UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Software

DISEÑO DE UN PLAN DE GESTIÓN DE RIESGOS TECNOLÓGICOS CON LA METODOLOGÍA MAGERIT V3 BASADA EN LA NORMA ISO/IEC 31000, PARA FORTALECER LA GESTIÓN DE AMENAZAS Y RIESGOS EN LOS LABORATORIOS DE INFORMÁTICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE.

Trabajo de grado previo a la obtención del título de Ingeniero de Software

Autor:

Erick Patricio Sevilla Erazo

Director:

MSc. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2023

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100476827-9		
APELLIDOS Y NOMBRES:	ERICK PATRICIO SEVILLA ERAZO		
DIRECCIÓN:	IBARRA, SAN FRANCISCO		
EMAIL:	epsevillae@utn.edu.ec		
TELÉFONO FIJO:	062604757	**TELÉFONO MÓVIL:**	0980801363

DATOS DE LA OBRA	
TÍTULO:	DISEÑO DE UN PLAN DE GESTIÓN DE RIESGOS TECNOLÓGICOS CON LA METODOLOGÍA MAGERIT V3 BASADA EN LA NORMA ISO/IEC 31000, PARA FORTALECER LA GESTIÓN DE AMENAZAS Y RIESGOS EN LOS LABORATORIOS DE INFORMÁTICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE.
AUTOR(ES):	ERICK PATRICIO SEVILLA ERAZO
FECHA:	29/03/2023
PROGRAMA:	PREGRADO
TÍTULO POR EL QUE OPTA:	INGENIERO DE SOFTWARE
DIRECTOR:	MSc. DAISY IMBAQUINGO
ASESOR 1:	MSc. SILVIA ARCINIEGA
ASESOR 2:	MSc. MARCO PUSDÁ

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de esta y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 29 días del mes de marzo de 2023

EL AUTOR:

Erick Patricio Sevilla Erazo

C.I: 100476827-9

CERTIFICACIÓN DIRECTOR

Ibarra 29 de marzo del 2023

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN

Por medio del presente yo MSc. Daisy Imbaquingo Esparza, certifico que el Sr. Erick Patricio Sevilla Erazo portador de la cedula de ciudadanía número 1004768279, ha trabajado en el desarrollo del proyecto de grado “Diseño de un plan de gestión de riesgos tecnológicos con la metodología MAGERIT V3 basada en la norma ISO/IEC 31000, para fortalecer la gestión de amenazas y riesgos en los laboratorios de informática de la Facultad de Ingeniería en Ciencias de la Universidad Técnica del Norte”, previo a la obtención del Título de Ingeniero en Software realizado con interés profesional y responsabilidad que certifico con honor de verdad.

Es todo en cuanto puedo certificar a la verdad

Atentamente

Facultad de Ingeniería en Ciencias Aplicadas FICA
IBARRA - ECUADOR

Firmado digitalmente por 1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA
Fecha: 2023.03.29 08:59:09 -05'00'

MSc. Daisy Imbaquingo

DIRECTOR DE TRABAJO DE GRADO

Dedicatoria

El presente trabajo de grado se lo dedico a mis padres Patricio Manuel Sevilla Meneses y Nancy Jeaneth Erazo Cadena, por todo su esfuerzo, amor y apoyo incondicional que me han brindado, por enseñarme a ser una persona con valores y afrontar los problemas que se me presentaran.

A mis hermanos Matías y Masciel Sevilla, espero ser ejemplo de dedicación y perseverancia para animarlos a cumplir sus metas.

A Darlyn por ser un gran apoyo e inspiración durante esta etapa y llegar a mi vida en el momento en que lo necesitaba.

A mis amigos y familiares que me apoyaron y estuvieron presentes durante toda mi vida universitaria.

Erick Patricio Sevilla Erazo

Agradecimientos

Agradezco infinitamente a mis padres por todo su apoyo incondicional, en especial a mi madre Jeaneth que me ha inspirado a cumplir cada uno de mis sueños, por motivarme a seguir adelante y no rendirme ante ninguna adversidad.

Agradezco a mis amigos que me ayudaron a convertir estos años de universidad en una aventura llena de sentimientos y emociones.

Agradezco a todos los docentes que tuve a lo largo de mi carrera universitaria, que con sus conocimientos, experiencias y enseñanzas me han permitido convertirme en un buen profesional.

