UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

GESTIÓN DEL RIESGO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN CON LA METODOLOGÍA MAGERIT EN EL INSTITUTO TECNOLÓGICO DEL ORIENTE DE TINGO MARÍA

Tesis

Para optar el título de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

PRESENTADO POR:

PAUL KEVIN RAMIREZ PORTOCARRERO

Tingo María – Perú

2021

Universidad Nacional Agraria de la Selva Facultad de Ingeniería en Informática y Sistemas	**ACTA DE SUSTENTACIÓN DE TESIS N.º 04-2021**	**COMISION DE GRADOS Y TITULOS** **Fecha:** 18/noviembre/2021

PARTE 1. FASE INICIAL

Siendo las **19:00 horas del día 19 de noviembre de 2021**; en la Sala Virtual MS-Teams de la FIIS, se instala el jurado calificador conformado por:

Jurado 1: Dr. Walter Rubén BERNUY BLANCO (Presidente)

Jurado 2: Ing. Pedro Crisólogo TRUJILLO NATIVIDAD

Jurado 3: Ing. Gregorio VÁSQUEZ PINEDO

Oficializado mediante **RESOLUCIÓN N° 065-2021-D-FIIS-UNAS** del 23 de agosto de 2021, para el proceso de sustentación del informe final de Tesis del bachiller **Paul Kevin RAMIREZ PORTOCARRERO,** titulado: **"GESTIÓN DEL RIESGO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN CON LA METODOLOGÍA MAGERIT EN EL INSTITUTO TECNOLÓGICO DEL ORIENTE DE TINGO MARIA".** ASESOR: **Ing. Edwin Jesús Vega Ventocilla.**

Se manifiesta que el bachiller cumple con los requisitos exigidos de Ley y se le invita a disertar su Tesis por espacio de 30 minutos, asimismo se dispondrá de igual tiempo para la absolver preguntas y sugerencias.

PARTE 2. FASE DE PREGUNTAS Y RESULTADO

Culminada la exposición se inicia la fase de preguntas por parte del jurado calificador; también se invita a los asistentes a formular preguntas sobre el tema de Tesis.

Absueltas todas las peticiones, el jurado calificador procede a deliberar en privado la calificación y resultado.

Concluida la deliberación y en presencia del público, el jurado calificador anuncia que el resultado de la Sustentación de Tesis es: APROBADO POR UNANIMIDAD.

(NOTA: consignar una de la siguientes: DESAPROBADO, APROBADO POR MAYORIA o APROBADO POR UNANIMIDAD)

Con calificativo de: BUENO (14).

(NOTA: consignar una de la siguientes: EXCELENTE, MUY BUENO, BUENO, DEFICIENTE, MUY DEFICIENTE)

Por lo que se comunicará a las instancias correspondientes para el trámite respectivo.

PARTE 3. CONFORMIDAD

De todo lo mencionado se firma al pie en señal de conformidad, siendo las 20:37 horas se da por finalizada la ceremonia de Sustentación de Tesis.

Firma: 	Firma: 	Firma: 
Jurado 1: Walter R. Bernuy Blanco	**Jurado 2:** Pedro C. Trujillo Natividad	**Jurado 3:** Gregorio Vasquez Pinedo
Firma: 	Firma:	
Sustentante: Paul Kevin Ramirez Portocarrero	**Asesor:** Edwin Jesús Vega Ventocilla	

UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

GESTIÓN DEL RIESGO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN CON LA METODOLOGÍA MAGERIT EN EL INSTITUTO TECNOLÓGICO DEL ORIENTE DE TINGO MARÍA

Autor	:	Ramírez Portocarrero, Paul Kevin
Asesor de Tesis	:	Vega Ventocilla, Edwin Jesús

Programa de Investigación	:	Tecnologías de Información (TI)
Grupo de Investigación	:	Redes, Seguridad y Gestión de TI
Línea(s) de Investigación	:	Gestión de Tecnologías de Información
Eje temático de Investigación	:	Gestión del riesgo en TICS a través de la Metodología MAGERIT
Lugar de ejecución	:	Instituto Tecnológico del Oriente de Tingo María
Duración		Diciembre del 2019 a noviembre del 2020
Financiamiento	:	Recursos propios S/. 4,500.00

Tingo María – Perú. 2021

ÍNDICE

Página.

ÍNDICE DE TABLAS

Tabla Página.

ÍNDICE DE FIGURAS

Figura Página.

ÍNDICE DE ANEXOS

Anexo Página.

RESUMEN

Tan importante que las empresas o instituciones se actualicen con tecnologías de punta para operar sus actividades en el mercado, es gestionar su riesgo, en ese contexto las instituciones tienen que adecuarse o asumir costos como la reputación y pérdida de información crucial para su sostenibilidad, de ahí la importancia de "determinar si con la implementación de la metodología MAGERIT como estrategia en los controles de seguridad mejora significativamente la gestión del riesgo de las TIC en el Instituto Tecnológico del Oriente de Tingo María". El estudio es experimental con diseño pre experimental, se empleó el método MAGERIT a través del software PilarBasic en su versión 7.4.3, se experimentó los procedimientos de identificar, analizar el riesgo y tratamiento del riesgo, eso permitió identificar el riesgo con y sin salvaguardas (activos con riesgo potencial 48%, identificado el riesgo potencial PilarBasic nos presenta el riesgo objetivo máximo a alcanzar que en este caso es del 35%, aplicando las salvaguardas sugeridas por el PilarBasic y contrastando con la evidencia de campo se llega a un riesgo aceptable del 16%), identificar los riesgos por cada dimensión (disponibilidad (13%), integridad (18%), confidencialidad (16%), autenticidad (15%), trazabilidad (18%), datos personales (17%)); el diagnóstico inicial se encuentra un nivel de madurez del 41% y aplicando salvaguardas se ubica en 87%; se recomienda a la institución continuar con la metodología como un plan de mejora continua en salvaguarda de los activos de la institución.

Palabras clave: integridad, disponibilidad, confidencialidad, autenticidad, trazabilidad.

ABSTRACT

It is so important that companies or institutions are updated with cutting-edge technologies to operate their activities in the market, it is to manage their risk, in this context the institutions have to adapt or otherwise assume costs such as reputation and loss of crucial information for their sustainability, hence the importance of "determining whether with the implementation of the MAGERIT methodology as a strategy in ICT security controls, risk management improves significantly at the Instituto Tecnológico del Oriente de Tingo María". For this, an experimental study with a quasi-experimental design was carried out, applying the MAGERIT methodology through the PilarBasic software in its version 7.4.3, the procedures of Identifying the risks, Analyzing the risks and treating the risks were experimented, that allowed to identify the risks risks with and without safeguards (assets with potential risk 57%, identified the potential risk PilarBasic presents us with the maximum target risk to be achieved, which in this case is 24%, applying the safeguards suggested by PilarBasic and contrasting with the field evidence is reaches an acceptable risk of 19%), identify the risks for each dimension (availability (13%), integrity (18%), confidentiality (16%), authenticity (15%), traceability (18%), personal data (17%)); Therefore, the institution is recommended to continue with the methodology as a continuous improvement plan to safeguard the institution's assets.

Keywords: integrity, availability, confidentiality, authenticity, traceability.

I. INTRODUCCIÓN

1.1 MARCO REFERENCIAL DEL PROBLEMA:

La Gestión del Riesgo de las TIC proporciona las condiciones básicas mínimas para proteger los datos de una organización. En un mundo competitivo donde predomina lo virtual exige tomar previsiones y en ese contexto la metodología MAGERIT propone un diagnóstico identificando los activos, evalúa el impacto del riesgo y propone mediante la ISO/IEC 27002:2013 las salvaguardas necesarias para proteger la información, dando cumplimiento a la Ley 29733 de protección de datos, de esa manera se convierte en un apoyo para la Gestión de la Seguridad de las Tecnologías de la Información en su dimensión de disponibilidad, integridad de los datos, confidencialidad de la información, autenticidad, trazabilidad y datos personales.

Según Ferruzola et al. (2019) los seguros al patrimonio pueden devolverte los bienes físicos, pero no el daño moral o la información, perjudicando la imagen de la Institución, ante ello se plantea "Determinar si con la implementación de la metodología MAGERIT como estrategia en los controles de seguridad la Gestión del riesgo de las TIC mejora significativamente en el Instituto Tecnológico del Oriente de Tingo María".

En ese sentido se buscó determinar si con la implementación de la metodología MAGERIT como estrategia en la gestión del riesgo de las TIC en el ISTO de Tingo María mejora significativamente, con ese fin se recurrió a la teoría general de sistemas, teoría de la información, la metodología MAGERIT y la norma técnica Peruana NTP-ISO/IEC 27001-2013, en el capítulo III, describe los resultados a los que siguiendo la metodología MAGERIT y a través de la aplicación del software PilarBasic se experimentó los procedimientos para analizar los riesgos y tratamiento de las inseguridades, eso permitió identificar los riesgos con y sin salvaguardas (activos con riesgo potencial 48%), identificado el riesgo potencial PilarBasic nos presenta el riesgo objetivo máximo a alcanzar que en este caso es del 35%, aplicando las salvaguardas sugeridas por el PilarBasic y contrastando con la evidencia de campo se llega a un riesgo aceptable del 16%), identificar los riesgos por cada dimensión (disponibilidad (13%), integridad (18%), confidencialidad (16%), autenticidad (15%), trazabilidad (18%), datos personales (17%)); siendo el siguiente paso encontrar el nivel de madurez determinado por control según la ISO: 27002:2013, de igual manera se determina un antes (41%) y un después (87%) del nivel de madurez aplicando las

salvaguardas, para ello se basó el proceso seguido en los trabajos de Ortiz (2018), Sandoval (2017) y Guevara (2015).

Las organizaciones necesitan planear, organizar y controlar sus actividades, para ello se emplea la tecnología en la búsqueda de la eficiencia y eficacia en la información a obtener, de esta manera la empresa se beneficie, facilitando la toma de decisiones (Chiavenato, 2001). Estos cambios estructurales no solo competen al ámbito industrial sino también al de servicios como la educación, porque ambos cuentan con clientes internos y externos, saber ser competitivos para mantenerse en un mercado que valora la importancia de las Tecnologías de la Información es crucial para su subsistencia, debe cumplir estándares mínimos que exige la sociedad o las instituciones gubernamentales es así que se considera como valor crítico dentro de las organizaciones para su éxito y supervivencia la administración eficiente de la información que posee y de la Tecnología de Información (TI) relacionada a ella por lo que es necesario adaptar un sistema de Gestión del riesgo orientado a proteger no solo la información sino todos los elementos descritos.

Dentro de los principales problemas generalizados sobre el uso de la TI en las empresas según Edutópica (2017, pp. 1-2) son:

1. La creencia que todo es un problema de implementación TI: creer que la solución a todos los problemas que nos rodea está en la tecnología.
2. El poco o nulo conocimiento frente al uso de la TI: Esta circunstancia puede ser peligrosa si pensamos que no tenemos, en muchos casos, información de la seguridad en la red.
3. El mal uso de la TI: desconocimiento del uso de la herramienta hace que las personas sigan haciendo lo mismo con artefactos distintos.
4. El poco acceso y uso de las TI: las limitaciones de uso en vez de potenciar hacen que se pierdan recursos económicos y horas productivas.
5. La dependencia tecnológica: El concepto de comunidad ha cambiado, el concepto de socialización se ha transformado, el modo de hacer negocio ha cambiado.
6. La relación tácita entre tecnología y ocio: No generar espacios de enseñanza-aprendizaje a través de las redes sociales para potenciar su uso y oportunidades de negocio.

7. La creencia que las TI reemplazan al recurso humano: Las TI en todos los campos laborales presentan retos que debemos aceptar y superar para ello el personal debe contar con la debida capacitación.

De lo descrito, el conjunto de recursos a generar a través de las TIC ayuda a la empresa a ser más eficiente frente a la competencia, pero para ello se necesita capacitar al personal, planear las actividades en un cambio organizacional lo que requiere de un trabajo conjunto dentro de la empresa (Oliveros y Martínez, 2017), porque son usadas indistintamente por empresas privadas o públicas, empresas que brindan servicios o industriales, por lo tanto trabajan bajo un marco de negocio que necesita ser Administrado y a su vez permita Gestionar las Tecnologías de la Información (TI) a fin de mejorar sus protocolos dentro de la empresa facilitando su uso al cliente interno y externo bajo parámetros de seguridad y productividad pero al mismo tiempo permita evaluar o auditar sus protocolos y el estado en que estas se encuentran.

Dentro del Instituto Superior Tecnológico del Oriente con fines de licenciamiento cuenta con TIC como parte de requerimiento del Ministerio de Educación para su licenciamiento, pero no es suficiente tener un Plan Estratégico de Tecnologías de la Información sino que se requiere Gestionar y evaluar adecuadamente para minimizar riesgos a corto y largo plazo de tal manera que lo construido y adquirido este Alineado, Planificado y Organizado, en función a los requerimientos normativos de los entes supervisores pero también sea eficiente para poder Entregar, dar servicio y soporte a sus usuarios internos y externos, de lo contrario se corre el riesgo de perder competitividad en el negocio, de ahí que se haya detectado los mismos problemas generalizados descritos anteriormente en el Instituto Superior Tecnológico del Oriente, al aplicar una tabla de cotejo contenidas en el Control de actividades.

Según Liras (2013) hace referencia que el fin en la gestión o administración de la garantía en la protección de la información que posee la empresa es proteger las tres bases fundamentales de la información: La Confidencialidad, Disponibilidad y la Integridad, y que evaluar los activos de las TIC determina la ruta y salvaguardas y controles a aplicar y que "la adopción de un determinado control puede afectar positiva o negativamente las otras dimensiones" (p. 6). De ahí la importancia de la Gestión del Riesgo de las TIC como parte de la protección de la información cuyo objetivo principal es, identificar, analizar y

cuantificar los riesgos en las TIC, en ese sentido Acevedo y Satizábal (2016) indican que el análisis del riesgo dentro de las organizaciones proyecta un panorama de la situación en que se encuentra y que actividades hacer para proteger las TIC, y el modelo que adopte tendrá un impacto en sus actividades.

Por otro lado se entiende como Gestión del Riesgo, según el Instituto Colombiano de Normas Técnicas y Certificación como: al conjunto coordinado de actividades para conducir y gobernar una institución con respecto a la inseguridad en la información (International Organization of Standarization, 2011) a su vez la ISO/IEC 27005:2011 señala que como parte en la evolución de la gestión del riesgo entre ellos los procedimientos y prácticas de la aplicación sistemática de políticas dentro de la organización y el contexto donde se desenvuelve, esto le permite identificar para luego analizar y evaluar aplicando las salvaguardas respectivas y seguimiento en la revisión de los riesgos identificados (Columba, 2016) se entiende entonces que para el éxito de la gestión del riesgo esta debe ser debidamente planificado a fin que se llegue a los objetivos propuestos en su evaluación, uno de estos instrumentos que ayuda al progreso en la Dirección del Riesgo de las Tecnologías de Información de la Comunicación es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información denominado (MAGERIT), mediante esta metodología es factible desarrollar políticas claras que permitan gestionar el riesgo con técnicas aplicadas a la información dentro de la institución u organización. MAGERIT se circunscribe a un marco de cumplimiento regulatorio (ISO 27001 y 31000) siendo la ISO 27001 la que gestiona el riesgo en la seguridad informática y la ISO 31000 lo realiza de forma integral, esta evaluación ayuda a incrementar valor al área de TI dentro de una organización. Actualmente MAGERIT ha institucionalizado una visión holística hacia el gobierno corporativo sea esta naturaleza pública o privada, pero se adapta muy bien a pequeñas empresas o instituciones que cuenten con información sensible en cuanto a garantía de la información y que utilizan de forma intensiva las tecnologías para cumplir sus propósitos. (Ministerio de Hacienda y Administraciones Públicas, 2012a).

En el caso del Perú MAGERIT permite compatibilizar la Norma Técnica ISO 27001:2013 en lo que corresponde a la seguridad informática y garantía de la información identificando los peligros asociados con la pérdida de la disponibilidad, integridad y confidencialidad (Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI, 2014), a su vez es necesario tener en cuenta que el nivel de

riesgo está en función a la posibilidad de ocurrencia y la conmoción que generaría en la organización si esta sucede.

Bajo lo expuesto es necesario que en el Instituto Superior Tecnológico del Oriente se evalúe la Gestión del Riesgo de las TIC a fin de que pueda diagnosticar su situación actual, analizar los riesgos asociados, adoptar salvaguardas y valorar en términos cualitativos el costo asociado para afrontar y brindar seguridad de sus activos en Tecnologías de las Información y Comunicación a sus clientes internos y externos involucrados institucionalmente y poder afrontar con solvencia el proceso de Licenciamiento iniciado por el Ministerio de Educación del Perú y la Ley No. 29733, ley de Protección de datos personales.

1.2 FORMULACIÓN DEL PROBLEMA

1.2.1 Interrogante general

¿La implementación de la metodología MAGERIT como estrategia en los controles de seguridad de las TIC mejoraría significativamente la Gestión del Riesgo en el Instituto Tecnológico del Oriente de Tingo María?

1.2.2 Interrogantes específicas

1. ¿Qué activos de las TIC que posee el ISTO de Tingo María, se encuentran bajo riesgo según la metodología MAGERIT?
2. ¿Cuál es la caracterización de los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT?
3. ¿Cuál es el resultado de la cuantificación cualitativa del impacto de los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT?

1.3 PLANTEAMIENTO DE LOS OBJETIVOS

1.3.1 Objetivo general

Determinar si con la implementación de la metodología MAGERIT como estrategia en los controles de seguridad de las TIC la gestión del riesgo mejora significativamente en el Instituto Tecnológico del Oriente de Tingo María.

1.3.2 Objetivo específico

1. Identificar los activos de las TIC que posee el ISTO Tingo María con la metodología MAGERIT.
2. Determinar los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT.
3. Determinar cualitativamente el impacto de los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT.

1.4 HIPÓTESIS

1.4.1 General

La metodología MAGERIT tiene una relación positiva con la Gestión del riesgo de la TIC del ISTO de Tingo María.

1.4.2 Específicos

1. El riesgo identificado en los activos de las TIC que posee el ISTO Tingo María con la metodología MAGERIT, es bajo.
2. El riesgo analizado sobre los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, es subsanable a corto tiempo.
3. El impacto del riesgo cualitativo identificado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, es bajo.

