environment), can get to bend the critical information assets in different ways: software manipulation, equipment theft, unauthorized access, espionage, natural disasters, disclosure and alteration of information, among others. That is why, in recent years, different types of IT risk management models have been tested in Peruvian public technological institutes, which can be adapted to the context, economic reality, current situation and other factors, to which such organization may be related, and that is where the objective of this study focuses on creating a model based on the ISO/IEC 27001:2017 standard to improve the development of IT insecurity management in a Peruvian public technological institute. An assessment of the current condition of the entity in IT insecurity management was carried out under 07 sub-activities, which were: analysis of the Peruvian public technological institute, definition of the current IT process of the institute, realization of data asset count, order and valuation of information assets. The answers obtained showed that the present management model to improve the IT process of a Peruvian public technological institute based on the ISO 27001:2017 standard obtained a final average of 85.00/100 in terms of model acceptance, relevance, consistency, coherence, objectivity, methodology, organization, sufficiency, intentionality, timeliness and clarity.

Keywords:

Risk management model, Security risk, Iso 27001, Process improvement, Information security.

I. INTRODUCCIÓN

1.1. Realidad Problemática.

En un instituto tecnológico público peruano, la gestión de riesgos de TI enfrenta desafíos significativos que comprometen la seguridad y eficacia de sus operaciones digitales, así como la protección de datos sensibles. Uno de los problemas más destacados es la falta de integración y coordinación entre los diversos departamentos académicos y administrativos en lo que respecta a la seguridad de TI. Cada departamento maneja sus riesgos de manera fragmentada, lo cual dificulta la implementación de estrategias de seguridad cohesivas y una respuesta unificada frente a incidentes. Esta fragmentación no solo debilita la postura general de seguridad, sino que también aumenta las posibilidades de divergencias de seguridad y violaciones de datos debido a la falta de una supervisión y control centralizado (Albrecht, 2016).

Además, la capacitación y concienciación sobre gestión de riesgos de TI son insuficientes entre el personal académico y administrativo. Los colaboradores deben recibir instrucción acerca de las convenientes praxis de seguridad y los peligros digitales más recientes. La falta de conciencia adecuada contribuye a un ambiente donde los empleados pueden no reconocer señales de alerta temprana de posibles ataques o vulnerabilidades, lo que aumenta la exposición del instituto a riesgos de seguridad (Ezell, 2018).

El instituto carece de un proceso metódico y sistemático para descubrir, evaluar y priorizar eficazmente los problemas informáticos a la hora de evaluar los riesgos. Las capacidades del instituto para prever y mitigar proactivamente tales peligros se ven obstaculizadas por la falta de evaluaciones de riesgos frecuentes y del uso de normas internacionalmente aceptadas en estas evaluaciones. para prever y evitar posibles riesgos con antelación. Esta ausencia de La distribución eficaz de los recursos para la instalación de controles de seguridad suficientes se ve obstaculizada aún más por este juicio inadecuado. establecimiento de medidas de seguridad adecuadas. (ISACA, 2017).

A nivel de recursos, el instituto enfrenta restricciones significativas tanto presupuestarias como de personal. Estas limitaciones afectan directamente la capacidad del instituto para implementar soluciones avanzadas de seguridad y para contratar expertos en gestión de riesgos de TI que puedan fortalecer su infraestructura de seguridad digital. La insuficiencia de recursos financieros también impide el avance de la tecnología necesaria para contrarrestar los riesgos emergentes. Los avances tecnológicos eran necesarios para contrarrestar los nuevos peligros. y mantener la seguridad informática conforme a las normas del sector, mantener la seguridad informática conforme a las mejores prácticas modernas (NIST, 2018).

El impacto potencial de estos desafíos es considerable. Además de la exposición a ciberataques y violaciones de datos, el instituto corre el riesgo de dañar su reputación y credibilidad institucional en caso de incidentes de seguridad importantes. Esto podría afectar su capacidad para atraer y retener estudiantes, colaboraciones académicas y financiamiento externo. Además, la falta de una administración de riesgos de TI eficaz podría poner al instituto en riesgo de incumplimiento de normativas locales e internacionales, con posibles repercusiones legales y financieras adicionales (ENISA, 2020; ICO, 2021).

Para abordar estos desafíos, se recomienda al instituto ejecutar un marco completo de gerencia de riesgos de TI. Esto incluiría establecer un comité interdepartamental dedicado a la seguridad de TI para fomentar la colaboración y la cohesión entre los diferentes sectores del instituto. Además, sería crucial desarrollar políticas y procedimientos estandarizados para la evaluación periódica de riesgos, así como para la respuesta ante incidentes. La instrucción constante de los colaboradores en seguridad digital y gestión de riesgos de TI también sería fundamental para mejorar la conciencia y competencia dentro de la institución. Consolidar la estrategia de seguridad informática del instituto exige, en última instancia, dedicar recursos suficientes y hacer exámenes frecuentes para comprobar la ejecución de la normativa y la eficacia de las precauciones de seguridad establecidas (PWC, 2019).

Implementar estas medidas no solo protegerá los activos digitales del instituto y sus datos sensibles, sino que también fortalecerá su capacidad para adaptarse y responder proactivamente a un escenario de amenazas en continua evolución, asegurando así un entorno digital seguro y confiable para toda su comunidad académica y colaboradores externos.

La pandemia ha generado grandes cambios a nivel mundial y nacional, el impacto causado en industrias, empresas y gobiernos ha dado origen a una nueva perspectiva sobre la visión y gestión de los riesgos empresariales. Tal es así, que muchos sectores empezaron a implementar o invertir en un área responsable de gestión de riesgos, buscando fortalecer el ambiente de control en TI de sus organizaciones. En la Figura 1, se evidencia el análisis de los sectores que invierten más en gestión de riesgos en TI, donde se tiene que los principales son s. minería, s. electricidad, s. construcción, s. transporte y s. comunicaciones. Sin embargo, en el sector Educación aún las inversiones tienen limitaciones, ya sea por ubicación, presupuesto, recursos, falta de conocimiento sobre gestión de riesgos o falta de capacitación de estándares internacionales y uso de prácticas óptimas para fortalecer y salvaguardar la protección de datos.

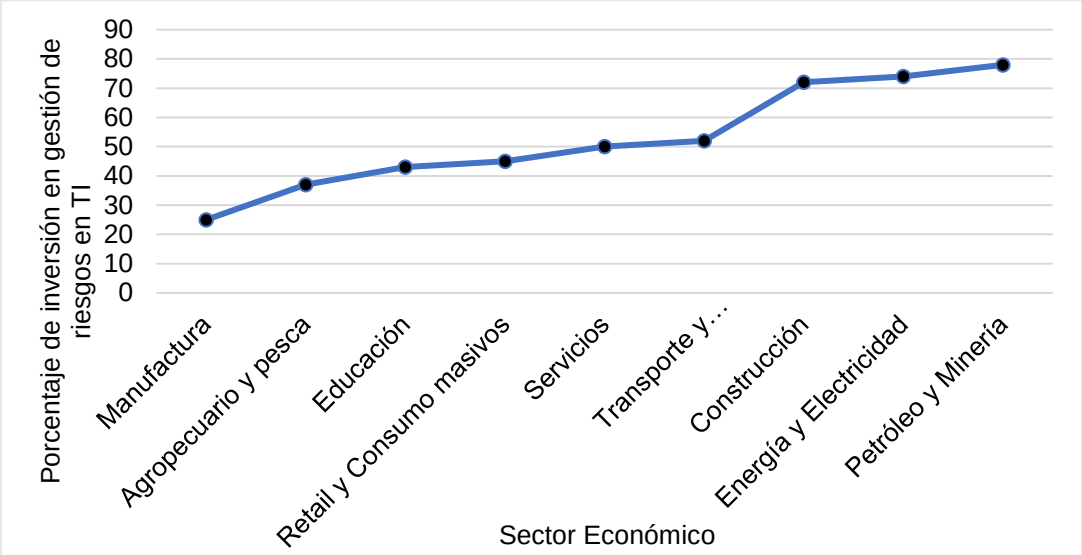


Figura 1. Distribución porcentual de empresas peruanas que han implementado un área para gestionar riesgos empresariales. Tomado de: Ernst & Young (2021)

En concerniente, al criterio de cuantificación de pérdidas económicas que sufre o podría sufrir una MYPE pública, con el tema de gestión, se encuentra la validación de probabilidad e impacto que conllevaría si se produjera una amenaza. (Feng, Wang, & Li, 2015)

Se desarrollaron soluciones de ingeniería para gestionar los riesgos en empresas, utilizando normas ISO, que ayuden a implementar controles de seguridad frente a las amenazas o endeble a las que puedan llegar a presentarse este tipo de organizaciones.

1.2. Formulación del Problema.

¿Cómo mejorar el proceso de gestión de riesgos de tecnologías de la información en un instituto tecnológico público peruano?

1.3. Hipótesis.

Mediante implementación del estándar ISO 27001:2017, se podrá mejorar el proceso de gestión de riesgos de tecnologías de la información en un instituto tecnológico público peruano.

1.4. Objetivos.

1.4.1. Objetivo general.

Implementar el estándar ISO 27001:2017 para mejorar el proceso de gestión de riesgos de tecnologías de la información en un instituto tecnológico público peruano.

1.4.2. Objetivos específicos.

a) Realizar un diagnóstico del estado actual de la institución en gestión de riesgos de TI.
b) Diseñar el modelo para la administración y evaluación de riesgos basado en el estándar ISO 27001:2017.
c) Validar con juicio de expertos el modelo de gestión propuesto.
d) Aplicar el modelo de gestión de riesgos TI en la institución.

1.5. Teorías concernientes al tema.

1.5.1 ISO 27000.

Esta serie estándar es propiedad de la Organización Internacional para la Normalización, centrado en la protección de SI y TI en una organización.

1.5.1.1 ISO 27001.

Estándar utilizado para las certificaciones. Proporciona las pautas a una empresa para organizar sus activos de información, su seguridad y el (SGSI). Proporciona procedimientos a una empresa para el alto nivel y seguridad de sus artículos y asistencias (Pineihro, 2016). Considera la gestión de peligros TI de TI como parte del cuadro general de la dirección de riesgos y aboga por la ejecución de controles para aquellos peligros que son inaceptables para la organización. Se han ofrecido 114 controles en este estándar y la empresa puede seleccionar los controles en función de sus necesidades en la tríada CIA, es decir, confidencialidad, integridad y disponibilidad o su evaluación de riesgos basada en activos. Por lo tanto, ISO 27001: 2013 es útil para aquellas empresas que buscan un estándar específico de protección de la información y pueden tener cualquier otro estándar para la administración general de riesgos en toda la empresa. Se precisa que, la evaluación y la mitigación de riesgos se han alineado con la norma ISO 31000, por lo que no es necesario implementar ambos en una empresa solo para la SI. La normativa ISO 27001:2005 utilizó un prototipo PDCA en la aplicación de SGSI. Este modelo comienza con la planificación de ISMS, luego pasa a la implementación de ISMS, seguido de la verificación de su efectividad y, por último, las mejoras basadas en la verificación. Sin embargo, ISO 27001:2013 no se basa en ningún prototipo específico, sino que aboga por el uso de mejoras continuas. Es importante tener en cuenta que este estándar proporciona un entorno que se puede utilizar a alto nivel. Carece de detalles a nivel operativo. Tampoco aprovisiona una guía secuencial para la evaluación de riesgos de los SI, pero la empresa puede usarla como guía para el entorno de evaluación de riesgos de nivel operativo correcto. En la inspección de la norma ISO 27001, se hizo un esfuerzo por desarrollar una estructura estandarizada para las aplicaciones informáticas para

que el núcleo de esta pueda aplicarse en cualquier contexto empresarial (Barafort, 2016)

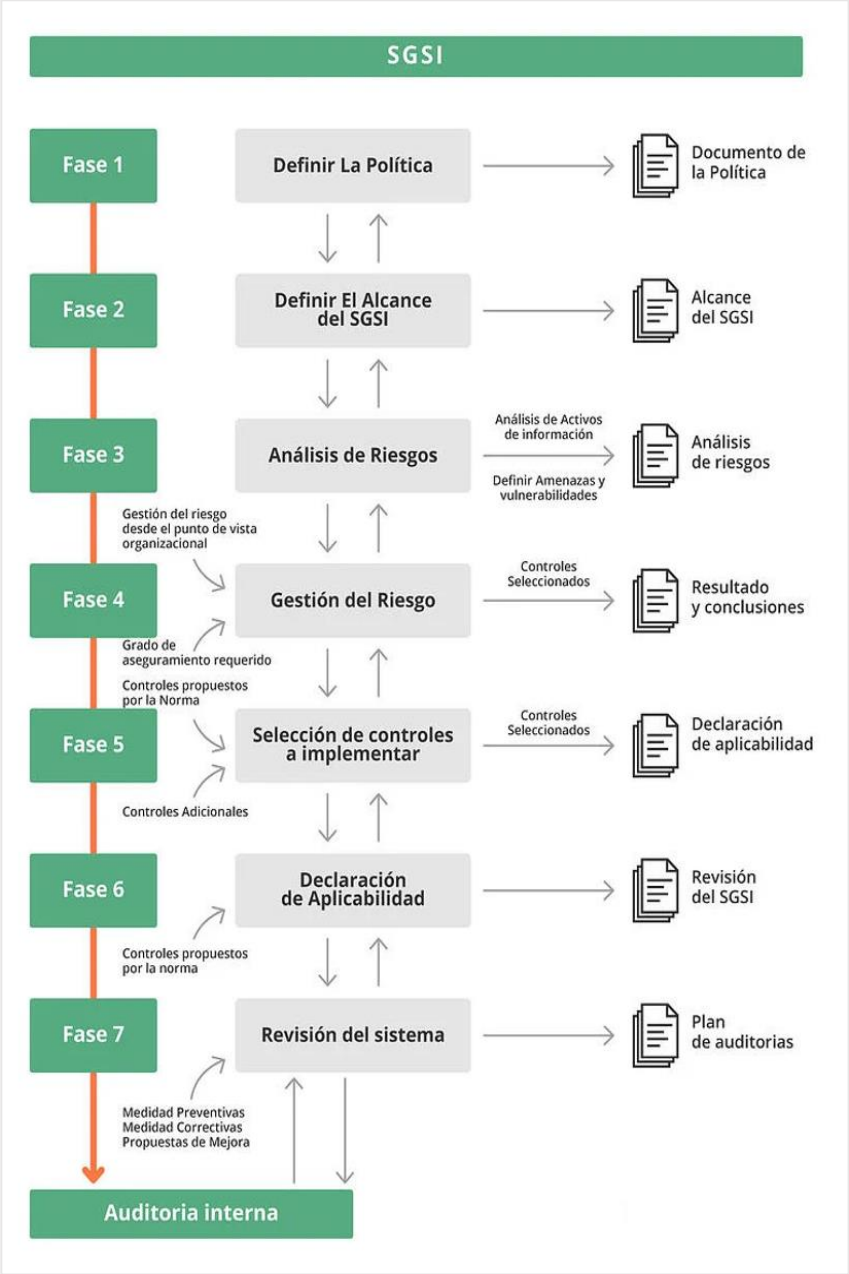


Figura 2. Vista general de un SGSI) implementado bajo ISO 27001. Fuente: Pirani (2018)

1.5.1.2 ISO 27002.

Este estándar ofrece detalles para la ejecución de los controles presentados en ISO 27001. El nombre de control utilizado en este estándar es el mismo que se usa en el Anexo de ISO 27001. No es un estándar de administración, por lo que no hay certificación para eso. (ISO 27002, 2013).

ISO 27005:2011 ofrece soporte al concepto general de SI, definido en ISO 27001 y la implementación de la misma. Requiere conocimiento de ISO 27001 & 27002 para su implementación y aplicable a cualquier institución (27005, 2011).

Su objetivo era cerrar las brechas entre ISO 27001 y 27002. Sin embargo, no especifica ni respalda ningún mecanismo de administración de riesgos para la aplicación. Este estándar puede considerarse, dedicado para la invulnerabilidad de la información. Los primordiales pasos iterativos involucrados en este estándar son el establecimiento del contexto, la categorización cualitativa y cuantitativa del riesgo, la disminución del riesgo y la interrelación con monitoreo constante. (ISO 27002, 2013).

1.5.2 ISO 31000.

Proporciona una visión colectiva y sistemática de los riesgos diversificados de la empresa repartidos entre varios departamentos de una empresa (Lalonde, 2012). Describe el marco de gerencia de riesgos, los principios y los procesos de gestión (ISO 31000, 2009). Independientemente de su sector, ya sea informáticas o no, se puede utilizar con todo tipo de aplicaciones. No se usa para certificaciones, pero brinda orientación para auditorías y se puede usar para comparar varios estándares de gerencia de riesgos y en caso de organizaciones, determinar su nivel de madurez ligada a manejo de riesgos. Se enfoca en la documentación y alienta a las empresas a ejecutar un marco de tratamiento de riesgos con el objetivo de integrar las metas comerciales de la empresa, los procesos comerciales, la cultura y las políticas de seguridad (Mesquida, 2016). Pero no proporciona un mecanismo para integrarlos. es difícil para aquellas empresas que carecen o tienen una experiencia inadecuada en

gestión de riesgos, lo que es especialmente cierto para las organizaciones pequeñas (Boiral, 2012)

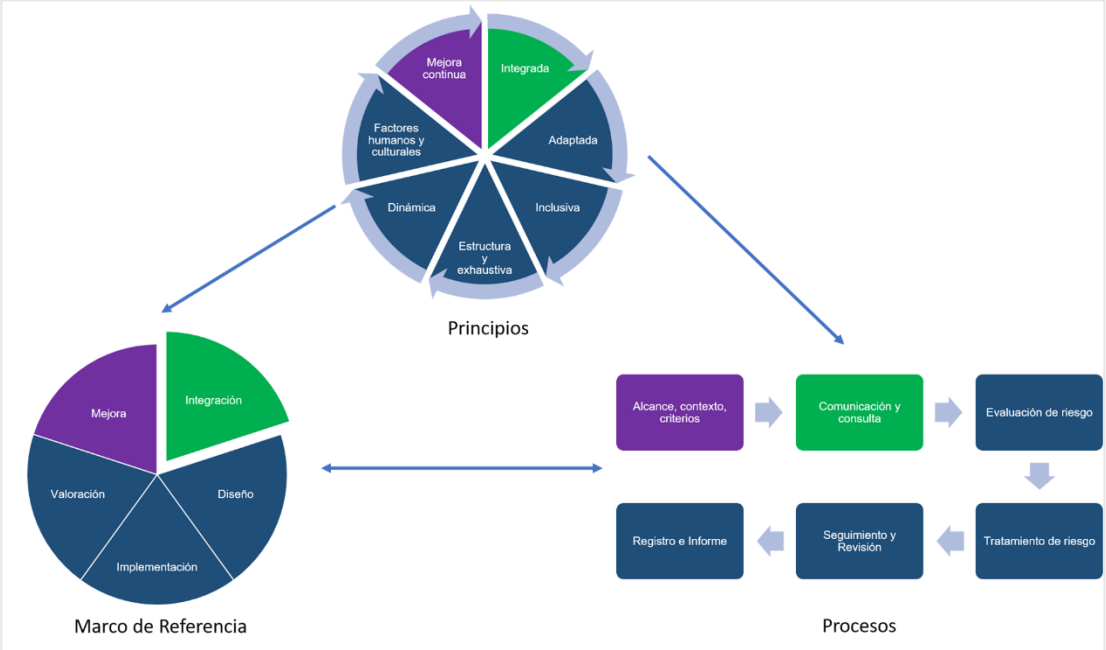


Figura 3. Marco de referencia, principio y proceso de ISO 31000. Adaptado de: ISO (2018)

1.5.3 COBIT 5

Es un marco para que las empresas mejoren su gobierno y obtengan lo mejor de su tecnología de la información mediante la optimización de los riesgos involucrados y los procesos comerciales. COBIT 5 no solo reestructuró COBIT 4.1 sino que también integró el marco de TI de riesgos y Val IT 2.0 (ISACA, 2012). Esta integración permite que COBIT 5 proporcione un grupo de controles, para gobernar y gestionar los riesgos de TI. Sincroniza los propósitos de TI con las finalidades generales de la entidad, garantizando que los objetivos empresariales se cumplen cuando se alcanzan estos objetivos de TI. (De Haes y Huygh, 2016).