Un agradecimiento especial a mi directora de Tesis a la MSc. Daisy Imbaquingo, quien, con su apoyo, conejos y recomendaciones, ayudo a que este trabajo se cumpliera de la mejor manera.

Agradezco a mis opositores MSc. Silvia Arciniega y MSc. Marco Pusdá por su tiempo y ayuda para el desarrollo de este trabajo de titulación.

Erick Patricio Sevilla Erazo

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Resumen

El presente documento se encuentra conformado por cuatro capítulos, en los cuales se detalla todo el proceso para realizar el Trabajo de Grado: “DISEÑO DE UN PLAN DE GESTIÓN DE RIESGOS TECNOLÓGICOS CON LA METODOLOGÍA MAGERIT V3 BASADA EN LA NORMA ISO/IEC 31000, PARA FORTALECER LA GESTIÓN DE AMENAZAS Y RIESGOS EN LOS LABORATORIOS DE INFORMÁTICA DE LA FACULTAD DE INGENIERÍA EN CIENCIAS DE LA UNIVERSIDAD TÉCNICA DEL NORTE.”

En la Introducción se definen los antecedentes, situación actual, prospectiva, planteamiento del problema, objetivo general y específico, alcance y justificación.

En el capítulo 1, con la revisión de bibliografía se presenta el marco teórico, en el cual se describen temas como la gestión de riesgos, conceptos relacionados a la gestión de riesgos, estándares y metodologías para la gestión de riesgos, una visión más enfocada en la Norma ISO 31000 y la metodología MAGERIT versión 3.0.

En el capítulo 2, se detalla la metodología de investigación y técnicas de recolección de información. Además, se realiza la evaluación del nivel actual de la gestión de riesgos dentro de los laboratorios de informática FICA-UTN para determinar y organizar las actividades pertinentes al Plan de Gestión de Riesgos.

En el capítulo 3, se desarrolla la implementación del Plan de Gestión de Riesgos con las actividades definidas en el capítulo 2, mismas que serán divididas en tres fases y un apartado de socialización a las partes interesadas.

En el capítulo 4, se valida el Plan de Gestión de Riesgos propuesto con ayuda del método Delphi de consulta a expertos, se analizan e interpretan los resultados obtenidos.

Finalmente se encuentran las conclusiones, recomendaciones, referencias bibliográficas y los Anexos.

Abstract

This document is made up of three chapters, in which the entire process to carry out the Degree Project is detailed: “DESIGN OF A TECHNOLOGICAL RISK MANAGEMENT PLAN WITH THE MAGERIT V3 METHODOLOGY BASED ON THE ISO/IEC 31000 STANDARD, FOR STRENGTHEN THE MANAGEMENT OF THREATS AND RISKS IN THE COMPUTER LABORATORIES OF THE FACULTY OF ENGINEERING IN SCIENCE OF THE UNIVERSIDAD TÉCNICA DEL NORTE.”

In the introductory part, the background, current situation, prospective, problem statement, general and specific objective, scope, and justification are defined.

In chapter 1, with literature review, the theoretical framework is presented, which describes topics such as risk management, concepts related to risk management, standards and methodologies for risk management, a vision more focused on the ISO 31000 Standard and the MAGERIT version 3.0 methodology.

In chapter 2, the research methodology and data collection techniques are detailed. In addition, the evaluation of the current level of risk management within the FICA-UTN computer laboratories is carried out to determine and organize the activities pertinent to the Risk Management Plan.

In chapter 3, the implementation of the Risk Management Plan is developed with the activities defined in chapter 2, which will be divided into three phases and a section for socialization with interested parties.

In chapter 4, the proposed Risk Management Plan is validated with the help of the Delphi method of consulting experts, the results obtained are analyzed and interpreted.

Finally, there are the conclusions, recommendations, bibliographic references and the Annexes.

Introducción

Tema

Diseño de un plan de gestión de riesgos tecnológicos con la metodología MAGERIT V3 basada en la norma ISO/IEC 31000, para fortalecer la gestión de amenazas y riesgos en los laboratorios de informática de la Facultad de Ingeniería en Ciencias de la Universidad Técnica del Norte.