1.4.3 Sistema de variables, dimensiones e indicadores

Variables	*Dimensiones*	*Indicadores*	*Escala de medición*	*Instrumento*
La metodología MAGERIT	**Planeación del examen y la administración de riesgos**	Programa por aplicar (planificación de actividades)	Nominal	Lista de cotejo observacional y revisión documentaria
	Examen de riesgos	Describir los activos Describir las amenazas Describir las salvaguardas Estimar el estado de riesgo	Nominal	
	Gestión de riesgos.	10. Muy alta 9. Alta 6-8. Media 3-5. Baja	Ordinal	

		1-2. Muy baja		
	Selección de salvaguardias.	5. Optimizado. 4. Gestionado 3. Proceso definido 2. Reproducible 1. Inicial 0. Inexistente		
Gestión del riesgo de las TIC.	***Identificar los activos***	➢ Tipo de activos ➢ Dependencia entre activos ➢ Valorar los activos	Nominal	Lista de cotejo observacional y revisión documentaria
	Determinar los riesgos	Números de amenazas Número de vulnerabilidad Probabilidad de ocurrencia % Riesgo potencial %	Nominal Nominal Ordinal Ordinal	
	Evaluar los riesgos	Valoración estimada cualitativamente	Nominal	

1.4.4 Definición operaciones de variables, dimensiones e indicadores

Tabla 1. Definición de la operacionalización de las variables

Variables/definición operacional	***Dimensiones/definición operacional***	***indicadores/definición operacional***	
Metodología MAGERIT: Según la norma técnica española: La Gestión de Riesgos sigue un proceso de implementación regido en parámetros de trabajo para facilitar la toma de decisiones sin perder de vista los peligros que conlleva la aplicación de técnicas para recabar información en las organizaciones. (Ministerio de Hacienda y Administraciones Públicas de España, 2012ª, p. 7)	**Planeación**: Actividades preliminares a desarrollar en el proceso del análisis de riesgos (Ministerio de Hacienda y Administraciones Públicas de España, 2012a)	Programa por aplicar	Plan de entrevista Calendario de actividades Comunicación del resultado
	Examen de riesgos: Diferenciar cada uno de los elementos que contribuyen a generar peligro y valorar el impacto. (Ministerio de Hacienda y Administraciones Públicas de España, 2012a)	Característica de los activos.	Este proceso identifica cuales son los elementos relevantes dentro de los activos del sistema para evaluar, describir y a la vez identificar la interrelación de cada uno de ellos lo que permite determinar la dimensión dentro de la seguridad en función a su importancia y valor. (Ministerio de Hacienda y Administraciones Públicas de España, 2012a, p. 36).
		Característica de la amenaza	Proceso que identifica que riesgo es importante los analiza y los prioriza por la

		posibilidad que ocurra y afecte el activo si llega a ocurrir. (Ministerio de Hacienda y Administraciones Públicas de España, 2012a, p. 36).
	Característica de salvaguardas	Identificado las amenazas y analizado estas se debe aplicar las salvaguardas para mitigar su efecto. (Ministerio de Hacienda y Administraciones Públicas de España, 2012a, p. 36).
	Estimación del estado de riesgo	Actividad que muestra el riesgo y la situación en que se encuentra expuesta, estima el efecto y el peligro. Presenta el reporte de insuficiencia, deficiencia o flaquezas en la protección del sistema, después de procesar los datos consolidados de las actividades precedentes.(Ministerio de Hacienda y Administraciones Públicas de España, 2012a, p. 37).
Gestión de riesgos: Identificar las salvaguardias potenciales, una vez detectado reducirlas.(Ministerio de Hacienda y Administraciones Públicas, 2012a)	10. Muy alta	Criterio definido como: daño extremadamente grave.
	9. Alta	Criterio definido como: daño muy grave.
	6-8. Media	Criterio definido como: daño importante.
	3-5. Baja	Criterio definido: daño menor.
	1-2. Muy baja	Criterio definido: intrascendente desde la praxis (Ministerio de Hacienda y Administraciones Públicas, 2012b, p. 19).
Selección de salvaguardias: Proceso para seleccionar contramedidas a aplicar o implementarse, diseñando un enfoque para la aplicación de las salvaguardias seleccionadas. (Ministerio de Hacienda y Administraciones Públicas, 2012a).	L5. Muy raro que ocurra.	Existe deficiencia o vacíos en el rendimiento identificado durante la prueba de análisis (Capability Maturity Model Institute, 2013, p. 30).
	L4. Poco probable que ocurra.	Se sigue una metodología establecida a través de fuentes estadísticas u otras técnicas cuantitativas, y para la información prospectiva se hace uso de estas (Capability Maturity Model Institute, 2013, p. 29).
	L3. Es posible que ocurra.	La organización a través de las TIC tiene establecido los propósitos, input, criterios del input, output y criterios del output de la información, así como los procesos de verificación de las

			actividades y responsabilidades (Capability Maturity Model Institute, 2013, p. 29).
		L2. Muy alto la posibilidad que ocurra.	La organización además de capacitar a las personas en sus responsabilidades durante el proceso, los servicios recursos que recibe de los proveedores son los adecuados para la organización (Capability Maturity Model Institute, 2013, p. 28).
		L1. Casi seguro que ocurra.	El entorno al soporte de los procesos en que se desarrolla la organización no es el adecuado o estable (Capability Maturity Model Institute, 2013, p. 27). Fuente: (Capability Maturity Model Institute, 2013, p. 23-26).
Gestión del riesgo de las TIC: (dependiente) "La Gestión del riesgo típicamente incluye la evaluación del riesgo, el tratamiento de riesgos, la aceptación del riesgo y la comunicación de los riesgos" (Columba, 2016, p. 14).	***Identificar riesgos*** "proceso de encontrar, reconocer y describir los riesgos" (Columba, 2016, p. 17).	Tipo de activo	Activos esenciales (información, servicios) Servicios internos Equipamiento informático El entorno Servicios subcontratados a terceros Instalaciones físicas Personal (Ministerio de Hacienda y Administraciones Públicas, 2012b, p. 7).
		Tipo de amenaza	**Amenaza:** Causa potencial de una eventualidad que causaría perjuicios a un sistema de informes o a una empresa o institución. [UNE 71504:2008]" (Ministerio de Hacienda y Administraciones Públicas, 2012b, p. 97).
		Tipo de vulnerabilidad	**Vulnerabilidad:** "Desperfecto o falla en su diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza" (Ministerio de Hacienda y Administraciones Públicas, 2012b, p. 105).
		Probabilidad de ocurrencia	**Impacto:** Si se materializa la amenaza la organización asume las consecuencias (Ministerio de Hacienda y Administraciones Públicas, 2012b, p. 101).
		Riesgo potencial	**Riesgo residual:** Riesgo que subsiste en el sistema después de aplicar salvaguardas al
	Analizar los peligros "Proceso para comprender la naturaleza de un riesgo y determinar el nivel de riesgo" (Columba, 2016, p. 17)	"Riesgos potenciales. Los riesgos del sistema de información en la hipótesis de que no hubiera salvaguardas presentes. [UNE 71504:2008]" (Ministerio de Hacienda y Administraciones Públicas, 2012b, p. 103).	

			peligro identificado. [UNE-ISO Guía 73:2010]" (Ministerio de Hacienda y Administraciones Públicas, 2012b, p. 103).
	Tratamiento del riesgo Proceso de discriminar para implementar medidas y modificar los peligros existentes (Columba, 2016, p. 18).	Valoración estimada	Costo que asume la organización en caso de verse afectado si se lleva a cabo la vulneración de su seguridad, se mide de forma cuantitativa y cualitativa y se asigna valores y escalas para una mejor referencia de la valorización (Ministerio de Hacienda y Administraciones Públicas, 2012ª, p. 25).

1.5 JUSTIFICACIÓN E IMPORTANCIA

1.5.1 Económica

Proporciona al Instituto Superior Tecnológico evidencia sobre el diagnostico actual en que se encuentra su TIC y que es necesario prever actividades que le permitan minimizar riesgos en equipos, financieros y operativos a corto y largo plazo.

1.5.2 Operativo

La Gestión del Riesgo de las TIC, permite alinear los procesos internos entre lo que requiere el usuario interno y externo, entregar, dar servicio y soporte como adquirir o implementar lo que falta, haciendo eficiente el uso de los equipos y la infraestructura, minimizando el impacto de los sucesos fortuitos o forzados.

1.5.3 Teórica

Permitió comprobar como la metodología MAGERIT se adapta para el sistema de las TIC en este caso el Instituto Superior Tecnológico del Oriente, dedicado al rubro de la educación, adaptar procesos en algunas dimensiones, adecuar o suprimir pasos, lo que permitirá que en el futuro se pueda replicar o adaptar algunos procesos en empresas públicas o privadas sirviendo de base para otros estudios.

1.5.4 Académica

Nos permite alinear los propósitos para una eficiente Gestión del Riesgo en los activos de las TIC aplicando los procesos adecuados contribuyen a la enseñanza-aprendizaje.

1.5.5 Tecnológica

Optimiza los procesos, ayuda a minimizar los riesgos asociados, no solo a las Tecnologías de la Información sino a todas las dimensiones que involucra, la planificación, implementación, entregar, dar servicio y soporte a los clientes internos y externos, dándoles seguridad y eficiencia en las transacciones diarias.

1.6 ALCANCE Y LIMITACIONES DE LA INVESTIGACIÓN

1.6.1 Teórica

El trabajo se basó en la Metodología de Análisis y Gestión del Riesgo de los Sistemas de Información (MAGERIT), metodología de uso obligatorio según la legislación española en las empresas e instituciones públicas de España, así como otros países de la comunidad europea como Italia. El modelo se adapta a una entidad pública o privada, en este caso se aplicó a la unidad de análisis.

1.6.2 Espacial

El trabajo se llevó a cabo en el Instituto Tecnológico del Oriente de Tingo María, siendo propicio su estudio por las exigencias planteadas por el Ministerio de Educación para su licenciamiento y cumplir la ley 29733, ley de protección de datos personales.

1.6.3 Temporal

El estudio es transversal, se trabajó la investigación en el Instituto Superior del Oriente, durante los meses de octubre-diciembre del año 2020, concluyendo en el mes de enero del año 2021.

1.7 METODOLOGÍA DE LA INVESTIGACIÓN

1.7.1 Tipo de investigación

El estudio que se desarrolló es aplicado (Bunge, 1987) porque se buscó solucionar un problema específico tomando como base el problema identificado.

El diseño es de tipo experimental, diseño cuasiexperimental, (Salas, 2013, p. 138), mide el efecto de la Metodología MAGERIT como estrategia en la Gestión del Riesgo, con un enfoque cuantitativo como método de recolección de datos las descripciones, observaciones y análisis de datos. Según la intervención del investigador, la variable

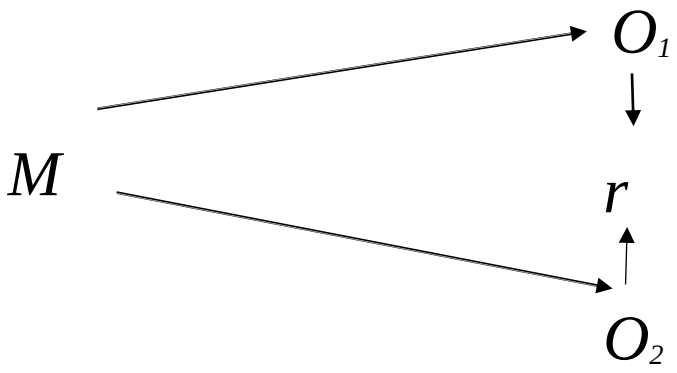
independiente a estudiar será manipulada para ver los efectos en la dependiente y determinar si mejora o no la Gestión del Riesgo, los datos recogidos serán estudiadas e interpretadas mediante la estadística descriptica (Hernández et al., 2006).

Se tomó en cuenta la categorización elaborada por Campbell y Stanley, el estudio es preexperimental por las características: a) existe un grupo como muestra (ISTO) con pre-test (Diagnostico); b) Objetivo-Aplicación (Salvaguardas); c) post test (mejora del riesgo después de aplicar salvaguardas) y propuesta de mejora (Salas, 2013), en este tipo de investigación según Bernal (2010) tiene como característica que las variables tienen un bajo control, no hay selección aleatoria de la muestra sujeta a experimento por lo tanto no hay grupo de control, así como de otras variables de naturaleza extraña o intervinientes durante el desarrollo de investigación, sus resultados solo son útiles en el campo aplicado no se puede generalizar, Salas (2013).

Por las veces en que la variable es medida es un estudio transversal, los datos serán tomados en un tiempo específico y no habrá seguimiento de los datos, por lo tanto, los resultados se interpretarán tal como nos muestra el momento del diagnóstico, la observación y revisión documentaria.

El diagnóstico nos permite realizar el análisis documental y observación de la unidad de análisis (ISTO), para ello se aplicó una lista de cotejo y revisión documental para cuantificar el grado de madurez de cada una de las dimensiones de la administración del peligro en las TIC bajo el parámetro referencial del método MAGERIT, el mismo que se encuentra validado a través de los manuales de procedimientos del Consejo Superior de Administración Electrónica de España (Ministerio de Hacienda y Administraciones Públicas de España, 2012a) al igual que la Norma Técnica Peruana NTP-ISO/IEC 27001-2014 (Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI, 2014). Por igual manera mediante coordinaciones de trabajo con el directivo a cargo se recogieron puntos de vista a las observaciones encontradas durante el proceso.

El esquema por trabajar es:



Donde:

M = muestra

O_1= Observación variable 1

O_2= Observación variable 2

1.7.2 Población y muestra

En este caso de está compuesta por la unidad de análisis, lo compone el Instituto Superior Tecnológico Privado del Oriente.

a) Muestra

La muestra lo compone la unidad de análisis, por lo que no es necesario determinar muestra alguna.

b) Criterios de selección

Teniendo en cuenta que la metodología de auditoria bajo MAGERIT te permite adecuar las áreas a evaluar en función las necesidades o realidad de la institución o empresa, durante la fase de diagnóstico se realizó la priorización de las áreas, así como de los procesos a auditar para determinar el nivel de madurez de las TIC y proponer mejoras.

c) Ubicación de la Unidad de análisis

La unidad de análisis está ubicada en la ciudad de Tingo María, Provincia de Leoncio Prado, del departamento de Huánuco.

d) Unidad de análisis

La unidad de análisis está formada por el Instituto Superior Tecnológico Privado del Oriente, institución educativa de Educación Superior, con más de 25 años de existencia,

habiendo recibido en el mes de junio su primera visita por parte del MINEDU-SUNEDU con fines de Licenciamiento.

1.7.3 Técnicas e instrumentos de recolección de datos

Fuente primaria: Se analizó la evidencia documental proporcionado por la institución, así como de todo el inventario de las TIC que posee la Institución.

Fuente secundaria: Se tomó en cuenta trabajos publicados referidos al tema, se analizó reglamentos y normas divulgados con la metodología MAGERIT, normas emitidas por el estado peruano en los que respecta a políticas para salvaguardar la información del usuario por la institución que cuenten o hacen uso de las TIC en su institución.

Técnicas

Sistematización bibliográfica

Se sistematizó la información bibliográfica a fin de articular el tema en estudio y los procedimientos seguidos por otros investigadores para cumplir con el objetivo planteado en la investigación, esto nos permitió revisar conceptos y teorías, así como los resultados obtenidos en otros trabajos de investigación, el mismo que nos sirve de fuente para la discusión de resultados que en algunos casos coinciden.

Sistematización Hemerográfica

Se recurrió a la sistematización de artículos de revistas indexadas y revistas presentes en la red sobre el marco teórico que atañe a la presente investigación con respecto a las Tecnologías de la Investigación y su Seguridad.

Entrevista

Tuvo como fin coordinar las diferentes actividades con el promotor del Instituto Superior Tecnológico del Oriente a fin de recabar información y coordinar actividades e intercambiar opiniones.

Instrumentos de Investigación.

a. Ficha bibliográfica

b. Ficha hemerográfica

c. Tabla de cotejo

d. Cédula de entrevista

e. Cédula de auditoría para evidenciar el nivel de madurez de los procesos revisados.

1.7.4 Procesamiento y presentación de datos

A través del software Pillar versión 7.4.3, se tomó en cuenta el siguiente proceso:

Revisión de datos

Se tomó en cuenta que todas las preguntas estén respondidas a fin de avalar la eficacia de la indagación.

Codificación de los datos

De acuerdo con el cuestionario las respuestas están codificadas en la escala de la Metodología MAGERIT, con la finalidad de determinar el grado de madures lo que permitirá codificar en números y ordenar las variables de forma categórica, numérica y ordinal.

Procesamiento de los datos

Los datos procesados fueron codificados de acuerdo con el nivel de madurez identificado es decir en códigos numéricos por cada una de las preguntas propuesta en el cuestionario o check list para generar una base y realizar los análisis.

Plan de tabulación de datos

En el proceso de tabular se utilizó la estadística descriptiva esto permite presentarlos en cuadros de frecuencias y porcentajes, permitiendo su interpretación de los resultados.

Presentación de datos

De acuerdo con el estilo de redacción APA se presentan las variables de estudio en figuras y tablas, estos resultados permiten visualizar tanto para su análisis como para su interpretación y luego contrastar estos hechos con el marco teórico.

1.8 LIMITACIONES

La metodología MAGERIT aplicada en una Institución Educativa, calificada de pequeña empresa por el volumen de negocios, con personal administrativo, equipos de cómputo y actividades de riesgo limitado los resultados servirán de base solo para nivel de empresas, con poco impacto en el riesgo.

II. REVISIÓN DE LITERATURA

2.1 ANTECEDENTES DE ESTUDIOS

2.1.1 Internacionales

Acevedo y Satizábal (2016). "*Metodologías de gestión y prevención de riesgos: una comparación".* Artículo que analiza nueve metodologías de gestión y prevención de riesgos comparando sus fases, OCTAVE, CORAS, Estándar Australiano; NTC-ISO/IEC 27005; CRAMM; MAGERIT; NIST para la gestión de riesgos y de gestión Metodología del BID para diagnosticar, prevenir y controlar la corrupción en proyectos de Seguridad ciudadana en los sistemas de TI; Metodología de prevención de incidentes de malware del NIST, incidiendo en la revisión si consideran o no al factor humano en el estudio e identificación del riesgo, concluyendo del total de metodologías el 42,85% considera este factor, incluye a la metodología MAGERIT. Todas las metodologías incluyen como dimensiones: a) contexto del desarrollo, b) identificación de peligros, c) análisis de los peligros y d) tratamiento de los peligros. Hace énfasis que la metodología MAGERIT es adaptable a pequeños negocios, queda a criterio del gestor adoptar todas las fases e identificar los riesgos, así como su posterior implementación.

Para el presente estudio se tomará como referencia el cuadro comparativo del marco teórico para definir e identificar los activos y riesgos, así como su implementación de seguimiento.

Holguín y Lema (2019). Artículo que realiza un análisis de las metodologías OCTAVE, MAGERIT, MEHARI, encontrando características disímiles pero que al adoptar el nivel de Madurez de los diferentes modelos comparados, las organizaciones mejoran su proceso adoptando las mejores prácticas, en ese sentido el Capability Maturity Model Integration. CMMI, ayuda a superar sus falencias o debilidades.

Este artículo aportará el modelo de madurez a aplicar en la presente investigación, así como el marco teórico comparativo desarrollado de las tres metodologías analizadas.

Ferruzola, et al. (2019). Artículo que analiza el método MAGERIT como gestor de riesgo en las TIC, en las empresas o instituciones públicas o privadas, para ello realiza un inventario de activos, requerimientos legales y comerciales, Identifica amenazas y vulnerabilidades, para determinar los riesgos plantea el requerimiento de la norma ISO

27001:2005; establecido los procesos aplica un simulacro de contingencia de los equipos y sistemas informáticos, para plantear posteriormente una propuesta de intervención o acciones en caso de emergencias, siendo la metodología MAGERIT la que mejor se adapta.

Para la presente investigación se tomará como referencia su marco teórico y el proceso usado para plantear un plan de contingencia en la etapa de selección de Salvaguardias.

Vicuña y Zhindón (2019). El objetivo del artículo de investigación fue desarrollar una metodología para gestionar el riesgo del soporte de su almacén de cómputo del centro Zona seis sur del INEC, para ello aplicó el método MAGERIT, tomando como dimensiones identificar los activos, definir y valorar los peligros, proponer y evaluar protección para mitigar el efecto y el peligro residual, así como el proceso de vigilar y revisar, concluyendo que el método MAGERIT se adapta para el estudio de peligros en todas sus fases.

El aporte para la presente investigación está en tomar como punto de apoyo los procesos adecuados a la realidad de la institución la metodología MAGERIT, así como su implementación y seguimiento.

Castillo, et al. (2018). El objetivo del artículo fue establecer un modelo de reducción de riesgo y seguridad informática aplicando la metodología MAGERIT, y la herramienta VEGA de Linux. Concluyendo que se logró reducir en un 80.59 por ciento las vulnerabilidades, son tres las debilidades más recurrentes: SQL Injection, PHP Error Detected y Directory Listing Detected.

El aporte para la presente investigación está en tomar como referencia su proceso aplicado en la web de la Institución educativa, el mismo que nos serviría como apoyo o modelo adecuándolo a la realidad del ISTO con la metodología MAGERIT, así como su implementación y seguimiento.

2.1.2 Nacionales

Guevara (2015). Tesis con el objetivo de describir los peligros a los que está expuesto los equipos de cómputo de la oficina de Gestión Académica de la Universidad Nacional Pedro Ruiz Gallo, para ello aplicó el método MAGERIT para el estudio y

administración del riesgo, planteando medidas que conviene adoptar en el control de los riesgos identificados, el proceso que siguió fue diagnóstico de los servidores, plan de mitigación y los costos que involucra aplicar la metodología MAGERIT a través del software PilarBasic. A pesar de que la institución había tomado sus previsiones anteriormente se descubrió que los equipos diversos están revelados a un riesgo crítico de peligros, entre ellos: Suspensión intermitente del sistema por carga de trabajo exagerada, deterioro de bienes material o lógico, falla en la provisión del servicio eléctrico, ambientes impropios afectos al clima del ambiente, sustracción de bienes, extravío de bienes de cómputo, caídas del administrador del sistema de cómputo y seguridad de las TIC.

Al hacer un diagnóstico de todo el sistema de Hardware, Software, infraestructura y los riesgos asociados a ello, esta metodología se adecua a los propósitos a investigar en el ISTO teniendo en cuenta que existen los mismos problemas y elementos a evaluar, como parte del Licenciamiento Institucional.

Sandoval y Quino (2017). Tesis que tuvo como objetivo combinar la metodología MAGERIT con la ISO 17799, y proponer un diseño de un proyecto de salvaguardas para proteger la información de los activos del sistema informático, utilizados y que al mismo tiempo generan durante los procesos institucionales, los cuáles son gestionados por la Oficina de Informática y Telecomunicaciones de la institución, contempla en el proceso 18 indicadores, encontrando falencias en los procesos de seguridad a través de la metodología MAGERIT y a través de la ISO 17799, plantea mejoras para la protección de los activos y de la infraestructura donde se procesan los datos.

Este modelo se tomará en la presente investigación en lo que se adecue para la seguridad de la información en el ISTO de Tingo María.

Romero (2018); Carrión (2016). Ambas investigaciones son tesis, la primera busca cuantificar e identificar los elementos de peligros en la TIC, identificado los elementos, cuantifica su rendimiento de la retransmisión por Internet (webcast) en la empresa Atogapan S.A. y el Grupo HCM comunicaciones S.A.C., para llegar al objetivo aplicó la metodología MAGERIT en sus dimensiones de estudio del riesgo y plan de seguridad evaluando la eficiencia, eficacia y calidad del servicio.

En la segunda tesis realizó el análisis de la administración de los peligros para la mejora de las tecnologías de la información en la Oficina General de Estudios de la

Universidad Nacional Santiago Antúnez de Mayolo, combinando la metodología MAGERIT para el diagnóstico y usó la ISO/IEC 27002:2008 como propuesta de mejora.

Contribuirá en la presente investigación como guía en los procedimientos de la Aplicación del método MAGERIT en cada una de sus etapas, y se tomará algunos elementos recomendados en la ISO/IEC 27002: 2008 como propuesta de mejora.