COBIT 5 se desarrolla entorno a cinco creencias principales que satisfacen las necesidades de los stakeholders, cubren la empresa completa, la aplicación de un marco integral único, un enfoque universal y la separación entre las áreas de gestión y gobierno. (Debreceny, 2013)

Estas dos áreas se dividen en 5 dominios y 37 procesos para controlar y garantizar la SI. Los objetivos de TI de COBIT 5, se focalizan primero en la evaluación de riesgos. (Tsai, 2015). La importante contribución de COBIT es la integración de personas, procesos y tecnología de una empresa. La interacción entre personas, proceso y tecnología en la Figura 5.

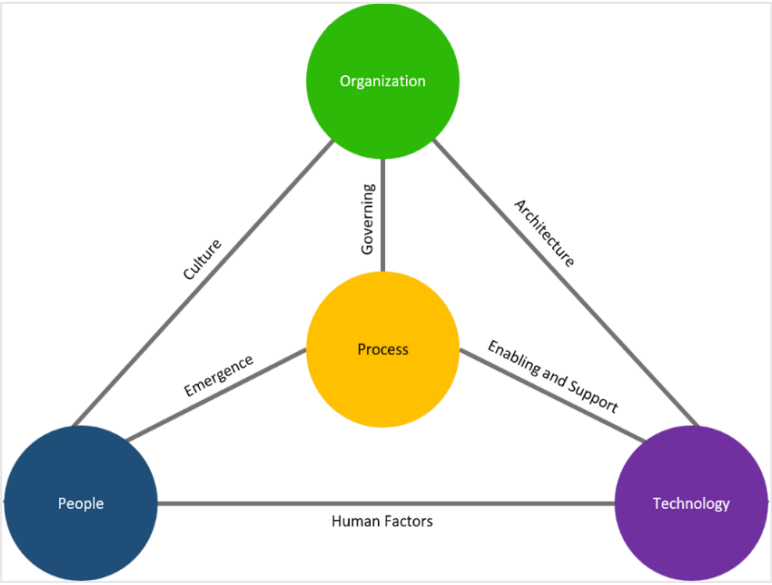


Figura 4. Personas, Proceso y Tecnología. Tomado de: ISACA *(2012)*

1.5.4 ITIL

Es un marco que proporciona un grupo de principios para la administración de prestación de servicios informáticos que hace un esfuerzo por alinear estos servicios con los objetivos comerciales. Considera como servicio cualquier acción realizada por las tecnologías de la información si tiene algún valor para el negocio o sus clientes. ITIL tiene 8 disciplinas, a saber: gestión de infraestructura de TI, aplicaciones, prestación de servicios, soporte de servicios, software y seguridad, implementación de gestión de servicios e implementación de pequeñas empresas. Varios marcos como el contexto de transacciones de Microsoft (MOF) y el marco para el soporte técnico de TIC (FITS) se basan en ITIL. (Marrone & Gacenga, 2015). Recientemente, la implementación de ITIL por parte de las empresas ha disminuido debido a problemas en su integración con los últimos planes de TI corporativos y los costos de aplicación involucrados. (Miller, 2013)

ITIL: 2007 estaba más enfocado hacia el nivel de gestión y operativo, pero ITIL: 2011 ha cambiado su enfoque hacia el nivel de gobierno y estratégico. (De Haes, 2016)

Se destaca aquí que no proporciona un entorno de administración de riesgos de TI, sino que madura la infraestructura de TI de una empresa como un marco de gobierno al tratar incidentes y respuestas. Por lo tanto, los riesgos de TI se atienden hasta cierto punto. (Brewster, 2012); también proporciona la libertad a una empresa para su implementación. Puede implementarse en fases o partes, pero es difícil asegurar el cumplimiento completo de ITIL. (Cots, 2014)

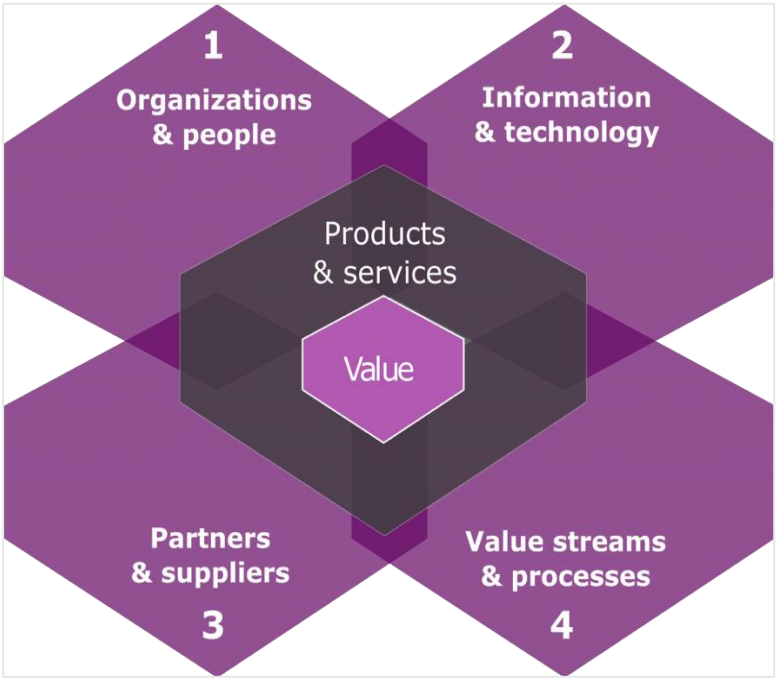


Figura 5. Gestión de servicios ITIL V4 y sus dimensiones. Tomado de: ADEK (2020)

1.5.5 Series NIST 800

Es un recurso conveniente que se puede utilizar para la administración de peligros de aplicaciones informáticas de la empresa. Proporciona orientación a nivel de aplicación para la administración de aplicaciones de información, cuestiones técnicas y de implementación, incluidos los requerimientos mínimos

para proporcionar una seguridad de la información aceptable con un presupuesto limitado para pequeñas empresas. (Lepofsky, 2014). Las publicaciones mencionadas a continuación se pueden utilizar como guía para la evaluación de riesgos para lograr una SI satisfactoria

a) NIST SP: 800-26 brinda pautas para la autoevaluación de la seguridad de TI.
b) NIST SP: 800-30 brinda pautas para la gerencia de peligros TI y evaluación de peligros TI.
c) NIST SP: 800-39 se ocupa del peligro de protección de la información - SI.

SP 800-30 y 800-39 son más específicos para la administración y valoración de riesgos. Entregan un mecanismo integral para la valoración de riesgos con ejemplos de ayuda para la aplicación. El mecanismo funciona teniendo en cuenta la categorización de la información, puesta en operación de controles, evaluación de controles y seguimiento.

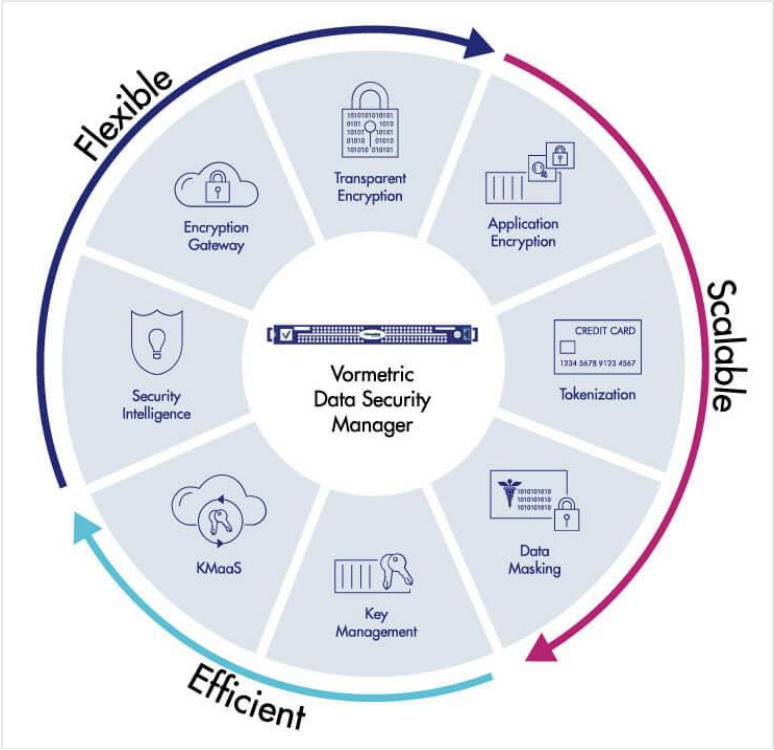


Figura 6. Catálogo de controles de NIST 800-53. Fuente: Thales G. (2020)

1.5.6 Metodologías de gestión de riesgos de TI.

A) OCTAVE:

La valoración de amenazas, activos y vulnerabilidades operativamente críticas, es un método detallado para acceder a la inseguridad de los datos en una entidad y agiliza el proceso de evaluación de riesgos. Tal herramienta fue propuesta por el IISUCM, conocido como Instituto de Ingeniería de Software de la Universidad Carnegie Mellon. Fue diseñado también con la finalidad de optimizar resultados en términos de presupuesto, recursos y tiempo en pequeñas o medianas empresas.

Utiliza un enfoque de evaluación cualitativo, y atiende los aspectos técnicos como no técnicos, proporcionando información clave que puede ser personalizada según los procesos del negocio establecidos por la institución.

Asimismo, cuenta con 02 versiones: Octave S y Octave Allegro, las cuáles se aplican según la libertad de expansión de los recursos de la empresa. Las PYMES pueden usar la primera, mientras que las grandes organizaciones deben utilizar la segunda. Asimismo, también es aplicable para computación en la nube.

Tres pasos controlan la operación de diagnóstico de peligros: a) Determinación de los activos críticos, b) Reconocimiento de inseguridades y c) planteamiento de controles de seguridad. Esta metodología ofrece plantillas, hojas de trabajo, hojas de cálculo, y procesos determinados para evaluar los riesgos, por lo que se convierte en una opción completa cuando se trata de realizar ER.

B) ERM- COSO

Conocido también, como marco de gestión de riesgos empresariales. Este framework proporciona métodos para desarrollar y evaluar los riesgos de la empresa, identificando brechas para a posteriori, implementar planes de resguardo. Cuenta con 03 dimensiones, la primera tiene 04 objetivos de gestión

de riesgos, la segunda tiene 04 a nivel de entidad, y la tercera 08 elementos de riesgo. Cabe mencionar, que este tipo de herramienta no se centra sólo en las TI, sino que orienta su método de evaluación hacia toda la empresa. Está catalogado para gestionar riesgos no técnicos.

C) COBRA.

El análisis de riesgos bifuncional, consultivo y objetivo, conocido como COBRA, fue desarrollado por la compañía C&A Systems Security. Utiliza una forma cualitativa para acceder al riesgo mediante el uso de varios formatos de cuestionario (tanto automatizados como manuales), encuestas y entrevistas donde se recogen los procesos empresariales. Una vez, realizado este análisis, se generan reportes o informes para la alta gerencia para evaluar los riesgos. Es importante mencionar que, se rige bajo las directrices de la ISO 17799.

D) MAGERIT.

El método MAGERIT de análisis y gestión de riesgos ha sido desarrollado por el Consejo Superior de Administración Electrónica de España. A la hora de tomar decisiones, los órganos de gobierno pueden tener en cuenta los riesgos asociados al uso de las tecnologías de la información, aplicando el Proceso de Gestión de Riesgos. Su proceso incluye:

- Reconocer los activos más influyentes para la compañía, su interacción y su valor, en la razón que afectaría su deterioro.
- Determinar las amenazas que están comprometidos los activos.
- Establecer medidas preventivas y que tan eficaces son.
- Medir el impacto, es decir cuánto afecta la amenaza al activo.
- Calcule el riesgo sopesando el impacto en relación con la probabilidad de que se materialice un peligro.
- Determinar las necesidades de protección del sistema, establecer salvaguardias y, a continuación, evaluar si el sistema de protección de que disponemos satisface nuestros requisitos.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

2.1.1. Tipo de Investigación.

El proyecto es cuantitativo, ya que se necesitan mediciones basadas en indicadores numéricos, y los resultados se revisarán para mostrar cuánto se ha mejorado. indicadores numéricos que se examinarán utilizando la norma ISO 27001:2017, implementada en el IESTP Utcubamba, para demostrar el grado de mejora en el proceso de gestión de riesgos de TI. El nivel de coherencia y pertinencia, así como la aceptación del modelo son los dos valores del modelo que estos datos pretenden cuantificar.

2.1.2. Diseño de Investigación.

El diseño del proyecto es en cierto modo experimental. Se mejorará efectivamente el procedimiento de gestión de riesgos informáticos del IESTP Utcubamba operando la variable independiente. La implementación del IESTP Utcubamba se apegará a los estándares establecidos en la norma 27001:2017. El esquema que sigue ilustra tal circunstancia. el plan que sigue:

GE:	O_1	x	O_2
GC:	O_3	x	O_4

Donde:

GE: Grupo experimental (Caso de estudio seleccionado)

GC: Grupo de control (Caso de estudio seleccionado)

O_1 y O_3: Realidad de la institución antes de la aplicación del modelo.

O_2 y O_4: Realidad de la institución después de la aplicación del modelo.

X: Mediante Implementación del estándar ISO/IEC 27001:2017

2.2. Variables, Operacionalización.

Variable Independiente: Mediante Implementación del estándar ISO/IEC 27001:2017

Variable Dependiente: Gestión de riesgos de tecnologías de información

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
VARIABLE INDEPENDIENTE		Tiempo promedio de implementación por fase	$\boldsymbol{TIF} = \frac{\sum (TTA)}{NF}$	T: Observación I: Ficha de observación
Mediante Implementación del estándar ISO/IEC 27001:2017	Evaluación del modelo	Nivel de intencionalidad	$\boldsymbol{NIN} = \frac{CE_1 + CE_2 + CE_3}{NE}$	T: Juicio de Expertos. I: Ficha de Expertos
		Nivel de Consistencia	$\boldsymbol{NCO} = \frac{CE_1 + CE_2 + CE_3}{NE}$	
		Nivel de Pertinencia	$\boldsymbol{NPE} = \frac{CE_1 + CE_2 + CE_3}{NE}$	

VARIABLE DEPENDIENTE		Nivel de impacto del activo	$\boldsymbol{NIA} = \frac{NCA\ x\ GA}{TA}$	
Gestión de riesgos de tecnologías de información	Evaluación de riesgos internos	Nivel de alcance de procesos	$\boldsymbol{NAP} = \frac{\sum TPGR}{\sum\ TPE}$	T: Documentación. I: Matriz de riesgos
		Media de riesgo por activo	$\boldsymbol{MRA} = \frac{TRI}{CA}$	
		Efectividad de los controles (R)	$\boldsymbol{EC} = \left(1 - \frac{COIP}{CON}\right) * 100$	T: Observación. I: Ficha de Observación

2.3. Población de estudio, muestra, muestreo y criterios de selección

En esta investigación, la población y muestra son iguales, corresponden al caso de estudio seleccionado, el Instituto de Educación Pública Superior Tecnológico Utcubamba. Para realizar dicha elección respecto esta organización TI, se efectuó bajo 03 criterios: a) manejo de tecnología, b) gestión de activos, y c) acceso a la información. El modelo que se desarrollará se aplicará en el IESTP Utcubamba, del cual ya se tiene previo consentimiento, mediante una carta de autorización para confirmar el proceso de recopilación de datos, que evidencien la validez de la investigación.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

Observación: Para estimar el tiempo promedio de implementación por fase, se llevará a cabo esta técnica, dado que, se requiere estudiar los tiempos trabajo, siguiendo el orden de actividades y realizando notaciones sobre tales situaciones. Asimismo, servirá para medir la capacidad de los controles una vez ya implementados, cotejándolo con los ya establecidos.

Juicio de expertos: Para validar los niveles de intencionalidad según el grado de idoneidad del modelo: consistencia según aportes teórico-científico y pertinencia según adecuación de la propuesta; será importante contar con esta herramienta para evidenciar mayor fiabilidad, y validez en la evaluación.

Documentación: Para conocer el nivel de impacto del activo dentro de la institución, el nivel alcance de procesos, o sea delimitar aquellos procesos que sólo participan en la administración TI, para ello se deberá contar con un mapa de procesos de la entidad; así poder diferenciar los relevantes de los secundarios. La media de riesgo por activo que sería el total de riesgos identificados en TI sobre la cantidad de activos de TI.

2.5. Procedimiento de análisis de datos.

Las fórmulas relacionadas con los indicadores anteriormente establecidos, que se efectuarán en el presente proyecto, se describen a continuación:

- Tiempo promedio de implementación por fase: Cuyo indicador nos permitirá estimar mediante observación, el tiempo de duración que conllevará la aplicación del modelo propuesto en un ITP peruano.

$$\boldsymbol{TIF} = \frac{\sum (TTA)}{NF}$$

Donde:
TIF: Tiempo promedio de implementación por fase.
TTA: Sumatoria total de tiempo transcurrido por actividad de una determinada fase, considerando la hora inicial y la hora final de la ejecución de dicha tarea.
NF: Número total de fases implementadas basada ISO 27001:2017.

- Nivel de Intencionalidad: Cuyo indicador nos permitirá valorar mediante juicio de expertos, si el modelo propuesto es idóneo para hacer más competente el proceso de administración de riesgos TI en un ITP peruano.

$$\boldsymbol{NIN} = \frac{CE_1 + CE_2 + CE_3}{NE}$$

Donde:
NIN: Nivel de intencionalidad.
CE1: Calificación experto 01
CE2: Calificación experto 02
CE3: Calificación experto 03
NE: Número total de expertos que calificaron el modelo bajo criterio de intencionalidad.

- Nivel de Consistencia: Cuyo indicador nos permitirá valorar mediante juicio de expertos, si el modelo presentado para perfeccionar el proceso de

administración de riesgos TI en un ITP peruano, está basado en aspectos teóricos científicos.

$$\boldsymbol{NCO} = \frac{CE_1 + CE_2 + CE_3}{NE}$$

Donde:

NCO: Nivel de consistencia.

CE1: Calificación experto 01

CE2: Calificación experto 02

CE3: Calificación experto 03

NE: Número total de expertos que calificaron el modelo bajo criterio de consistencia.

- Nivel de Pertinencia: Cuyo indicador nos permitirá valorar mediante juicio de expertos, si el modelo presentado para perfeccionar el proceso de administración de riesgos TI en un ITP peruano, es adecuado y útil para la investigación.

$$\boldsymbol{NPE} = \frac{CE_1 + CE_2 + CE_3}{NE}$$

Donde:

NPE: Nivel de pertinencia.

CE1: Calificación experto 01

CE2: Calificación experto 02

CE3: Calificación experto 03

NE: Número total de expertos que calificaron el modelo bajo el criterio de pertinencia.

- Nivel de Impacto del Activo: Cuyo indicador se calcula mediante la matriz de riesgos, y es igual al grado de clasificación del activo, multiplicado por el grado de amenaza del activo, cuyo resultado es dividido sobre el total de activos identificados dentro de un ITP peruano.

$$\boldsymbol{NIA} = \frac{NCA\ x\ GA}{TA}$$

Donde:

NIA: Nivel de impacto del activo.

NCA: Nivel de clasificación del activo.

GA: Grado de amenaza del activo.

TA: Total de activos identificados.

- Nivel de alcance de procesos: Cuyo indicador se calcula mediante la matriz de riesgos, y representa la sumatoria total de procesos incluidos dentro de la gestión de riesgos TI de un ITP peruano, divididos sobre la sumatoria total de procesos de todas las áreas de dicha institución.

$$\boldsymbol{NAP} = \frac{\sum TPGR}{\sum TPE}$$

Donde:

NAP: Nivel de alcance de procesos.

TPGR: Sumatoria total de procesos incluidos dentro de la gestión de riesgos pertenecientes al ITP peruano.

TPE: Sumatoria total de procesos pertenecientes al ITP peruano.

- Media de riesgo por activo

$$MRA = \frac{TRI}{CA}$$

Donde:

MRA: Media de riesgo por activo.

TRI: Total, de riesgos identificados en TI

CA: Cantidad de activos de información en TI

- Efectividad de los controles:

$$\boldsymbol{EC} = \left(1 - \frac{COIP}{CON}\right) * 100$$

Donde:

EC: Efectividad de los controles

COIP: Controles implementados en el ITP peruano antes del modelo basado en el estándar 27001:2017

CON: Controles implementados en el ITP peruano después del modelo basado en el estándar 27001:2017.