Problema

Antecedentes

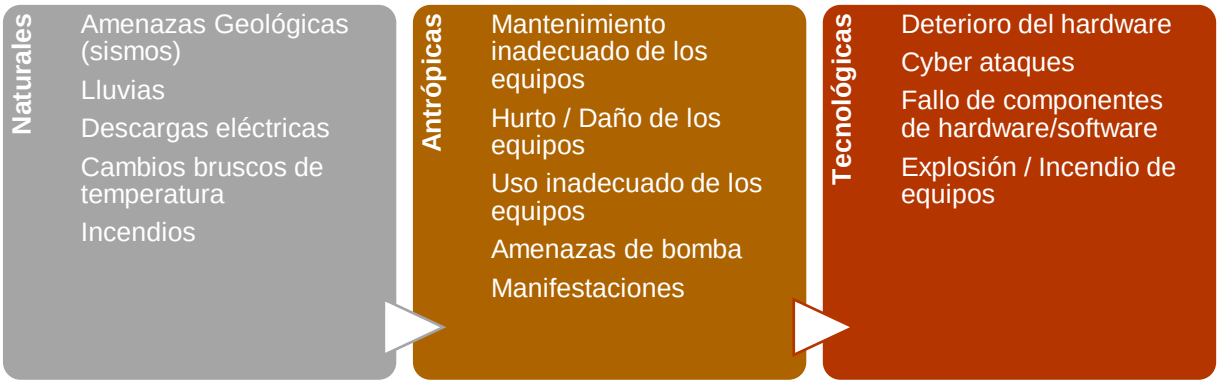
Dentro de los departamentos de Tecnologías de la Información (TI) de cualquier organización, la gestión de riesgos tecnológicos debe ser parte integral de la seguridad. Según García & Moreta (2018), “La ausencia de políticas de seguridad, protocolos de prevención y corrección, y, control de riesgos denota en un perfil con alto grado de vulnerabilidades”.

Los laboratorios de informática de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte (UTN) desde su consolidación en el año 1996 disponen de varios artefactos tecnológicos, tales como: redes de comunicación, software especializado, equipos de alta prestación, entre muchos otros. Este departamento ha ido evolucionando y mejorando los niveles de seguridad, pero aún existen varias brechas que no han sido correctamente atendidas, la más notable es la falta de aplicación de una metodología para el análisis de riesgos tecnológicos.

La Organización de Estándares de Conservación (2016) distingue 3 tipos de amenazas posibles presentes en las organizaciones, estas son: Naturales, Antrópicas y Tecnológicas. Desde la fecha de creación de los laboratorios FICA-UTN hasta la actualidad se han podido registrar los 3 tipos de amenazas ya mencionados, como se puede observar en la Figura 1.

Figura 1

Tipos de Amenazas en los Laboratorios FICA-UTN

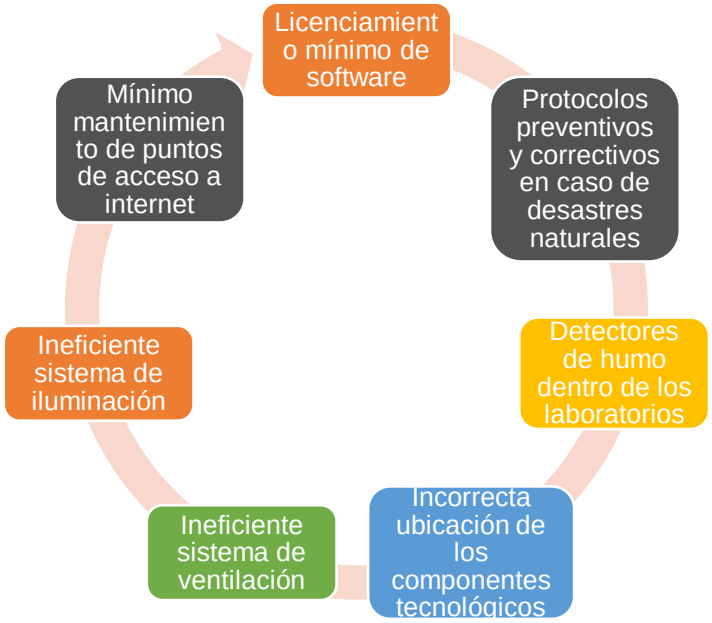


Nota: La figura representa los distintos tipos de amenazas identificados de manera preliminar en los laboratorios de informática FICA-UTN. Elaboración propia

Estas amenazas son producto de distintas vulnerabilidades presentes en los laboratorios FICA-UTN que no han sido controladas correctamente por parte de los encargados de los laboratorios, estas pueden ser apreciadas en la Figura 2.