Valdiviezo (2016). La tesis tuvo como objetivo diagnosticar los peligros de los componentes informáticos que generan información en la Clínica Internacional – Piura aplicando el método MAGERIT, teniendo como proceso la identificación y valoración de los activos, determinar y analizar las amenazas, analizar las vulnerabilidades y proponer las salvaguardas. Determina la valoración de los resultados de manera cuantitativa usando porcentajes para luego darles un valor cualitativo de nivel medio a alto.

La investigación nos guiará en los procedimientos de la Aplicación del método MAGERIT y la madurez en cada una de sus etapas y la propuesta de un manual para implantar políticas de implementación, control, seguimiento y mejora continua.

2.1.3 Locales

Ortiz (2018). Tesis tuvo como objetivo determinar tres aspectos predominantes para la aplicación de la ISO 27002:2013 a) diagnóstico b) aplicación o salvaguardas c) recomendaciones, para ello aplicó la metodología MAGERIT como instrumento de medición. La investigación fue experimental con diseño cuasiexperimental, como unidad de análisis el área de "CETIC" Tecnología de Información y Comunicación vigentes de la Universidad Nacional Agraria de la Selva. Entre su principal conclusión menciona que la aplicación de la ISO motivo de estudio mejoró los cuadros claves de un 12% a un 14%, los cuadros operativos en un 16% a 20%, de manera general hay una mejora del 28% a un 34%.

El aporte de la tesis en la investigación a desarrollar será una guía de trabajo el mismo que nos permitirá comparar procesos y resultados.

Espinoza (2017). Tesis que tuvo como objetivo cuantificar el grado de madurez de las fases de las Tecnologías de la Información en la empresa GEOSURVEY S.A usando el protocolo de los procesos contenidos del COBIT 1.4, el mismo que establece los procesos para determinar el nivel de madurez, mediante una investigación descriptiva, a través de la observación en las áreas de publicidad, marketing y contabilidad, así como los de

operaciones, medio ambiente, ventas, seguridad y el área de topografía, estableciendo 34 procesos y 210 objetivos de control de procesos COBIT, y una variación de la madurez del nivel 0 hasta el nivel 5, concluyendo que según el método COBIT que algunos ítems cumplen los procedimientos y se encuentran implementados y otros falta cumplir ciertos protocolos, y algunos deben implementarse.

Aportará la tesis descrita en el análisis para determinar la madurez de los ítems a auditar de los activos y procesos comparando sus resultados.

Se ha realizado la búsqueda en el repositorio de la Universidad Nacional Agraria de la Selva, referente a la presente investigación con procesos aplicados a MAGERIT y no se evidencia antecedentes de este tipo de estudio.

2.2 BASES TEÓRICAS

2.2.1 Teoría general de Sistemas

Su máximo exponente es L. Von Bertalanffy (1976). La Teoría General de Sistemas se define como, la representación del mundo real aproximado de manera ordenada y científica de forma simultánea, es un trabajo transdisciplinario cuya orientación se distingue por su representación integradora, donde prevalece su esencia de interacción con los elementos con los que interactúa (Instituto Nacional de Estadística e Informática, 2000, p. 8).

Entre sus principales características tenemos: la Interrelación entre los elementos del sistema; Totalidad, se interrelaciona con todos sus componentes; la búsqueda de Objetivos, para cruzar las metas que se propone la empresa; Insumos y Productos, no es otra cosa más que generar las actividades necesarias para los objetivos; Transformación, búsqueda a través de las entradas y salidas; Entropía, no se pueden dejar al azar o manejar de forma aislada dejando de lado la interrelación de sus partes; Regulación, al integrarse forman parte del todo por lo tanto es necesario que cada parte se adecue frente a los objetivos deseados; Jerarquía, cada sistema tiene un conjunto de subsistemas, Diferenciación, por cada parte tiene funciones específicas que diferencian unos a otros, Equifinalidad, porque cada parte puede seguir objetivos específicos pero que al final suma al todo. (Instituto Nacional de Estadística e Informática, 2000, p. 13).

Al definirse entonces a la TGS como una organización que interactúan entre ella a su vez son interdependientes a través de las actividades que se generan en ellas es decir

ingresos como información, recursos humanos o recursos materiales, luego estas actividades se procesan mediante tareas asignadas para obtener información, productos o servicios, los cuales generarán entradas para otros procesos continuando nuevamente la interacción, es un modelo propicio dentro de la investigación de la gestión del riesgo en las TIC.

El mismo autor clasifica a los sistemas como cerrados y abiertos, dentro de los cerrados clasifica a la física y la termodinámica por estar aislados del medio circundante y los abiertos están interrelacionados con su medio circundante como la biología, la cibernética, las ciencias sociales, recae la presente investigación dentro del grupo de abierto al estar interrelacionado la Administración de los peligros de las TIC con la gerencia empresarial, recursos humanos, normas legales, políticas de estado, tales como la implantado por el Ministerio de Hacienda y Administraciones Públicas de España en su manual Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I (2012) refiere desde el enfoque de la auditoría en TIC y específicamente la metodología MAGERIT tiene como propósito lo siguiente:

a) Sensibilizar en administradores de las instituciones públicas y privadas y organizaciones sobre la existencia real del riesgo y la obligación de tomar acciones al respecto.
b) El uso de la TIC no está exenta de riesgo, es necesario consensuar un método que sistematice la información del riesgo.
c) Es necesario dar tratamiento a los riesgos identificados de manera planificada y oportuna.

Busca como objetivo indirecto

a) Toda organización debe estar preparada de forma periódica para afrontar auditorías, certificaciones o con fines de acreditación, de acuerdo con la realidad y contexto donde se desarrolla la organización.

Bajo este enfoque se aplicará la teoría sistémica para comprender el proceso de la investigación y la aplicación de la auditoría bajo la metodología MAGERIT.

2.2.2 Teoría de la información

A esta teoría también se conoce como la Teoría Matemática de la Comunicación, siendo Hartley (1928) quien dio los primeros lineamientos que gobiernan sus leyes, posteriormente Claude E. Shannon planteó los principios definitivos de la teoría cuyo trabajo

planteaba las dificultades que se suscitan en sistemas consignados a operar información, entre ellos comunicar métodos idóneos a utilizar por los numerosos sistemas de comunicación, así como determinar una buena técnica para aislar los signos del murmullo y cómo cuantificar la frontera posible de un canal (Uscatescu, 1973).

Esta teoría nos ayudó durante la investigación a comprender los procesos de comunicación en la Institución, como sale la información, las interferencias que pueda existir durante la comunicación (interna o externa), la recepción de la comunicación, interpretación de la comunicación por parte del receptor, los costos y beneficios asociados a este proceso y los costos y beneficios más convenientes para la institución en estudio.

2.2.3 Gestión de los Riesgos a través de la Metodología de Análisis y de los Sistemas de Información "MAGERIT" versión 3.0

Diversas instituciones generaron modelos de control todos ellos en función a su idioma y culturas empresariales adecuándolos a su realidad, pero partiendo todos que la adopción de tecnologías de la información y comunicación (TIC) por los usuarios ciudadanos facilita sus actividades diarias, pero a su vez genera riesgos asociados los que deben ser gestionados de manera responsable a fin de que los usuarios sientan seguridad en las actividades que realiza a través de los servicios brindados por la institución (Ministerio de Hacienda y Administraciones Públicas de España, 2012).

Siendo una necesidad de las empresas no solo ser competitivos sino sostenibles en el tiempo necesitan combinar costos con eficiencia y maximizar los recursos con los que cuentan y adquirir los que faltan, para minimizar los riesgos que con ello lleva, siendo MAGERIT 3.0 que mantiene esa dinámica entre sus fortalezas el estándar de prácticas de trabajo donde establece una clara distinción entre administración y gestión. Gobierno y Gestión tienen diferentes tipos de actividades, la estructura organizativa de cada uno sirve a diferentes propósitos, en ese aspecto la ISO 27001 proporciona una perspectiva trascendental integral en la prevención de vulnerabilidades del sistema de información, que comprende Entidades, Eventos y procesos (Toro, 2019).

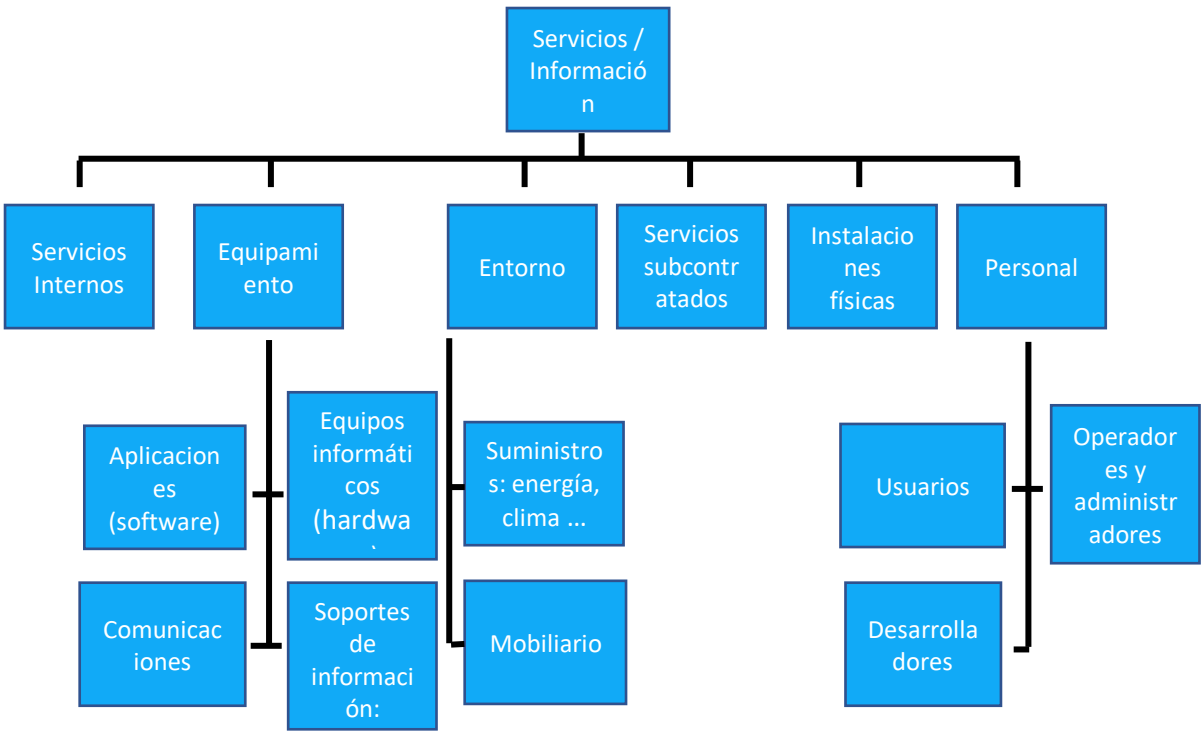
Al tomar en cuenta los procesos en el análisis del riesgo se adapta a cualquier empresa sea de servicios, transformación, comercialización, de naturaleza corporativa, PYMES o MYPES, debido a que no todas las empresas tienen los mismos requerimientos, empresas de poca envergadura pueden tener pocos requerimientos y empresas más grandes

pueden tener requerir mayores requerimientos, pero todos buscan cubrir las vulnerabilidades.

Columba (2016) refiere que toda gestión del riesgo se basa en tres principios de seguridad: integridad, disponibilidad, confidencialidad, MAGERIT va más allá y considera seis principios fundamentales de seguridad: disponibilidad (D); integridad (I); confidencialidad (C); autenticidad (A); trazabilidad (T); datos personales (DP). Los principios de MAGERIT son concordantes con la Ley peruana 29733 ley de protección de datos personales que toma en cuenta 12 principios los mismos que son concordantes con la ISO/IEC 27002:2013 código de buenas prácticas para controles de seguridad de la información.

Al estar establecidos las dimensiones de la seguridad según MAGERIT, el primer paso es valorar los activos el proceso lo observamos en la figura 1.

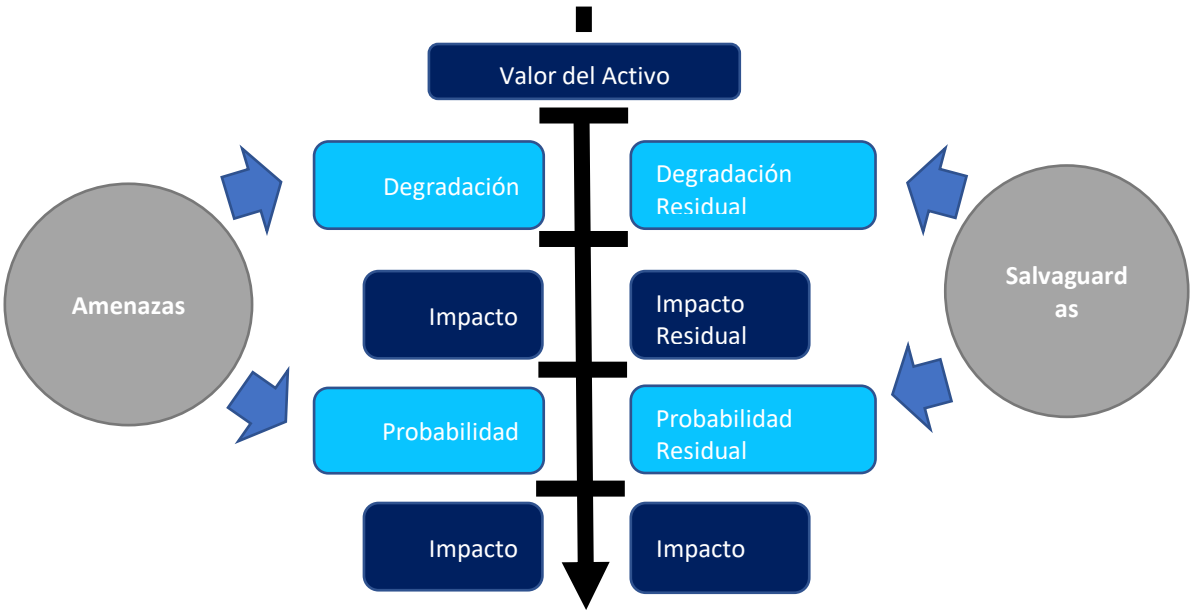
Figura 1. Activos por valorar según la metodología MAGERIT



Fuente. Rodríguez y Peralta (2013)

Determinados los Activos se analiza las amenazas y las salvaguardas a aplicar como parte del proceso de mejorar los mismos (ver figura 2).

Figura 2. Proceso de determinación de amenazas y salvaguardas



Fuente. Rodríguez y Peralta (2013).

Es sobre este marco de la figura 1 y 2 que se adaptará y trabajará en la investigación a aplicar en la unidad de análisis y estudio.

2.2.4 La Norma Técnica Peruana NTP-ISO/IEC 27001-2013

Esta norma publicada el 20 de noviembre del año 2014, norma el Sistema de gestión de seguridad de la información en el Perú, tomado de su equivalente en inglés ISO/IEC 27001:2013+ISO/IEC 27001:2013/COR 1. Information technology – security techniques – Information security management systems – Requeriments, este documento se oficializó con Resolución 0129-2014/CNB-INDECOPI.

La norma obliga a las entidades públicas y privadas a adoptar un método de gestión de seguridad en las TIC en afín a los requerimientos y objetivos de la institución, debiendo proteger: confidencialidad, integridad y disponibilidad de la información aplicando bajo una gestión de riesgos que proporcione confianza entre la empresa y los usuarios de tal manera que los riesgos se manejen adecuadamente.

2.2.5 Integración de Sistemas modelos de madurez de capacidades para servicio (Capability Maturity Model Institute para servicios V.1.3 - CMMI)

Es un modelo que ayuda al evaluar los procesos de una organización, específicamente de acuerdo con la investigación a realizar se adopta el de servicios, su característica principal radica en establecer dos parámetros de comparación, pero vinculados al proceso, primero establece la capacidad de los procesos de la organización y a cada área lo asigna un nivel de madurez (Capability Maturity Model Institute, 2013).

Tabla 2. Representaciones y niveles del CMMI por servicios

Nivel	Representaciones y Niveles Continua Capacidad	 Por etapas Madurez
0	Incompleto	
1	Realizado	Inicial
2	Gestionado	Gestionado
3	Definido	Definido
4		Gestionado Cuantitativamente
5		En optimización
Se seleccionan las áreas mejorar		**Definido por áreas por nivel**

Fuente. Capability Maturity Model Institute, 2013 p. 23-27

El CMMI define al Servicio como: un bien no almacenable con características de intangible. Es necesario considerar que este concepto pueda malinterpretarse o generar sutilezas de interpretación teniendo en cuenta que la palabra "servicio" no expresa en su totalidad el significado que busca expresar el contexto de CMMI" (Capability Maturity Model Institute, 2013, p. 39), considera al servicio como un tipo de producto, los procesos como las actividades.

2.3 DEFINICIONES DE TÉRMINOS BÁSICOS

Activo en las TIC: Cada uno de los elementos funcionales que compone el sistema de información que puede ser fácilmente vulnerado de manera intencional o por accidente, generando un costo cuantitativo o cualitativo en la organización, esos pueden ser recursos administrativos, recursos humanos, información, físicos, comunicaciones, datos, hardware, servicios o software [UNE 71504:2008] (Ministerio de Hacienda y Administraciones Públicas de España, 2012a)**.**

Amenaza. la organización en su sistema de información sufre posibles daños como producto de un incidente de causa potencial [UNE 71504:2008] (Ministerio de Hacienda y Administraciones Públicas de España, 2012a).

Autenticidad: según Columba (2016) lo define como la cualidad de que una entidad es lo que afirma ser y se puede verificar.

Control Interno. Alfonso, Blanco y Loy (2012) mencionan a la Resolución 60/11 que define al control interno como mejoramiento continuo de un conjunto de procesos como resultado de una gestión, esto involucra a todas las actividades, así como a toda la organización, son regidas por normas reglamentos y procedimientos, esto ayuda a prever o minimizar el riesgo externo o interno, de esta manera ayuda a rendir cuentas y adicionar seguridad para el cumplimiento de las metas propuestas en la institución.

Confidencialidad. Busca la accesibilidad y disponibilidad de la información solo a las personas autorizadas limitando el acceso a las no autorizadas. (Columba, 2016).

Datos personales: la identificación de las personas naturales a través de sus identificaciones puede usar de forma sensata por medios autorizados.

Disponibilidad. "La disponibilidad garantiza que los sistemas estén en marcha cuando sea necesario" (Columba, 2016, p. 12).

Gestión del riesgo. Columba (2016) lo define como acciones ordenadas para gestionar y fiscalizar una organización en correlación a las inseguridades identificadas en las TIC; del mismo modo afirma que: **"**Según la ISO/IEC 27005:2011, la norma ISO para la Gestión de riesgos de seguridad de la información utiliza el término "proceso" para describir la gestión del riesgo global y los elementos internos en el proceso de la gestión del riesgo se denominan, actividades" (p. 12).

Por otro lado la metodología MAGERIT considera como actividades dentro de la Gestión del Riesgo al "análisis y tratamiento" del riesgo (Ministerio de Hacienda y Administraciones Públicas de España, 2012a, p. 19).

Gestión de la información. Para Columba (2016) toda organización gestiona su información de manera que le permita planificar, coleccionar, organizar, utilizar, controlar, diseminar para poder disponer eficientemente su información, de esta manera se garantiza el valor de la información y su uso.

Integridad. "evita la modificación no autorizada del software o hardware, no se debe permitir modificaciones no autorizadas a los datos, ni al personal autorizado, ni al no autorizado y/o a los procesos y los datos deben ser consistentes interna y externamente" (Columba, 2016, p. 15).

Nivel de Madurez. El Instituto CMMI lo define como un modelo de procesos progresivo mediante la cual se asigna un código numérico a un conjunto de datos dentro del proceso de la organización, de acuerdo con el progreso alcanzado se denomina nivel de madurez, estos se miden de acuerdo a un catálogo de logros y objetivos definidos en metas de manera genérica y específica para cada área definida dentro del proceso, el nivel de madurez al tener una escala de menos a más (de 1 a 5) hace que el proceso se convierta en mejora continua (Capability Maturity Model Institute, 2013).

Proceso de gestión de riesgos. La revisión y seguimiento de las vulnerabilidades requieren que de forma metódica se ponga en práctica las políticas y procedimientos relacionadas a las actividades de consultorías y comunicación, esto permite ir progresivamente desde la identificación al análisis, evaluación, tratamiento en la identificación de los riesgos.
(Columba, 2016).

Riesgo. Columba (2016) lo define como: "la combinación de la probabilidad de un evento y su consecuencia. El efecto es una desviación de los esperado, que puede ser positivo y/o negativo" (p. 16).

Salvaguarda: "medida implantada para proteger el propio activo". (Liras, 2013, p. 6)

Sistema: El Instituto Nacional de Estadística e Informática del Perú define al sistema como la interrelación de las partes que forma un todo de alguna manera esta relación se ve influenciada de alguna manera por ese parte relacionada, el cual se mantiene en el tiempo, en el campo de la informática, en contexto en que se utiliza la palabra sistema se da en

diferentes contextos, entre ellos se tiene el hardware y el sistema operativo que lo integra o al conjunto de programas que integra ese hardware, a estos programas que integran se denominan en conjunto como sistemas, por ejemplo el sistema contable, o sistema de gestión administrativa “SIGA”, sistema integrado de información financiera “SIAF”.