Importante las siglas, ITP, representan el caso estudio (Instituto Tecnológico Publico Peruano, en esta ocasión refiere al IESTP Utcubamba ubicado en Bagua Grande).

2.6. Criterios éticos.

Confidencialidad.

Los datos que proporcionará el Instituto de Educación Público Superior Tecnológico Utcubamba, se adquirirán de manera formal y legal, siguiendo el procedimiento establecido para políticas internas de custodia de datos y suministro de información privada de TI. Asimismo, se respetará lo instaurado por la Ley 29733, que indica la salvaguardar los datos personales.

Derechos de Autor.

La bibliografía se citará siguiendo los procedimientos establecidos por el ente universitario donde se está realizando el presente proyecto, con el fin de no incidir en la adulteración de los datos recolectados.

Búsqueda del bien.

Se tendrá sumo cuidado de no tergiversar ni manipular la información obtenida, para evidenciar resultados en base a datos reales y veraces, generando así un ambiente de seguridad.

Conformidad.

El proyecto irá alineado bajo la legislación del Colegio de Ingenieros del Perú, que instaura internamente en sus políticas, la ética profesional aplicada a dicha ciencia y en caso, de incumplimiento de objetividad, atenerse a las penalidades.

2.7. Criterios de Rigor Científico.

Consistencia.

La investigación, en el acápite de resultados deberá evidenciar datos concretos, reales y medibles dentro de lo que se plantea en las métricas establecidas. Permitiendo así, adaptar dicha información a la realidad y contexto del Instituto de Educación Superior Tecnológico Público Utcubamba.

Originalidad.

Cada componente, fase y/o actividad, del modelo desarrollado para mejorar los procesos de administración de riesgos de TI del IESTP Utcubamba, deberán ser aplicados siguiendo la documentación oficial y actualizada que presenta ISO 27001:2017, buscando así alinearlos al contexto, objetivos y políticas de la organización, llámese también, caso de estudio.

III. RESULTADOS Y DISCUSIÓN.

3.1. Resultados

Resultados de la Evaluación Global del Modelo Propuesto

CRITERIO / EXPERTO	CLARIDAD	OBJETIVIDAD	ACTUALIDAD	ORGANIZACIÓN	SUFICIENCIA	INTENCIONALIDAD	CONSISTENCIA	COHERENCIA	METODOLOGÌA	PERTINENCIA
Experto 01	85	85	85	85	85	85	85	85	85	85
Experto 02	90	90	90	90	90	90	90	90	90	90
Experto 03	80	80	80	80	80	80	80	80	80	80

Promedio de Validación del Modelo

Experto	Promedio de Ponderación	Aceptación del Modelo
Experto 01	85,00	
Experto 02	90,00	85,00
Experto 03	80,00	

3.2 Discusión

De acuerdo con lo planteado en la fase A1, utilizando las fichas de captura de datos establecidas por la metodología Magerit, se identificaron y valoraron 114 activos (bases de datos, sistemas, usuarios, equipos informáticos y documentos físicos entre otros), de los cuales 29 se clasificaron como críticos según su disponibilidad, confidencialidad e integridad, sumando como una de sus variables de criticidad la dependencia o no con otros activos del instituto.

Acto seguido, y con base en el inventario de activos se reconocieron 56 amenazas, de las cuales 48% fueron clasificadas como críticas. Las amenazas se clasificaron como revelación, modificación, pérdida o destrucción, o interrupción del servicio. (Ver detalles Anexo 06).

Finalizada la etapa anterior, se tiene claro la magnitud que perjudica a los activos, las amenazas y el riesgo. Denotando los vacíos de controles para ciertas amenazas. Debido a esto, se plantearon controles basándose en el tratamiento de riesgo determinado en la Tabla 10, que ayudarán a mitigar las diferentes vulnerabilidades, ante las amenazas del entorno institucional.

3.3 Aporte de la investigación (opcional).

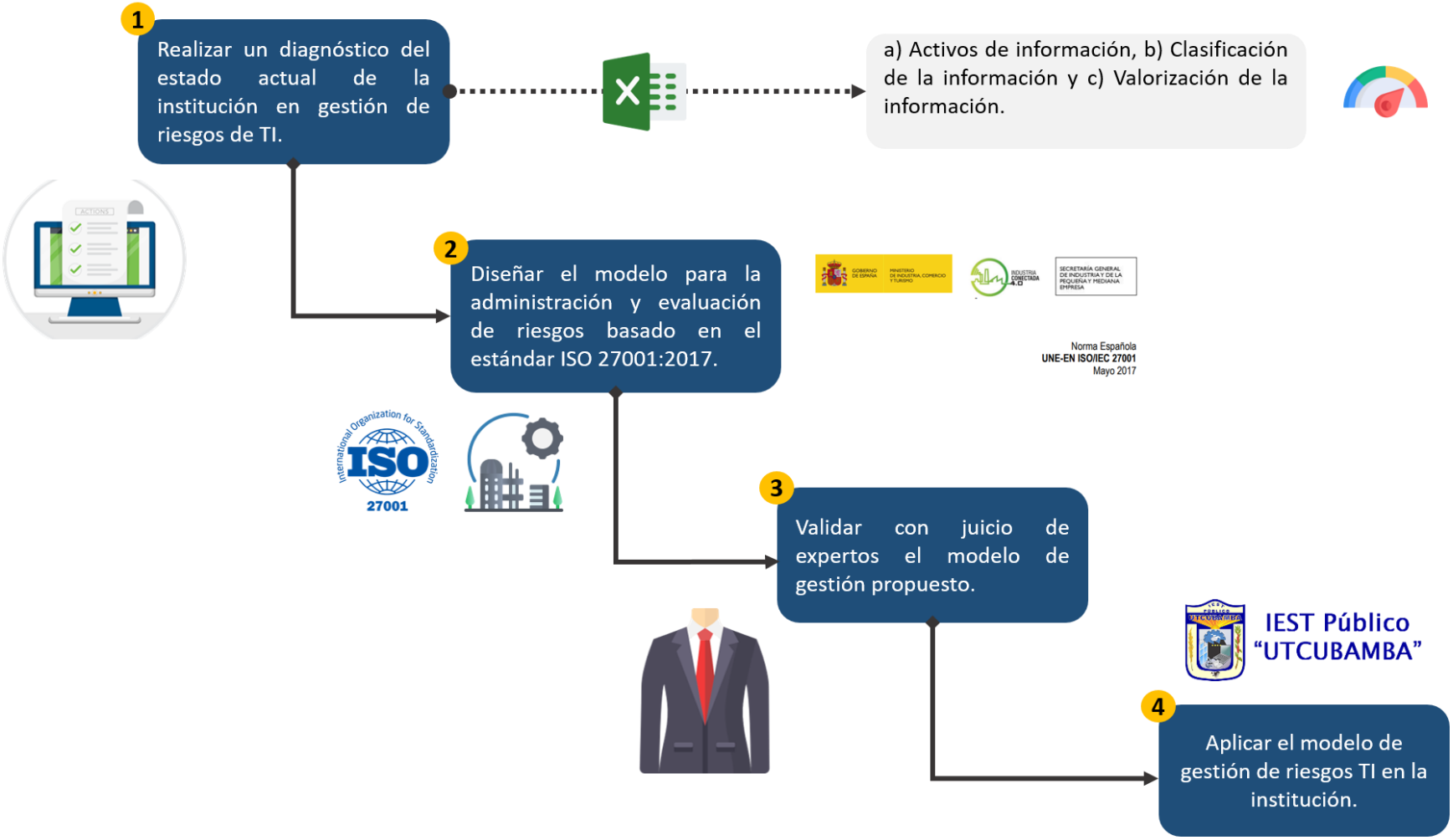


Figura 7. Gráfica del método propuesto. Fuente: Producción personal.

1. Realizar un diagnóstico del aspecto actual de la institución en gestión de riesgos de TI.

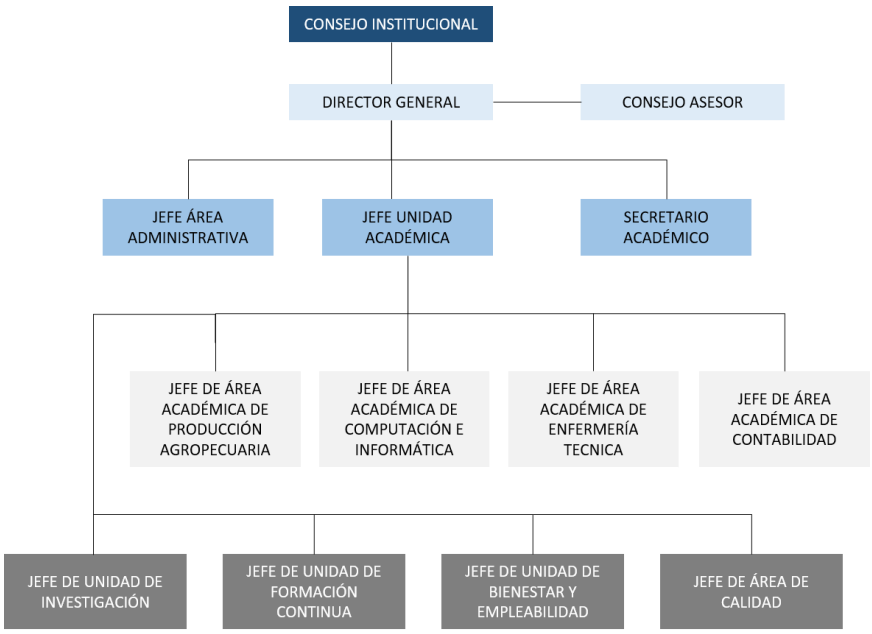
1.1 Analizar datos de la institución peruana

- Razón social: Instituto de Educación Público Superior Tecnológico Utcubamba.
- Geolocalización: Jr. Las Delicias Nro. 380 Sector Vislot Amazonas, Utcubamba.
- Director general de la Institución: Víctor Manuel Feria Puelles – DNI 33640105.
- Sector económico: Enseñanza superior, centro de educación y cultura.
- Email de contacto: istputcubamba@hotmail.com
- RUC del IESTP: 20437454419
- Valores institucionales: Responsabilidad, cooperación, democracia, honestidad, y emprendedorismo.
- Visión: Ser una organización que desarrolla líderes, emprendedores e innovadores adaptables al cambio.
- Misión: Somos una comunidad académica que ofrece instrucción de primera categoría en tecnología, al tiempo que mantiene fuertes vínculos con el entorno.
- Breve historia: Se instauró en 1987, el 28 de agosto, a través del decreto N° 626-87-ED, como respuesta a las carencias de educación superior que tenían los jóvenes que egresaban de los colegios de educación secundaria de las provincias aledañas a Utcubamba, quienes no tenían los suficientes medios económicos para salir a otros lugares donde existan instituciones que brinden el servicio de enseñanza superior; así como también con la intencionalidad de contribuir al progreso étnico de la provincia de Utcubamba, y el crecimiento de la región Amazonas.
- Programas de estudio actuales: Computación e Informática, Contabilidad, Producción agropecuaria, y Enfermería técnica.
- Aspectos estratégicos: Gestión estratégica, Formación integral, Desarrollo Tecnológico e Innovación, Soporte Institucional e Infraestructura, Vinculación con el entorno y Perfil del egreso.
- Procesos de Soporte: Servicios de Bienestar, Gestión de RRHH, y Gestión de Infraestructura, Equipamiento y Soporte TI.

1.2 Describir el proceso TI actual

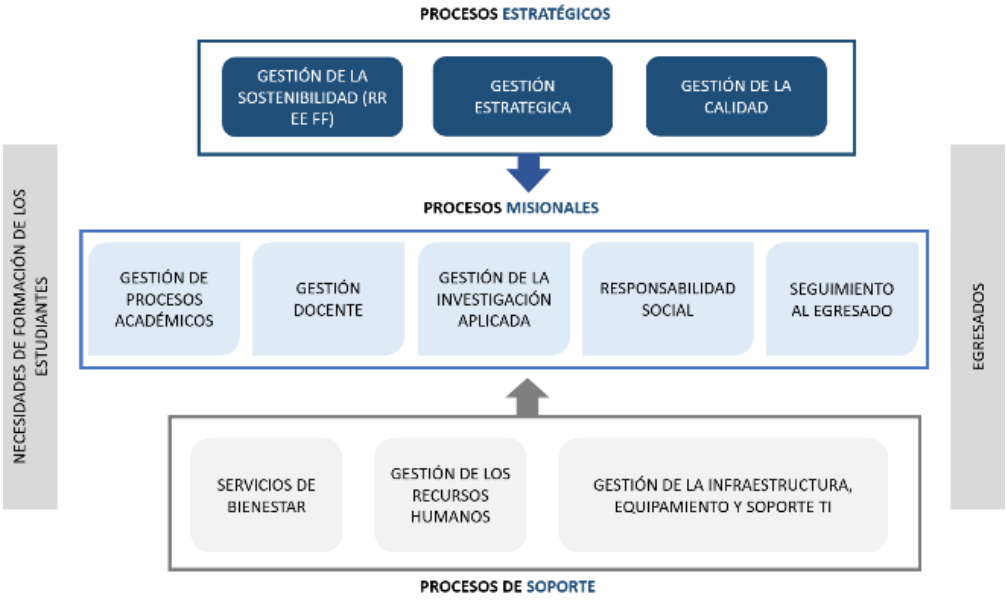
Antes de empezar con esta actividad, se consideró importante conocer la estructura organizacional y el mapa de procesos que sostiene el IESTP Utcubamba para mayor alcance y determinar quiénes están involucrados en el aspecto TI.

Organigrama del IESTP



Fuente: Elaboración del IESTP

Mapa Procesos IESTP



Fuente: Elaboración propia

Proceso de Gestión de la Infraestructura, Equipamiento y Soporte TI:

El IESTP Utcubamba, cuenta con 02 sistemas de información definidos, el primero es el Sistema Q10 que se le contrató a una empresa colombiana, cuyo uso está ligado a la gestión administrativa, académica y de educación virtual; y el segundo, el Sistema Registra para la gestión del proceso de admisión, matrículas y calificación de estudiante proporcionado por MINEDU. Debido al escaso presupuesto y a la carencia de recursos, actualmente no existe un sistema integrado de diligencia de la protección de la información. Asimismo, los servidores están almacenados en proveedores de terceros, es decir existe una tercerización de los servicios TI. En resumen, el proceso TI que se lleva a cabo, está relacionado al uso y apoyo de los sistemas de información mencionados, configuración de ingreso para docentes-estudiantes, y mantenimiento de las herramientas, cableado del laboratorio de cómputo-ensamblaje-redes.

El responsable o jefe del área TI, es el Dr. Ing. Quiroga Honorio Carlos Ramos.

1.3 Elaborar un inventario de activos de información

Antes de iniciar el proceso de este acápite, se requirió en varias oportunidades visitar al IESTP Utcubamba, dado que, debido a trámites y asuntos internos, que estaba atravesando la institución se dificultaba conseguir información. Asimismo, el área TI indicó que carecían de información documentada en esos momentos, por lo que todo lo descrito a continuación se recopiló en reuniones presenciales con la colaboración de 02 ingenieros del área. Para ello, se emplearon varias matrices, en primer lugar, se definieron los tipos de activos involucrados, para clasificar según su tipo (software, información, hardware, servicios del sistema, red de comunicación, y equipo auxiliar).

Tabla 1 Tipos de Activos

Código	Tipo	Descripción
SW	Software	Aplicaciones escritorio o web. Sistema de Gestión de Base Datos, Uso de ofimática (Word, Excel, M. Team, Power Point, etc.), Uso de Sistema Operativo (Windows, Linux, IOS)
HW	Hardware	Laptops, tablets, impresoras, módems, switches, routers, teléfonos IP, cámaras de vigilancia, etc.
IN	Información	Archivos, documentación del sistema, bases datos, material de capacitación, manuales, procedimientos de contingencia, etc.
RC	Red de Comunicación	Red telefónica, internet, wifi, telefonía móvil alámbrica, red local
EA	Equipo auxiliar	Mobiliario, carpetas, mesas, escritorios, generador eléctrico, caja fuerte, entre otros.
SS	Servicios del Sistema	Hosting, dominio, accesos remotos, almacenamiento de ficheros

Fuente: Producción personal.

Asimismo, se tomó en cuenta, el nivel de confidencialidad (no clasificado, confidencial de empleados, confidencial de institución, confidencial del estudiante), nivel de criticidad (muy alto, alto, medio, bajo, muy bajo) y el tipo de ubicación (física, lógica o física-lógica), lo cual se muestra:

Tabla 2 Nivel de Confidencialidad

Código	Nivel	Descripción
NC	No Clasificado	Información que se puede ser conocido, sin que implique resultados adversos para la institución, como la información que es de saber público.
CT	Confidencial del trabajador	Incluye datos como, registros médicos, salarios, entre otros.

CI	Confidencial de institución	Contratos, códigos fuente, password para sistemas críticos de TI, contratos de clientes, cuentas, etc.
CS	Confidencial del estudiante	Incluye datos de identificación: como nombre, dirección, password de acceso al sistema, histórico de planes curriculares, información sensible interna, etc.

Fuente: Producción personal.

Tabla 3 Nivel de Criticidad

Código	Nivel	Descripción
MA	Muy Alto	El activo es primordial para el proceso del negocio. Si se deja de operar, el riesgo de imagen reputacional y la seguridad se ven perjudicados.
AL	Alto	El activo es necesario para el proceso del negocio. Puede no estar utilizable el activo o el proceso, pero solo por un breve tiempo. Puede originar pérdida reputacional.
ME	Medio	El activo es relevante para el proceso del negocio. Su ausencia no interrumpe proceso, así como menos aún la continuidad de negocio. El riesgo es operativo.
BA	Bajo	El activo tiene poca relevancia en el proceso. La disponibilidad no es crítica, podría ser escaso y no perjudica a la calidad y la prolongación del proceso.
MB	Muy Bajo	En el proceso, el activo tiene relativamente poca relevancia. No requiere salvaguardas ni cuidados particulares.

Fuente: Producción personal.

Tabla 4 Tipo de Ubicación de Activo

Código	Tipo	Descripción
FI	Física	Medio de almacenamiento físico.
LG	Lógica	Medio de almacenamiento electrónico.

FL	Fisica-Logica	Medio de almacenamiento físico- electrónico.

Fuente: Producción personal.

Consecutivamente a ello, se realizó el inventario de activos, según lo estipulado para obtener la ponderación en cuanto a diagnóstico preliminar. Los ítems que se tomaron en cuenta como inventario fueron (código de registro, nombre activo, descripción, sistemas implicado, tipo activo, tipo ubicación, nivel de confidencialidad, propietario de activo).

Tabla 5 Catalogo de ítems para clasificar inventario inicial

Ítem	**Descripción**
Código de registro	Identificador único de activos según la clasificación del activo y tipo del mismo.
Nombre Activo	Recurso del Instituto de Educación Superior Tecnológico Publico Utcubamba
Descripción	Determinar tipo, concepto o asignación del activo.
Sistema involucrado	Plataforma que gestiona el recurso que interviene como activo de información.
Tipo activo	Representa si es software, información, hardware, servicios del sistema, red de comunicación, o equipo auxiliar.
Tipo ubicación	Según el medio de almacenamiento físico o electrónico.
Nivel de confidencialidad	No Clasificado, Confidencial del trabajador, Confidencial de la institución, y Confidencial del estudiante.
Propietario de activo	El responsable del recurso o activo de información del IESTP Utcubamba.

Fuente: Producción personal.

Mediante la matriz que se presenta a continuación se detallaron los activos más importantes en aspectos de relevancia, tipo y clasificación, véase Tabla 6.