Figura 2

Vulnerabilidades en los laboratorios FICA-UTN



Nota: La figura presenta las distintas vulnerabilidades identificadas de manera preliminar en los laboratorios de informática FICA-UTN. Elaboración propia.

Situación Actual

Actualmente, la FICA cuenta con un determinado personal dedicado a los laboratorios, entre los cuales está: un jefe de Laboratorios/analista de sistemas y dos asistentes de laboratorios de enseñanza. La distribución tecnológica de los laboratorios de informática FICA-UTN es la siguiente:

3 laboratorios con prestaciones de equipos Apple y sistema operativo Macintosh.

7 laboratorios con prestaciones de equipos Lenovo, Acer, Clon y sistema operativo Windows.

“La distribución de espacios de trabajo de los laboratorios está diseñada para ser utilizados por las 7 carreras pertenecientes a la FICA y tienen una capacidad promedio de 20 equipos por laboratorio” (Jaramillo & Sevilla, 2021).

Según Starodub & Sevilla (2021) el costo de infraestructura tecnológica en los laboratorios no es el mismo, debido a la distribución de las distintas marcas de equipos en los espacios. Además, encontró que el nivel de seguridad de los laboratorios no es equilibrado, lo cual se evidencia en los distintos sistemas de acceso a los laboratorios (físicos y biométricos).

Si bien se han desarrollado varios documentos en los cuales se detalla el uso recomendado de los equipos durante el horario académico, no existen políticas aprobadas por las autoridades y tampoco un plan para el análisis y gestión de riesgos que minimice la presencia de vulnerabilidades existentes en Laboratorios FICA-UTN.

Prospectiva

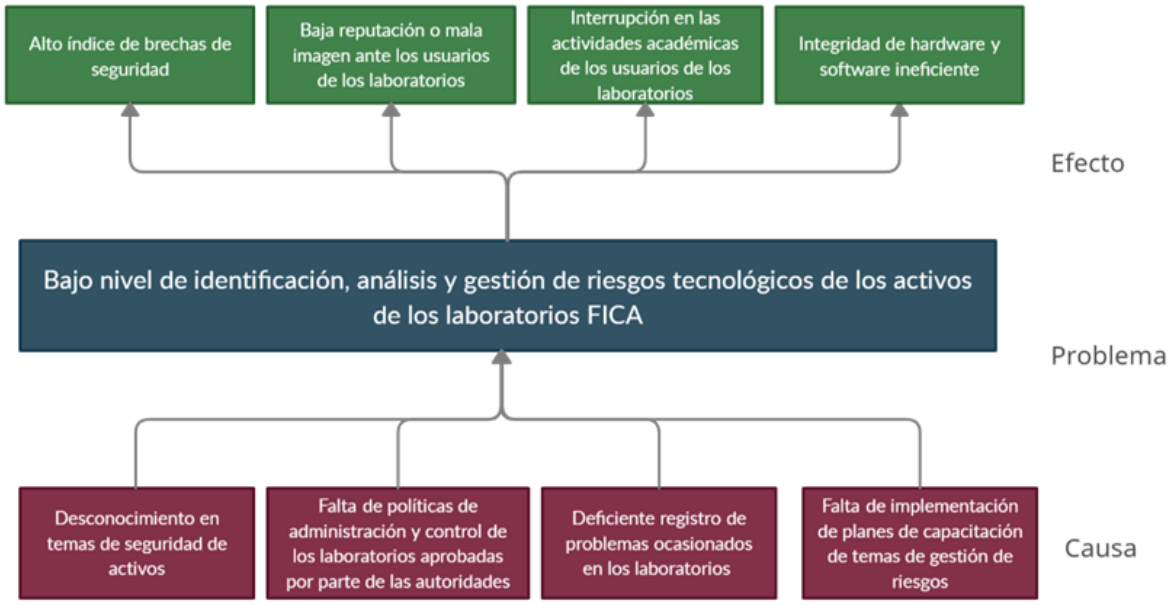
El presente trabajo plantea diseñar un plan de gestión para el análisis de riesgos tecnológicos basado en la identificación de activos y riesgos asociados. El plan tiene como finalidad minimizar las probabilidades de sufrir afectaciones y pérdidas económicas, informáticas, ambientales y humanas como consecuencia del funcionamiento ineficiente de los activos tecnológicos. El plan de gestión será diseñado con base en la metodología de análisis de riesgos MAGERIT en su versión 3 para ser aplicado al departamento de estudio, que en este caso son los laboratorios de informática de la FICA de la Universidad Técnica del Norte.