Sistema cerrado: El contexto en que varía es medible y conocido, pero la frecuencia de la ocurrencia no, por lo tanto, se afirma que las variaciones se conocen de antemano por los factores en el contexto que se desarrolla (Instituto Nacional de Estadística e Informática, 2000).

Sistema Abierto: Se conoce así cuando el subsistema con el sistema intercambia flujos de información dentro del contexto en que se desarrolla los hechos. (Instituto Nacional de Estadística e Informática, 2000, p. 16).

Seguridad de la Información. El sistema relacionado a la información debe contar con protocolos que garanticen la confidencialidad de los bienes que posee la institución, pero del mismo modo este debe estar disponible para quien lo requiera, dando autenticidad, así como responsabilidad del quien hace uso (Columba, 2016). Es decir, la información de la entidad debe protegerse, pero a su vez garantizar minimizando los riesgos su continuidad en bienestar de la inversión del negocio.

Trazabilidad: Según Columba (2016) considera la conformidad a que un ente tiene que cumplir con las políticas y reglamentos internos constituidos en acorde con las leyes y normas que la rigen.

III. MATERIALES Y MÉTODOS

3.1 LUGAR DE EJECUCIÓN

Como unidad de análisis se tiene al Instituto de Educación Superior Tecnológico Privado del Oriente se fundó el 04 de setiembre 1994, es el primer Instituto Privado en la Provincia de Leoncio Prado, brinda las carreras de Secretariado Ejecutivo, Computación e Informática e Idiomas, se encuentra en un plan de mejora continua, lo que obliga a adoptar por la responsabilidad y el sector en que se desenvuelve TIC de acorde a sus necesidades para cumplir sus objetivos institucionales, adecuándose a los requerimientos del Ministerio de Educación del Perú para el licenciamiento, esto permite cumplir con las exigencias de calidad, entre ellas infraestructura y equipamiento, gestión académica, gestión institucional, contar con personal docente calificado y prever los recursos financieros necesarios para su sostenibilidad, esto lo permitiría dar cumplimiento a la ley Nº29733 ley de protección de datos personales.

3.2 MATERIAL Y MÉTODOS: METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT).

3.2.1 Planeación del análisis y la gestión de riesgos

Primer paso por aplicar en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) es adaptar a la realidad del Instituto Superior Tecnológico catalogado como Mediana y Pequeña Empresa (MYPE) según la normativa tributaria peruana, a su vez compatibilizar con la normativa educativa gestionada por el Ministerio de Educación peruano, los estándares de Protección de datos, así como la Norma Técnica Peruana NTP-ISO/IEC 27001-2013, Ley 30512; Decreto supremo Nº010-2017-MINEDU; Ley Nº29733.

Procedimiento seguido:

a) Estudio de oportunidad del proyecto de análisis de riesgos

Se revisa el cumplimiento de requisitos y normas relacionadas al licenciamiento teniendo como insumo los siguientes documentos fuentes:

- Artículos 25, 38, 39 de la Ley 30512. Ley de institutos y escuelas de educación superior y de la carrera pública de sus docentes.
- Reglamento de la ley 30512, decreto supremo Nº010-2017-MINEDU. artículo 59 manual de uso del sistema de registro de información académica.
- Ley de protección de datos personales y sus principios rectores. Ley Nº29733.
- NTP-ISO/IEC-27001-2013, norma técnica peruana.

b) Determinación del alcance del proyecto

En este proceso se definieron dos metas: Cumplimiento de las normas para el Licenciamiento y la Aplicación de salvaguardas para el soporte administrativo y académico del Instituto a corto plazo.

A largo plazo se define como objetivo el sostenimiento y mantenimiento de las TI del Instituto.

Información requerida de ingreso:

Selección de la información documentada correspondiente de la institución: Manuales de todos los procesos tanto administrativo como académicos.

Producto de salida

- Lista de las áreas de la institución que se involucrarán como parte del plan (área administrativa y académica).
- Inventario de actividades que desarrolla cada área identificada incluidas en el alcance del plan de trabajo a desarrollar.
- Clasificación de los activos fundamentales.
- La interrelación entre áreas u otros sistemas
- los prestadores de servicios externos

c) Planificación del proyecto

En esta tapa se definió los interlocutores, es decir con quienes se realizaría las coordinaciones dentro de las áreas involucradas (Promotor, Coordinador académico y secretaria).

Así mismo las horas apropiadas para las consultas y absolución de preguntas.

Plan de entrevistas para el inventario de los activos

Técnicas, prácticas y pautas antes, durante y después de los procesos, Académicos y administrativos.

d) Lanzamiento del proyecto

En este punto el objetivo del trabajo es el acceso a los bienes tangibles e intangibles de la Institución, realizándose las siguientes actividades:

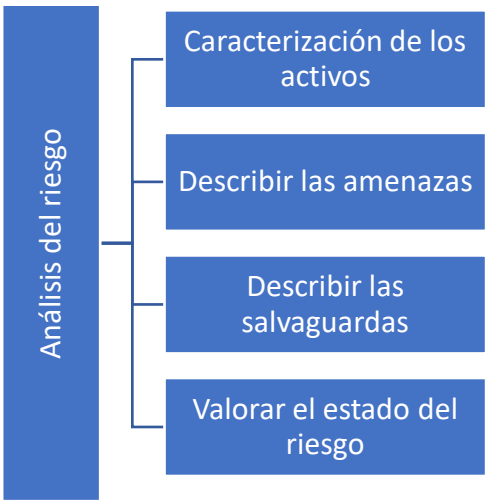
- Aplicación de los cuestionarios (ver anexo 2).
- Elaborar la lista de activos por tipo identificado.
- Valorar los activos por dimensiones.
- Valorar los activos por criterio teniendo en cuenta la guía de MAGERIT, asignando los niveles al que corresponde cada activo.
- Identificar las amenazas por degradación y frecuencia de acuerdo con el nivel de valoración.
- Determinar las necesidades en recursos humanos, financieros o técnicos para la ejecución del proyecto.
- Coordinar con las áreas a trabajar.
- Comunicar asertivamente los procedimientos y objetivos a seguir tanto al personal como a los gestores de la institución.
- Aplicación del cuestionario de la lista de elementos en la institución (p. 13 manual de MAGERIT Vol. 1)

3.3 GESTIÓN DEL RIESGO DE LAS TIC.

3.3.1 Análisis del riesgo

Para MAGERIT (2012) el estudio del riesgo consiste en establecer con que activos cuenta la Organización y evaluar lo que podría pasar ante una eventualidad (riesgo), la ruta que nos ofrece es la siguiente:

Figura 3. Fases del análisis del riesgo según el método (MAGERIT, 2012)



Del mismo modo se establecen las actividades por realizar en cada una de las fases para el análisis del riesgo.

Tabla 3. Procedimiento según MAGERIT para la estimación del riesgo

Método de análisis de riesgos (MAR)	
MAR.1	**Descripción de los activos**
MAR.11	Identificar los activos
MAR.12	Establecer dependencia entre activos
MAR.13	Valorar los activos
MAR.2	**Descripción de las amenazas**
MAR.21	Identificar las amenazas
MAR.22	Valorar las amenazas
MAR.3	**Descripción de las salvaguardas**
MAR.31	Identificar las salvaguardas pertinentes
MAR.32	Valorar las salvaguardas
MAR.4	**Valorar el estado de riesgo**
MAR.41	Estimar el impacto
MAR.42	Estimar el riesgo

3.3.1.1 MAR. 11 Identificar los activos

La metodología indica identificar que activo es relevante para la institución, el valor del activo y la capacidad de interrelación entre activos, de tal manera que permita que de ocurrir un evento negativo cual sería el costo del perjuicio y su degradación que sufre durante el tiempo de actividad. (Ministerio de Hacienda y Administraciones Públicas de España, 2012a).

El criterio aplicado para la identificación del activo es de acuerdo con la información y el inventario que tiene el Instituto Superior Tecnológico del Oriente, el que se presenta en la tabla 4 y 5.

Tabla 4. Identificación de los activos en el ISTO según MAGERIT

ACTIVOS	
AE *Activos esenciales*	
	1. Récord de notas
	2. Expediente de los estudiantes - matricula
	3. Examen virtual y presencial
	4. Programación de cursos y horarios
SI *Servicios internos*	
	1. Acceso de los usuarios
	2. Aula virtual - Salón de clase
	3. Aula virtual - Material de estudio - módulos
	4. Documentos administrativos- Actas virtuales
EI *Equipamiento informático*	
	Aplicaciones (software)
	1. Portal web institucional
	2. Correo electrónico corporativo.
	3. Aplicaciones para E-A
	Equipos informáticos (hardware)
	1. Computadoras - HARDWARE
	2. TV
	3. Proyector multimedia
	4. Herramientas de testeo e instalación de redes.
	5. Impresoras
	6. Monitores
	7. Cámaras video vigilancia
	Comunicaciones
	1. Router Movistar
	2. Swicht 24 puertos
	Soportes de información: discos, cintas etc.
	1. Discos de almacenamiento de datos
	2. Uninterruptible power supply (UPS)
	3. Impresión de Actas de notas - respaldo

Tabla 5. Identificación de los activos en el ISTO según MAGERIT

ACTIVOS		
EE	*El entorno*	
		Energía Eléctrica
		Fluido de agua potable y desagüe
		Para rayos y conexión a tierra
		Mobiliario
SS	*Servicios subcontratados a terceros*	
		ADSL
		Hosting web (para hospedar la página web y dominio.com y correos electrónicos)
IF	*Instalaciones físicas*	
		Laboratorios de cómputo
		Salón de clases
		Área de control computo
		Área de atención
P	*Personal*	
		Usuarios - Estudiantes
		Operadores - Docentes
		Operadores - Administrativos
		Administradores - Soporte Información

3.3.1.2 MAR. 12 Dependencias entre activos

Establecido los activos el siguiente paso es determinar la dependencia entre activos, porque cada activo interactúa con otro activo de tal manera que es necesario evaluar los activos en su integridad, la metodología MAGERIT (2012) lo considera como afectaría un activo si fuera vulnerado a otro activo con el que esta interrelacionado (superior e inferior) por ejemplo la interrelación entre los activos esenciales y los servicios internos, equipamiento informático, el entorno, las instalaciones físicas, personal y los servicios subcontratados a terceros, el resumen lo apreciamos en la tabla 5 y 6.

Tabla 6. Diagrama de dependencia por tipo de activos

	ACTIVOS	*AE*	*SI*	*EI*	*EE*	*SS*	*IF*	*P*
AE	*Activos esenciales*		X	X	X	X	X	X
	1. Récord de notas							
	2. Expediente de los estudiantes - matricula							
	3. Examen virtual y presencial							
	4. Programación de cursos y horarios							
SI	*Servicios internos*			X		X		X
	1. Acceso de los usuarios							
	2. Aula virtual - Salón de clase							
	3. Aula virtual - Material de estudio - módulos							
	4. Documentos administrativos- Actas virtuales							
EI	*Equipamiento informático*				X		X	X
	Aplicaciones (software)							
	1. Portal web institucional							
	2. Correo electrónico corporativo.							
	3. Aplicaciones para E-A							
	Equipos informáticos (hardware)							
	1. Computadoras - HARDWARE							
	2. TV							
	3. Proyector multimedia							
	4. Herramientas de testeo e instalación de redes.							
	5. Impresoras							
	6. Monitores							
	7. Cámaras video vigilancia							
	Comunicaciones							
	1. Router Movistar							
	2. Swicht 24 puertos							
	Soportes de información: discos, cintas etc.							
	1. Discos de almacenamiento de datos							
	2. Uninterruptible power supply (UPS)							
	3. Impresión de Actas de notas - respaldo							

Leyenda:

SI: Servicios internos **AE:** Activos esenciales **EI:** Equipamiento informático
EE: El entorno **IF:** Instalaciones físicas **P:** Personal
SS: Servicios subcontratados a terceros

Tabla 7. Diagrama de dependencia por tipo de activo

	ACTIVOS	*AE*	*SI*	*EI*	*EE*	*SS*	*IF*	*P*
EE	*El entorno*						X	X
	Energía Eléctrica							
	Fluido de agua potable y desagüe							
	Para rayos y conexión a tierra							
	Mobiliario							
SS	*Servicios subcontratados a terceros*						X	X
	ADSL							
	Hosting web (para hospedar la página web y dominio.com y correos electrónicos)							
IF	*Instalaciones físicas*							X
	Laboratorios de cómputo							
	Salón de clases							
	Área de control computo							
	Área de atención							
P	*Personal*	X	X	X	X	X	X	X
	Usuarios - Estudiantes							
	Operadores - Docentes							
	Operadores - Administrativos							
	Administradores - Soporte Información							

Leyenda:

SI: Servicios internos **AE:** Activos esenciales **EI:** Equipamiento informático
EE: El entorno **IF:** Instalaciones físicas **P:** Personal
SS: Servicios subcontratados a terceros

3.3.1.3 MAR.13 Valorar los activos

Al definir el valor de un activo se refiere no al valor monetario sino desde la importancia que cobra dentro de la institución su protección tanto que si fuese un bien tangible (equipos, productos) como si fuese un bien intangible (servicios) MAGERIT (Versión3.0) lo define como los activos que deben protegerse, cuanto más alto este en la escala de valor requiere el activo requiere mayor protección, en las dimensiones o dimensión correlacionada, en acorde a la realidad de la organización (Ministerio de Hacienda y Administraciones Públicas de España, 2012a). En este tema hace referencia a la interdependencia entre los activos, en caso del ISTO quedaría definido de la siguiente manera: dentro de los activos esenciales si esta interrelacionado o no con las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, al procesar los datos el programa Pillar nos da el siguiente resumen expresado en la tabla 8 y 9.

Tabla 8. Interdependencia de los activos por dimensión

	Activos	Valoración				
		Confidencialidad de la información	**Integridad de los datos**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
AE	***Activos esenciales***					
	1. Gestión de notas - récord de notas	**X**	**X**	**X**	**X**	**X**
	2. Expediente de los estudiantes - matricula	**X**	**X**	**X**	**X**	**X**
	3. Examen virtual y presencial	**X**	**X**	**X**	**X**	**X**
	4. Programación de cursos y horarios		**X**	**X**		
SI	***Servicios internos***					
	1. Acceso de los usuarios		**X**	**X**	**X**	**X**
	2. Aula virtual - Salón de clase		**X**	**X**	**X**	**X**
	3. Aula virtual - Material de estudio -módulos		**X**	**X**	**X**	**X**
	4. Documentos administrativos- Actas virtuales		**X**	**X**	**X**	**X**
EI	***Equipamiento informático***					
	Aplicaciones (software)					
	1. Portal web institucional		**X**	**X**		
	2. Correo electrónico corporativo.	**X**	**X**	**X**	**X**	**X**
	3. Aplicaciones para E-A		**X**	**X**	**X**	**X**
	Equipos informáticos (hardware)					
	1. Computadoras - HARDWARE			**X**		
	2. TV			**X**		
	3. Proyector multimedia			**X**		
	4. Herramientas de testeo e instalación de redes.			**X**		
	5. Impresoras			**X**		
	6. Monitores			**X**		
	7. Cámaras video vigilancia			**X**		
	Comunicaciones					
	1**.** Router Movistar			**X**		
	2. Switch 24 puertos			**X**		
	Soportes de información: discos, cintas etc.					
	1. Discos de almacenamiento de datos	**X**	**X**	**X**	**X**	**X**
	2. Uninterruptible power supply (UPS)			**X**		
	3. Impresión de Actas de notas - respaldo		**X**	**X**	**X**	**X**

Tabla 9. Interdependencia de los activos por dimensión

	Activos	Valoración				
		Confidencialidad de la información	**Integridad de los datos**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
EE	***El entorno***					
	Energía Eléctrica			**X**		
	Fluido de agua potable y desagüe			**X**		
	Para rayos y conexión a tierra					
	Mobiliario			**X**		
SS	***Servicios subcontratados a terceros***					
	ADSL			**X**		
	Hosting web (para hospedar la página web y dominio.com y correos electrónicos)			**X**		
IF	***Instalaciones físicas***					
	Laboratorios de cómputo			**X**		
	Salón de clases			**X**		
	Área de control computo			**X**		
	Área de atención			**X**		
P	***Personal***					
	Usuarios - Estudiantes			**X**		
	Operadores - Docentes			**X**		
	Operadores - Administrativos			**X**		
	Administradores - Soporte Información			**X**		

3.3.1.4 MAR. 21 Identificar las amenazas

Se entiende como tal a la posibilidad de sufrir un acto no deseado que afecte la actividad principal de la entidad o los activos de la entidad, en esta fase según la metodología MAGERIT es necesario determinar que activos son susceptibles de sufrir daño o que pueda sufrir daño o su posible ocurrencia afectando su continuidad (Ministerio de Hacienda y Administraciones Públicas de España, 2012a) estos son ordenados de más a menos y considera los siguientes ítems, se observa en la tabla 10.

Tabla 10. Identificación de las amenazas por dimensiones

	Amenazas	(C) Confidencialidad de la información	(I) Integridad de los datos	(D) Disponibilidad	(A) Autenticidad	(T) Trazabilidad
N	Catástrofes naturales			X		
I	de origen industrial			X		
E	Errores y fallos no intencionados	X	X	X		X
A	Ataques intencionados	X	X	X	X	X

También toma en cuenta la metodología la dualidad de ataques y errores "Amenazas y Errores conforman con frecuencia la misma cosa" la metodología MAGERIT (2012) considera tres modalidades:

- ✓ existencia de errores como amenazas, que no constituyen ataques deliberados
- ✓ existencia de errores que son amenazas, que se constituyen en ataques deliberados
- ✓ existencia de errores que pueden ser o no amenaza por la forma deliberada como suceden los hechos

Como parte del proceso de identificación de las amenazas toma en cuenta la correlación de errores y ataques incluido en el programa PilarBasic (v.7.4.3), la correlación de estos valores se observa en la tabla 11 el cual considera 30 ítems.

Tabla 11. Correlación de errores y ataques

Ítem	**error**	**Ataque**
1	Errores de los usuarios	
2	Errores del administrador	
3	Errores de monitorización (log)	Manipulación de los registros de actividad
4	Errores de configuración	Manipulación de la configuración
5		Suplantación de la identidad del usuario
6		Abuso de privilegios de acceso
7	Deficiencias en la organización	Uso no previsto
8	Difusión de software dañino	Difusión de software dañino
9	Errores de (re)encaminamiento	(Re)encaminamiento de mensajes
10	Errores de secuencia	Alteración de secuencia
11		Acceso no autorizado
12		Análisis de tráfico
13		Repudio
14	Escapes de información	Interceptación de información (escucha)
15	Alteración accidental de la información	Modificación deliberada de la información
18	Destrucción de información	destrucción de información
19	Fugas de información	Revelación de información
20	Vulnerabilidades de los programas (software)	
21	Errores de mantenimiento/actualización de programas (software)	
22		Manipulación de programas
23	Errores de mantenimiento/actualización de equipos (hardware)	Manipulación de los equipos
24	Caída del sistema por agotamiento de recursos	Denegación de servicio
25	Pérdida de equipos	Robo
26		Ataque destructivo
27		Ocupación enemiga
28	Indisponibilidad del personal	Indisponibilidad del personal
29		Extorsión
30		Ingeniería social (picaresca)

Fuente. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II (Ministerio de Hacienda y Administraciones Públicas de España, 2012b, p. 48)

Después de identificar y correlacionar los ítems de errores y ataques el programa valora la amenaza por tipo de activo y dimensión.

3.3.1.5 MAR. 22 Valorar las amenazas

Las amenazas se valoran y está dada por la posibilidad que pueda afectar a un activo por degradación y por la probabilidad de ocurrencia, considera así mismo que todo activo se degrada por lo tanto considera que tanto se vería perjudicado o resultaría el activo si se concretara esta ocurrencia “que posibilidad existe que se concrete la vulnerabilidad” (Ministerio de Hacienda y Administraciones Públicas de España, 2012a).

MAGERIT nos brinda la siguiente tabla de equivalencias para interpretar la valoración de los resultados de la probabilidad de la amenaza.

Probabilidad de la amenaza	
Factor	**Niveles de madurez del CMMI**
0%	-.-
10%	1. Casi seguro que ocurra
50%	2. Muy alto la posibilidad que ocurra
90%	3. Es posible que ocurra
95%	4. Poco probable que ocurra
100%	5. Muy raro que ocurra

Como primer paso determina la posibilidad que suceda la amenaza por dominio de seguridad y factores agravantes y atenuantes sobre la red interna y conexión a internet cuantificando los valores de riesgos por cada criterio, se observa en los valores determinados, cuanto más se acerca al 0% es casi seguro que ocurra la amenaza y cuanto más se acerca al 100% es muy raro que ocurra. Al procesar los datos obtenemos la tabla 12 y 13.