Tabla 6 Inventario de activos TI del Instituto de Educación Superior Tecnológico Público Utcubamba (Ver Anexo 06 – Detalles de Activos)

Código Registro	Nombre Activo	Descripción	Sistema	Tipo Activo	Tipo Ubicación	Nivel C.	Propietario Activo	Valorización		
								CO	IN	DI
HW01	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW02	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW03	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW04	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW05	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW06	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW07	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3

HW08	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW09	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW10	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW11	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW12	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW13	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW14	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW15	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW16	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW17	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3

HW18	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW19	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW20	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW21	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW22	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW23	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW24	PC LG	Asignada a LAB-PQ	Software Q10	Hardware	Física	C.I	Estudiante IESTP	2	4	3
HW25	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW26	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW27	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3

HW28	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW29	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW30	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW31	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW32	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW33	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW34	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW35	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW36	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW37	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3

HW38	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW39	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW40	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW41	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW42	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW43	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW44	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW45	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW46	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW47	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3

HW48	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW49	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW50	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW51	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW52	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW53	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW54	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW55	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW56	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW57	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3

HW58	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW59	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW60	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW61	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW62	PC DELL	Asignada a LAB-GR	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW63	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW64	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW65	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW66	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW67	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3

HW68	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW69	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW70	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW71	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW72	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW73	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW74	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW75	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3
HW76	PC HP	Asignada a LAB-COM	Software Q10	Hardware	Física	C.I	Estudiante IESTP	3	4	3

HW77	Laptop Compaq	Asignada al área de Dirección Académica	Software Registra y Q10	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	4	4	4
HW78	Impresora Epson L365	Asignada al área de Dirección Académica	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3
HW79	Impresora Epson L365	Asignada al área de Almacén	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3
HW80	Impresora Epson L575	Asignada al área de Secretaría Académica	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3
HW81	Impresora Epson L575	Asignada al área de Dirección General	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3

HW82	Impresora Epson L575	Asignada al área de Coordinación Contabilidad	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3
HW83	Impresora Epson L575	Asignada al área de Coordinación Enfermería Técnica	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3
HW84	Impresora Epson L575	Asignada al área de Coordinación Producción Agropecuaria	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3
HW85	Impresora Epson L575	Asignada al área de Coordinación APSTI	N/A	Hardware	Física	C.I	Ing. Rommel Montenegro Guerrero	3	3	3

HW86	Switch Integrado	Asignado al laboratorio de informática	N/A	Hardware	Física	C.I	Ing. Dennys Clever Parihauche Julcahuanga	5	4	4
HW87	Switch Integrado	Asignado al laboratorio de informática	N/A	Hardware	Física	C.I	Ing. Dennys Clever Parihauche Julcahuanga	5	4	4
HW88	Soplador para mantenimiento	Asignado al laboratorio de informática	N/A	Hardware	Física	C.I	Ing. Dennys Clever Parihauche Julcahuanga	3	3	3
HW89	Proyector Multimedia	Asignada al área de Contabilidad	N/A	Hardware	Física	C.I	Cpc. Carlos Sandoval Davila	4	4	4
HW90	Proyector Multimedia	Asignada a LAB-PQ	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW91	Proyector Multimedia	Asignada a LAB-GR	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4

HW92	Proyector Multimedia	Asignada a LAB-COM	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW93	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW94	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW95	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW96	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW97	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4

HW98	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW99	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
HW100	Proyector Multimedia	Aula	N/A	Hardware	Física	C.I	Estudiante IESTP	4	4	4
SW101	Sistema de Gestión Académica Q10	Plataforma de educación virtual del IESTP	N/A	Software	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	5	5	5
SW102	Microsoft Office	Suite Ofimática	N/A	Software	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	5	4	4
SW103	Sistema de	Servidor del Estado	N/A	Software	Lógica	C.I	Ing. Carlos Honorio	5	5	5

	Gestión Registra						Quiroga Ramos			
SW104	Antivirus ESET 32	Servidor local	N/A	Software	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	5	4	4
IN105	Contrato de prestación de servicios TI	Servidor local	N/A	Información	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4
IN106	Plan Operativo y Estratégico del IESTP	Servidor local	N/A	Información	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4
IN107	Política de uso	Servidor local	N/A	Información	Lógica	C.I	Ing. Carlos Honorio	4	4	4

	de plataforma estudiantil						Quiroga Ramos			
IN108	Política de uso de plataforma docente	Servidor local	N/A	Información	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4
RC109	Red Intercomunicador CLARO	Conexión CLARO local	N/A	Información	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4
RC110	Router Switch	Router Switch Integrado para optimizar red	N/A	Información	Físico	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4

RC111	Router Switch	Router Switch Integrado para optimizar red	N/A	Información	Físico	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4
RC112	Router Switch	Router Switch Integrado para optimizar red	N/A	Información	Físico	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4
RC113	Archivo de Selección de Personal Docente	Documento con información de las habilidades, experiencia y valores humanos	N/A	Información	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4

EA114	Estante de archivos de historial del estudiante	Protocolo de seguimiento al estudiante	N/A	Equipo auxiliar	Lógica	C.I	Ing. Carlos Honorio Quiroga Ramos	4	4	4

El siguiente paso, es realizar la valoración de los activos anteriormente detallados, para ello se utilizaron matrices de valorización, donde se asevera la interpretación según el nivel o grado.

Tabla 7 Valorización Activos TI - Confidencialidad

Valor Activo	Confidencialidad
5 - Muy Alto	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría perjudicialmente a la institución.
4 - Alto	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, pues su divulgación afectaría gravemente a la institución.
3 -Medio	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la institución.
2 - Bajo	La información asociada al activo es de uso interno y solo personal autorizado puede acceder a ella, pues su divulgación afectaría parcialmente a la institución.
1 - Muy Bajo	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la institución.

Fuente: Producción personal.

Tabla 8 Valorización Activos TI - Integridad

Valor Activo	Integridad
5 - Muy Alto	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0%, pues la vulneración de su integridad afectaría perjudicialmente a la institución.
4 - Alto	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 15%, pues la vulneración de su integridad afectaría gravemente a la institución.
3 -Medio	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50%, pues la vulneración de su integridad afectaría considerablemente a la institución.

2 - Bajo	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85%, pues la vulneración de su integridad afectaría parcialmente a la institución.
1 - Muy Bajo	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100%, pues la vulneración de su integridad no impacta a la institución.

Fuente: Producción personal.

Tabla 9 Valorización Activos TI - Disponibilidad

Valor Activo	**Disponibilidad**
5 - Muy Alto	Se requiere que el activo nunca se encuentre indisponible, pues su carencia afectaría perjudicialmente a la institución.
4 - Alto	Se considera que como máximo el activo puede estar indisponible por una hora, pues su carencia afectaría gravemente a la institución.
3 -Medio	Se considera que como máximo el activo puede estar indisponible por un día, pues su carencia afectaría considerablemente a la institución.
2 - Bajo	Se considera que como máximo el activo puede estar indisponible por una semana, pues su carencia afectaría parcialmente a la institución.
1 - Muy Bajo	Se considera que como máximo el activo puede estar indisponible por tiempo indefinido, pues su carencia no impacta a la institución.

Fuente: Producción personal.

1.4 Adaptar instrumento para diagnóstico preliminar

Una vez, se haya estimado el valor del activo mediante la matriz de inventario para conocer el nivel de tasación y luego evaluarlos en la matriz de riesgos, se procedió a calcular porcentualmente mediante un formulario basado en una norma de gestión TI, el grado de cumplimiento respecto a políticas, organización,

administración de activos, seguridad RRHH, gestión de comunicaciones, seguridad física, controles de acceso, elaboración de sistemas, manejo de incidentes del IESTP Utcubamba. A continuación, se visualiza el instrumento adaptado:

IEST Público "UTCUBAMBA"		Criterio de Respuestas (SI / NO)
Formulario: Diagnóstico según estándar de gestión TI aplicado a IESTP Utcubamba		
Responsable: Dr. Ing. Quiroga Honorio Carlos Ramos		
Puesto: Secretario Académico, Gestión de Sistemas Q10 y Registra.		
A. Políticas de Seguridad		
¿Existen documentación de políticas de protección de S.I en el IESTP?	SI	~~NO~~
¿Existe documentación legal a la seguridad de S.I en el IESTP?	SI	~~NO~~
¿Existen acciones relacionados a la protección de S.I en el IESTP?	~~SI~~	NO
¿Existe un encargado de las políticas, normas y procedimientos del IESTP?	SI	~~NO~~
¿Existen mecanismos para la comunicación a los usuarios de las normas del IESTP?	SI	~~NO~~
¿Existen controles regulares para verificar la efectividad de las políticas del IESTP?	SI	~~NO~~
TOTAL	17%	83%
B. Organización de la Seguridad		
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad del IESTP?	SI	~~NO~~
¿Existe un encargado de evaluar la adquisición y cambios de S.I en el IESTP?	SI	~~NO~~

¿La Dirección Académica y las áreas de la institución participan en temas de seguridad del IESTP?	SI	~~NO~~
¿Existen condiciones contractuales de seguridad con terceros y outsourcing en el IESTP?	SI	~~NO~~
¿Existen criterios de seguridad en el manejo de terceras partes del IESTP?	~~SI~~	NO
¿Existen programas de formación en seguridad para los empleados, clientes y terceros del IESTP?	~~SI~~	NO
¿Existe un acuerdo de confidencialidad de la información que se Accesa en el IESTP?	~~SI~~	NO
¿Se revisa la organización de la seguridad periódicamente por una empresa externa en el IESTP?	SI	~~NO~~
TOTAL	37%	63%
C. Administración de Activos		
¿Existe un registro de activos actualizado en el IESTP?	~~SI~~	NO
¿El inventario contiene activos de datos, software, equipos y servicios del IESTP?	~~SI~~	NO
¿Se dispone de una clasificación de la información según la criticidad de la misma en el IESTP?	~~SI~~	NO
¿Existe un encargado de los activos en el IESTP?	~~SI~~	NO
¿Existen procedimientos para clasificar la información del IESTP?	SI	~~NO~~
¿Existen procedimientos de etiquetado de la información?	~~SI~~	NO
TOTAL	83%	17%

D. Seguridad de RRHH		
¿Cuenta con compromisos claros y responsabilidades de protección en el IESTP?	SI	~~NO~~
¿Se considera la protección en la alta y baja del colaborador del IESTP?	SI	~~NO~~
¿Se representa las circunstancias de confidencialidad y compromisos en los contratos del IESTP?	~~SI~~	NO
¿Se imparte la formación adecuada de seguridad y tratamiento de activos en el IESTP?	~~SI~~	NO
¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad en el IESTP?	SI	~~NO~~
¿Se recogen los datos de los incidentes de forma detallada en el IESTP?	SI	~~NO~~
¿Informan los usuarios de las vulnerabilidades observadas o sospechadas del IESTP?	~~SI~~	NO
¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades en el IESTP?	~~SI~~	NO
¿Existe un proceso disciplinario de los S.I en el IESTP?	~~SI~~	NO
TOTAL	56%	44%
E. Seguridad Física		
¿Existe perímetro de seguridad física en el IESTP?	~~SI~~	NO
¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado en el IESTP?	~~SI~~	NO

¿Un área segura ha de estar cerrada, aislada y protegida de eventos naturales en el IESTP?	~~**SI**~~	NO
¿En las áreas seguras existen controles adicionales al personal propio y ajeno del IESTP?	~~**SI**~~	NO
¿Las áreas de carga y expedición están aisladas de las áreas de SI en el IESTP?	SI	~~**NO**~~
¿La localización del equipamiento reduce ingresos redundantes en el IESTP?	SI	~~**NO**~~
¿Existen protecciones frente a fallos en la alimentación eléctrica del IESTP?	~~**SI**~~	NO
¿Existe seguridad en el cableado frente a daños e intercepciones del IESTP?	SI	~~**NO**~~
¿Se asegura la disponibilidad e integridad de todos los equipos del IESTP?	SI	~~**NO**~~
¿Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente del IESTP?	~~**SI**~~	NO
¿Se considera la protección en dispositivos móviles del IESTP?	SI	~~**NO**~~
TOTAL	55%	45%
F. Gestión de Comunicaciones		
¿Todos los procedimientos operativos identificados del IESTP en la política de seguridad han de estar documentados?	SI	~~**NO**~~
¿Están establecidas las responsabilidades para controlar los cambios en equipos del IESTP?	~~**SI**~~	NO
¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad en el IESTP?	~~**SI**~~	NO

¿Hay alguna forma de que el IESTP reduzca el uso inadvertido o intencionado del sistema?	~~SI~~	NO
¿Existe una separación de los entornos de desarrollo y producción del IESTP?	~~SI~~	NO
¿Existen contratistas externos para la gestión de los Sistemas de Información en el IESTP?	~~SI~~	NO
¿Existe un plan de capacidad en el IESTP que garantice una capacidad de procesamiento y almacenamiento suficiente?	~~SI~~	NO
¿Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones en el IESTP?	~~SI~~	NO
¿Existen controles contra software maligno en el IESTP?	~~SI~~	NO
¿Realiza copias de Backup de la información esencial para el negocio?	~~SI~~	NO
¿Existen logs para las actividades realizadas por los administradores del IESTP?	~~SI~~	NO
¿Existen logs de los fallos detectados?	~~SI~~	NO
¿Existen rastro de auditoría?	SI	~~NO~~
¿Existe algún control en las redes?	SI	~~NO~~
¿Hay establecidos controles para realizar la gestión de los medios informáticos?	SI	~~NO~~
¿Eliminación de los medios informáticos? ¿Pueden disponer de información sensible?	SI	~~NO~~
¿Existe seguridad de la documentación de los Sistemas?	~~SI~~	NO

¿Existen acuerdos para intercambio de información y software?	~~SI~~	NO
¿Existen medidas de seguridad de los medios en el tránsito?	~~SI~~	NO
¿Existen medidas de seguridad en el comercio electrónico?	~~SI~~	NO
¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?	~~SI~~	NO
¿Existen salvaguardias para las transacciones realizadas en línea?	SI	~~NO~~
¿Se monitorean las actividades relacionadas a la seguridad?	SI	~~NO~~
TOTAL	80%	20%
G. Control de Acceso		
¿Existe una política de control de accesos en el IESTP?	SI	~~NO~~
¿Existe un proceso formal para que el IESTP registre y dé de baja el acceso?	SI	~~NO~~
¿Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario del IESTP?	SI	~~NO~~
¿Utiliza el IESTP un sistema de gestión de contraseñas de usuario?	SI	~~NO~~
¿Existe una revisión de los derechos de acceso de los usuarios en el IESTP?	~~SI~~	NO
¿Existe el uso del password en el IESTP?	~~SI~~	NO
¿Se protege el acceso de los equipos desatendidos?	~~SI~~	NO
¿Existen políticas de limpieza en el puesto de trabajo?	~~SI~~	NO
¿Existe una política de uso de los servicios de red?	SI	~~NO~~

¿Se asegura la ruta (path) desde el terminal al servicio?	SI	~~NO~~
¿Existe una autenticación de usuarios en conexiones externas?	SI	~~NO~~
¿Existe una autenticación de los nodos?	SI	~~NO~~
¿Existe un control de la conexión de redes?	SI	~~NO~~
¿Existe un control del routing de las redes?	SI	~~NO~~
¿Existe una identificación única de usuario y una automática de terminales?	SI	~~NO~~
¿Existen procedimientos de log-on al terminal?	SI	~~NO~~
¿Se ha incorporado medidas de seguridad a la computación móvil?	SI	~~NO~~
¿Está controlado el teletrabajo por la organización?	SI	~~NO~~
TOTAL	25%	75%
H. Desarrollo y Mantenimiento de Sistemas		
¿Está garantizada la seguridad de los sistemas de información?	~~SI~~	NO
¿Son seguras las aplicaciones?	~~SI~~	NO
¿Existen salvaguardias criptográficas?	~~SI~~	NO
¿Los archivos del sistema tienen seguridad?	~~SI~~	NO
¿Son seguros los procesos de desarrollo, prueba y soporte?	~~SI~~	NO
¿Los resultados del sistema están sujetos a controles de seguridad?	SI	~~NO~~
¿Existe la gestión de los cambios en los SO?	SI	~~NO~~
¿Se controlan las vulnerabilidades de los equipos?	~~SI~~	NO
TOTAL	75%	25%

I. Administración de Incidentes		
¿Se comunican los eventos de seguridad en el IESTP?	**SI**	NO
¿Se comunican las debilidades de seguridad en el IESTP?	**SI**	NO
¿Existen definidas las responsabilidades antes un incidente en el IESTP?	**SI**	NO
¿Existe un procedimiento formal de respuesta en el IESTP?	**SI**	NO
¿Existe la gestión de incidentes en el IESTP?	**SI**	NO
TOTAL	100%	0%
J. Gestión de Continuidad del Negocio		
¿Existen procedimientos para la gestión de la continuidad?	SI	~~**NO**~~
¿Existe un plan de continuidad del negocio y análisis de impacto?	SI	~~**NO**~~
¿Existe un diseño, redacción e implantación de planes de continuidad?	SI	~~**NO**~~
¿Existe un marco de planificación para la continuidad del negocio?	SI	~~**NO**~~
¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?	SI	~~**NO**~~
TOTAL	0%	100%
K. Cumplimiento		
¿Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas?	~~**SI**~~	NO
¿Existe el resguardo de la propiedad intelectual en el IESTP?	~~**SI**~~	NO
¿Existe el resguardo de los registros de la institución?	~~**SI**~~	NO

¿Existe una revisión de la política de seguridad y de la conformidad técnica?	SI	~~NO~~
¿Existen consideraciones sobre las auditorías de los sistemas?	SI	~~NO~~
TOTAL	60%	40%

1.5 Verificar resultados del diagnóstico

El formato anterior sirvió para tener mayor alcance y referencia de cómo se lleva la dirección de tecnologías de información en el IESTP Utcubamba vista desde la calificación que otorga un estándar, dicho esto se procedió elaborar una matriz donde se evidencien los resultados alcanzados en cuanto a los niveles de cumplimiento y detectar en que aspectos se tiene que mejorar, corregir o mantener.

Tabla 10 Resultados del diagnóstico preliminar realizado en el IESTP Utcubamba

Referencia	Sección	% Cumplimiento	% No Cumplimiento	Status
A-01	Políticas de Seguridad	17%	83%	Critico
B-02	Organización de la Seguridad	37%	63%	Requiere Mejora
C-03	Administración de Activos	83%	17%	Aceptable
D-04	Seguridad de RRHH	56%	44%	Aceptable
E-05	Seguridad Física	55%	45%	Aceptable
F-06	Gestión de comunicaciones	80%	20%	Aceptable
G-07	Control de Acceso	25%	75%	Critico

H-08	Desarrollo y Mantenimiento de Sistemas	75%	25%	Aceptable
I-09	Administración de Incidentes	100%	0%	Óptimo
J-10	Gestión de Continuidad del Negocio	0%	100%	Critico
K-11	Cumplimiento	60%	40%	Aceptable

Fuente: Producción personal.

2. Especificación de controles para el estado que requiere mejora y crítico

2.1. Controles para sección Organización de la Seguridad que requiere mejora

- Definir el comité de seguridad, integrado por los siguientes roles propuestos: Líder de la protección de la información (Director General), Presupuesto (Jefe de Área Administrativa), Informática (Jefe de Área Académica de Computación e Informática), Asesor Jurídico (Jefe de la Oficina de Asesoría Jurídica de la UGEL Utcubamba) y Contabilidad (Jefe de Área Académica de Contabilidad).
- Designar al Jefe de Área Administrativa quien tiene el deber de valorar la adquisición y los cambios de Sistemas de Información (S.I.) en el IESTP.

- El comité de seguridad deberá reunirse mensualmente durante una o dos horas para tratar temas de seguridad del IESTP, según la agenda establecida (incluyendo el reconocimiento de amenazas y propuestas de controles).

- Al menos una vez al año, consultar con especialistas en protección de la información y expertos en la norma ISO 27001 para implementar controles y disminuir riesgos.

- Revisar anualmente la estructura de protección de la información para detectar nuevas amenazas y proponer controles. Este proceso debe incluir

un acta de verificación firmada por el Líder de protección de la Información y los profesionales contratados.

2.2. Controles para sección crítico

2.2.1. Políticas de seguridad

- Se define la siguiente propuesta de políticas de protección de S.I
  - El responsable de informática debe asignar cuentas de usuario y password de acceso a los sistemas de información según los módulos que vaya a utilizar el usuario, autorizado por el jefe del Área Administrativa.
  - Cada usuario es responsable del uso adecuado del nombre del usuario y password de acceso a los sistemas de información.
  - El sistema de información debe requerir de manera automática la actualización de la clave de acceso de cada usuario cada tres meses.
  - El responsable del Área Académica de Computación e Informática realizará una copia de protección de los datos de los sistemas de información diariamente, además de verificar regularmente su restauración para garantizar su integridad.
  - Los backup de seguridad de los datos de los sistemas de información se almacenarán tanto internamente como en la nube contratada.
  - El uso de los sistemas de información estará permitido exclusivamente durante las horas laborales.
- Formular y aprobar mediante resolución la normativa sobre la protección de la información, especificando el responsable de las políticas, normas y procedimientos del IESTP.
- Realizar charlas de concientización sobre protección de la información para todos los funcionarios, docentes y estudiantes del IESTP.
- Publicar las políticas de protección de la información en el portal institucional para su descarga por parte de funcionarios, docentes y usuarios.
- Comprobar los controles de protección trimestralmente y documentar los hallazgos en un acta como evidencia, orientada a mejorar la seguridad de la información.