Planteamiento del problema

El personal encargado de los laboratorios de informática de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte no cuenta con el nivel necesario de competencias útiles para identificar, analizar y gestionar riesgos tecnológicos, como se muestra en la Figura 3.

Figura 3

Árbol de problemas



Nota: La figura representa el árbol de problemas con las causas, efectos y problema identificado para el presente trabajo. Elaboración propia.

Objetivos

Objetivo General

Diseñar un plan de gestión de riesgos tecnológicos con la metodología MAGERIT V3 basada en la norma ISO/IEC 31000, para fortalecer la gestión de amenazas y riesgos en los laboratorios de informática de la Facultad de Ingeniería en Ciencias de la Universidad Técnica del Norte.

Objetivos Específicos

- Establecer un marco teórico sobre la gestión y análisis de riesgos dentro de áreas de TI de las Instituciones Públicas de Educación Superior.

- Desarrollar un Plan de Gestión de Riesgos mediante la recopilación de información del caso de estudio con base en la metodología MAGERIT V3 y lineamientos fundamentados en la norma ISO/IEC 31000.
- Implementar el plan de gestión para el análisis de riesgos tecnológicos aplicado a los laboratorios de informática de la FICA-UTN.
- Validar el plan de gestión para el análisis de riesgos tecnológicos mediante el método Delphi de consulta a expertos.

Alcance

El alcance de este trabajo de tesis es diseñar un plan de gestión de riesgos tecnológicos con base en la metodología MAGERIT V3 desarrollada por el Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital, con la colaboración del Centro Criptológico Nacional (CCN).

"Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina Proceso de Gestión de los Riesgos en la sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del Marco de Gestión de Riesgos" (ISOTools Excellence, 2022).

En la Figura 4 se puede apreciar el proceso que sigue la metodología MAGERIT.

Figura 4

Proceso Metodología MAGERIT

Nota: La figura presenta los distintos pasos a seguir para el análisis y gestión de activos presentes en la metodología MAGERIT. Tomado de *Calidad en las TIC. Gestión del Riesgo*, por A. Samblás, 2014, (http://calidadtic.blogspot.com/2014/02/gestion-del-riesgo.html).

Mediante el análisis, estudio y recolección de información de la situación actual de laboratorios de informática de la FICA de la Universidad Técnica del Norte, se identificó el nivel de madurez de riesgos en el caso de estudio. El nivel de madurez de riesgos se evaluó con el Modelo de Madurez de Riesgos (RMM) desarrollado por la Sociedad de Gestión de Riesgos (RIMS) en 2006 y actualizado por la Empresa Logic Manager en 2020.

Este análisis se lo realizó con el fin de fortalecer la motivación por parte de los interesados para la aceptación del plan de gestión de riesgos.

Es importante mencionar que, adicional se hizo uso del software PILAR en su versión RM demo, que es una herramienta de software desarrollada por el Centro Nacional de Inteligencia de España. que permite realizar el análisis y la gestión de los riesgos en el marco de los Criterios.

Metodología

El desarrollo de los 4 objetivos del trabajo de tesis se lo realizó de la manera expuesta en la Figura 5.

Para cumplir con el objetivo 1, el marco teórico tuvo un enfoque investigativo/analítico de tipo empírico, se llevó a cabo una búsqueda de numerosas referencias sobre temas de Gestión de Riesgos, especialmente enfocados en los de índole tecnológico. Todas estas referencias fueron provenientes de artículos confiables, veraces y que tengan sustento científico. El proceso de investigación se ejecutó a través de una Revisión Bibliográfica en bases de datos de cuartil 1 a cuartil 4. Manterola et al. (2013) afirma que, este método resulta ser un diseño eficiente y sólido, que además genera resultados consistentes.

Para cumplir con el objetivo 2, como primera instancia del desarrollo del Plan de Gestión de Riesgos, se planteó el estado actual del caso de estudio con el desarrollo de 3 tareas:

- Recopilación de información: se realizará mediante entrevistas al equipo encargado de los laboratorios de informática FICA.
- Evaluación del problema: se realizará mediante la tabulación de encuestas realizadas a usuarios y encargados de los laboratorios de informática FICA.