Tabla 12. Valoración de las amenazas del activo por factores agravantes y atenuantes

Factores agravantes y atenuantes				Total	Red Interna	Conexión Internet
Criterios				%	%	%
101	Identificación del atacante					
	101	a	Público en general			
	101	b	Competidor comercial	5%	5%	5%
	101	c	Proveedor de servicios	5%	5%	
	101	d	Grupos de presión política/activistas	5%		
	101	e	Periodistas	5%		
	101	f	Criminales/Vándalos	8%		8%
	101	g	Personal interno	10%	10%	10%
	101	h	bandas criminales	10%		
	101	i	grupos terroristas	10%		
	101	j	servicios de inteligencia - negocios	20%		20%
102	Motivación del atacante					
	102	a	económica (beneficios en dinero)	5%	5%	5%
	102	b	beneficios comerciales	5%	5%	
	102	c	personal propio con problemas de conciencia	10%	10%	
	102	d	personal propio con problemas de interés	10%	10%	10%
	102	e	personal propio con pertenencia a un grupo extremista	30%		
	102	f	con ánimo destructivo	5%	5%	5%
	102	g	con ánimo de causar daño	5%	5%	
	102	h	con ánimo de provocar pérdidas	5%	5%	
103	Beneficio del atacante					
	103	a	moderadamente interesado	5%	5%	
	103	b	muy interesado	10%	10%	10%
	103	c	extremadamente interesado	20%	20%	
106	Atracción del objetivo					
	106	c	objetivo atractivo	5%		5%
	106	d	objetivo muy atractivo	10%	10%	
	106	e	objetivo extremadamente atractivo	15%	15%	
104	Motivación del personal interno					
	104	b	baja calificación profesional / escasa formación	5%	5%	
	104	c	sobrecargados de trabajo	5%	5%	
	104	d	con problemas de conciencia	10%	10%	10%
	104	e	con conflictos de interés	10%	10%	
	104	f	personal asociado a grupos extremistas	30%	30%	

Leyenda: Factor 0% - casi seguro que ocurra; factor 10% - casi seguro que ocurra; factor 50% - muy alto la posibilidad que ocurra; factor 90% - es posible que ocurra; factor 95% - poco probable que ocurra; factor 100% - muy raro que ocurra

Tabla 13. Valoración de las amenazas del activo por factores agravantes y atenuantes

Factores agravantes y atenuantes				Total	Red Interna	Conexión Internet
Criterios				%	%	%
105	Permisos de los usuarios (derechos)					
	105	a	Se permite el acceso a internet	10%	10%	
	105	b	Se permite la ejecución de programas sin autorización previa	20%	20%	20%
	105	c	Se permite la instalación de programas sin autorización previa	30%	30%	30%
	105	d	Se permite la conexión de dispositivos removibles	10%	10%	10%
111	Conectividad del sistema de información					
	111	a	sistema aislado	20%		
	111	b	Conectado a un conjunto reducido y controlado de redes			
	111	c	Conectado a un amplio colectivo de redes conocidas	10%		10%
	111	d	conectado a internet	30%	30%	30%
112	Ubicación del sistema de información					
	112	b	en un área de acceso abierto	10%	10%	10%
	112	c	en un entorno hostil	30%		
301	Disponibilidad					
	301	l	Bajos requerimientos	90%	90%	
302	Integridad					
	302	l	Bajo requerimiento	90%	90%	
303	Confidencialidad					
	303	n	ningún requerimiento	100%		100%
304	Autenticidad					
	304	n	ningún requerimiento	100%		100%
305	Trazabilidad					
	305	l	Bajo requerimiento	90%	90%	

Leyenda: Factor 0% - casi seguro que ocurra; factor 10% - casi seguro que ocurra; factor 50% - muy alto la posibilidad que ocurra; factor 90% - es posible que ocurra; factor 95% - poco probable que ocurra; factor 100% - muy raro que ocurra

En la valoración de las amenazas por activos y dimensiones al consolidar la información obtenemos la tabla 14 con los siguientes resultados. La posibilidad que suceda la amenaza es medida en la dimensión integridad (I), trazabilidad (T) con una valoración de 6,30 en ambos casos en la dimensión datos personales (DP) 6,0 lo que indica que de materializarse ocasionarían un daño grave al activo, del mismo modo en las dimensiones confidencialidad (C) 5,70; disponibilidad (D) 5,60; autenticidad (A) 5,4 se ubica en la posibilidad que el evento ocurra en un nivel bajo, que de materializarse la amenaza generaría un daño importante al activo.

Tabla 14. Resumen de la valoración de las amenazas por activos y dimensiones

Amenazas		D	I	C	A	T	DP
Activos		5,6	6,3	5,7	5,4	6,3	6
AE.1	Récord de notas	3,2	4,5	5,4	3,3	3,8	6
AE.2	Expediente de los estudiantes - matrícula	3,7			3,4	3,9	5,4
AE.3	Examen virtual y presencial	1,9	5,1	5,7	5,1	6,3	4,8
AE.4	Programación de cursos y horarios	3,7					
SI.1	Acceso de los usuarios	2,5		5,1	5,1	5,1	
SI.2	Aula virtual	3,7	2,8	2,8	4,2	3,3	3,6
SI.3	Aula virtual material de estudio	1,9	3,9	3,9	3,9	3,9	2,4
SI.4	Documentos administrativos	5,6	5,4	4,8	5,4	3,9	4,8
EIS.1	Portal web institucional	4,8	6,3	2,8	5,1	5,1	2,4

Leyenda: disponibilidad (D); integridad (I); confidencialidad (C); autenticidad (A); trazabilidad (T); datos personales (DP).
Los valores de 9 (catástrofe); 8 (desastre); 7 (extremadamente grave); 6 (muy crítico); 5 (crítico); 4 (muy alto), 3 (alto); 2 (medio); 1 (bajo); 0 (despreciable).

3.3.1.6 MAR. 31 Identificar las salvaguardas pertinentes

Según Columba (2016) define las salvaguardas o protecciones o contra medidas, son los mecanismos o procedimientos cuyo fin es mitigar el riesgo, pero a través de la tecnología, la mitigación de la amenaza requiere diferentes medidas, algunos requieren organización de los recursos humanos, otra protección física, aplicación de programas o protección técnica del equipo, otras requieren solo organización en los procesos. Según la metodología MAGERIT (2012) esto permite prevenir y hacer frente a las posibles amenazas poniendo énfasis en las técnicas a aplicar, debido a los cambiante de los riesgos, sea por obsolescencia de los equipos, modernización de los atacantes, mejoras en la protección, o es necesario renovar los activos por exigencias legales, estas están orientadas a su vez según la metodología para salvaguardar todo el sistema de las TIC de ataques contra las dimensiones contenidas en la gestión del riesgo (Ministerio de Hacienda y Administraciones Públicas de España, 2012b).

Determinado la posibilidad de amenaza por dominio a través del programa informático PilarBasic se realiza el diagnóstico a nivel de Salvaguardas el tipo de protección a aplicar y el peso relativo asignado a cada uno de los ítems.

En la tabla 15 y 16 apreciamos en la primera columna se refiere a cada aspecto de seguridad si corresponde a) gestión administrativa; b) soluciones técnicas (software,

hardware, comunicaciones) c) seguridad física; d) gestión del personal; la segunda columna está referida al tipo de protección a aplicar, la tercera columna está referida al tipo de recomendación que refiere el programa: 0,1 (blanco) no recomendable porque no aplica; 2,3 (amarillo) recomendable; 4,5 (marrón claro) bastante recomendable; 6,7 (marrón oscuro) muy recomendable; 8,9 (rojo) necesaria; la cuarta columna actual se refiere al nivel de riesgo que se encuentra actualmente expuesto los activos sin aplicar salvaguardas, la columna objetivo se refiere a las salvaguardas que tiene que aplicar la institución recomendadas por la metodología, la columna PILAR indica la situación de la empresa después de aplicar las salvaguardas para dar cumplimiento a la norma, reduciendo su exposición al riesgo y por último la columna paraguas indica la importancia de la salvaguarda y la siguiente columna el peso relativo asignado; el color gris (1) interesante, verde (1) importante; marrón claro (2) muy importante; rojo (3) crítica. La columna salvaguardas indica el tipo de protección a aplicar para dar cumplimiento a la normativa legal.

Tabla 15. Análisis de riesgos, medidas técnicas y organizativas de la seguridad de la información

									Nivel de madurez
Aspecto	**T. de protecc.**	**Recomendació**	**Actual**	**Objetivo**	**PIL/AR**	**Paraguas**			**Salvaguardas**
								Salvaguardas	
G	EL	7				3	**IA**	**Identificación y autenticación**	
G	std	3				1	IA.1	Se dispone de normativa de identificación y autenticación	
G	proc	3				1	IA.2	Se dispone de procedimientos para las tareas de identificación y autenticación	
G	EL	5				1	IA.3	Identificación de los usuarios	
G	EL	5				3	IA.3.1	Cada usuario recibe un identificador exclusivo (no compartido)	
G	EL	3				0	IA.3.2	La identificación del usuario no indica ni su función ni su nivel de privilegios	
T	EL	3				1	IA.3.3	Las cuentas de invitados están sometidas a un control estricto	
G	EL	5				1	IA.4	Gestión de la identificación y autenticación del usuario	
G	AD	2				1	IA.4.1	Se mantiene un registro de todos los usuarios con su identificador	
G	AD	5				3	IA.4.2	Alta, activación, modificación y baja de las cuentas de usuario	
G	AD	2				1	IA.4.2.1	Altas. Creación de nuevas cuentas	
G	AD	2				1	IA.4.2.2	Activación de cuentas de usuario	
G	AD	2				1	IA.4.2.3	Modificación de cuentas de usuario	
G	AD	2				1	IA.4.2.4	Suspensión temporal de cuentas de usuario	
G	AD	5				3	IA.4.2.5	Terminación: eliminación de cuentas	
G	EL	5				3	IA.4.2.5.1	Las cuentas que ya no son necesarias se eliminan o se bloquean	
G	AD	2				1	IA.4.2.5.2	Los identificadores no se reutilizan	
G	AD	2				1	IA.4.2.5.3	La información relevante se retiene de acuerdo con la normativa de seguridad	
G	EL	4				2	IA.4.3	Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar	
G	EL	3				1	IA.4.4	Se limita el número de autenticadores necesarios por usuario	
G	EL	3				1	IA.4.5	Los autenticadores se distribuyen de forma segura	
G	AD	2				1	IA.4.6	El usuario se compromete por escrito a mantener la confidencialidad del autenticado	
G	AD	2				1	IA.4.7	El usuario confirma la recepción del autenticador	
G	AD	2				1	IA.4.8	El usuario se hace cargo personalmente del control del autenticador	
G	MN	2				1	IA.4.9	Existen canales para la comunicación de incidentes que afecten a los autenticadores	
G	IM	5				3	IA.4.a	Las cuentas se suspenden al ser comprometidas o existir sospecha de ello	
G	EL	5				2	IA.5	Cuentas especiales (administración)	
G	EL	4				2	IA.5.1	Hay cuentas específicas para administradores del sistema	
G	EL	5				3	IA.5.2	Hay cuentas específicas para administradores de seguridad	
G	EL	3				1	IA.5.3	Hay cuentas específicas para actividades de auditoría	
G	AD	2				1	IA.5.4	Sólo se utilizan para ejecutar un número limitado y controlado de actividades: las que requieren sus privilegios especiales	
G	AD	2				1	IA.5.5	Las cuentas especiales están sujetas a procesos específicos de gestión	

Fuente. Herramienta Pilar Basic (v. 1.7.1)

Tabla 16. Análisis de riesgos, medidas técnicas y organizativas de la seguridad de la información

									Nivel de madurez
Aspecto	**T. de protecc.**	**Recomendació**	**Actual**	**Objetivo**	**PIL/AR**	**Paraguas**		**Salvaguardas**	**Salvaguardas**
T	EL	6				2		IA.6	Canal seguro de autenticación
G	PR	7				3		IA.7	(xor) Factores de autenticación que se requieren:
G	PR	7				1		IA.7.2	Algo que se conoce (ej. Contraseña)
G	PR	7				1		IA.7.3	Certificados software (criptografía de clave pública)
G	PR	7				1		IA.7.4	Algo que se es. - biometría (ej. Huella dactilar)
G	PR	7				1		IA.7.5	Factores: token + contraseña
T	EL	7				3	AC		Control de acceso lógico
G	PR	7				3	D		Protección de la información
G	EL	0				3	K		Protección de claves criptográficas
G	PR	6				1	S		Protección de los servicios
G	PR	0				2	SW		Protección de las aplicaciones informáticas (SW)
G	PR	7				2	HW		Protección de los equipos Informáticos (HW)
G	PR	0				3	COM		Protección de las comunicaciones
G	PR	0				1	IP		Sistema de protección de frontera lógica
G	PR	0				2	MP		Protección de los soportes de información
G	PR	6				1	AUX		Elementos Auxiliares
F	EL	5				1	PPE		Protección física de los equipos
F	PR	7				2	L		Protección de las instalaciones
F	EL	0				1	PPS		Protección del perímetro físico
P	PR	6				2	PS		Gestión del personal
G	PR	0				1	PDS		Servicios potencialmente peligrosos
G	CR	5				2	IR		Gestión de incidentes
T	PR	7				3	Tools		Herramientas de seguridad
G	CR	0				1	V		Gestión de vulnerabilidades
T	MN	6				2	A		Registro y auditoria
G	RC	5				2	BC		Continuidad del negocio
G	AD	4				1	G		Organización
G	AD	6				1	E		Relaciones externas
G	AD	4				0	NEW		Adquisición / desarrollo

Fuente. Herramienta Pilar Basic (v. 1.7.1)

Leyenda:

	Aspecto de la salvaguarda		**Tipo de protección**	**Peso relativo**	
G	Para Gestión	PR	Prevención	Máximo peso	Critica
T	Para Técnico	DR	Disuasión	Peso alto	Muy importante
F	Para seguridad física	EL	Eliminación	Peso normal	Importante
P	Para gestión del personal	IM	Minimización del impacto	Peso bajo	Interesante

	CR	Corrección	Aseguramiento: componentes certificados
	RC	Recuperación	
	AD	Administrativa	
	AW	Concienciación	
	DC	Detección	
	MN	Monitorización	
	std	Norma	
	proc	Procedimiento	
	cert	Certificación o acreditación	
	(o)	La salvaguarda es excesiva para el riesgo a cubrir	
	(u)	La salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger	

Fuente. Metodología Magerit (Ministerio de Hacienda y Administraciones Públicas de España, 2012a, p. 31).

3.3.1.7 MAR. 32 Valoración de las salvaguardas

La valoración de las salvaguardas toma como criterio de eficacia de protección indicado en MAGERIT a través de la herramienta PilarBasic, la tabla 17 y 18 nos brinda tres columnas ubicadas a la derecha, la situación actual (diagnóstico), el objetivo (recomendación) y la sugerencia a mejorar o mantener según la metodología MAGERIT, indicando a su vez el nivel de madurez con la siguiente simbología.

Nivel de salvaguarda	**Significado - MAGERIT**
L0	Inexistente
L1	Inicial/ad hoc
L2	Reproducible, pero intuitivo
L3	Proceso definido
L4	Gestionado y medible
L5	Optimizado

Tabla 17. Valoración de las salvaguardas por nivel de madurez

			Nivel de madurez		
		Salvaguardas	**Actual**	**Objetivo**	**PILAR**
Salvaguardas			**L1-L3**	**L3-L5**	**L2-L4**
IA	**Identificación y autenticación**		**L3**	**L4**	**L2-L4**
	IA.1	Se dispone de normativa de identificación y autenticación	L3	L4	L3
	IA.2	Se dispone de procedimientos para las tareas de identificación y autenticación	L3	L4	L3
	IA.3	**Identificación de los usuarios**	L3	L4	L3
		IA.3.1 Cada usuario recibe un identificador exclusivo (no compartido)	L3	L4	L3
		IA.3.2 La identificación del usuario no indica ni su función ni su nivel de privilegios	L3	L4	L3
		IA.3.3 Las cuentas de invitados están sometidas a un control estricto	L3	L4	L3
	IA.4	Gestión de la identificación y autenticación del usuario	L3	L4	L2-L3
		IA.4.1 Se mantiene un registro de todos los usuarios con su identificador	L3	L4	L2
		IA.4.2 Alta, activación, modificación y baja de las cuentas de usuario	L3	L4	L2-L3
		IA.4.2.1 Altas. Creación de nuevas cuentas	L3	L4	L2
		IA.4.2.2 Activación de cuentas de usuario	L3	L4	L2
		IA.4.2.3 Modificación de cuentas de usuario	L3	L4	L2
		IA.4.2.4 Suspensión temporal de cuentas de usuario	L3	L4	L2
		IA.4.2.5 Terminación: eliminación de cuentas	L3	L4	L2-L3
		IA.4.2.5.1 Las cuentas que ya no son necesarias se eliminan o se bloquean	L3	L4	L3
		IA.4.2.5.2 Los identificadores no se reutilizan	L3	L4	L2
		IA.4.2.5.3 La información relevante se retiene de acuerdo con la normativa de seguridad	L3	L4	L2
		IA.4.3 Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar	L3	L4	L3
		IA.4.4 Se limita el número de autenticadores necesarios por usuario	L3	L4	L3
		IA.4.5 Los autenticadores se distribuyen de forma segura	L3	L4	L3
		IA.4.6 El usuario se compromete por escrito a mantener la confidencialidad del autenticado	L4	L5	L2
		IA.4.7 El usuario confirma la recepción del autenticador	L5	L6	L2
		IA.4.8 El usuario se hace cargo personalmente del control del autenticador	L6	L7	L2
		IA.4.9 Existen canales para la comunicación de incidentes que afecten a los autenticadores	L7	L8	L2
		IA.4.a Las cuentas se suspenden al ser comprometida o existir sospecha de ello	L3	L4	L3

Tabla 18. Valoración de las salvaguardas por nivel de madurez

			Nivel de madurez		
		Salvaguardas	**Actual**	**Objetivo**	**PILAR**
	IA.5	Cuentas especiales (administración)	L3	L4	L2-L3
	IA.5.1	Hay cuentas específicas para administradores del sistema	L4	L5	L3
	IA.5.2	Hay cuentas específicas para administradores de seguridad	L5	L6	L3
	IA.5.3	Hay cuentas específicas para actividades de auditoría	L6	L7	L3
	IA.5.4	Sólo se utilizan para ejecutar un número, limitado y controlado de actividades: las que requieren sus privilegios especiales	L7	L8	L2
	IA.5.5	Las cuentas especiales están sujetas a procesos específicos de gestión	L8	L9	L2
	IA.6	Canal seguro de autenticación	L3	L4	L4
	IA.7	(xor) Factores de autenticación que se requieren:	L3	L4	L3-L4
	IA.7.1	Algo que se tiene - token físico (ej. Tarjeta)	n.s	n.s	L3-L4
	IA.7.2	Algo que se conoce (ej. Contraseña)	L3	L4	L3-L4
	IA.7.3	Certificados software (criptografía de clave pública)	n.s	n.s	L3-L4
	IA.7.4	Algo que se es - biometría (ej. Huella dactilar)	n.s	n.s	L3-L4
	IA.7.5	Factores: token + contraseña	n.s	n.s	L3-L4
AC		Control de acceso lógico	L3	L4	L2-L4
D		Protección de la información	L3	L3	L2-L4
K		Protección de claves criptográficas	L3	L3	n.a.
S		protección de los servicios	L3	L3	L2-L4
SW		Protección de las aplicaciones informáticas (SW)	L2	L3	n.a.
HW		Protección de los equipos Informáticos (HW)	L2	L3	L2-L4
COM		Protección de las comunicaciones	L3	L4	n.a.
IP		Sistema de protección de frontera lógica	L1	L4	n.a.
MP		Protección de los soportes de información	L2	L4	n.a.
AUX		Elementos Auxiliares	L2	L4	L2-L4
PPE		Protección física de los equipos	L2	L4	L3
L		Protección de las instalaciones	L3	L5	L2-L4
PPS		Protección del perímetro físico	L1	L5	n.a.
PS		Gestión del personal	L1	L4	L2-L4
PDS		Servicios potencialmente peligrosos	L1	L4	n.a.
IR		Gestión de incidentes	L1	L5	L2-L3
Tools		Herramientas de seguridad	L1	L3	L2-L4
V		Gestión de vulnerabilidades	L2	L3	n.a.
A		Registro y auditoria	L2	L3	L2-L4
BC		Continuidad del negocio	L1	L3	L2-L3
G		Organización	L1	L4	L2-L3
E		Relaciones externas	L1	L3	L2-L4
NEW		Adquisición / desarrollo	L1	L3	L2-L3

3.3.1.8 MAR. 41 Estimar el impacto del riesgo potencial

Después de conocer las salvaguardas que debemos aplicar según las recomendaciones realizado el diagnostico, debemos estimar el impacto del riesgo de los activos de manera cuantificada, es decir cuál es el riesgo sino aplicamos salvaguardas (diagnóstico), el siguiente paso es valorar el riesgo repercutido por la dependencia de los activos entre el nivel inferior y superior y por último valorar el peligro restante después de aplicar protecciones. El efecto del peligro por activo nos muestra la tabla 19, los activos esenciales se encuentran en la situación de catástrofe nivel 9 en la dimensión de disponibilidad, las demás dimensiones en situación extremadamente crítico nivel 7.