- Revisar el acta de control de protección con el comité de protección, planificar y ejecutar mejoras en el cuidado de la información.

2.2.2. Control de acceso

- **Propuesta de políticas de ingreso a la red de datos**
  - Está estrictamente prohibida la conexión de equipos de cómputo externos a la red de datos institucional.
  - Toda computadora personal o laptop institucional conectada a la red debe tener un antivirus licenciado y actualizado.
  - Cada computadora personal o laptop institucional debe autenticarse en un servidor de dominio de usuarios.
  - Cada usuario institucional debe poseer un nombre de cuenta y un password de acceso al servidor de dominio de usuarios.
  - El Área Administrativa debe informar al Área Académica de Computación e Informática sobre las bajas y altas de usuarios (exclusivamente para trabajadores nombrados y contratados bajo el régimen CAS) en la institución, para mantener actualizados los servicios informáticos.
  - La unidad Académica de Computación e Informática deberá realizar copias de seguridad del servidor de dominio de usuarios diariamente, y verificar regularmente su restauración.
  - Dos veces al año se actualizará la clave de acceso al dominio de usuarios. El servidor solicitará automáticamente la actualización de la clave de acceso.
  - El servicio de internet será utilizado por los funcionarios y servidores públicos exclusivamente para fines institucionales o para el cumplimiento de sus funciones.

- Se propone implementar un servidor de dominio de usuarios para gestionar de manera centralizada los usuarios y los servicios informáticos utilizados en el IESTP.
- Se propone segmentar la red de datos en VLANs (Redes Virtuales) para aislar los laboratorios de la parte administrativa del IESTP, como medida de seguridad.

- Se propone aplicar listas de acceso basadas en la MAC (Media Access Control) en los switches de comunicación para controlar el ingreso a la red de datos, permitiendo únicamente a los usuarios permitidos de la institución.
- Se propone formular un procedimiento para el registro y la baja de permisos en el IESTP.
- Se propone establecer un procedimiento para el acceso a los servicios informáticos (Sistemas de Información, Internet, Portal Web Institucional, etc.) en el IESTP.

2.2.3. Gestión de continuidad del negocio

- Se propone se formule un plan de continuidad del negocio el cual contenga los siguientes sub controles:
  - Realizar backup de protección de los datos, aplicaciones (fuente y ejecutable), y configuración de equipos informáticos y comunicaciones en ubicaciones seguras dentro de la institución y en la nube de un país extranjero.
  - Establecer procedimientos para la restauración rápida de los servicios informáticos, cuando exista interrupción.
  - Asignar roles específicos en los procedimientos para el restablecimiento de los servicios.
  - Proporcionar herramientas y equipos tecnológicos adecuados para la restauración de los servicios.
  - Asignar un presupuesto apropiado acorde con las acciones necesarias para restaurar los servicios.
  - Implementar mecanismos automáticos de restauración, utilizando software para recuperar sistemas operativos, aplicaciones de ofimática, antivirus, entre otros, en servidores y computadoras personales.
  - Implementar una nueva red de datos con cableado estructurado y equipos que cumplan con las tecnologías y estándares actuales.
  - Realizar una verificación y cumplimiento del plan de continuidad de servicios de TI mediante un acta al menos dos veces al año.

3. Diseñar el prototipo para la administración y evaluación de riesgos basado en el estándar ISO 27001:2017

3.1 Selección del estándar ISO 27001

Para plantear el siguiente modelo, inicialmente se realizó una revisión de los estándares que estén avocados a la gestión de riesgos TI. Por lo cual, para la comparación se tomaron en cuenta 03 normas: ISO 31000, ISO 9001 e ISO 27001; siendo está última la más relevante dado el caso de estudio que se tomó como referencia, el cual fue el IESTP Utcubamba. La propuesta está relacionada a diseñar un modelo para administrar y evaluar riesgos TI en un instituto tecnológico público peruano, usando la documentación publicada de ISO 27001 en el año 2017. Como parte del proceso comparativo de estándares, se emplearon los siguientes criterios: a) Organización, b) Aplica Mejores Prácticas, c) Reconocimiento en el nicho, d) Adaptación en empresas latinoamericanas, e) Aplicación en casos institucionales tecnológicos peruanos, f) Fácil de entender e interpretar, g) Integra procesos de desarrollo y gestión TI, y h) Métodos formales para gestionar riesgos TI.

Tabla 11 Comparativa y Selección de Estándares basado en criterios

Código	Criterio Selección	ISO 31000	ISO 9001	ISO 27001
C1	Organización	ISO	ISO	ISO
C2	Aplica Mejores Practicas	SI	SI	SI
C3	Reconocimiento en el Nicho/Mercado	Internacional	Internacional y Nacional	Internacional y Nacional
C4	Adaptación en institutos tecnológicos latinoamericanos	SI	SI	SI
C5	Aplicación en institutos	NO	NO	SI

	tecnológicos peruanos			
C6	Fácil de entender e interpretar la norma	NO	NO	SI
C7	Integra procesos de desarrollo y gestión TI	NO	SI	SI
C8	Evidencia métodos formales para gestionar riesgos TI	SÍ	NO	SI

Nota: Tomado de Holguín, & Cuadros, (2017, pág. 327) y adaptado.

Asimismo, se empleó que permita valorar mediante una clasificación-ponderativa según su respuesta al criterio delimitado, por ello se visualiza la siguiente tabla.

Tabla 12 Clasificación de estándares según desempeño

N°	DESEMPEÑO	DESCRIPCIÓN
1	Deficiente	El estándar o norma no cubre el criterio.
2	Insuficiente	El estándar o norma cubre el criterio inadecuadamente.
3	Aceptable	El estándar o norma cubre el criterio bien, pero quedan vacíos ciertos contenidos.
4	Excelente	El estándar o norma cubre el criterio satisfactoriamente.

Nota: Tomado de Holguín, & Cuadros, (2017, pág. 21) y adaptado.

Por tal razón, una vez ya definidos los criterios de selección - Tabla 11 y teniendo en cuenta la clasificación para la valoración - Tabla 12, se completó la siguiente matriz, para así obtener un fundamento de la selección de un estándar sobre otro.

Tabla 13 Evaluación cuantitativa y selección de estándares basado en criterios

Criterio Selección	ISO 31000	ISO 9001	ISO 27001
Organización	4	4	4
Aplica Mejores Practicas	4	4	4

Reconocimiento en el Nicho/Mercado	3	4	4
Adaptación en institutos tecnológicos latinoamericanos	4	4	4
Aplicación en institutos tecnológicos peruanos	2	2	4
Fácil de entender e interpretar la norma	3	3	4
Integra procesos de desarrollo y gestión TI	2	4	4
Evidencia métodos formales para gestionar riesgos TI	3	2	4
Total, de Puntaje	25	27	32

Nota: Tomado de Holguín, & Cuadros, (2017, pág. 327) y adaptado.

Existen diversos estándares de gestión de riesgos TI, obviamente hay otras maneras o criterios de seleccionar, pero para este caso, se consideró así dado el caso de estudio, la realidad de la institución o contexto y si aplicaba métodos formales para dicha gestión e integraba la parte del desarrollo a su vez, es decir se buscó un modelo que se ajuste a las condiciones del instituto y a necesidades que desee afrontar con la aceptación del modelo, buscando alcanzar los objetivos. Dicho esto, la mayor ponderación como se observó fue de la legislación ISO 27001.

3.2 Documentación de términos ISO 27001:2017

Campo de aplicación

El objetivo de esta norma internacional es definir las especificaciones de los numerosos componentes de un sistema de gestión de la protección de la información, como su creación, ejecución, mantenimiento y mejora continua. Además, la decisión de una institución de implantar un SGSI es estratégica. Las palabras iniciales vienen determinadas por las exigencias, los objetivos, las

especificaciones de protección, los procedimientos empresariales y la estructura organizativa de la organización. Es crucial recordar que se trata de una variable porque los elementos se alterarán con el tiempo. Esta norma cubre la comprensión y el manejo de los peligros de protección de la información de acuerdo con los requisitos de la organización.

Términos y Definiciones

La ISO 27001 utiliza conceptos en su guía a continuación. Es importante destacar que la información fue obtenida a través de la plataforma Industria Conecta 4.0 del gobierno de España, donde se publicó la norma con el ANEXO A y los controles correspondientes. Se llevó a cabo una comparación entre la información proporcionada por la NTP ISO 27001:2014 y la de la UNE-EN ISO/IEC 27001:2017 para determinar los cambios mínimos realizados.

Tabla 14 Lista de términos y definiciones de la ISO 27001:2017

UNE-EN ISO/IEC 27001	
T4. Contexto de la organización	
Apartado	Descripción
4.1 Comprensión de la organización y de su contexto	Cuestiones externas e internas que son pertinentes para el propósito de la organización y que afectan su capacidad para lograr los resultados previstos de su SGSI.
4.2 Comprensión de las necesidades y perspectiva de las partes involucradas	Partes interesadas de mayor relevancia para el SGSI.
4.3 Determinación del alcance del sistema de gestión de la seguridad de la información	Determinación de límites y aplicabilidad del SGSI, interfaces y dependencias que incluye.
4.4 Sistema de gestión de la seguridad de la información	Establecimiento, mantenimiento y mejora continua del SGSI
T5. Liderazgo	
Apartado	Descripción

5.1 Liderazgo y compromiso	Aseguramiento de integración de RQ del SGSI, compatibilidad con la alta dirección, dirigir y asistir a personas, contribuir a la mejora continua, entre otros.
5.2 Política	Incluya objetivos de SI, la política debe estar documentada correctamente, disponible para la organización y tener cohesión.
5.3 Roles y Responsabilidades y autoridades de la organización	Conformidad de los RQ del SGSI, comunicar, informar y asignar responsabilidades dentro de la organización.

T6. Planificación

Apartado	Descripción
6.1 Acciones para tratar los riesgos y oportunidades	Prevenir o reducir efectos colaterales indeseados, permitir una mejora continua, integrar e implementar acciones para cumplir con tal fin en el SGSI. Criterios de aceptación de riesgos, identificación, análisis y evaluación de riesgos de SI. Determinar y comparar controles, elaborar una declaración soa de aplicabilidad, gestionar y formular un plan de tratamiento de riesgos de SI
6.2 Objetivos de seguridad de la información y planificación para su consecución	Deben ser medibles, coherentes, lógicos, alcanzables, actualizados, autónomos, comunicados e informados.

T7. Soporte

Apartado	Descripción
7.1 Recursos	La organización debe brindar los recursos necesarios para las 04 fases del SGSI
7.2 Competencia	El perfil del personal debe estar basado en la experiencia de campo profesional, aptitudes, habilidades, formación evidenciada, dado que las situaciones requieren un buen desempeño de la SI

7.3 Concienciación	Mejora del desempeño en SI, políticas de SI
7.4 Comunicación	Interrogantes: ¿Cuándo?, ¿A quién?, ¿Dónde? y ¿Quién debe comunicar?
7.5 Información documentada	Alcance de la organización, complejidad de procesos, habilidades del personal
T8. Operación	
Apartado	Descripción
8.1 Planificación y control operacional	Mitigar efectos adversos con el control de cambios planificados y revisión de consecuencias
8.2 Apreciación de los riesgos de seguridad de la información	Escenarios probables de ocurrencia de riesgos o modificaciones relevantes
8.3 Tratamiento de los riesgos de seguridad de la información	Plan de tratamiento de riesgos de SI
T9. Evaluación del desempeño	
Apartado	Descripción
9.1 Planificación y control operacional	Métodos de seguimiento, medición, análisis y evaluación de resultados.
9.2 Auditoría interna	Definición de criterios y alcance, selección de auditores, comunicación con la alta dirección, programas de auditoría
9.3 Revisión de la dirección	Acciones correctivas, no conformidades, medición y seguimiento de controles, velar por el cumplimiento de los objetivos de SI, entre otros.
T10. Mejora	
Apartado	Descripción
10.1 No conformidad y acciones correctivas	Controles correctivos para las no conformidades, evaluación de acciones implementadas, determinación de causas, verificación de acciones ejecutadas en la SI

10.1 Mejora continua	La organización debe mejorar de manera continua la idoneidad, adecuación y eficacia del SGSI

Fuente: Norma Española UNE-EN ISO/IEC 27001, mayo 2017.

Tabla 15 Lista de controles de referencia de la ISO 27001:2017

UNE-EN ISO/IEC 27001	
A5. Políticas de seguridad de la información	
Apartado	Aplicado en casos de estudio peruanos
5.1 Política para la SI	SI
5.2 Revisión de las políticas para la SI	SI
A6. Organización de la seguridad de la información	
Apartado	Aplicado en casos de estudio peruanos
6.1 Roles y responsabilidades en SI	SI
6.2 Segregación de tareas	SI
6.3 Contacto con las autoridades	SI
6.4 Contacto con grupo de interés especial	SI
6.5 Seguridad de la información en gestión de proyectos	SI
A7. Seguridad relativa a los recursos humanos	
Apartado	Aplicado en casos de estudio peruanos
7.1 Investigación de antecedentes	SI
7.2 Términos y condiciones del empleo	SI
7.3 Proceso disciplinario	SI
7.4 Responsabilidades ante cambio	
A8. Gestión de activos	

Apartado	Aplicado en casos de estudio peruanos
8.1 Inventario de activos	SI
8.2 Propiedad de los activos	SI
8.3 Uso aceptable de los activos	SI
8.4 Devolución de activos	SI
8.5 Clasificación de la información	SI
8.6 Etiquetado de la información	SI

A9. Control de acceso

Apartado	Aplicado en casos de estudio peruanos
9.1 Política de control de acceso	SI
9.2 Acceso a los servicios de red	SI
9.3 Gestión de privilegios de acceso de usuario	SI
9.4 Sistema de gestión de contraseñas	SI

A10. Criptografía

Apartado	Aplicado en casos de estudio peruanos
10.1 Política de uso de los controles criptográficos	SI
10.2 Controles físicos de entrada	SI
10.3 Mantenimiento de los equipos	SI

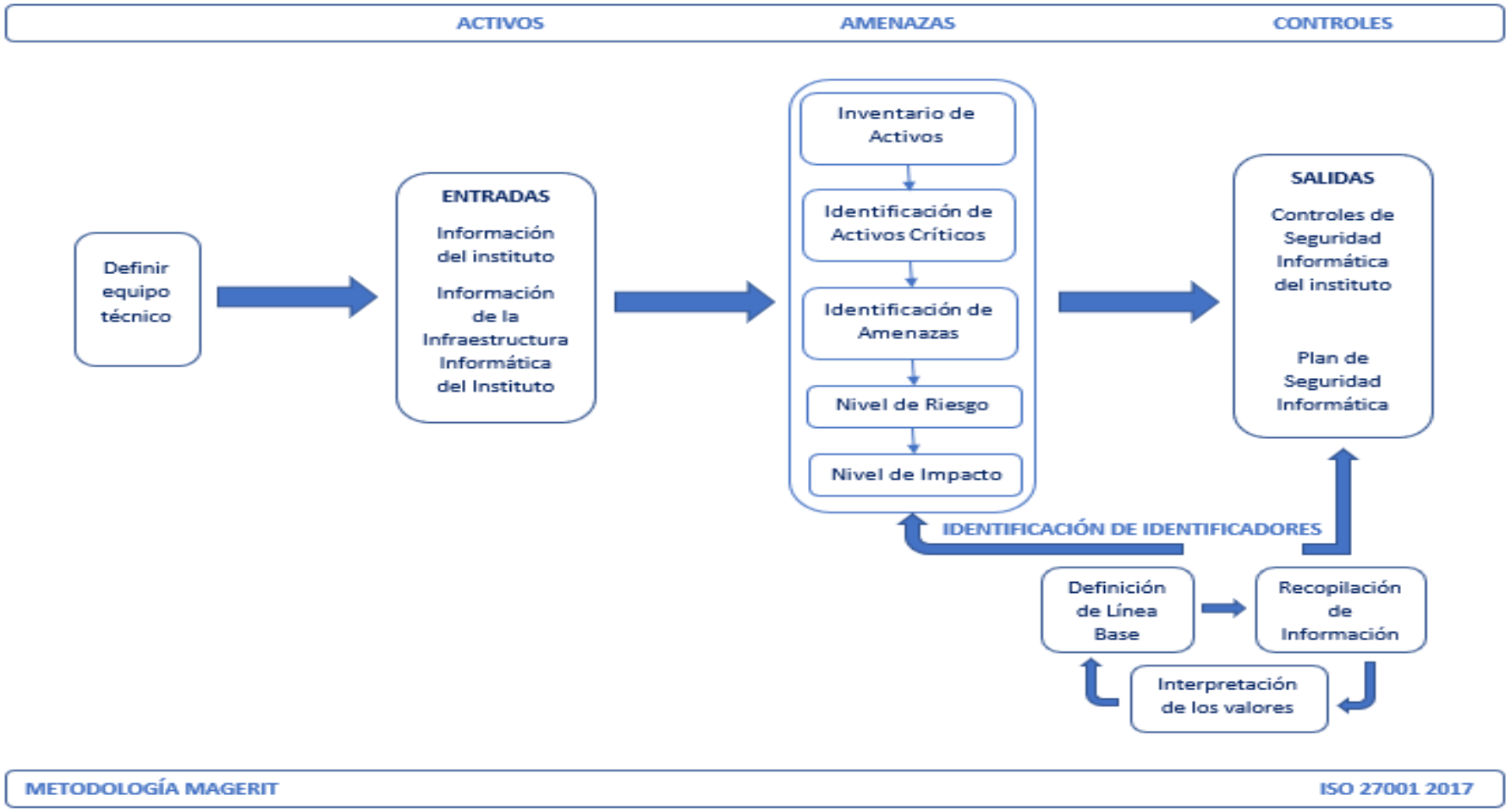
A12. Seguridad de las operaciones

Apartado	Aplicado en casos de estudio peruanos
12.1 Documentación de procedimientos operacionales	SI
12.2 Gestión de cambios	SI
12. 3 Copias de seguridad de la información	SI
12.4 Controles contra el código malicioso	SI

A13. Seguridad de las comunicaciones	
Apartado	Aplicado en casos de estudio peruanos
13.1 Controles de red	SI
13.2 Acuerdos de confidencialidad o no revelación	SI
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información	
Apartado	Aplicado en casos de estudio peruanos
14.1 Protección de las transacciones de servicios de aplicaciones	SI
14.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI
A15. Relación con proveedores	
Apartado	Aplicado en casos de estudio peruanos
15.1 Requisitos de seguridad en contratos con terceros	SI
15.2 Gestión de cambios en la provisión del servicio del proveedor	SI
A16. Gestión de incidentes de seguridad de la información	
Apartado	Aplicado en casos de estudio peruanos
16.1 Responsabilidades y procedimientos	SI
16.2 Respuesta a incidentes de seguridad de la información	SI
16.3 Recopilación de evidencias	SI
A17. Gestión de incidentes de seguridad de la información	
Apartado	Aplicado en casos de estudio peruanos

17.1 Implementar la continuidad de la seguridad de la información	SI
17.2 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI

En relación a lo mencionado anteriormente, se diseñó este modelo de gestión de riesgos.



3. Justificación del modelo de gestión propuesto.

El modelo sugerido, que consta de los componentes mencionados y se centra en la legislación ISO27001 2017 y en la metodología MAGERIT, se apoya en su enfoque global y metódico de la gestión de riesgos informáticos. Aquí se detalla la justificación de cada componente y cómo contribuye al éxito del modelo:

- Definir equipo de trabajadores: La gestión de riesgos informáticos es esencial, y empieza por crear un equipo especializado. Esto garantiza que se destinen recursos a las actividades de valoración de peligros, aplicación de controles y mantenimiento del plan de seguridad, así como una rendición de cuentas inequívoca. Un equipo bien constituido también facilita la coordinación de especialistas de otros campos para identificar y reducir eficazmente los peligros.

- Entrada de información del instituto: Es fundamental contar con una entrada de información clara y completa que describa la estructura organizativa, los procesos operativos, las políticas y normativas internas, así como cualquier contexto específico del instituto. Esta información proporciona el marco inicial para identificar activos de información, amenazas potenciales y evaluar el impacto de probables incidentes de protección.