- Estado de gestión de riesgos: se realizará utilizando la calificación obtenida por Risk Management Model (RMM) aplicados en los laboratorios de informática FICA.

Para determinar las fases comprendidas en el Plan de Gestión de Riesgos se tomó en cuenta las recomendaciones del sistema para la Gestión de Riesgos presente en la Norma ISO 31000.

I. Principios
II. Liderazgo y compromiso
III. Diseño del marco de trabajo
IV. Implementación de la gestión de riesgo
V. Seguimiento y Evaluación
VI. Mejora continua

Dentro del apartado 4 “Implementación de la gestión de riesgos”, la metodología MAGERIT V3 responde al proceso de gestión de riesgos con sus cuatro actividades principales:

I. Identificación y valoración de activos.
II. Identificación y valoración de amenazas.
III. Determinación del riesgo.
IV. Identificación y valoración de salvaguardas.

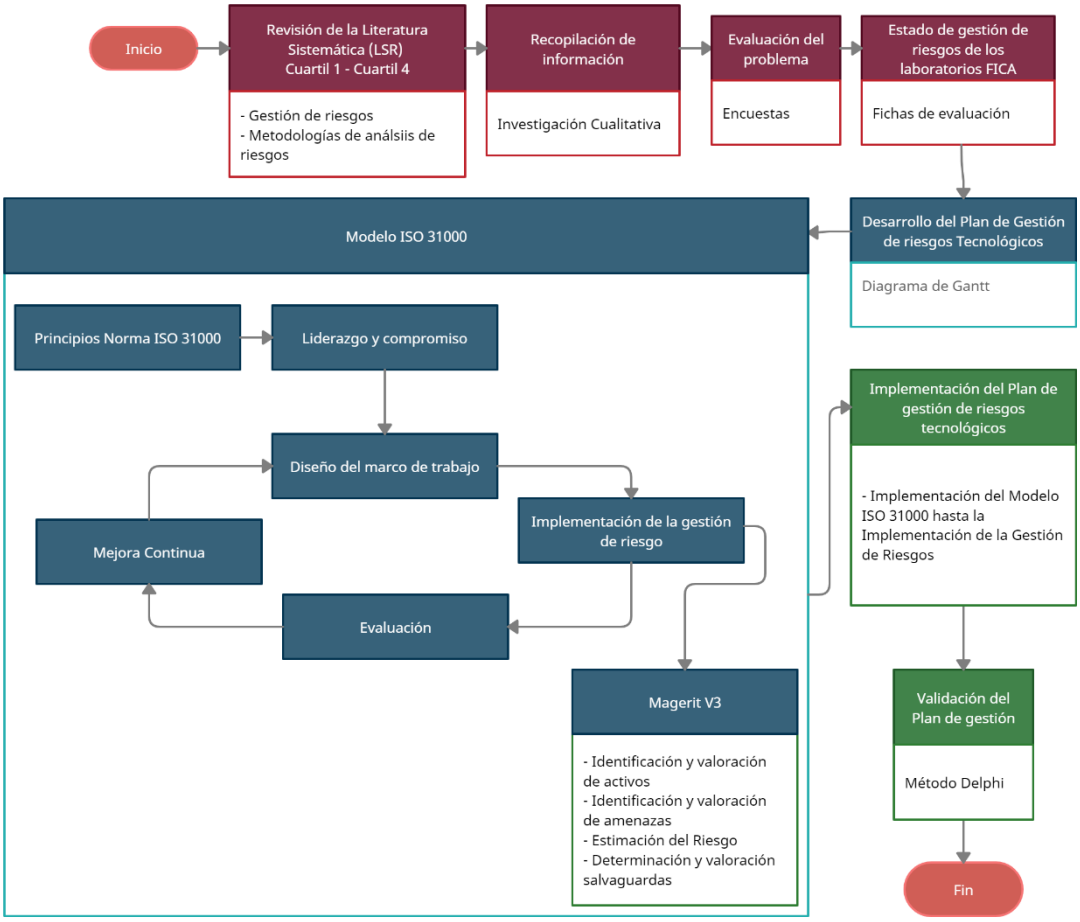
Después se realizó el desarrollo del Plan de Gestión de Riesgos con la herramienta Diagrama de Gantt, la cual Bitrix (2021) plantea como una herramienta visual que permite gestionar tareas, responsabilidades y tiempos de entrega de manera sencilla para su comprensión.