Tabla 19. Estimación del impacto del riesgo de los activos por dimensiones

	Activos /Dominios de seguridad		Valoración (D) Disponibilidad	(I) Integridad de los datos	(C) Confidencialidad de la información	(A) Autenticidad	(T) Trazabilidad	(DP) Datos Personales
AE	*Activos esenciales*		9	7	7	7	7	7
	AE.1	1. Gestión de notas - récord de notas	5	6	7	4	7	7
	AE.2	2. Expediente de los estudiantes - matricula	4	n.a.	n.a.	2	3	6
	AE.3	3. Examen virtual y presencial	1	5	6	5	7	5
	A3.4	4. Programación de cursos y horarios	4	n.a.	n.a.	n.a.	n.a.	n.a.
SI	*Servicios internos*							
	SI.1	1. Acceso de los usuarios	2	n.a.	5	5	5	n.a.
	SI.2	2. Aula virtual - Salón de clase	4	1	1	4	4	3
	SI.3	3. Aula virtual - Material de estudio -módulos	1	3	3	3	3	1
	SI.4	4. Documentos administrativos- Actas virtuales	9	7	6	7	5	5
EI	*Equipamiento informático*							
	EIS.1	1. Portal web institucional	6	7	1	5	5	1

Nota: ver leyenda en la tabla 21.

El impacto del riesgo por dominio de seguridad nos muestra la tabla 20, la base de la red interna se encuentra en situación de catástrofe nivel 9 en la dimensión de disponibilidad, las demás dimensiones en situación extremadamente crítico nivel 7. La base de conexión a internet se encuentra en situación muy crítico en nivel 6, la dimensión disponibilidad, confidencialidad, datos personales, la dimensión integridad y trazabilidad, se encuentran en el nivel 7 extremadamente crítico, y la dimensión autenticidad, se encuentra en el nivel 5 crítico.

Tabla 20. Estimación del impacto del riesgo por dominios de seguridad y dimensiones

Dominios de seguridad / Activos		Valoración					
		(D) Disponibilidad	(I) Integridad de los datos	(C) Confidencialidad de la información	(A) Autenticidad	(T) Trazabilidad	(DP) Datos Personales
Base - Red Interna		*9*	*7*	*7*	*7*	*7*	*7*
AE.1	1. Gestión de notas - récord de notas	5	6	7	4	7	7
SI.4	4. Documentos administrativos- Actas virtuales	9	7	6	7	5	5
Conexión a Internet		*6*	*7*	*6*	*5*	*7*	*6*
AE.2	2. Expediente de los estudiantes - matricula	4	n.a.	n.a.	2	3	6
AE.3	3. Examen virtual y presencial	1	5	6	5	7	5
A3.4	4. Programación de cursos y horarios	4	n.a.	n.a.	n.a.	n.a.	n.a.
SI.1	1. Acceso de los usuarios	2	n.a.	5	5	5	n.a.
SI.2	2. Aula virtual - Salón de clase	4	1	1	4	4	3
SI.3	3. Aula virtual - Material de estudio -módulos	1	3	3	3	3	1
EIS.1	1. Portal web institucional	6	7	1	5	5	1

Leyenda: Nivel del riesgo, catástrofe (9); desastre (8); extremadamente crítico (7); muy crítico (6); 5 (crítico); muy alto (4); alto (3); medio (2); bajo (1); despreciable (0).

3.3.1.9 MAR. 42 Estimar el riesgo indirecto repercutido

Se denomina riesgo indirecto repercutido al riesgo que se genera entre un activo (un activo tiene su propio valor) de orden superior y un activo de orden inferior debido a que existe entre ambos una dependencia, al recibir una amenaza uno de ellos afecta al otro activo de orden inferior o de orden superior de esa manera este riesgo valora el daño dentro de la institución, lo valora de manera explícita, calcula el daño de la siguiente manera: riesgo repercutido = impacto repercutido * probabilidad.

El programa PilarBasic nos muestra el resumen en la tabla 21, este muestra el impacto del riesgo indirecto repercutido potencial actual (diagnostico) por dimensión donde se encuentra valor más alto en la dimensión integridad y trazabilidad con un valor ambos de 6,30 y la dimensión datos personales con un valor de 6,00 lo que indica que la dimensión se encuentra en un nivel muy crítico, la dimensión disponibilidad con un valor de 5,60; la dimensión confidencialidad con un valor de 5,70 se encuentran en un nivel crítico.

Tabla 21. Valoración del riesgo indirecto repercutido de los activos esenciales sin salvaguardas

Amenazas / Activos		(D) Disponibilidad	(I) Integridad de los datos	(C) Confidencialidad de la información	(A) Autenticidad	(T) Trazabilidad	(DP) Datos Personales
ACTIVOS		4,50	4,10	4,00	3,00	4,20	6,00
AE.1	Récord de notas	2,10	2,90	4,00	1,10	2,90	6,00
AE.2	Expediente de los estudiantes - matricula	2,50			1,10	1,90	5,40
AE.3	Examen virtual y presencial	0,95	2,90	3,50	2,90	4,20	4,80
AE.4	Programación de cursos y horarios	2,50					
SI.1	Acceso de los usuarios	1,40		2,90	2,90	3,00	
SI.2	Aula virtual	2,50	0,90	0,90	2,00	2,50	3,60
SI.3	Aula virtual material de estudio	0,95	1,70	1,70	1,70	1,90	2,40
SI.4	Documentos administrativos - actas	4,50	3,50	3,40	3,00	1,70	4,80
EIS. 1	Portal web institucional	3,70	4,10	0,90	2,90	3,00	2,40

Para la interpretación de la tabla 22 se sigue la siguiente leyenda

-9	catástrofe	-8	desastre	-7	extremadamente crítico
-6	muy crítico	-5	crítico	-4	muy alto
-3	alto	-2	medio	-1	bajo
0	despreciable				

3.3.1.10 Selección de salvaguardas

Después de estimar el riesgo potencial y repercutido se debe seguir las recomendaciones de la tabla 15 y 16, en lo que respecta a la aplicación de las salvaguardas, las salvaguardas se basan en la ISO 27002:2013, y según los procedimientos contenidos en la metodología MAGERIT versión 3.0 y descritos en el manual de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I, II y III, los valores quedan

establecidos en la tabla 22 donde se observa el riesgo residual o remanente que queda posterior o después de la adopción las salvaguardas aplicadas.

La dimensión datos personales con una valoración de 1,60; autenticidad 1,60; confidencialidad 1,90; disponibilidad 1,60 se encuentran en una situación de riesgo bajo; las dimensiones de integridad y trazabilidad con un valor de 2,50 cada uno se encuentran en una situación de riesgo medio, se visualiza el resumen en la tabla 22.

Tabla 22. Valoración del riesgo indirecto repercutido de los activos esenciales después de aplicar salvaguardas

Valoración de los riesgos: Riesgo PILAR - Aplicando salvaguardas							
Amenazas / Activos		(D) Disponibilidad	(I) Integridad de los datos	(C) Confidencialidad de la información	(A) Autenticidad	(T) Trazabilidad	(DP) Datos Personales
ACTIVOS		1,60	2,50	1,90	1,60	2,50	1,60
AE.1	Récord de notas	0,4	0,94	1,60	0,70	0,77	1,60
AE.2	Expediente de los estudiantes - matricula	0,77			0,71	0,83	0,99
AE.3	Examen virtual y presencial	0,42	1,30	1,90	1,30	2,50	0,87
AE.4	Programación de cursos y horarios	0,77					
SI.1	Acceso de los usuarios	0,53		1,30	1,30	1,30	
SI.2	Aula virtual	0,77	0,59	0,58	0,86	0,68	0,64
SI.3	Aula virtual material de estudio	0,42	0,83	0,83	0,83	0,83	0,40
SI.4	Documentos administrativos - actas	1,60	1,60	1,00	1,60	0,83	0,89
EIS.1	Portal web institucional	1,00	2,50	0,59	1,30	1,30	0,40

Leyenda: Nivel del riesgo, catástrofe (9); desastre (8); extremadamente crítico (7); muy crítico (6); 5 (crítico); muy alto (4); alto (3); medio (2); bajo (1); despreciable (0).

El siguiente proceso es determinar el nivel de madurez para evaluar las salvaguardas aplicadas, PilarBasic utiliza su propia nomenclatura, pero adaptado del modelo de madurez de capacidades o CMM (capability Maturity Model), tal como mostramos a continuación:

eficacia	nivel	significado	administrativo
0%	L0	inexistente	inexistente
10%	L1	inicial / ad hoc	iniciado
50%	L2	reproducible, pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Se observa en la tabla 23 que en el global de los controles de la información de seguridad ubicado en la cuarta línea y en la columna con salvaguarda se encuentra con un valor de 87 (L3-L5) en el dominio de Base de la Red Interna, eso quiere decir que se encuentra en un nivel de madurez entre parcialmente realizado y en funcionamiento, superando la recomendación del programa PilarBasic mantener un valor esperado entre 65 y 73 (L2-L4) es decir iniciado y parcialmente realizado.

Tabla 23. Valoración del riesgo indirecto repercutido de los dominios de seguridad después de aplicar las salvaguardas

Tabla de valoración de las dimensiones por nivel de madurez y salvaguardas		Promedio			
		Nivel (índice) de madurez		Nivel (índice) de madurez	
BASE - RED INTERNA Dominios	Control: 27002:2013	Con salvaguarda	Recomendación	Con salvaguarda	Recomendación
	Resumen de la información a través de los controles de seguridad	L3-L5	L2-L4	87	73-65
5	Políticas de seguridad de la información	L4	L2	90	50
6	Organización de la seguridad de la información	L3-L5	L2-L4	88	72-69
7	Seguridad relativa a los recursos humanos	L4	L3-L4	90	81-71
8	Gestión de activos	L3-L5	L2-L3	87	76-69
9	Control de acceso	L3-L4	L2-L4	89	83-73
10	Criptografía	L3-L4	L2	83	50
11	Seguridad física y del entorno	L3-L5	L2-L4	91	75-71
12	Seguridad de las operaciones	L3-L5	L2-L4	82	80-71
13	Seguridad de las comunicaciones	L3-L4	L3-L4	88	85-74
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	L3-L4	L2-L3	80	70-59
15	Relación con proveedores	L3	L2-L4	80	72-57
16	Gestión de incidentes de seguridad de la información	L5	L3	100	80-68
17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	L3-L5	L3-L4	85	72-74
18	Cumplimiento	L3-L4	L2-L3	87	66-58

3.4 VERIFICACIÓN DE LA HIPÓTESIS

En la demostración de la hipótesis se plantea primero la prueba estadística de normalidad en base los resultados obtenidos de las variables, esto nos permitirá definir si esta es paramétrica o no paramétricas:

Teniendo en cuenta que son 9 ítems para evaluar, planteamos la prueba estadística de Shapiro-Wilk para evaluar la normalidad de la muestra con respecto a la población.

Pruebas de normalidad			
	Shapiro-Wilk		
	Estadístico	gl	Sig.
Diagnostico - antes	,970	9	,892
Después con salvaguardas	,919	9	,384

*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors

Regla de decisión:

Si p valor calculado < al 5% entonces la muestra no se distribuye normalmente

Si p valor calculado > al 5% entonces la muestra se distribuye normalmente

Resultado:

p valor (0,892) y (0,384) > 5% entonces afirmamos que la muestra se distribuye normalmente por lo tanto es paramétrico la prueba a usar en la demostración de la hipótesis.

En este estudio se usará como estadístico de prueba, el coeficiente de correlación de Pearson, ya que de acuerdo con la investigación planteada se busca la asociación o interdependencia entre dos variables que pueden ser continuas o discretas. (Hernández et al., 2006).

El planteamiento de la hipótesis tenemos

H_o: la metodología MAGERIT no tiene una relación positiva con la Gestión del riesgo en la TIC del ISTO de Tingo María.

H_1: la metodología MAGERIT tiene una relación positiva con la Gestión del riesgo en la TIC del ISTO de Tingo María.

Para proceder con el cálculo se necesita establecer el nivel de significancia (máximo error permisible que se está dispuesto aceptar) teniendo en cuenta que está establecido convencionalmente un nivel de significancia del 5%.

Tabla 24. Correlación de Pearson

		Diagnostico - antes	Después con salvaguardas
Diagnostico - antes	Correlación de Pearson	1	,828**
	Sig. (bilateral)		,006
	N	9	9
Después con salvaguardas	Correlación de Pearson	,828**	1
	Sig. (bilateral)	,006	
	N	9	9

**. La correlación es significativa en el nivel 0,01 (bilateral).

Regla de decisión

Si el p valor > 5% aceptamos la H_o nula

Si p valor < 5% rechazamos la H_o nula

Resultados

P valor (0.006) < 5% rechazamos la hipótesis nula y aceptamos la hipótesis alterna, es decir "la metodología MAGERIT tiene una relación positiva con la Gestión del riesgo en la TIC del ISTO de Tingo María".

El grado de asociación a su vez está representado por el coeficiente de correlación. Martínez, et al. (2009) establece en su investigación el rango de relación:

Rango de Relación	
0 – 0,25	Escasa o nula
0,26-0,50	Débil
0,51- 0,75	Entre moderada y fuerte
0,76- 1,00	Entre fuerte y perfecta 5

Al ser el resultado de medida del coeficiente de correlación de 0.828, se afirma que esta relación es fuerte y positiva, es decir a mayor riesgo mayor salvaguardas.

3.4.1 Demostración de las hipótesis específicas

A) Primera hipótesis específica

H_o: El riesgo identificado en los activos de las TIC que posee el ISTO Tingo María con la metodología MAGERIT, no es bajo.

H_1: El riesgo identificado en los activos de las TIC que posee el ISTO Tingo María con la metodología MAGERIT, es bajo.

Para la demostración de la hipótesis determinamos el valor de los riesgos calculados por el Programa Pilar, que nos da los siguientes resultados:

Tabla 25. Valoración del riesgo indirecto repercutido de los activos actual

Amenazas / Activos	(D) Disponibilidad	(I) Integridad de los datos	(C) Confidencialidad de la información	(A) Autenticidad	(T) Trazabilidad	(DP) Datos Personales
ACTIVOS	4,50	4,10	4,00	3,00	4,20	6,00

Fuente: resumen de la tabla 21

Al promediar el riesgo actual de los activos, nos da un valor de 4,30; según la tabla de valoración del riesgo de MAGERIT – se ubicaría en un nivel muy alto.

Leyenda

(9) catástrofe
(8) desastre
(7) extremadamente crítico
(6) muy crítico
(5) crítico
(4) muy alto
(3) alto
(2) medio
(1) bajo
(0) despreciable

Fuente. Manual Pilar. Niveles de riesgo (p. 1034)

Como el promedio se ubica según la tabla de valoración en el nivel 4 (muy alto) aceptamos la hipótesis nula, es decir “El riesgo identificado en los activos de las TIC que posee el ISTO Tingo María con la metodología MAGERIT, no es bajo”.

B) Para analizar la segunda hipótesis específica planteamos lo siguiente:

H_o: El riesgo analizado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, no es subsanable a corto tiempo.

H_1: El riesgo analizado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, es subsanable a corto tiempo.

Para Chiavenato (2001, p. 346, 347) el control es la actividad que controla que se llegue al objetivo deseado y los divide en control estratégico que corresponda al nivel institucional y ve el cumplimiento de las políticas institucionales, el control táctico ejercido a nivel intermedio o control gerencial (integra presupuesto, costos, finanzas, contabilidad), el control operacional que son actividades no desempeñadas por el personal administrativo como las actividades del proceso cibernético.

Habiendo definido los tipos de controles el control táctico queda descartado por ser un tipo de control que no se adecua a los propósitos de la investigación, para demostrar esta hipótesis específica se toma en cuenta la ISO/IEC de Normas Técnicas 27002:2013 MAGERIT toma 14 controles de acuerdo con la norma indicada (ver tabla 26), los mismos que son necesarios definirlos de acuerdo a los tipos de control estratégico (cumplimiento de políticas institucionales) y operativos (controles de las TIC) a fin de determinar las áreas competentes de su gestión, si es por la propia entidad o por personal especializado en sistemas e informática.

Además, basándonos en la tesis de Ortiz (2018, p. 108) aplica el criterio sobre la definición de las áreas en estratégico y operativo queda definido de la siguiente manera:

a) Control estratégico: control administrativo que depende de la gerencia o propietarios del negocio para el cumplimiento de las políticas institucionales.
b) Control operativo: a cargo de personal de sistemas.

Quedando clasificado en los siguientes criterios:

Tabla 26. Riesgos y controles aplicados en el ISTO Tingo María

Control: 27002:2013	Tipo de control	
Código de prácticas para los controles de seguridad de la información	Estratégico	Operativo
Políticas de seguridad de la información	X	
Organización de la seguridad de la información	X	
Seguridad relativa a los recursos humanos	X	
Gestión de activos		X
Control de acceso		X
Criptografía		X
Seguridad física y del entorno		X
Seguridad de las operaciones		X
Seguridad de las comunicaciones		X
Adquisición, desarrollo y mantenimiento de los sistemas de información		X
Relación con proveedores		X
Gestión de incidentes de seguridad de la información		X
Aspectos de seguridad de la información para la gestión de la continuidad del negocio	X	
Cumplimiento de políticas y normas de seguridad	X	

Fuente. ISO 27002:2013 y adaptado de Ortiz (2018).

Teniendo en cuenta el proceso y las coordinaciones con la gerencia del ISTO, la implementación:

Los controles de tipo estratégico se analizan y definen con el gerente quedando a su cargo el cumplimiento de los controles de las políticas institucionales. Los controles de naturaleza operativa quedan a cargo de la gerencia para el contrato de un ingeniero en sistemas.

Después de coordinar los controles sobre el riesgo analizado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, es subsanable a corto tiempo.

C) Para analizar la tercera hipótesis planteamos lo siguiente:

Ho: El impacto del riesgo cualitativo identificado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, no es bajo.

H1: El impacto del riesgo cualitativo identificado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, es bajo.

Tabla 27. Valoración del riesgo de las amenazas

Valoración de los riesgos: Riesgo Potencial - Impacto								
Amenazas / Activos		(D) Disponibilidad	(I) Integridad de los datos	(C) Confidencialidad de la información	(A) Autenticidad	(T) Trazabilidad	(DP) Datos Personales	Promedio
ACTIVOS		5,60	6,30	5,70	5,40	6,30	6,00	5,88
AE.1	Récord de notas	3,20	4,50	5,40	3,30	3,80	6,00	4,37
AE.2	Expediente de los estudiantes - matricula	3,70			3,40	3,90	5,40	4,10
AE.3	Examen virtual y presencial	1,90	5,10	5,70	5,10	6,30	4,80	4,82
AE.4	Programación de cursos y horarios	3,70						3,70
SI.1	Acceso de los usuarios	2,50		5,10	5,10	5,10		4,45
SI.2	Aula virtual	3,70	2,80	2,80	4,20	3,30	3,60	3,40
SI.3	Aula virtual material de estudio	1,90	3,90	3,90	3,90	3,90	2,40	3,32
SI.4	Documentos administrativos - actas	5,60	5,40	4,80	5,40	3,90	4,80	4,98
EIS.1	Portal web institucional	4,80	6,30	2,80	5,10	5,10	2,40	4,42

Leyenda: Nivel del riesgo, catástrofe (9); desastre (8); extremadamente crítico (7); muy crítico (6); 5 (crítico); muy alto (4); alto (3); medio (2); bajo (1); despreciable (0). Manual Pilar. Niveles de riesgo (p. 1034).

Regla de decisión:

Si rango del riesgo > 3 es alto

Si rango del riesgo < 3 es bajo

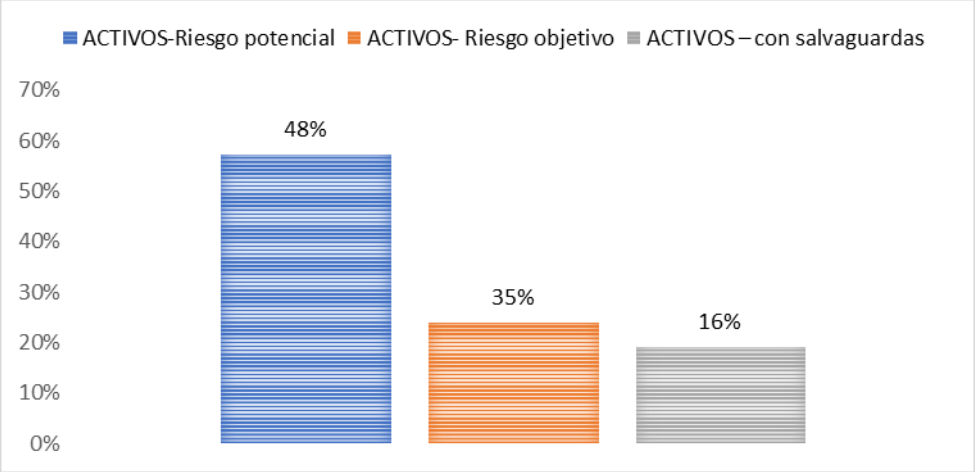
Para determinar si es alto o bajo, nos guiamos de la tabla de valoración del riesgo, donde se observa que en todos los casos en promedio superan el rango del número 3 en el detalle de los activos, y de manera global en el activo se observa que se obtiene una media del 5,88 admitimos la hipótesis nula, entonces el impacto del riesgo cualitativo identificado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, no es bajo, es decir el impacto del riesgo potencial en los activos es alto.

IV. RESULTADOS Y DISCUSIÓN

Identificar el riesgo en los activos de las Tecnologías de la Información y Comunicación que posee el Instituto Superior Tecnológico del Oriente de Tingo María con la metodología MAGERIT, aplicando el Software PILAR Basic versión (7.4.3) permitió demostrar la hipótesis que "la implementación de la metodología MAGERIT como estrategia de controles en la seguridad de las TIC la gestión del riesgo mejora significativamente en el Instituto Tecnológico del Oriente de Tingo María".