- Infraestructura de TI: La infraestructura de TI incluye todos los componentes tecnológicos que soportan las operaciones del instituto. Identificar y documentar adecuadamente esta infraestructura es esencial para comprender las vulnerabilidades y riesgos asociados. Además, permite la implementación de controles específicos que protejan adecuadamente los sistemas y datos críticos.

- Inventario de activos: Contar con un inventario completo de las infraestructuras y los activos de información cruciales es esencial para una gestión más efectiva de la protección. Esto incluye todo lo relacionado con hardware, software, datos y recursos humanos asociados. Mantener un inventario actualizado ayuda a asignar prioridades y recursos para salvaguardar los activos más críticos de la organización. La actualización del

inventario, la cobertura de activos críticos y la valoración de la depreciación de los activos tecnológicos son indicadores relevantes.

- Identificación de activos críticos: No todos los activos tienen el mismo valor o importancia para la entidad. Identificar los activos en peligro es fundamental para dirigir el ahínco de protección y asignar recursos de manera adecuada. Esta identificación se basa en la función y valor estratégico de cada activo para el funcionamiento del instituto. Los indicadores podrían incluir la evaluación de impacto de negocio, la priorización de activos críticos y la alineación con objetivos estratégicos.

- Identificación de amenazas: Evaluar y categorizar las amenazas potenciales que perjudican a los activos críticos es crucial para conocer los escenarios de riesgo. Esto implica identificar fuentes de amenazas en el interior y exterior, así como posibles fragilidades que podrían ser explotadas por los adversarios. Indicadores aquí podrían medir la frecuencia de incidentes de seguridad relacionados con amenazas identificadas, la variación en el nivel de riesgo y la efectividad de las respuestas a incidentes.

- Nivel de riesgo y nivel de impacto: Evaluar la posibilidad de que ocurra una amenaza y la consecuencia potencial de esa amenaza en los activos críticos es parte de la determinación del nivel de riesgo. Esta evaluación cuantitativa o cualitativa guía la priorización de actividades y entrega de recursos para reducir de manera efectiva los riesgos más significativos. La tasa de riesgos aceptada, la reducción de la exposición a riesgos y la perfección en la capacidad de atención para atender los incidentes son algunos de los indicadores.

- Salida: Establecer controles de seguridad adecuados y un plan de seguridad: El proceso de evaluación de riesgos conduce al establecimiento de los controles de seguridad necesarios para mitigar o gestionar los peligros identificados. Estos controles pueden consistir en formación del personal, determinadas tecnologías, normas y procesos. La seguridad de la

información se gestiona de forma eficaz y continua gracias a la estrategia de seguridad, que sirve de base para implantar estos controles y mantenerlos actualizados. Aquí se pueden utilizar indicadores clave para calibrar el éxito de las políticas de seguridad adoptadas, la aplicación de los controles y el cumplimiento de las normas de seguridad y respuesta a incidentes.

En conjunto, este modelo orientado a indicadores proporciona un entorno completo para la gestión de riesgos de TI, desde la identificación inicial de activos y amenazas hasta la implementación de controles específicos y la gestión permanente de la seguridad. Esto no solo fortalece la resiliencia de la entidad frente a las amenazas cibernéticas, sino que también ayuda a ejecutar estándares de seguridad reconocidos y a preservar la confianza de los stakeholders en la protección de la información crítica del instituto.

4. Validar con juicio de expertos el modelo de gestión propuesto.

Se empleó el siguiente formato de ficha de expertos, para evaluar el modelo que se planteó basado en la ISO 27001

VALIDACIÓN DE JUICIO DE EXPERTO
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:
APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO

Autor:

- FARROÑAN TERAN NIXON PAUL

Objetivo:
El objetivo del presente informe es someter a evaluación el presente modelo basado en la norma ISO/IEC 27001:2017 para mejorar los procesos de gestión de riesgos de tecnologías de la información en un instituto superior privado peruano.

I. DATOS GENERALES DEL EXPERTO
1.1. Apellidos y nombres del experto: _____
1.2. Grado Académico y Profesión: _____
_____
1.3. Áreas de Experiencia Profesional: _____
1.4. Institución donde labora: _____
1.5. Nombre del instrumento motivo de evaluación: _____

II. VALIDACIÓN
Se utilizará los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - [250-400], **Regular -** [450-600], **Buena:** [650-800], **Muy Buena -** [850-1000]

ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE				BAJA				REGULAR				BUENA				MUY BUENA			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Está formulada con lenguaje apropiado																				
OBJETIVIDAD	Está expresada en conductas observables																				
ACTUALIDAD	Adecuada al avance de la gestión riegos de TI																				
ORGANIZACIÓN	Existe una organización lógica																				
SUFICIENCIA	Comprende los aspectos en cantidad y calidad																				
INTENCIONALIDAD	Adecuada para valorar la gestión de riesgos de TI en un instituto superior tecnológico privado																				
CONSISTENCIA	Basado en aspectos teóricos científicos																				
COHERENCIA	Entre cada uno de los pasos de la metodología																				
METODOLOGÌA	El planteamiento responde al objetivo del estudio.																				
PERTINENCIA	Es práctico y apropiado para el estudio.																				

VALORACIÓN: _____

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Pimentel, ___ noviembre del 2022.

_____

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

Se realizó una diagnosis del estado situacional de la entidad en gestión de riesgos de TI bajo 07 subactividades, las cuales fueron: análisis del instituto tecnológico publico peruano, definición del proceso TI actual de instituto, elaboración de relación de activos de información, clasificación y valorización de activos de información. Asimismo, se adaptó un instrumento de diagnóstico preliminar el cual estuvo fundamentado en los controles referencia del anexo A que proporciona la normativa ISO 27001:2017, y finalmente se verificaron los resultados alcanzados, donde se encontraron que las políticas de SI, el control de acceso y la gestión de continuidad del negocio están en estado crítico; mientras que la organización de la seguridad requiere algunas mejoras. Ante ello se ha propuesto controles para el estado que requiere mejora y también en situaciones críticas.

Se identificaron y valoraron 114 activos (bases de datos, sistemas, usuarios, equipos informáticos y documentos físicos entre otros), de los cuales 29 se clasificaron como críticos según su disponibilidad, confidencialidad e integridad; así mismo dentro de ello se identificaron 56 amenazas de las cuales 27 son criticas representando el 48%. A fin de mitigar la inseguridad se propuso controles en las sesiones críticas de forma específica dentro de las políticas de seguridad, control de acceso y gestión de continuidad del negocio.

Se diseñó un modelo para la administración y valoración de riesgos basada en la normativa ISO 27001:2017, tomando como referencia la documentación publicada por Norma Española UNE-EN ISO/IEC 27001 mayo 2017, la cual nos proporciona los controles del anexo A, y la definición de términos y dominios, para usar como cimiento en la elaboración del modelo.

4.2. Recomendaciones.

Todos los controles mencionados deben ponerse en marcha para reducir los riesgos y los efectos potenciales de las amenazas.

También son necesarias auditorías internas periódicas para confirmar que la norma ISO 27001-2017 se está aplicando de acuerdo con los requisitos necesarios de la norma.

Se actualice constantemente la tecnología informática y comunicaciones con el fin de reducir los peligros a que está expuesto la institución.

Para disminuir los peligros a los que se enfrenta la institución, se debe actualizar periódicamente las tecnologías de la información y la comunicación.

Para disminuir la vulnerabilidad informática, el personal administrativo, los profesores y los alumnos deben ser conscientes de aplicar normas de protección de la información y recibir formación sobre la tecnología de protección de la información actual.

REFERENCIAS.

ADEK. (2020). *Las 4 dimensiones en la gestión de servicios de formación ITIL 4*. Obtenido de https://www.adek.es/las-4-dimensiones-la-gestion-servicios-formacion-itil-4/

Amable, M., & Millones, R. (2019). Uso de modelos de calidad en las mypes productoras de software de Lima. *Revista de Ingeniería Industrial*(37). Obtenido de https://www.researchgate.net/publication/337451066

Ambit. (07 de Mayo de 2020). *Análisis de riesgos informáticos y ciberseguridad*. Obtenido de https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

Angraini, Megawati, & Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. 1-4. Parapat, Indonesia. doi:10.1109/CITSM.2018.8674294

Azizi, N., Miah, S., & Masmali, F. (2019). Development of an Innovative Framework for IT Risk Management. 1-4. Melbourne, Australia. doi:10.1109/CSDE48274.2019.9162399

Bayona, S., Chauca, W., Lopez, M., & Maldonado, C. (2015). ISO/IEC 27001 implementation in public organizations: A case study. Aveiro, Portugal. doi:10.1109 / CISTI.2015.7170355

Carnero Garay , D., Carbajal Ramos , M., Armas Aguirre , J., & Madrid Molina, J. (2020). Information security risk management model for mitigating the impact on SMEs in Peru. Sevilla, España. doi:10.23919/CISTI49556.2020.9140980

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. 1-6. Coimbra, Portugal. doi:10.23919/CISTI.2019.8760870

Deloitte. (Julio de 2016). *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información*. Obtenido de Encuesta 2016 sobre tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica: https://www2.deloitte.com/pe/es/pages/risk/articles/la-evolucion-de-la-gestion-de-ciber-riesgos-y-seguridad.html

Digiware. (2017). *El impacto económico ciberataques en la región*. Obtenido de https://www.digiware.net/blog

Ernst & Young. (08 de Febrero de 2021). *56% de organizaciones en el Perú afirma contar con un área de gestión de riesgos empresariales*. Obtenido de https://www.ey.com/es_pe/news/2021/02/organizaciones-peru-area-gestion-riesgos-empresariales#:~:text=56%25%20de%20organizaciones%20en%20el,de%20gesti%C3%B3n%20de%20riesgos%20empresariales

Fahrurozi, M., Tarigan, S., Tanjung, M., & Mutijarsa, K. (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). 86-91. Yogyakarta, Indonesia. doi:10.1109/ICITEE49829.2020.9271748

Feng, N., Wang, H., & Li, M. (2015). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. doi:https://doi.org/10.1016/j.ins.2013.02.036

Foncodes. (2019). *MYPEs contribuyen al crecimiento de la economía nacional*. Obtenido de http://www.foncodes.gob.pe/portal/index.php/comunicacion-e-imagen/noticias-y-comunicaciones/item/1018-mypes-contribuyen-al-crecimiento-de-la-economia-nacional#:~:text=Seg%C3%BAn%20la%20Asociaci%C3%B3n%20de%20Emprendedores,del%20crecimiento%20econ%C3%B3mic

García Porras , C., Huamani Pastor, S., & Armas Aguirre, J. (2018). Information Security Risk Management Model for Peruvian SMEs. Lima, Peru. doi:10.1109/SHIRCON.2018.8592994

INEI. (2018). *Perú - Tecnologías de información y Comunicación en las Empresas*. Obtenido de Encuesta Económica Anual 2018: https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1719/libro.pdf

INEI. (11 de junio de 2021). *En el Perú existen más de 2 millones 838 mil empresas*. Obtenido de https://www.inei.gob.pe/media/MenuRecursivo/noticias/nota-de-prensa-no-087-2021-inei.pdf

ISACA. (2012). COBIT 5 for Information Security. Obtenido de https://www.isaca.org/

ISO. (2018). *ISO 31000:2018(es) - Directrices*. Obtenido de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Jimenez, H., Rodriguez, R., & Tiparra, J. (1978). *Diagnóstico de TEA.* Madrid: Latinoamérica SA.

Joshi, C., & Kumar Singh, U. (2017). Quantitative Information Security Risk Assessment Model for University Computing Environment. Bhubaneswar, India. doi:10.1109/ICIT.2016.026

Mejia, I., Ramirez, R., Jimenez, H., & Rosas, J. (2019). A new method a architecture entreprise. *Conference IEEE bussines*, 200-215.

Mejia, I., Tuesta, M., & Forero, M. (2020). A new method of enterprise archicture small organizations. *Computer Science Techology*, 150-170.

Mesones, A., & Roca, E. (2017). Factores que limitan el crecimiento de las producciones Micro y Pequeñas Empresas en el Perú (MYPES). *CENTRUM Catolica*, 11. Obtenido de https://revistas.pucp.edu.pe/index.php/strategia/article/view/4126/4094

Minkevics, V., & Slihte, J. (2017). Modelling IT security risk management in academic environment. 1-4. Riga, Latvia. doi:10.1109/AIEEE.2017.8270562

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. 1-5. Varna, Bulgaria. doi:10.1109/InfoTech49733.2020.9211066

Mumtaz, N. (2016). Analysis of information security through asset management in academic institutes of Pakistan. Karachi, Pakistan. doi:10.1109/ICICT.2015.7469581

Palma, J., & Marín, R. (2008). *Inteligencia Artificial.* Madrid: McGrawHill. doi:978-84-481-5618-3

Pasha, M., Qaiser, G., & Pasha, U. (2018). A Critical Analysis of Software Risk Management Techniques in Large Scale Systems. 12412-12424. Pakistan. doi:10.1109/ACCESS.2018.2805862

Pirani. (2018). *ISO 27001: de qué se trata y cómo implementarla*. Obtenido de https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

Putra, S., Gunawan, M., Sobri, A., Muslimin, J., Amilin, & Saepudin, D. (2020). Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company. 1-5. Pangkal, Indonesia. doi:10.1109/CITSM50537.2020.9268845

Rojas, K. (2018). Identificación de efectos negativos de la TEA en el aprendizaje. *IEEE conference Techology children especial*, 200-215.

Ruiz Sanchez, D. (2014). *DISEÑO DE ARQUITECTURA EMPRESARIAL EN EL SECTOR EDUCATIVO COLOMBIANO: CASO COLEGIO PRIVADO EN BOGOTÁ.* Universidad Católica de Colombia, Facultad de Ingeniería Programa de Ingeniería de Sistemas, Bogotá. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/1691/1/Trabajo%20de%20Grado%20Arquitectura%20Empresarial.pdf

Setiawan, H., Putra, F., & Pradana, A. (2017). Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute. 251-256. Bandung, Indonesia. doi:10.1109/ICITSI.2017.8267952

Suárez, D., & León, G. (2019). Las PyME de desarrollo de software. Modelos de mejora de sus procesos en Latinoamérica. *Revista Espacios, 40*(28), 9. Obtenido de https://www.revistaespacios.com/a19v40n28/19402809.html

SZNAJDLEDER, P. (2012). *Java a fondo - estudio del lenguaje y desarrollo de aplicaciones - 2a ed.* México: Alfaomega.

Thales Group. (2020). *NIST 800-53, Revisión 4*. Obtenido de https://cpl.thalesgroup.com/es/compliance/americas/nist-800-53-fedramp/nist-800-53-revision-4

Yoseviano, H., & Retnowardhani, A. (2018). The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: case study in xyz, ltd. 21-26. Jakarta, Indonesia. doi:10.1109/ICIMTech.2018.8528096

ANEXOS.

Anexo 01. RESOLUCIÓN DE PROYECTO.

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N° 0758-2022/FIAU-USS

Pimentel, 05 de diciembre de 2022

VISTOS:

El Acta de reunión N° 01711 – 2022 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante oficio N° 0261-2022/FIAU-II-USS de fecha 30 de noviembre de 2022, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48º que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y *tesis* son *aprobados por el Comité de Investigación* y derivados a la facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24º señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, según documentos de vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerda aprobar el tema tesis en el extremo de la tesis a cargo de los estudiantes oegresados que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el tema tesis en el extremo de la tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los estudiantes o egresados del Programa de estudios de INGENIERÍA DE SISTEMAS según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N° 0758-2022/FIAU-USS

Pimentel, 05 de diciembre de 2022

ANEXO

APROBACION DE TEMA DE TESIS

SECCION A

	APELLIDOS	TESIS
1	TAPIA FUENTES MARIANO HERNANDO	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE SERVICIOS DE TI PARA UNA PEQUEÑA EMPRESA PERUANA BASADA EN ITIL V4
2	RIVAS PLATA CASAS CARLOS GUALBERTO	CLASIFICACIÓN DE CÁNCER DE PULMÓN EN IMÁGENES DE TOMOGRAFÍAS MEDIANTE PROCESAMIENTO DE IMÁGENES Y APRENDIZAJE AUTOMÁTICO
3	FARROÑAN TERAN NIXON PAUL	APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO
4	LUNA BECERRA JHERSON ISAC	MÉTODO DE CLASIFICACIÓN AUTOMÁTICA DE DEFICIENCIAS NUTRICIONALES EN HOJAS DE CAFETO MEDIANTE PROCESAMIENTO DE IMÁGENES DIGITALES Y APRENDIZAJE PROFUNDO
5	CABREJOS SEVERINO LUZ ANTONELLA	DESARROLLO DE UN MÉTODO DE LECTURA AUDIBLE DE LIBROS DE TEXTO BASADO EN PROCESAMIENTO DIGITAL DE IMÁGENES Y DEEP LEARNING
6	RABANAL SENMACHE MARRY CECY SÁNCHEZ RUBIO OMAR ALBERTO	DISEÑO DE UN MODELO DE AUDITORÍA DE TI PARA EL CUMPLIMIENTO DE NORMAS Y POLÍTICAS DE UNA EMPRESA RETAIL PERUANA
7	JULCA BRUNO HOLVER KABIR VILCHEZ BAILA ERICKSON YOVANI	EVALUACIÓN DE LA CALIDAD EN USO DE UN SISTEMA DE GESTIÓN EDUCATIVA PARTICULAR BASADO EN LA NORMA ISO/IEC 25022
8	FIESTAS TELLO, TATIANA MERCEDES TEJADA PAREDES, JORGE LUIS	IMPLEMENTACIÓN DE UN MODELO BASADO EN ITIL 4, PARA MEJORAR LA EFICIENCIA DE ITSM EN UNA INSTITUCIÓN REGIONAL DEL ESTADO.
9	AYALA SÁNCHEZ MARIO FRANKLIN TEPE LEON EDWIN ANTONIO	MÉTODO DE DETECCIÓN DE ATAQUES A UNA RED DEFINIDA POR SOFTWARE DE UNA EMPRESA PERUANA BASADO EN MACHINE LEARNING

SECCION B

	APELLIDOS	TESIS
1	SANCHEZ PARDO SAMUEL MORE VILLEGAS FIORELLA JHAJAIRA	DESARROLLO DE MÉTODO PARA LA CLASIFICACIÓN POR MADUREZ DE LA FRESA UTILIZANDO PROCESAMIENTO DE IMÁGENES DIGITALES Y MACHINE LEARNING
2	LOPEZ VALLEJOS ROBER YUBELDER	IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN ASOCIANDO USUARIO Y DISPOSITIVO PARA MEJORAR LA SEGURIDAD EN LA AUTENTICACIÓN DE CREDENCIALES DE ACCESO
3	LOZANO DELGADO KELKIN HEIMINN GUERRERO VEGA ERICKS TITO	IMPLEMENTACIÓN DE ALGORITMOS CRIPTOGRÁFICOS PARA MEJORAR LA SEGURIDAD EN EL ENVIO DE TEXTO PLANO POR INTERNET
4	GARCIA CHOZO DIANA KATHERINE MAQUEN MUJICA MIGUEL ANGEL	DESARROLLO DE APLICATIVO MOVIL DE REALIDAD AUMENTADA PARA MEJORAR EL APRENDIZAJE DE INGLES EN ESTUDIANTES DE PRIMERO DE SECUNDARIA