Para cumplir el objetivo 3, se desarrolló las tareas establecidas en el Plan de Gestión de Riesgos aplicado a los laboratorios de informática FICA-UTN, además de socializaciones de este al personal encargado de los laboratorios, y, elaboración de material de ayuda como posters y folletos para los estudiantes usuarios de los laboratorios.

Para cumplir el objetivo 4, se realizó una evaluación al Plan de Gestión de Riesgos anteriormente desarrollado con el método Delphi de consulta a expertos en el área.

Figura 5

Metodología Trabajo de Investigación



Nota: La figura presenta los pasos con la metodología correspondiente para cumplir con cada objetivo del trabajo de investigación. Elaboración propia.

Justificación

Según Solarte et al. (2018), “Actualmente los datos contenidos en los sistemas de información son los activos más valiosos para las organizaciones y es necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad”.

El presente proyecto de tesis busca contribuir con el Objetivo de Desarrollo Sostenible de las Naciones Unidad N16 “Promover sociedades justas, pacíficas e inclusivas”.

Específicamente con la meta 16.6 “Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas” (Organización de las Naciones Unidas, 2020).

Además, coopera con las metas nacionales establecidas por el Plan de Creación de Oportunidades 2021-2025. Dentro del Eje de Seguridad Integral, al ser un tema muy relacionado en la confianza y seguridad de las personas, se ve involucrado con el Objetivo 9: “Garantizar la seguridad ciudadana, orden pública y gestión de riesgos, específicamente” (Consejo Nacional de Planificación, 2021)

El Plan de Desarrollo Informático de la Universidad Técnica del Norte, en su misión correspondiente a la Dirección de Informática indica que:

“Se tiene que proponer y desarrollar proyectos que involucren tecnologías computacionales y de información que aseguren la competitividad tecnológica local, nacional e internacional” (Universidad Técnica del Norte, 2017).

Justificación Metodológica

La selección de la metodología MAGERIT V3 se realizó con base en las consideraciones tecnológicas, de adaptabilidad y de evolución expuestas en el artículo de investigación “Comparing Methodologies for IT Risk Assessment and Analysis” desarrollada por expertos de Gartner Research, empresa de investigación Tecnológica Estadounidense (Robins et al., 2014).

La metodología MAGERIT V3 servirá como ayuda al marco de trabajo del Plan de Gestión de riesgos que responde al “Proceso de Gestión de Riesgos” de la sección 4.4 dentro del “Marco de Gestión de Riesgos” de la normativa ISO/IEC 31000.

Justificación Tecnológica

La Universidad Técnica del Norte es una institución educativa de nivel superior que siempre ha buscado las herramientas más adecuadas para mejorar la calidad de aprendizaje de sus estudiantes. Por esta razón, implementa espacios como los laboratorios de informática en Facultades como la FICA que cuenta con muchas carreras de carácter práctico.

Estos laboratorios son de uso común para los estudiantes y docentes, por este motivo están conectados por redes, tienen acceso exterior a internet y son propensos a diversos riesgos informáticos.

La implementación de técnicas o metodologías para el análisis y gestión de riesgos es fundamental para identificar las amenazas y las acciones que atenten contra la seguridad de los activos.