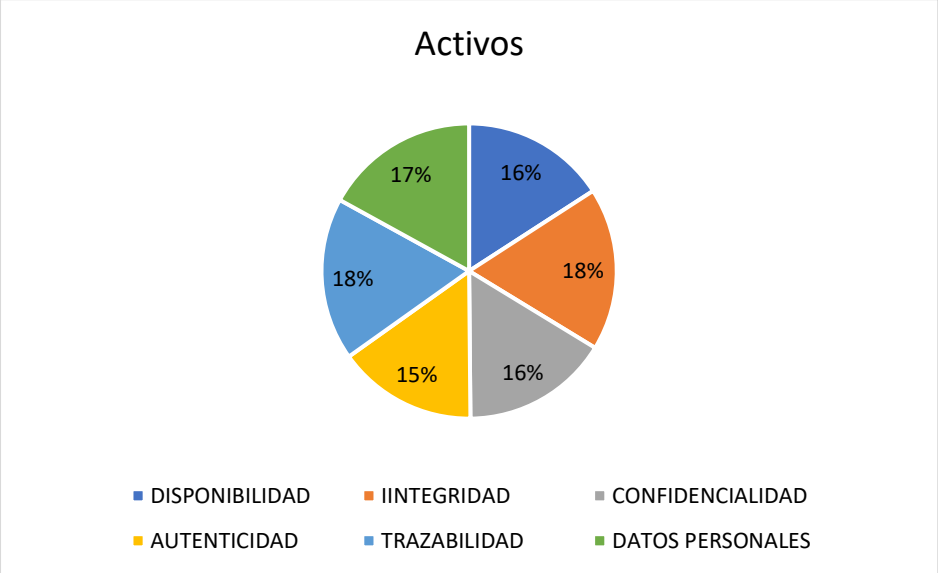
Al sumar la tabla 14, 21 y 22, nos muestra la valoración del riesgo potencial (diagnostico) el objetivo (riesgo repercutido) y el riesgo después de aplicar salvaguardas que nos muestra el software PilarBasic, cuyo resumen se visualiza en la figura 4, el 48% en promedio de los activos se encontraban inicialmente con riesgo potencial, bajo riesgo repercutido se encontraba el 35% de los activos, después de aplicar las salvaguardas queda bajo riesgo el 16% de los activos.

Figura 4. Nivel del riesgo sin y con salvaguardas



Del mismo modo la metodología nos permite identificar y analizar los riesgos en las TIC por dimensión, donde se observa la proporción identificada del riesgo por cada dimensión en la figura 5.

Figura 5. Riesgos identificados en los activos por dimensión



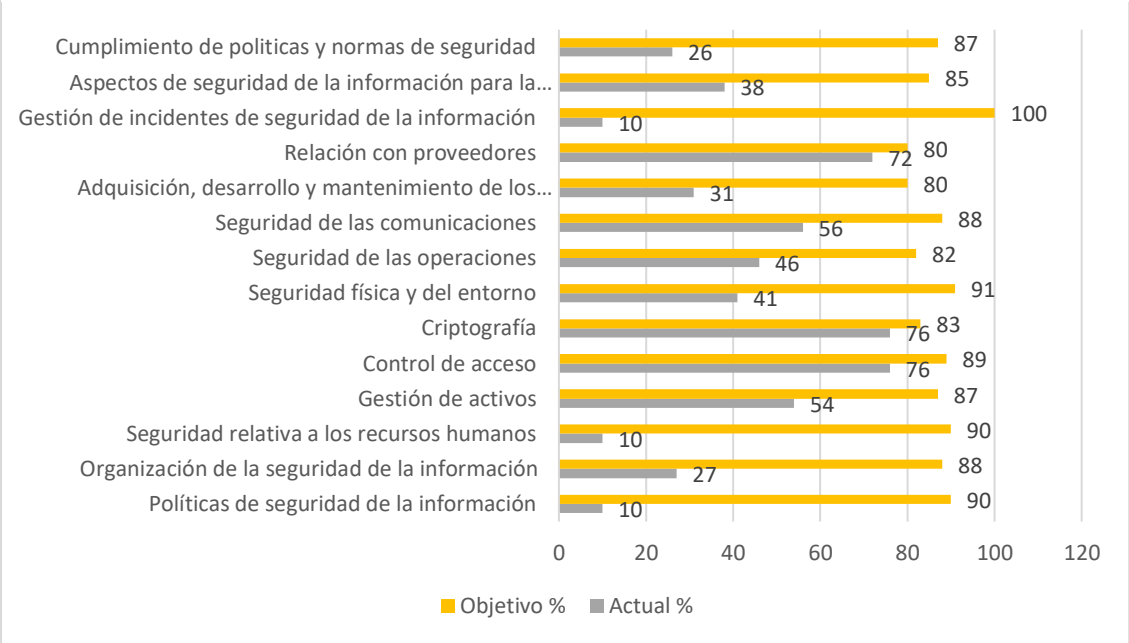
Al inicio se observa que los riesgos según la valoración de MAGERIT usando el programa Pilar (V.7.3.) en la dimensión disponibilidad un riesgo del 16%, integridad un riesgo del 18%, confidencialidad 16%, autenticidad 15%, trazabilidad del 18%, y de datos personales el 17%.

Así mismo la metodología MAGERIT nos permite medir el índice de madurez, observándose, desde el diagnostico hasta la aplicación de las salvaguardas, siendo esto un medio de control acertado para las instituciones saber en qué nivel se encuentran, sobre esa base tomar acciones que mejoren los procesos y exigencias tanto en la parte legal como técnica, esto queda a criterio de la institución en función a sus necesidades y presupuesto aplicar en su totalidad o en parte.

Así mismo MAGERIT realiza el control en función a la ISO: 2013, la fase actual se refiere al diagnóstico inicial sin aplicar las salvaguardas, lo que indica que cuanto más se acerca a cero necesita una mayor atención, un nivel igual o menor al 50% significa que se encuentra parcialmente realizado la acción de control, en la figura 6 se observa que los controles objetivo después de aplicar las salvaguardas tenemos valores mínimos de 80% hasta 89%, esto indica que se encuentran parcialmente realizado camino a estar plenamente en funcionamiento; también existen controles como en los recursos humanos con respecto a

su seguridad relativa y normas de garantía de la información, se encuentra en 90% y seguridad física y del entorno en un 91% esto indican que están plenamente en funcionamiento, y administración de ocurrencias en la seguridad de la información se encuentra en un 100% es decir estado óptimo.

Figura 6. Nivel de madurez por control según la ISO: 27002:2013



Así mismo al contrastar los antecedentes, encontramos trabajos similares con las investigaciones de Ortiz (2018), Sandoval (2017), Guevara (2015), investigaciones que aplican la metodología MAGERIT, siguiendo el mismo proceso, de realizar identificación de activos y evaluación de los riesgos, analizar y tratar los riesgos, aplicación de las políticas de seguridad y diseño de un plan para tratar los riesgos, en todos los casos concluyen por mejorar las condiciones iniciales (diagnóstico) para después de valorar las amenazas en cada uno de las dimensiones en la gestión del riesgo en las TIC, aplicar las salvaguardas teniendo en cuenta la ISO 27000:2013, todo este proceso lo realiza automáticamente el software PILAR en su versión 7.4.3, simplificando el proceso manual.

V. CONCLUSIONES

1. Al aplicar la metodología MAGERIT como estrategia en los controles de seguridad de las TIC, que a su vez implementa los controles de seguridad según la norma ISO/IEC 27002:2013, mejoró significativamente el riesgo analizado en el Instituto Tecnológico del Oriente de Tingo María, tal como se aprecia en la figura 4, al disminuir el riesgo total del 48% al 16%, aplicando salvaguardas, este proceso se coordinó con el Gerente de la institución.

2. En la tabla 1, se identificó los activos de las TIC que posee el ISTO Tingo María con la metodología MAGERIT. Lo clasifica en 7 grupos, Activos esenciales (4 componentes); Servicios Internos (4 componentes); Equipamiento informático (Aplicaciones, Equipos informáticos, Comunicaciones, Soportes de información); El entorno (4 componentes); Servicios subcontratado a terceros (2 componentes); Instalaciones físicas (4 componentes) y Personal (4 componentes).

3. Se determinó y analizó los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT, la tabla 19 nos visualiza, el nivel del riesgo por dimensión de las TIC, se observa un nivel 9 (catástrofe) para la dimensión disponibilidad, y un nivel 7 (extremadamente crítico) para el resto de dimensiones, al recomendar las salvaguardas, estos niveles de riesgo disminuyen, se puede comprobar en la tabla 18, donde la dimensión disponibilidad baja a 1,60 (bajo); la dimensión Integridad de los datos, disminuye a 2,50 (medio), Confidencialidad de la información baja a 1,90 (bajo), Autenticidad 1,60 (bajo), Trazabilidad 2,50 (medio), Datos personales (1,60) bajo.

4. Se determinó cualitativamente la valoración del efecto de los riesgos identificados en los activos de la TIC en el ISTO Tingo María con la metodología MAGERIT, se basó en la guía de la tabla de valoración del riesgo donde indica que a partir del rango 3 se considera como alto, y partiendo de los datos consolidados de la tabla 20 los promedios superan el rango de 3, por lo tanto, se concluye que el impacto del riesgo potencial en los activos es alto.

VI. PROPUESTAS A FUTURO

1. Continuar aplicando la metodología para el control del riesgo de sus activos todos los años, a fin de asegurar la buena marcha del negocio en óptimas condiciones, y hacer frente a la competencia, esto permitirá cumplir con las normas legales Ley Nº 29733 de protección de datos personales, además de cumplir con las políticas educativas para su acreditación.

2. Elaborar un manual de procedimientos según la metodología MAGERIT por activo identificado y sus componentes, a fin de realizar controles periódicos y pruebas de riesgo a través de otros softwares existentes en el mercado por profesionales especializados, esto garantizaría que el negocio esté preparado para competir en un mercado creciente y exigente como es la educación técnica superior.

3. Elaborar un plan de contingencia en función a los riesgos identificados en los activos de las TIC con la metodología MAGERIT, esto le permitirá contar con herramientas para afrontar eventualidades, como cortes de luz, interrupción del servicio de internet, o problemas morales por parte del personal, de ahí la importancia de los controles y acceso a los registros personales de los estudiantes.

4. Debe programarse por semestre académico de forma periódica coordinación entre el responsable del control estratégico y el responsable del control operativo para establecer metas y responsabilidades al determinarse en el diagnostico un riesgo alto y tomar en cuenta las salvaguardas aplicadas.

VII. REFERENCIAS

Alfonso Martínez, Y., Blanco Alfonso, B., y Loy Marichal, L. (2012). Auditoría con Informática a Sistemas Contables. *Revista de Arquitectura e Ingeniería*, *6*(2), 1-14. recuperado el 15/04/2021 http://www.redalyc.org/pdf/1939/193924743004.pdf

Bunge, M. (1987). La Investigación científica: su estrategia y su filosofía. En *editorial Ariel* (Segunda). Editorial Planeta.

Bernal Torres, C. A. (2010). *Metodología de la Investigación: administración, economía, humanidades y ciencias sociales* (3era ed.). Pearson Educación.

Capability Maturity Model Institute. (2013). *Integración de sistemas modelos de madurez de capacidades para Servicios, Versión 1.3* (C. Institute (ed.)). Recuperado el 06/03/2020 https://cmmiinstitute.com/getattachment/adec972f-5500-42b7-81cc-6c748a13e74d/attachment.aspx

Carrión Apéstegui, S. G. (2015). *Diagnostico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008 para la oficina general de estudios UNASAM-Huaraz, 2014* [Universidad Nacional Santiago Antúnez de Mayolo]. http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/1146/T05-SI

Castillo Fiallos, J., Cisneros Barahona, A., Méndez Naranjo, P., y Jácome Segovia, D. (2018). Modelo para la reducción de riesgos de seguridad informática en servicios web. *Revista Cumbres*, *4*(2), 19-30. http://investigacion.utmachala.edu.ec/revistas/index.php/Cumbres

Chiavenato, I. (2001). Proceso administrativo. En Makron Books Do Brasil (Ed.), *McGraw-Hill Colombia* (3a.). Mcgraw-Hill Interamericana.

Columba, E. S. (2016). *Fundamentos de Seguridad de la Información basado en ISO 27001 e ISO 27002* [Ebook]. Kindle.

Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI. (2014). Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. En *Normas Técnicas Peruanas*. http://www.istpargentina.edu.pe/wp-content/uploads/2019/04/ntp-ISO-IEC-27001-2014__48690__-1.pdf

Ley Nº 29733, El Peruano 445746 (2013). recuperado el 31.10.2021 ftp://ftp2.minsa.gob.pe/descargas/ogei/SINADEF/Ley-29733.pdf

Edutópica. (2017). *8 problemas de las TIC en Educación*. Edutópica. Recuperado el 10/02/2020 http://edutopica.co/inicio/2017/02/8-problemas-las-tic-educacion.html

Encalada, C., y Tenecela, A. (2015). *Guía de auditoría para la evaluación del control interno de seguridad de la información en la Universidad Catolica de Cuenca basada en COBIT 5* [De las Fuerzas Aradas]. https://doi.org/https://doi.org/10.26423/rctu.v3i3.204

Espinoza Fretel, A. A. (2017). *Diagnóstico del nivel de madurez de los procesos de las tecnologías de información de la empresa Geosurvey usando el marco de trabajo COBIT* [Universidad de Huánuco]. http://repositorio.udh.edu.pe/bitstream/handle/123456789/695/ESPINOZA FRETEL%2C ALAN ALBERTH.pdf?sequence=1&isAllowed=y

Ferruzola Gómez, E., Duchimaza S., J., Ramos Holguín, J., y Alejandro Lindao, M. F. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, *6*(1), 34-41. https://doi.org/10.26423/rctu.v6i1.429

Frayssinet Delgado, M. (2013). *Taller de transición de la norma ISO/IEC 27001:2005 a la ISO/IEC 27001:2013*. https://www.gobiernodigital.gob.pe/docs/Tallerv01 6.pdf

Guevara Chumán, J. G. (2015). *Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo'*. Universidad Nacional Pedro Ruiz Gallo.

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2006). *Metodologia de la investigacion* (4ta ed.). Mcgraw-Hill Interamericana.

Holguín García, F. Y., y Lema Moreta, L. M. (2019). Modelo para medir la madurez del análisis de riesgo de los activos de información en el contexto de las empresas navieras. *RISTI - Revista Ibérica de Sistemas y Tecnologias de Información*, *31*, 1-17. https://doi.org/10.17013/risti.31.1-17

Instituto Nacional de Estadística e Informática. (2000). *¿Que es la Teoria General de Sistemas?* (INEI (ed.)). https://cmapspublic.ihmc.us/rid=1G8TFJM82-16RKYJR-M62/TGS.pdf

International Organization of Standarization. (2011). Norma Técnica Colombiana NTC-ISO 31000. Gestión de Riesgo. Principios y Directrices. *Icontec*, *571*, 34.

https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

Liras, L. M. (2013). Protección de la Información. *Instituto Nacional de Ciberseguridad de España*, 22. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Ministerio de Hacienda y Administraciones Públicas. (2012a). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I* (Ministerio de Hacienda y Administraciones Públicas (ed.); Version 3.). Secretaría General Técnica. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Ministerio de Hacienda y Administraciones Públicas. (2012b). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de Elementos* (Ministerio de Hacienda y Administraciones Púbicas (ed.); Version 3). https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

Ministerio de Hacienda y Administraciones Públicas. (2012c). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas* (M. de Hacienda y Administraciones Púbicas (ed.); Version 3). Secretaría General Técnica. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

Oliveros Contreras, D., y Martínez, G. M. (2017). Efecto de las TIC sobre la gestión de las empresas hoteleras afiliadas a Cotelco de Bucaramanga (Santander, Colombia). *Revista EAN, 83*, 15-30. https://doi.org/10.21158/01208160.n83.2017.1827

Ortiz Morales, E. A. (2018). Controles de seguridad según la norma ISO/IEC 27002:2013 para el mejoramiento de la Gestión de Seguridad de la Información en la Universidad Nacional Agraria de la Selva. En *Repositorio de la Universidad Nacional Agraria de la Selva*. Universidad Nacional Agraria de la Selva.

Rafael Samillan, G., y Castillo Oviedo, E. (2016). *Auditoria Informática usando las normas COBIT en el centro de sistemas de información del Hospital Regional docente las Mercedes de Chiclayo - 2016* [Pedro Ruiz Gallo]. http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/1221/BC-TES-

5923.pdf?sequence=1&isAllowed=y

Rodriguez, J. M., y Peralta, I. (2013, abril). Gestión de Riesgos. *TiThink*, 1. Recuperado el 31/10/2020 https://www.tithink.com/publicacion/MAGERIT.pdf

Romero Camones, J. E. (2018). Factores de riesgo de las tecnologías de información y el desempeño de WEBCAST en las empresas ATOGAPAN S.A. y grupo HCM COMUNICACIONES S.A.C. [Universidad Cesar Vallejo]. En *Universidad César Vallejo*. http://repositorio.ucv.edu.pe/handle/UCV/34359

Salas Blas, E. (2013). Diseños Preexperimentales en Psicología y en Educación: una revisión conceptual. *Liberabit: Lima (Perú)*, *19*(1), 133-141. http://www.scielo.org.pe/pdf/liber/v19n1/a13v19n1

Sandoval Quino, J. P., y Quino, J. P. S. (2017). Diseño de un plan de seguridad de la información para el centro de informática y telecomunicaciones de la Universidad Nacional de Piura, periodo 2015-2018. En *Universidad Nacional de Piura*. Universidad Nacional de Piura.

Toro, R. (2019). *ISO 27001: El método MAGERIT*. 2015. https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Uscatescu Barrón, J. (1973). Teoría de la Información. *Revista de estudios políticos*, *192*, 53-74.

Valdiviezo Mogollon, Y. S. (2019). *Análisis de riesgos de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT* (Vol. 53, Número 9) [Universidad César Vallejo]. https://doi.org/10.1017/CBO9781107415324.004

Vícuña Altamirano, E. del R., y Zhindón Mora, M. G. (2019). Gestión de riesgos en la infraestructura de un centro de datos. Caso de estudio: Coordinación Zonal 6 Sur del Instituto Nacional de Estadística y Censos, Ecuador. *Dominio de las Ciencias*, *5*(3), 317-342. https://doi.org/10.23857/dc.v5i3.937

ANEXOS

Anexo 1. Formato de lista de cotejo

Evaluación de controles: Lista de cotejo

INSTITUTO SUPERIOR PRIVADO TECNOLÓGICO DEL ORIENTE				
Código Formato	IDENT-RIESGO-FORM-TIC-N°01.			Evaluación de controles
Dominio:				
Proceso:				
Practica:				
Auditor:				
Responsable	Fecha			
Verificación	Si	No	Parcial	Observaciones
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	
	☐	☐	☐	

Fuente: adaptado de Encalada y Tenecela (2015). Guía de auditoría para la evaluación del control interno de seguridad de la Información en la Universidad Católica de Cuenca Basada en COBIT 5.
Rafael Samillan y Castillo Oviedo (2016)**.** Auditoría Informática usando las normas COBIT 5 en el centro de sistemas de Información del Hospital Regional Docente las Mercedes de Chiclayo – 2016.

Anexo 2. Formato de identificación del riesgo

INSTITUTO SUPERIOR PRIVADO TECNOLÓGICO DEL ORIENTE		
Código Formato	IDEN-RIESGOS-FORM-TIC-N° 02.	Hallazgo de riesgo
Dominio:		
Proceso:		
Practica:		
Evidencia:		
Condición		
Criterio		
Causa		
Efecto		
Conclusión		
Recomendación		

Fuente. Encalada y Tenecela (2015). Guía de auditoría para la evaluación del control interno de seguridad de la Información en la Universidad Católica de Cuenca Basada en COBIT 5.
Rafael Samillan y Castillo Oviedo (2016)**.** Auditoría Informática usando las normas COBIT 5 en el centro de sistemas de Información del Hospital Regional Docente las Mercedes de Chiclayo – 2016.

Anexo 3. Matriz de consistencia

LA METODOLOGÍA MAGERIT PARA LA GESTIÓN DEL RIESGO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN EN EL INSTITUTO TECNOLÓGICO PRIVADO DEL ORIENTE DE TINGO MARÍA.