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N° 0758-2022/FIAU-USS

Pimentel, 05 de diciembre de 2022

	APELLIDOS	TESIS
5	MONJA VASQUEZ FERNANDO JOEL	IMPLEMENTACIÓN DE UNA APLICACIÓN WEB PARA COMPARTIR Y EJECUTAR COMPLEMENTOS DE IMAGEJ
6	BENAVIDES CIURLIZZA OSCAR JAVIER DIAZ CORONADO JENNIFFER GERALDINE	IMPLEMENTACIÓN DE UN MODELO BASADO EN LA TECNOLOGÍA BLOCKCHAIN PARA LA GESTIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS
7	HERNA LOJA BRYAM ALEXANDER	DESARROLLO DE UN ENFOQUE ÁGIL PARA OPTIMIZAR LA CONSTRUCCIÓN DE SOFTWARE EN UN EMPRESA LAMBAYECANA
8	PACHECO CONTRERAS NICOLETTE ISIS SANTISTEBAN OSTOS ANDY JOSUE	IMPLEMENTACIÓN DE UN MODELO DE APRENDIZAJE PROFUNDO PARA LA TRADUCCIÓN DEL LENGUAJE DE SEÑAS
9	ASENJO SAAVEDRA SEGUNDO VICTOR PAICO SANTOS PERLA PAOLA	EVALUACIÓN DE SOFTWARE DE UN LABORATORIO CLÍNICO BAJO LA NORMA ISO/IEC 25000 PARA ASEGURAR LA CALIDAD ÓPTIMA DEL SISTEMA
10	TARRILLO CHIRINOS ANGELA CAROLINA GUARNIZ PAREDES CARLOS ALONSO	DESARROLLO DE UN MÉTODO PARA DETECTAR PERSONAS ARMADASUTILIZANDO MACHINE LEARNING EN VIDEOVIGILANCIA
11	PISFIL SUGARAY ALBERTO ESTUARDO	IMPLEMENTACION DE MODELO DE SERVICIOS DE TI MEDIANTE ISO/IEC 20000 EN EMPRESAS DE DESARROLLO DE SOFTWARE
12	LEYVA CRUZ SILVANA YAOSKELLINEY VASQUEZ TORRES YAMIR	ALGORITMOS DE DATA MINING PARA PREDECIR LA DESERCIÓN Y DESAPROBACIÓN ESTUDIANTIL EN LA ENSEÑANZA Y APRENDIZAJE EN ENTORNOS VIRTUALES
13	ALBARRAN SALAZAR HARVY JEFFERSON DELGADO FARRO JAVIER MANUEL	EVALUACION DE ENFOQUES PARA LA OPTIMIZACIÓN DE PROYECTOS DE DESARROLLO DE SOFTWARE: CASO DE ESTUDIO EMPRESA SOFTCLOUD
14	DAMIAN DIAZ CESAR ALBERTO	IMPLEMENTACIÓN DE UNA APLICACIÓN WEB HÍBRIDA PARA LA INTEGRACIÓN DE DATOS EN LA MICRORED DE SALUD OLMOS, LAMBAYEQUE
15	DAVILA GONZALES GIOVANNY ALEXIS AYMA VELASQUEZ SEBASTIAN ALEJANDRO	MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN PARA MITIGAR EL IMPACTO NEGATIVO EN UNA PYME PERUANA
16	CHUMAN LLUEN DAGNER ANIBAL	DESARROLLO DE UNA APLICACIÓN MÓVIL BASADA EN MICROSERVICIOS PARA AGUILIZAR EL PROCESO DE VENTAS DE UN MINIMARKET
17	CALDERON PIZANGO FLAVIO CESAR CARRANZA MORALES JUAN TOMAS GERALD	IMPLEMENTACIÓN DE TECNOLOGIA BLOCKCHAIN PARA GESTIONAR LAS TRANSACCIONES DE PAGOS Y VENTAS EN UNA EMPRESA LAMBAYECANA

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N° 0758-2022/FIAU-USS

Pimentel, 05 de diciembre de 2022

INVESTIGACION II

	APELLIDOS	TESIS
1	CIRILO ESCUDERO FRANCK	COMPARACIÓN DE HERRAMIENTAS DE VIRTUALIZACIÓN DE SOFTWARE LIBRE PARA MEJORAR LA DISPONIBILIDAD DE LOS SERVICIOS DE RED EN UNA EMPRESA MICROFINANCIERA
2	MENDOZA HUANGAL WALTER MARTINEZ CASUSOL ENRIQUE VALENTIN	SISTEMA WEB PARA MEJORAR LA GESTIÓN DE ESTUDIO JURÍDICO UTILIZANDO WEB SCRAPING Y ARQUITECTURA DE MICRO SERVICIOS EN CLOUD COMPUTING
3	CASTRO FERNANDEZ IRVIN GREGORY	MODELO DE GESTIÓN DE RIESGOS PARA MEJORAR LA CONFIDENCIALIDAD DE PROYECTOS DE UNA EMPRESA DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN
	CAYACA CAJUSOL MARIA JUANA	DESARROLLO DE UN MÉTODO DE ADQUISICIÓN BASADO EN NORMAS INTERNACIONALES PARA LA MEJORA DEL PROCESO ADQUISITIVO DE SOFTWARE EN MYPES PERUANAS

APROBACION DE TEMA DE TESIS

	APELLIDOS	TESIS
1	BARRERA TORRES JORGE LUIS	GESTIÓN DEL SERVICIO BASADO EN ITIL V4 PARA EVALUAR LA CALIDAD DEL SOFTWARE DE RECAUDACIÓN DE AGUA POTABLE Y ALCANTARILLADO DE LA EPS JUCUSBAMBA EIRL

DR. VICTOR ALEXCI TUESTA MONTEZA
DECANO (E) FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
UNIVERSIDAD SEÑOR DE SIPÁN SAC.
CHICLAYO

DR. HALYN ALVAREZ VÁSQUEZ
SECRETARIO ACADÉMICO | FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
UNIVERSIDAD SEÑOR DE SIPÁN SAC.
CHICLAYO

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Cc: Interesado, Archivo

Anexo 02. ACTA DE APROBACIÓN DE ASESOR

USS	DIRECTIVA PARA EL DESARROLLO DE LOS CURSOS DE INVESTIGACIÓN Y TRABAJOS CONDUCENTES A TÍTULOS PROFESIONALES PREGRADO	Código:	PP2-DI.03
		Versión:	04
		Fecha:	06/11/2023
		Hoja:	1 de 140

Universidad Señor de Sipán

ACTA DE APROBACIÓN DEL ASESOR

Yo **Tuesta Monteza Víctor Alexci.** quien suscribe como asesor designado mediante Resolución de Facultad N° **0758-2022/FIAU-USS,** del proyecto de investigación titulado **APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO,** desarrollado por el(los) estudiante(s): **Farroñan Teran Nixon Paul,** del programa de estudios de **Ingeniería de Sistemas,** acredito haber revisado, ydeclaro expedito para que continue con el trámite pertinentes.

En virtud de lo antes mencionado, firman:

Tuesta Monteza Victor Alexci (Asesor)	DNI: 42722929	

Pimentel, 09 de octubre de 2024

Anexo 03. Autorización del Autor (ES) Licencia de Uso – Formato TI

	AUTORIZACIÓN DEL AUTOR (ES) (LICENCIA DE USO)	Código:	F1.PP2-PR.02
		Versión:	02
		Fecha:	18/04/2024
		Hoja:	1 de 1

Pimentel, 09 de octubre del 2024

Señores

Vicerrectorado de investigación

Universidad Señor de Sipán S.A.C

Presente. -

El suscrito:

FARROÑAN TERAN NIXON PAUL con DNI 70070528

En mí (nuestra) calidad de autor (es) exclusivo (s) del trabajo de investigación/tesis titulada: **APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO.** presentado y aprobado en el año 2023 como requisito para optar el título de Ingeniero de Sistema de la facultad de ingeniería, arquitectura y urbanismo de la escuela profesional de ingeniería de sistemas de posgrado, programa , Programa de estudios de ingeniería de sistemas, por medio del presente escrito autorizo (autorizamos) al Vicerrectorado de investigación de la Universidad Señor de Sipán para que, en desarrollo de la presente licencia de uso total, pueda ejercer sobre mi (nuestro) trabajo y muestre al mundo la producción intelectual de la Universidad representado en este trabajo de investigación/tesis, a través de la visibilidad de su contenido de la siguiente manera:

- Los usuarios pueden consultar el contenido de este trabajo de investigación a través del Repositorio Institucional en el portal web del Repositorio Institucional - https://repositorio.uss.edu.pe. así como de las redes de información del país y del exterior.
- Se permite la consulta, reproducción parcial, total o cambio de formato con fines de conservación, a losusuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de investigación/informe o tesis y a su autor.

De conformidad con la ley sobre el derecho de autor decreto legislativo N° 822. En efecto, la Universidad Señor de Sipán está en la obligación de respetar los derechos de autor, para lo cual tomará las medidas correspondientes para garantizar su observancia.

APELLIDOS Y NOMBRES	NÚMERO DE DOCUMENTO DE IDENTIDAD	FIRMA
FARROÑAN TERAN NIXON PAUL	DNI: 70070528	

Anexo 04. AUTORIZACIÓN PARA RECOJO DE INFORMACIÓN

IEST Público "UTCUBAMBA"

AUTORIZACIÓN PARA RECOJO DE INFORMACIÓN

BAGUA GRANDE, 11 de Julio de 2024

Quien suscribe:

Sr. Ing. Dr. Ever Cobba Terrones

Director General – INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO "UTCUBAMBA"

AUTORIZA: Permiso para recojo de información pertinente en función del proyecto de investigación, denominado: **APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO.**

Por el presente, suscribe, Sr. Ing. Dr. Ever Cobba Terrones, Director General – INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO "UTCUBAMBA", **AUTORIZO** al alumno: Nixon Paul Farroñan Teran, identificado con DNI N° 70070528, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipan S.A.C, con la finalidad de desarrollar su trabajo de investigación PARA PROYECTO DE TESIS denominado: **APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO**, al uso de dicha información que conforma el expediente técnico, así como hojas de memorias, cálculos entre otros como planos para efectos exclusivamente académicos de la elaboración de tesis, enunciada líneas arriba de quien solicita se garantice la absoluta confidencialidad de la información solicitada.

Atentamente.

MINISTERIO DE EDUCACIÓN I.E.S.T.P. "UTCUBAMBA" DIRECCIÓN GENERAL BAGUA GRANDE

Director General: Sr. Ing. Dr. Ever Cobba Terrones

Dirección: Jr. Las Delicias 380
E-mail: istputcubamba@hotmail.com
Telefono: 041 – 474438

Anexo 05. VALIDACIÓN DE JUICIO DE EXPERTO INSTRUMENTO DE INVESTIGACIÓN

FORMATO DE FICHA DE EXPERTOS.

VALIDACIÓN DE JUICIO DE EXPERTO
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:
APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO

Autor:

- Farroñan Teran Nixon Paul

Objetivo:
El objetivo del presente informe es someter a evaluación la presente metodología basada en la norma ISO/IEC 27001:2017 para mejorar los procesos de gestión de riesgos de tecnologías de la información en un instituto superior privado peruano.

I. DATOS GENERALES DEL EXPERTO
1.1. Apellidos y nombres del experto: Quinteros Gonzáles Hermes Marino
1.2. Grado Académico y Profesión: Magister - Ing. de Sistemas
1.3. Áreas de Experiencia Profesional: Implementador Lider ISO 27001
1.4. Institución donde labora: Gobierno Regional de Lambayeque.
1.5. Nombre del instrumento motivo de evaluación: Aplicación del estandar ISO 27001-2017.

II. VALIDACIÓN
Se utilizará los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - [250-400], **Regular -** [450-600], **Buena:** [650-800], **Muy Buena -** [850-1000]

ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE				BAJA				REGULAR				BUENA				MUY BUENA			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Está formulada con lenguaje apropiado																	X			
OBJETIVIDAD	Está expresada en conductas observables																		X		
ACTUALIDAD	Adecuada al avance de la gestión riegos de TI																	X			
ORGANIZACIÓN	Existe una organización lógica																		X		
SUFICIENCIA	Comprende los aspectos en cantidad y calidad																		X		
INTENCIONALIDAD	Adecuada para valorar la gestión de riesgos de TI en un instituto superior tecnológico privado																	X			
CONSISTENCIA	Basado en aspectos teóricos científicos																	X			
COHERENCIA	Entre cada uno de los pasos de la metodología																		X		
METODOLOGÍA	La estrategia responde al propósito de la investigación																		X		
PERTINENCIA	Es útil y adecuado para la investigación																			X	

VALORACIÓN: Muy Buena (885)

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Pimentel, 22 agosto del 2024.

Mag. Hermes M. Quinteros Gonzáles
CIP: 82142

FORMATO DE FICHA DE EXPERTOS.

VALIDACIÓN DE JUICIO DE EXPERTO
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:

APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO

Autor:

- Farroñan Teran Nixon Paul

Objetivo:

El objetivo del presente informe es someter a evaluación la presente metodología basada en la norma ISO/IEC 27001:2017 para mejorar los procesos de gestión de riesgos de tecnologías de la información en un instituto superior privado peruano.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: Guevara Vasquez Diego Martin
1.2. Grado Académico y Profesión: Ingeniero de Sistemas - CIP 338547
1.3. Áreas de Experiencia Profesional: Municipalidad de Comas, Gobierno Regional Lambayeque
1.4. Institución donde labora: Gobierno Regional Lambayeque
1.5. Nombre del instrumento motivo de evaluación: Aplicacion de Estandar ISO 27001-2017

II. VALIDACIÓN

Se utilizará los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - [250-400], **Regular -** [450-600], **Buena:** [650-800], **Muy Buena -** [850-1000]

ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE				BAJA				REGULAR				BUENA				MUY BUENA			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Está formulada con lenguaje apropiado																			X	
OBJETIVIDAD	Está expresada en conductas observables																		X		
ACTUALIDAD	Adecuada al avance de la gestión riegos de TI																	X			
ORGANIZACIÓN	Existe una organización lógica																		X		
SUFICIENCIA	Comprende los aspectos en cantidad y calidad																		X		
INTENCIONALIDAD	Adecuada para valorar la gestión de riesgos de TI en un instituto superior tecnológico privado																		X		
CONSISTENCIA	Basado en aspectos teóricos científicos																			X	
COHERENCIA	Entre cada uno de los pasos de la metodología																		X		
METODOLOGÌA	La estrategia responde al propósito de la investigación																		X		
PERTINENCIA	Es útil y adecuado para la investigación																			X	

VALORACIÓN: Muy Buena 90

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Pimentel, 22 agosto del 2024.

GOBIERNO REGIONAL LAMBAYEQUE
SEDE REGIONAL

Ing. Diego Martín Guevara Vásquez
Oficina de Organización y Tecnología de la Información (E)
CIP: 338542

FORMATO DE FICHA DE EXPERTOS.

VALIDACIÓN DE JUICIO DE EXPERTO
INSTRUMENTO DE INVESTIGACIÓN

Título de la investigación:

APLICACIÓN DEL ESTÁNDAR ISO 27001:2017 PARA MEJORAR EL PROCESO DE GESTIÓN DE RIESGOS TI EN UN INSTITUTO TECNOLÓGICO PÚBLICO PERUANO

Autor:

- Farroñan Teran Nixon Paul

Objetivo:

El objetivo del presente informe es someter a evaluación la presente metodología basada en la norma ISO/IEC 27001:2017 para mejorar los procesos de gestión de riesgos de tecnologías de la información en un instituto superior privado peruano.

I. DATOS GENERALES DEL EXPERTO

1.1. Apellidos y nombres del experto: ALTAMIRANO TAVARA JULIO CESAR

1.2. Grado Académico y Profesión: INGENIERO DE SISTEMAS — CIP 125736

1.3. Áreas de Experiencia Profesional: ADMINISTRACION DE LA RED

1.4. Institución donde labora: GOBIERNO REGIONAL DE CAJAMARCA

1.5. Nombre del instrumento motivo de evaluación: APLICACION DEL ESTANDAR ISO 27001 - 2017.

II. VALIDACIÓN

Se utilizará los siguientes indicadores y criterios para la evaluación del instrumento: CLARIDAD, OBJETIVIDAD, ACTUALIDAD, ORGANIZACIÓN, SUFICIENCIA, INTENCIONALIDAD, CONSISTENCIA, COHERENCIA, METODOLOGÌA, PERTINENCIA.

Valoración: Deficiente - [50-200], Baja - [250-400], **Regular -** [450-600], **Buena:** [650-800], **Muy Buena -** [850-1000]

ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE					BAJA			REGULAR				BUENA				MUY BUENA			
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Está formulada con lenguaje apropiado																			X	
OBJETIVIDAD	Está expresada en conductas observables																		X		
ACTUALIDAD	Adecuada al avance de la gestión riegos de TI																		X		
ORGANIZACIÓN	Existe una organización lógica																			X	
SUFICIENCIA	Comprende los aspectos en cantidad y calidad																		X		
INTENCIONALIDAD	Adecuada para valorar la gestión de riesgos de TI en un instituto superior tecnológico privado																			X	
CONSISTENCIA	Basado en aspectos teóricos científicos																			X	
COHERENCIA	Entre cada uno de los pasos de la metodología																		X		
METODOLOGÍA	La estrategia responde al propósito de la investigación																		X		
PERTINENCIA	Es útil y adecuado para la investigación																			X	

VALORACIÓN: MUY BUENO 925

OPINIÓN DE APLICABILIDAD: _____

Lugar y fecha: Pimentel, 22 agosto del 2024.

Ing. Julio Cesar Altamirano Tapiama

CIP : 125736

Anexo 06. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

IEST Público "UTCUBAMBA"

		CRITERIO		T	SI	NO
FORMULARIO PRELIMINAR PARA DIAGNÓSTICO						
(ISO 27001)						
POLÍTICAS DE SEGURIDAD						
> Existen documento(s) de políticas de seguridad de SI	☐ FALSO	0				
> Existe normativa relativa a la seguridad de los SI	☐ FALSO	0				
> Existen procedimientos relativos a la seguridad de SI	☑ VERDADERO	1				
> Existe un responsable de las políticas, normas y procedimientos	☐ FALSO	0				
> Existen mecanismos para la comunicación a los usuarios de las normas	☐ FALSO	0				
> Existen controles regulares para verificar la efectividad de las políticas	☐ FALSO	0			SI	NO
ORGANIZACIÓN DE LA SEGURIDAD		1			16,67	83,33
> Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☐ FALSO	0				
> Existe un responsable encargado de evaluar la adquisición y cambios de SI	☐ FALSO	0				
La Dirección y las áreas de la Organización participa en temas de seguridad	☐ FALSO	0				
> Existen condiciones contractuales de seguridad con terceros y outsourcing	☐ FALSO	0				
> Existen criterios de seguridad en el manejo de terceras partes	☑ VERDADERO	1				
> Existen programas de formación en seguridad para los empleados, clientes y terceros	☑ VERDADERO	1				
> Existe un acuerdo de confidencialidad de la información que se accesa.	☑ VERDADERO	1				
> Se revisa la organización de la seguridad periódicamente por una empresa externa	☐ FALSO	0			SI	NO

ADMINISTRACIÓN DE ACTIVOS		3		37,50	62,50	
> Existen un inventario de activos actualizado	☑ VERDADERO	1				
> El Inventario contiene activos de datos, software, equipos y servicios	☑ VERDADERO	1				
> Se dispone de una clasificación de la información según la criticidad de la misma	☑ VERDADERO	1				
> Existe un responsable de los activos	☑ VERDADERO	1				
> Existen procedimientos para clasificar la información	☐ FALSO	0				
> Existen procedimientos de etiquetado de la información	☑ VERDADERO	1		SI	NO	
SEGURIDAD DE LOS RRHH		5		83,33	16,67	
> Se tienen definidas responsabilidades y roles de seguridad	☐ FALSO	0				
> Se tiene en cuenta la seguridad en la selección y baja del personal	☐ FALSO	0				
> Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	☑ VERDADERO	1				
> Se imparte la formación adecuada de seguridad y tratamiento de activos	VERDADERO	1				
> Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	☐ FALSO	0				
> Se recogen los datos de los incidentes de forma detallada	FALSO	0				
> Informan los usuarios de las vulnerabilidades observadas o sospechadas	☑ VERDADERO	1				
> Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	☑ VERDADERO	1		SI	NO	
> Existe un proceso disciplinario de la seguridad de la información	☑ VERDADERO	1				
SEGURIDAD FÍSICA Y DEL AMBIENTE		5		55,56	44,44	
> Existe perímetro de seguridad física(una pared, puerta con llave).	☑ VERDADERO	1				
> Existen controles de entrada para protegerse frente al acceso de personal no autorizado	☑ VERDADERO	1				
> Un área segura ha de estar cerrada, aislada y protegida de eentos naturales	☑ VERDADERO	1				
> En las áreas seguras existen controles adicionales al personal propio y ajeno	☑ VERDADERO	1				
> Las áreas de carga y expedición están aisladas de las áreas de SI	☐ FALSO	0				
> La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	☐ FALSO	0				
> Existen protecciones frente a fallos en la alimentación eléctrica	VERDADERO	1				
> Existe seguridad en el cableado frente a daños e intercepciones	☐ FALSO	0				
> Se asegura la disponibilidad e integridad de todos los equipos	☐ FALSO	0				
> Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	☑ VERDADERO	1				
>Se incluye la seguridad en equipos moviles	☐ FALSO	0				

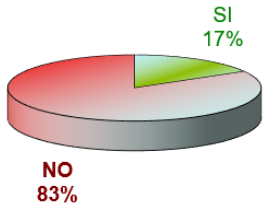
GESTIÓN DE COMUNICACIONES Y OPERACIONES		6		54,55	45,45	
> Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	FALSO	0				
> Estan establecidas responsabilidades para controlar los cambios en equipos	VERDADERO	1				
> Estan establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	VERDADERO	1				
> Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	VERDADERO	1				
> Existe una separación de los entornos de desarrollo y producción	VERDADERO	1				
> Existen contratistas externos para la gestión de los Sistemas de Información	VERDADERO	1				
> Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	VERDADERO	1				
> Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	VERDADERO	1				
> Controles contra software maligno	VERDADERO	1				
> Realizar copias de backup de la información esencial para el negocio	VERDADERO	1				
> Existen logs para las actividades realizadas por los operadores y administradores	VERDADERO	1				
> Existen logs de los fallos detectados	VERDADERO	1				
> Existen rastro de auditoría	FALSO	0				
> Existe algún control en las redes	FALSO	0				
> Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)	FALSO	0				
> Eliminación de los medios informáticos. Pueden disponer de información sensible	FALSO	0				
> Existe seguridad de la documentación de los Sistemas	VERDADERO	1				
> Existen acuerdos para intercambio de información y software	VERDADERO	1				
> Existen medidas de seguridad de los medios en el tránsito	VERDADERO	1				
> Existen medidas de seguridad en el comercio electrónico.	VERDADERO	1				
> Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	VERDADERO	1		SI	NO	
> Existen medidas de seguridad en las transacciones en linea	FALSO	0				
> Se monitorean las actividades relacionadas a la seguridad	FALSO	0				

CONTROL DE ACCESOS		16		80,00	20,00
> Existe una política de control de accesos	FALSO	0			
> Existe un procedimiento formal de registro y baja de accesos	FALSO	0			
> Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	FALSO	0			
> Existe una gestión de los password de usuarios	FALSO	0			
> Existe una revisión de los derechos de acceso de los usuarios	VERDADERO	1			
> Existe el uso del password	VERDADERO	1			
> Se protege el acceso de los equipos desatendidos	VERDADERO	1			
> Existen políticas de limpieza en el puesto de trabajo	VERDADERO	1			
> Existe una política de uso de los servicios de red	FALSO	0			
> Se asegura la ruta (path) desde el terminal al servicio	FALSO	0			
> Existe una autenticación de usuarios en conexiones externas	FALSO	0			
> Existe una autenticación de los nodos	FALSO	0			
> Existe un control de la conexión de redes	FALSO	0			
> Existe un control del routing de las redes	FALSO	0			
> Existe una identificación única de usuario y una automática de terminales	FALSO	0			
> Existen procedimientos de log-on al terminal	FALSO	0			
> Se ha incorporado medidas de seguridad a la computación móvil	FALSO	0			
> Está controlado el teletrabajo por la organización	FALSO	0		SI	NO
DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS		4		25,00	75,00
> Se asegura que la seguridad está implantada en los Sistemas de Información	VERDADERO	1			
> Existe seguridad en las aplicaciones	VERDADERO	1			
> Existen controles criptográficos.	VERDADERO	1			
> Existe seguridad en los ficheros de los sistemas	VERDADERO	1			
> Existe seguridad en los procesos de desarrollo, testing y soporte	VERDADERO	1		SI	NO
> Existen controles de seguridad para los resultados de los sistemas	FALSO	0			
> Existe la gestión de los cambios en los SO.	FALSO	0			
> Se controlan las vulnerabilidades de los equipos	VERDADERO	1		75,00	25,00

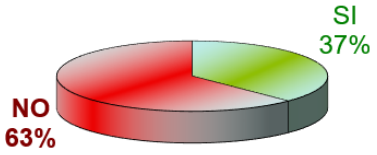
ADMINISTRACIÓN DE INCIDENTES		6			
> Se comunican los eventos de seguridad	☑ VERDADERO	1			
> Se comunican los debilidadesde seguridad	☑ VERDADERO	1			
> Existe definidas las responsabilidades antes un incidente.	☑ VERDADERO	1			
> Existe un procedimiento formal de respuesta	☑ VERDADERO	1			
> Existe la gestión de incidentes	☑ VERDADERO	1			
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		5		100,00	0,00
> Existen procesos para la gestión de la continuidad.	☐ FALSO	0			
> Existe un plan de continuidad del negocio y análisis de impacto	☐ FALSO	0			
> Existe un diseño, redacción e implantación de planes de continuidad	☐ FALSO	0			
> Existe un marco de planificación para la continuidad del negocio	☐ FALSO	0			
> Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	☐ FALSO	0		SI	NO
CUMPLIMIENTO		0		0,00	100,00
> Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	☑ VERDADERO	1			
> Existe el resguardo de la propiedad intelectual	☑ VERDADERO	1			
> Existe el resguardo de los registros de la organización	☑ VERDADERO	1			
> Existe una revisión de la política de seguridad y de la conformidad técnica	☐ FALSO	0			
> Existen consideraciones sobre las auditorías de los sistemas	☐ FALSO	0			
		3		60,00	40,00
		54	85		
		64	36		
		si	no		

POR ÁREAS

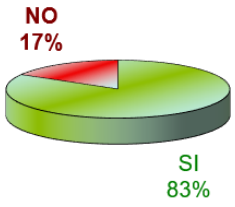
POLÍTICAS DE SEGURIDAD



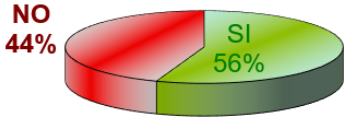
ORGANIZACIÓN DE LA SEGURIDAD

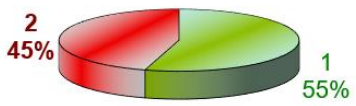
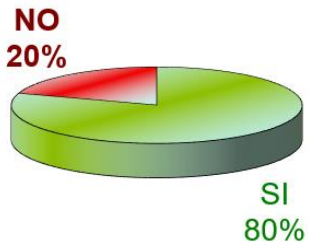
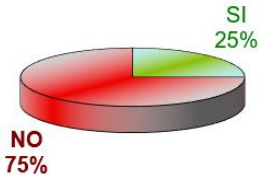
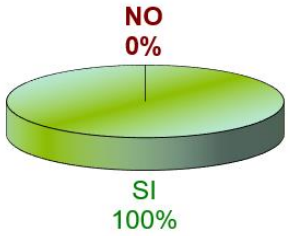
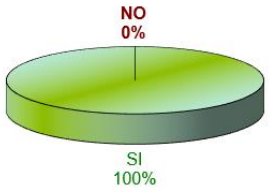
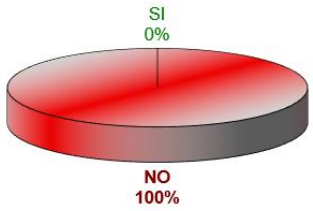
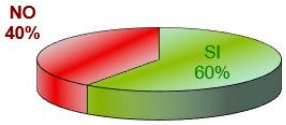


CLASIFICACIÓN Y CONTROL DE ACTIVOS

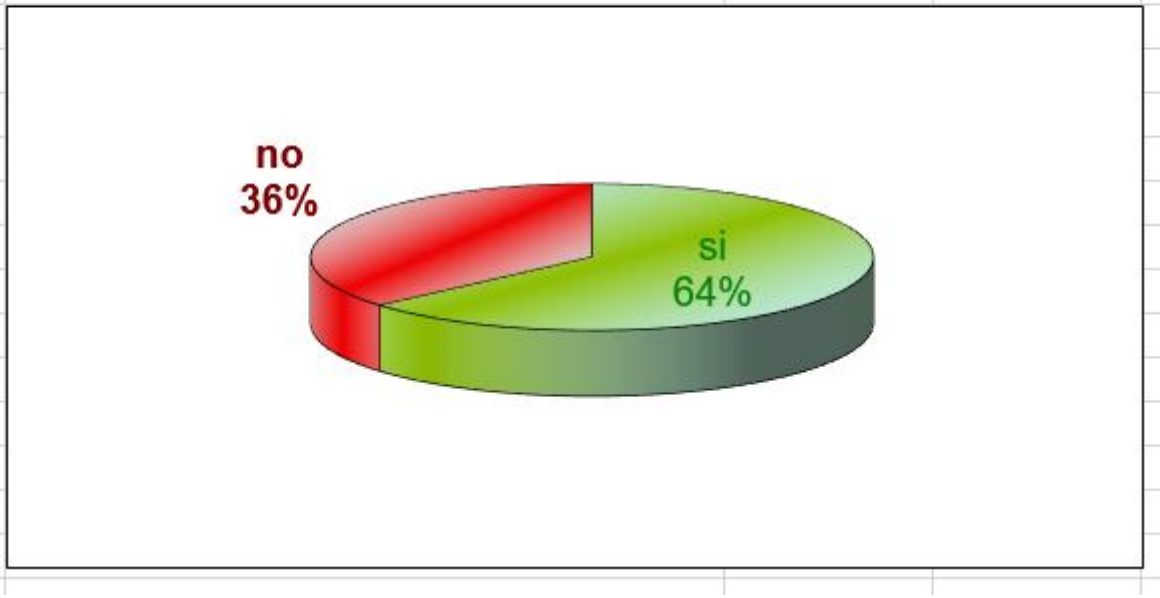


SEGURIDAD DEL PERSONAL

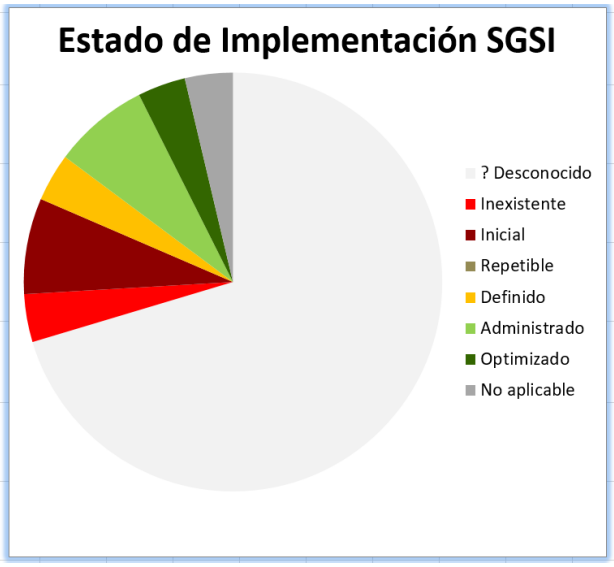


SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIÓN DE COMUNICACIONES Y OPERACIONES
	
CONTROL DE ACCESOS	**DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
	
ADM. DE INCIDENTES	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
	
CONFORMIDAD	
	

RESULTADOS AUTODIAGNÓSTICO GENERAL



Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	70%	97%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	4%	1%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	7%	0%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%	0%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	4%	0%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	7%	2%



Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	4%	0%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	4%	0%
	Total	100%	100%

Anexo 07. Detalle de los activos

Hardware

Item	Descripción	Marca	Modelo	Datos Técnicos	Cantidad	Estado	Ubicación
1	Computadora de Escritorio	LG	Case Slim Micro Atx Fuente 600/250 Gris/negro	Core i3 - G5ta- RAM 4GB - HD 500GB - SO Windows 10	24	Operativo	Lab PQ
2	Computadora de Escritorio	DELL	Case Slim Micro Atx Fuente 600/250 Gris/negro	Core i3 - G6ta- RAM 4GB - HD 500GB	38	Operativo	Lab GR
3	Computadora de Escritorio	HP	Case Slim Micro Atx Fuente 600/250 Gris/negro	Core i3 - G6ta- RAM 4GB - HD 500GB	14	Operativo	Lab Comunicaciones
4	Laptop	HP	240	Core™ i3 de 10.ª generación - 4 GB de RAM - HD 500GB	3	Operativo	Dirección Académica
5	Proyector Multimedia	Epson	EH-TW5820	2700 lúmenes ANSI - Resolución de imagen 1920 x 1080 píxeles, 16:9 - Tamaño de imagen 30 pulgadas – 300 pulgadas	12	Operativo	Distribuidos en el Instituto
6	Impresora	Epson	L575	Tecnología de inyección de tinta - Hasta 5760 x 1440 dpi de resolución	6	Operativo	Secretaria Académica, Dirección General, Coordinación Contabilidad, Coordinación Enfermería Técnica, Coordinación Producción Agropecuaria, Coordinación APSTI
7	Impresora	Epson	L365	EPSON Micropiezo punto variable Impresión a 4 colores (CMYK) - Hasta 5760 x 1440 dpi de resolución	2	Operativo	Dirección Académica, Almacen, etc

Red de Datos

Item	Descripción	Marca	Modelo	Datos Técnicos	Cantidad	Estado	Ubicación
1	Switch	D-Link	DES-1210-52	• Administrable • 48 puertos 10/100BASE-TX • 2 puertos 1000BASE-T • 2 Combo 10/100/1000BASE-T / 100/1000SFP	1	Operativo	Laboratorio 1
2	Switch	D-Link	DES-1210-52	• Administrable • 48 puertos 10/100BASE-TX • 2 puertos 1000BASE-T • 2 Combo 10/100/1000BASE-T / 100/1000SFP	1	Operativo	Laboratorio 2
3	Router	TPLINK	940N	Enlace WAN y LAN	3	Operativo	Oficina Administrativa
4	Puntos de red de datos	No especifica	No especifica	Cable Categoria 6A	250	Operativo	Distribuidos en el Instituto

Dirección de Red: 192.168.0.0
Mascara: 255.255.255.0
Puerta de enlace: 192.168.0.1
Intervalo de direcciones de host: 192.168.0.1 - 192.168.0.254

Software

Item	Descripción	Cantidad	Estado	Ubicación
1	Sistema Operativo W10	77	Operativo	Computadora de Escritorio y Laptop
2	Microsoft Office	77	Operativo	Computadora de Escritorio y Laptop
3	Antivirus ESET 32 Corporativo	1	Operativo	Servidor Local
4	Sistema de Gestión Académica Q10	1	Operativo	Servidor del Estado
5	Sistema de Gestión Académica Registra	1	Operativo	Servidor del Estado

Documentos Importantes

Item	Descripción	Cantidad	Ubicación
1	Contrato de prestación de servicios TI	1	Servidor local
2	Plan Operativo y Estratégico del IESTP	1	Servidor local
3	Política de uso de plataforma estudiantil	1	Servidor local
4	Política de uso de plataforma docente	1	Servidor local
5	Archivo de Selección de Personal Docente	1	Servidor local

Servicio internet

Proveedor:	Geral Explorer
Tipo:	Linea Comercial
Ancho de banda (Mbps)	80 mbps
Dirección de Red:	192.172.10.23
Mascara:	255.255.255.0
Puerta de enlace:	192.172.10.1

Router

Item	Marca	Modelo	Cantidad	Estado	Ubicación
1	Mikrotik	rb4011iGS+5Hac	1	Operativo	Dirección
2	Mikrotik	ccr2004-16g-2s+	2	bueno	Administración
3	Mikrotik	RB2011UIAS-RM	1	bueno	Administración

Anexo 08. Amenazas

Amenazas			
Item	**Descripción**	**Tipo**	**Crítico**
1	Falla de las computadoras de los laboratorios por virus, troyanos, spyware, Ransomware,	Incidencia tecnológica	Gestión de continuidad del negocio
2	Equipos de cómputo de tecnología desfasada.	Incidencia tecnológica	Gestión de continuidad del negocio
3	Equipos de cómputo con software desactualizado.	Incidencia tecnológica	Gestión de continuidad del negocio
4	Falla de las computadoras de administrativos por virus, troyanos, spyware, Ransomware,	Incidencia tecnológica	Gestión de continuidad del negocio
5	Copia de seguridad de datos no se restaura	Incidencia tecnológica	Gestión de continuidad del negocio
6	Robo de identidad.	Incidencia tecnológica	Gestión de continuidad del negocio
7	Falla el servicio de internet	Incidencia tecnológica	Gestión de continuidad del negocio
8	Ataques informáticos a Sistemas de Información (DDoS - Denegación de servicios,	Incidencia tecnológica	Gestión de continuidad del negocio
9	No existe procesos para la gestión de continuidad de los servicios informáticos.	Incidencia tecnológica	Gestión de continuidad del negocio
10	No existe un plan de continuidad de los servicios informáticos.	Incidencia tecnológica	Gestión de continuidad del negocio
11	El personal no realiza testeo de seguridad informática.	Incidente Humano	Gestión de continuidad del negocio
12	No se contrata a terceros o empresas para realizar testeo de seguridad informática.	Incidente Humano	Gestión de continuidad del negocio
13	Sin copias de backup de la información esencial para el negocio.	Incidente Humano	Gestión de continuidad del negocio
14	Sismo	Incidente Natural	Gestión de continuidad del negocio
15	Inundación o aniego en el centro de datos.	Incidente Natural	Gestión de continuidad del negocio
16	Incendio en el centro de datos.	Incidente Natural	Gestión de continuidad del negocio
17	Pandemia y/o epidemia	Incidencia ambiental	Gestión de continuidad del negocio
18	No tener políticas de seguridad.	Incidente Humano	Politicas de Seguridad
19	No contar con normativas de seguridad.	Incidente Humano	Politicas de Seguridad
20	No contar con responsables de políticas y normativas de seguridad.	Incidente Humano	Politicas de Seguridad
21	No contar con mecanismos de comunicación.	Incidente Humano	Politicas de Seguridad
22	No se administra las cuentas y claves de los usuarios de los sistemas de información.	Incidente Humano	Control de acceso
23	Sin niveles de seguridad de acceso a la red informática del IESTP.	Incidencia tecnológica	Control de acceso
24	Sin control de autenticación de usuarios a la red.	Incidencia tecnológica	Control de acceso
25	No existe procedimientos para logearse a un terminal.	Incidencia tecnológica	Control de acceso

Item	Descripción	Tipo	Crítico
26	No existe control del teletrabajo.	Incidencia tecnológica	Control de acceso
27	No existe control de acceso a la red desde el movil.	Incidencia tecnológica	Control de acceso
28	Sin acuerdos de confidencialidad de la información.	Incidente Humano	No
29	Sin medidas de seguridad en el comercio electrónico.	Incidencia tecnológica	No
30	No existe roles y responsabilidades definidos para las personas implicadas en la seguridad del IESTP?	Incidencia tecnológica	No
31	No existe un responsable encargado de evaluar la adquisición y cambios de S.I en el IESTP	Incidencia tecnológica	No
32	Personal técnico no está capacitado en cursos especializados de segurdad informática.	Incidencia tecnológica	No
33	No participan en temas de seguridad informática.	Incidente Humano	No
34	Sin registro de proveedores de servicios y equipos informáticos.	Incidencia tecnológica	No
35	Inventario de activos desactualizados.	Incidente Humano	No
36	No tener responsables de los activos.	Incidente Humano	No
37	No tener la información organizada.	Incidente Humano	No
38	Daños físicos al equipamiento.	Incidente Humano	No
39	No tener un canal y procedimientos claros a seguir en caso de incidente de seguridad.	Incidente Humano	No
40	No registrar los incidentes.	Incidente Humano	No
41	No Informar a los usuarios de las vulnerabilidades observadas o sospechadas.	Incidente Humano	No
42	No contar con perímetro de seguridad física.	Incidente Humano	No
43	No contar con controles de entrada para protegerse frente al acceso de personal no autorizado.	Incidente Humano	No
44	Equipos de cómputo mal distribuidos que no minimizan los accesos innecesarios.	Incidente Humano	No
45	Sin proteccion frente a fallos en la alimentación eléctrica.	Incidencia tecnológica	No
46	No se asegura la disponibilidad e integridad de todos los equipos.	Incidente Humano	No
47	Sin seguridad para los equipos retirados o ubicados exteriormente del IESTP.	Incidente Humano	No
48	Sin procedimientos operativos identificados del IESTP.	Incidente Humano	No
49	Sin algún método para reducir el mal uso accidental o deliberado de los Sistemas en el IESTP.	Incidente Humano	No
50	Sin criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas	Incidente Humano	No

Item	Descripción	Tipo	Crítico
51	No contar con controles contra software maligno.	Incidente Humano	No
52	Cuentas de usuarios de los sistemas de información habilitados de personal que ya	Incidencia tecnológica	No
53	Sin registros de Logs.	Incidente Humano	No
54	No realizar auditorias de tecnologías de la información.	Incidente Humano	No
55	No existe un control de usuarios a la red informática del IESTP.	Incidente Humano	No
56	Sin seguridad la documentación de los sistemas.	Incidencia tecnológica	No