PROBLEMA	*OBJETIVOS*	*HIPÓTESIS*	*VARIABLES*	*DIMENSIONES*	*INDICADORES*	*METODOLOGÍA/TÉCNICAS E INSTRUMENTOS*
¿La implementación de la metodología MAGERIT como estrategia en los controles de seguridad de las TIC la Gestión del riesgo mejora significativamente en el Instituto Tecnológico del Oriente de Tingo María?	Determinar en qué medida la metodología MAGERIT se relaciona con la Gestión del Riesgo de las TIC en el ISTO de Tingo María**.**	La metodología MAGERIT tiene una relación positiva con la Gestión del riesgo en la TIC del ISTO de Tingo María.	***La metodología MAGERIT: (Independiente)***	**Planeación** del análisis y la gestión de riesgos	Planificación del Proyecto	**Por su finalidad:** Es de carácter aplicado, porque se utiliza la metodología con la finalidad Gestionar el riesgo de las Tecnologías de la Información en el ISTO de Tingo María. **Por su profundidad:** Es relacional porque determina la relación de la variable aplicación de la Metodología MAGERIT en la Gestión del riesgo de las Tecnologías de la información y la comunicación en el ISTO de Tingo María. **Método** será una investigación de nivel descriptivo, de campo, cuantitativo, no experimental y de corte transversal. **Instrumento:** Para la medición del nivel de gestión de las TIC en el ISTO se utilizarán cuestionarios obtenidos de la estructura de la metodología MAGERIT.
				Análisis de riesgos: permite identificar y evaluar los elementos que intervienen en el riesgo.	➢ Caracterización de los activos. ➢ Caracterización de las amenazas ➢ Caracterización de las salvaguardas ➢ Estimación del estado de riesgo	
				Gestión de riesgos: permite identificar las salvaguardias potenciales que reducen el riesgo detectado.	10. Muy alta 9. Alta 6-8. Media 3-5. Baja 1-2 Muy baja	
				Selección de salvaguardas: permite seleccionar las contramedidas a implementarse, diseñando un enfoque para la aplicación de las salvaguardias seleccionadas.	L5. Optimizado L4. Gestionado L3. Proceso definido L2. Reproducible, pero intuido L1. Inicial L0. Inexistente	
¿Qué activos de las TIC que posee el ISTO de Tingo María, se	Identificar los riesgos en los activos de las TIC que posee	El riesgo identificado en los activos de las TIC	***Gestión del riesgo de las***	***Identificar los activos***	➢ Identificación de los activos ➢ Dependencia entre activos	

encuentran bajo riesgo según la metodología MAGERIT? ¿Cuál es la caracterización de los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT? ¿Cuál es el resultado de la cuantificación cualitativa el impacto de los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT?	el ISTO Tingo María con la metodología MAGERIT. Determinar los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT. Determinar cualitativamente el impacto de los riesgos identificados en los activos de las TIC en el ISTO Tingo María con la metodología MAGERIT.	que posee el ISTO Tingo María con la metodología MAGERIT, es bajo. El riesgo analizado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, es subsanable a corto tiempo. El impacto del riesgo cualitativo identificado en los activos de las TIC del ISTO Tingo María con la metodología MAGERIT, es bajo.	***TIC: (dependiente)***		➢ Valoración de los activos	
				Determinar los riesgos	Numero de amenazas	
					Numero de vulnerabilidad	
					Probabilidad de ocurrencia %	
					Riesgo potencial %	
				Evaluar los riesgos	Valoración estimada – Cualitativamente	

Anexo 4. Nivel de madurez según la ISO 27002:2013

VALORES DE MADUREZ POR NIVEL E INDICE (%)											
Tabla de valoracion de las dimensiones por nivel de madurez y salvaguardas					Promedio						
					Nivel (índice) de madurez			Nivel (índice) de madurez			
BASE - RED INTERNA					Actual	Objetivo	PILAR	Actual %	Objetivo %	PILAR %	
Dominios											
Recomendación	27002:2013	Control		Código de prácticas para los controles de seguridad de la información	L1-L3	L3-L5	L2-L4	41	87	73-65	
2		**5**		**Politicas de seguridad de la información**	L1	L4	L2	10	90	50	
2		5.1		Directrices de gestión de la seguridad de la información	L1	L4	L2	10	90	50	
2			5.1.1	Políticas para la seguridad de la información	L1	L4	L2	10	90	50	
2			5.1.2	Revisión de las políticas para la seguridad de la información	L1	L4	L2	10	90	50	
7		**6**		**Organización de la seguridad de la información**	L1-L3	L3-L5	L2-L4	27	88	72-69	
7		6.1		Organización interna	L1-L3	L3-L5	L2-L4	24	92	72-69	
3			6.1.1	Roles y responsabilidad en seguridad de la información	L1	L4	L2-L3	10	90	62-55	
7			61.2	Separación de tareas	L3	L4	L4	80	90	90-81	
3			6.1.3	Contacto con las autoridades	L1	L5	L3	10	100	80	
3			6.1.4	Contacto con grupos de interés especial	L1	L5	L3	10	100	80	
2			6.1.5	Seguridad de la información en la gestión de proyectos	L1	L5	L2	10	80	50	
0		6.2		Los dispositivos moviles y el teletrabajo	L1-L2	L3-L4	n.a.	30	85	n.a	
0			6.2.1	Política de dispositivos móviles	L2	L3	n.a.	50	80	n.a	
0			6.2.2	Teletrabajo	L1	L4	n.a.	10	90	n.a	
6		**7**		**Seguridad relativa a los recursos humanos**	L1	L4	L3-L4	10	90	81-71	
4		7.1		Antes del empleo	L1	L3	L3	10	90	80-70	
4			7.1.1	Investigación de antecedentes	L1	L4	L3	10	90	80	
4			7.1.2	Términos y condiciones del empleo	L1	L4	L3	10	90	80-61	
6		7.2		Durante el empleo	L1	L4	L3-L4	10	90	83-69	
3			7.2.1	Responsabilidades de gestión	L1	L4	L3	10	90	80-63	
6			7.2.2	Concienciación, educación y capacitación en seguridad de la información	L1	L4	L3	10	90	90-73	
3			7.2.3	Proceso disciplinario	L1	L4	L4	10	90	80-70	
5		7.3		Finalización del empleo o cambio en el puesto de trabajo	L1	L4	L3	10	90	80-75	
5			7.3.1	Responsabilidades ante la finalización o cambio	L1	L4	L3	10	90	80-75	
5		**8**		**Gestión de activos**	L1-L3	L3-L5	L2-L3	54	87	76-69	
5		8.1		Responsabilidad sobre los activos	L1-L3	L3-L5	L2-L3	45	87	73-67	
5			8.1.1	Inventario de activos	L1-L3	L3-L5	L3	59	86	80-70	
3			8.1.2	Propiedad de los activos	L1-L3	L3-L5	L3	59	86	80-68	
2			8.1.3	Uso aceptable de los activos	L1-L3	L3-L5	L2	53	85	50	
5			8.1.4	Devolución de los activos	L1	L4	L3	10	90	80	
5		8.2		Clasificación de la información	L2-L3	L3-L4	L3	67	84	80-71	
4			8.2.1	Clasificación de la información	L3	L3	L3	80	80	80-62	
5			8.2.2	Etiquetado de la información	L2-L3	L3-L4	L3	70	83	80	
0			8.2.3	Manipulado de la información	L2	L4	n.a.	50	90	n.a	
0		8.3		Manipulación de los soportes	L2	L4	n.a.	50	90	n.a	
0			8.3.1	Gestión de soportes extraibles	L3	L5	n.a.	50	90	n.a	
0			8.3.2	Eliminación de soportes	L4	L6	n.a.	50	90	n.a	
0			8.3.3	Soportes físicos en tránsito	L5	L7	n.a.	50	90	n.a	

VALORES DE MADUREZ POR NIVEL E INDICE (%)											
Tabla de valoracion de las dimensiones por nivel de madurez y salvaguardas					Promedio						
					Nivel (índice) de madurez			Nivel (índice) de madurez			
BASE - RED INTERNA					Actual	Objetivo	PILAR	Actual %	Objetivo %	PILAR %	
Dominios											
Recomendación	27002: 2013	Control		Código de prácticas para los controles de seguridad de la información	L1-L3	L3-L5	L2-L4	41	87	73-65	
7	**9**	**Control de acceso**			L1-L3	L3-L4	L2-L4	76	89	83-73	
4		9.1	Requisitos de negocio para el control de acceso		L3	L4	L3	80	90	80-63	
4			9.1.1	Política de control de acceso	L3	L4	L3	80	90	80-63	
0			9.1.2	Acceso a las redes y a los servicios de red	L3	L4	n.a.	80	90	n.a	
7		9.2	Gestión de acceso de usuario		L2-L3	L3-L4	L2-L4	79	90	79-71	
5			9.2.1	Registro y baja de usuario	L3	L4	L3	80	90	80-70	
3			9.2.2	Provisión de acceso de usuario	L3	L4	L3	80	90	80-60	
7			9.2.3	Gestión de privilegios de acceso	L3	L4	L4	80	90	90-79	
			9.2.4	Gestión de la información secreta de auntenticación de los usuarios	L2-L3	L3-L4	L2-L3	74	88	65	
			9.2.5	Revisión de los derechos de acceso de usuario	L3	L4	L3	80	90	80	
			9.2.6	Retirada o reasignación de los derechos de accreso	L3	L4	L2-L3	80	90	80-73	
7		9.3	Responsabilidades del usuario		L3	L4	L4	80	90	90-81	
			9.3.1	Uso de la información secreta de autenticación	L3	L4	L3-L4	80	90	90-81	
6		9.4	Control de acceso a sistemas y aplicaciones		L1-L3	L3-L4	L3-L4	66	88	83-76	
			9.4.1	restricción del aaceso a la información	L3	L4	L3	80	90	80	
			9.4.2	Procedimientos seguros de inicio de sesción	L3	L4	L3	80	90	80-74	
			9.4.3	Sistema de gestión de contraseñas	L3	L4	L4	80	90	90-81	
			9.4.4	Uso de utilidades con privilegios del sistema	L3	L4	L3	80	90	80-68	
			9.4.5	Control de acceso al código fuente de clos programas	L1	L3	n.a.	10	80	n.a	
2	**10**	**Criptografía**			L2-L3	L3-L4	L2	76	83	50	
2		10.1	Controles criptográficos		L2-L3	L3-L4	L2	76	83	50	
			10.1.1	Política de uso de los controles criptográficos	L2-L3	L3-L4	L2	73	85	50	
			10.1.2	Gestión de claves	L3	L3-L4	n.a.	80	80	n.a	
7	**11**	**Seguridad física y del entorno**			L1-L3	L3-L5	L2-L4	41	91	75-71	
7		11.1	Áreas seguras		L1-L3	L5	L2-L4	31	100	73-70	
			11.1.1	Perímetro de seguridad fisica	L1	L5	n.a.	10	100	n.a	
			11.1.2	Controles físicos de entrada	L1	L5	n.a.	10	100	n.a	
			11.1.3	Seguridad de offifcna, despachos y recursos	L1-L3	L5	L3	45	100	80	
			11.1.4	Protección contra las amenazas externas y ambientales	L3	L5	L4	80	100	90-80	
			11.1.5	El trabajo en áreas seguras	L1-L3	L5	L2	33	100	50	
			11.1.6	Áreas de carga y descarga	L1	L5	n.a.	10	100	n.a	
6		11.2	Seguridad de los equipos		L1-L3	L3-L5	L2-L4	50	83	78-72	
			11.2.1	Emplazamiento y protección de equipos	L1-L2	L3-L5	L3	37	87	80	
			11.2.2	Instlaciones de suministros	L2	L3	L3	50	80	80-76	
			11.2.3	Seguridad de clableado	L2	L3	L3	50	80	90-77	
			11.2.4	Mantenimiento de los equipos	L2	L3	L4	50	80	80-67	
			11.2.5	Retirada de materiales propiedad de la empresa	L2	L3	L3	50	80	80-74	
			11.2.6	Seguridad de los equipos fuera de las instalaciones	L2	L3	L3	50	80	80-68	
			11.2.7	Reutilizacion o eliminación segura de equipos	L2	L3	L2	50	80	50	
			11.2.8	Equipo de usuario desatendido	L2	L3	L3	80	90	80	
			11.2.9	Política de puestos de trabajo despejado y pantalla limpia	L3	L4	n.a.	37	90	n.a	

VALORES DE MADUREZ POR NIVEL E INDICE (%)										
Tabla de valoracion de las dimensiones por nivel de madurez y salvaguardas				Promedio						
				Nivel (índice) de madurez			Nivel (índice) de madurez			
BASE - RED INTERNA				Actual	Objetivo	PILAR	Actual %	Objetivo %	PILAR %	
Dominios										
Recomendación	27002: 2013	Control	Código de prácticas para los controles de seguridad de la información	L1-L3	L3-L5	L2-L4	41	87	73-65	
7	**12**		**Seguridad de las operaciones**	L1-L3	L3-L5	L2-L4	46	82	80-71	
4		12.1	Procedimientos y responsabilidades operacionales	L1-L3	L3-L4	L2-L3	31	84	75-65	
			12.1.1 Documentación de los procedimientos de operación	L1-L2	L3-L4	L2-L3	40	85	65-51	
			12.1.2 Gestioón de cambvios	L2-L3	L3-L4	L3	65	83	80-67	
			12.1.3 Gestión de capacidades	L1	L4	L3	10	90	80-77	
			12.1.4 Separación de los recursos de desarrollo, prueba y operación	L1	L3	n.a.	10	80	n.a	
		12.2	Protección contra el software malicioso (malware)	L1-L2	L3-L5	n.a.	23	87	n.a	
			12.2.1 Controles contra el código malicioso	L1-L2	L3-L5	n.a.	23	87	n.a	
7		12.3	Copias de seguridad	L2-L3	L3	L4	70	80	90-66	
			12.3.1 Copias de seguridad de la información	L2-L3	L3	L4	70	80	90-66	
6		12.4	Registros y supervisión	L2	L3	L2-L4	50	80	75-72	
			12.4.1 Registros de eventos	L2	L3	L3	50	80	80-73	
			12.4.2 Protección de la información de registro	L2	L3	L3	50	80	80	
			12.4.3 Registros de administración y operación	L2	L3	L2	50	80	50	
			12.4.4 Sincronización del reloj	L2	L3	L4	50	80	90-83	
		12.5	Conrtroles de software de explotación	L2	L3	n.a.	50	80	n.a	
			12.5.1 Instalación del software en explotación	L2	L3	n.a.	50	80	n.a	
		12.6	Gestión de la vulnerabilidad técnica	L2	L3	n.a.	50	80	n.a	
			12.6.1 Gestión de las vulnerabilidades técnicas	L2	L3	n.a.	50	80	n.a	
			12.6.1 Restricción en la instalación de software	L2	L3	n.a.	50	80	n.a	
5		12.7	Consideraciones sobre la auditoria de sistemas de información	L2	L3	L3	50	80	80	
			12.7.1 Controles de auditoría de sistemas de información	L2	L3	L3	50	80	80	
6	**13**		**Seguridad de las comunicaciones**	L1-L3	L3-L4	L3-L4	56	88	85-74	
		13.1	Gestión de la seguridad de redes	L1-L3	L4	n.a.	77	90	n.a.	
			13.1.1 Controles de red	L3	L4	n.a.	80	90	n.a.	
			13.1.2 Seguridad de los servicios de red	L1-L3	L4	n.a.	70	90	n.a.	
			13.1.3 Segregación en redes	L3	L4	n.a.	80	90	n.a.	
6		13.2	Intercambio de información	L1-L3	L3-L4	L3-L4	36	85	85-74	
			13.2.1 Politicas y procedimoientos de intercambio de informacion	L3	L3-L4	n.a.	80	86	n.a.	
			13.2.2 Acuerdos de intercambio de información	L1	L3	L4	10	80	90-76	
			13.2.3 Mensajería electronica	L1-L3	L3-L4	n.a.	45	85	n.a.	
			13.2.4 Acuerdos de confidencialidad o no revelacion	L1	L4	L3	10	90	80-73	
5	**14**		**Adquisición, desarrollo y mantenimiento de los sistemas de información**	L1-L3	L3-L4	L2-L3	31	80	70-59	
5		14.1	Requisitos de seguridad en sistemas de información	L1-L3	L3-L4	L2-L3	57	81	70-59	
			14.1.1 Analisis de los requisitos y especiaficaciones de segrudiad de la informacion	L1	L3	L2	10	80	50	
			14.1.2 Asegurar los serviicos de aplicaciones en redes publicas	L3	L3	L3	80	80	80-58	
			14.1.3 Protección de las transacciones de servicios de aplicaciones	L3	L3-L4	L3	80	83	80-70	
		14.2	Seguridad en el desarollo y en los procesos de soporte	L1-L3	L3	n.a.	27	80	n.a.	
			14.2.1 Politica de desarrollo seguro	L1	L3	n.a.	10	80	n.a.	
			14.2.2 Procedimiento de control de cambios en sistemas	L2	L3	n.a.	50	80	n.a.	
			14.2.3 Revisón técnica de las acplicaciones tras efectuar cambios en el sistema ope	L2	L3	n.a.	50	80	n.a.	
			14.2.4 Restricciones a los cambios en los paquetes de doftware	L1	L3	n.a.	10	80	n.a.	
			14.2.5 Principios de ingenieria de sistemas seguros	L1-L2	L3	n.a.	30	80	n.a.	
			14.2.6 Entorno de desarrollo xseguro	L1	L3	n.a.	10	80	n.a.	
			14.2.7 Externalización del desarrollo de software	L1-L2	L3	n.a.	20	80	n.a.	
			14.2.8 Pruebas funcionales de seguridad de sistemas	L1	L3	n.a.	10	80	n.a.	
			14.2.9 Pruebas de aceptación de sistemas	L2	L3	n.a.	50	80	n.a.	
		14.3	Datos de prueba	L1	L3	n.a.	10	80	n.a.	
			14.3.1 Protección de los datos de prueba	L1	L3	n.a.	10	80	n.a.	

VALORES DE MADUREZ POR NIVEL E INDICE (%)											
Tabla de valoracion de las dimensiones por nivel de madurez y salvaguardas					Promedio						
					Nivel (índice) de madurez			Nivel (índice) de madurez			
BASE - RED INTERNA					Actual	Objetivo	PILAR	Actual %	Objetivo %	PILAR %	
Dominios											
Recomendación	27002: 2013	Control		Código de prácticas para los controles de seguridad de la información	L1-L3	L3-L5	L2-L4	41	87	73-65	
6	**15**	**Relación con proveedores**			L1-L3	L3	L2-L4	72	80	72-57	
6		15.1	Seguridad en las relaciones con proveedores		L1-L3	L3	L2-L4	75	80	73-57	
			15.1.1	Política de seguridad de la información en las relaciones con los proveedore	L1-L3	L3	L4	66	80	90-55	
			15.1.2	Requisitos de seguridad en contratos con terceros	L3	L3	L3	80	80	80-65	
			15.1.3	Cadena de suministro de tecnología de la información y de las comnicaciobr	L3	L3	L2	80	80	50	
6		15.2	Gestión de la provisión de servicios del proveedor		L1-L3	L3	L2-L4	68	80	70-57	
			15.2.1	Control y revisión de la provisión de servicios del proveedores	L1-L3	L3	L4	57	80	90-63	
			15.2.2	Gestión de cambios en la provisión del servicio del proveedor	L3	L3	L2	80	80	50	
4	**16**	**Gestión de incidentes de seguridad de la información**			L1	L5	L3	10	100	80-68	
4		16.1	Gestión de incidentes de seguridad de la información y mejoras		L1	L5	L3	10	100	80-68	
			16.1.1	Responsablidqades y procedimientois	L1	L5	L3	10	100	80-60	
			16.1.2	Norificación deceventos de seguridad de la información	L1	L5	L3	10	100	80	
			16.1.3	Notificación de puntos debiles de la seguridad	L1	L5	L3	10	100	80-60	
			16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	L1	L5	L3	10	100	80-54	
			16.1.5	Respeusta a incidentes de seguridad de la información	L1	L5	L3	10	100	80-70	
			16.1.6	Aprendizaje de los incidentes de seguridad de la información	L1	L5	L3	10	100	80-75	
			16.1.7	Recopilación de evidencias	L1	L5	L3	10	100	80	
6	**17**	**Aspectos de seguridad de la información para la gestión de la continuidad del n**			L1-L3	L3-L5	L3-L4	38	85	72-74	
6		17.1	Continuidad de la seguridad de la información		L1-L3	L3-L5	L3-L4	20	80	83-73	
			17.1.1	Planificacion de la continuidad de la seguridad de la información	L1	L3	L3	10	80	80-65	
			17.1.2	Implmentar la continuidad de la seguridad de la información	L1-L3	L3-L4	L3	41	81	90-73	
			17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la in	L1	L3	L4	10	80	80	
5		17.2	Redundancia		L1-L3	L3-L5	L3	55	90	80-76	
			17.2.1	Dsiponibilidad de los recursos de tratamiento de la información	L1-L3	L3-L5	L3	55	90	70-76	
4	**18**	**Cumplimiento**			L1-L3	L3-L4	L2-L3	26	87	66-58	
3		18.1	Cumplimiento de los requisitos legales y contractuales		L1-L3	L3-L4	L2-L3	37	85	62-53	
			18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	L1	L4	L2	10	90	50	
			18.1.2	Derechos de propiedad intelectual (DPI)	L1-L3	L3	L2	38	80	50	
			18.1.3	Protección de los registros de la organización	L1	L4	L3	10	90	80-55	
			18.1.4	Proteción y proivacidad de la informaci``on de carácter personal	L1-L3	L3	L3	57	80	80-60	
			18.1.5	Regulación de los controles criptograficos	L2-L3	L3-L4	L2	70	83	50	
4		18.2	Revisiones de la seguridad de la información		L1-L3	L3-L4	L2-L3	14	89	70-62	
			18.2.1	Revisión indpendiente de la seguridad de la información	L1-L2	L3-L4	L3	23	87	80-70	
			18.2.2	Cumplimiento de las políticas y normas de seguridad	L1	L4	L2	10	90	50	
			18.2.3	Comprobación del cumplimiento técnico	L1	L4	L3	10	90	80-67	