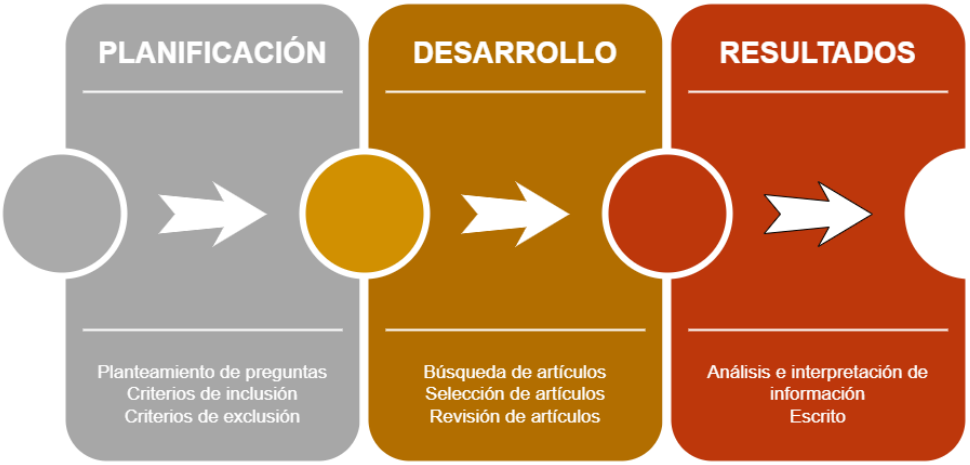
CAPÍTULO 1

Marco Teórico

Para el establecimiento del Marco Teórico sobre el análisis y gestión de riesgos dentro de áreas de TI de las Instituciones de Educación Superior se utilizó el método de revisión bibliográfica que comprende las fases presentadas en la Figura 6.

Figura 6

Proceso Revisión Bibliográfica



Nota: La figura presenta las tres fases con sus tareas pertinentes a la Revisión de bibliografía en el desarrollo del Marco Teórico. Elaboración propia.

Para la fase de planificación se plantearon distintos enfoques con preguntas relevantes al tema de Gestión de riesgos, estos son:

- Caracterización del concepto de Gestión de Riesgos de TI en Instituciones de Educación Superior

  I. ¿Qué es la Gestión de Riesgos?

  II. ¿Qué conceptos relacionados existen en torno a la gestión de riesgos?

  III. ¿Qué beneficios presenta el proceso de Gestión de Riesgos en las organizaciones?

- Caracterización de metodologías para la Gestión de Riesgos de TI

I. ¿Qué metodologías para la Gestión de Riesgos existe?

II. ¿Cuáles son los pasos o fases para seguir de estas metodologías?

III. ¿Qué ventajas o desventajas presentan estas metodologías?

- Caracterización de Normas para la Gestión de Riesgos de TI

I. ¿Qué normas nacionales o internacionales existen para la Gestión de Riesgos?

II. ¿Qué recomendaciones o cumplimiento exigen estas normas?

III. ¿Qué ventajas o desventajas presentan dichas normas?

Los criterios de inclusión comprenden varias condiciones que funcionan como filtros para la selección del material; este puede ser de tipo artículo científico, entrevista, informe oficial, libro, página web, o tesis. En caso de los artículos científicos, estos deben ser de revistas científicas de cuartil Q1 a Q4, y en idioma español o inglés.

Para la fase de desarrollo se llevó a cabo la búsqueda de artículos en bases de datos bibliográficas como: Elibro, Elsevier, IEEE, Scopus, Springer, Taylor & Francys, Informa UK Limited, IntechOpen y repositorio de instituciones de educación superior. Una vez aplicado el filtrado con los criterios de inclusión se realizó una matriz de fichaje con los datos de este material. Para la fase de resultados se analizó la información más relevante y se la presenta a continuación.

1.1. Análisis y Gestión de Riesgos.

1.1.1. Definiciones

Al riesgo comúnmente se lo relacionaba como suceso referente al azar o fortuna junto con el desarrollo social, la definición ha ido evolucionando hasta llegar a tener diversos conceptos. “Un riesgo es una posible pérdida producida por eventos peligrosos e inciertos ligados a vulnerabilidades existentes” (Soler et al., 2018).

Tamayo et al. (2020) definen al riesgo como “Un fenómeno inherente a la humanidad y está presente en todas las esferas de la actividad humana, al punto de que no existe proyecto, empresa o decisión, que no sea ensombrecida por la presencia de uno o varios riesgos” (p.9).

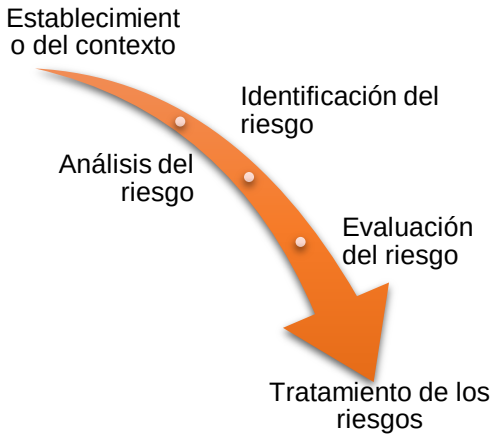
Las dos definiciones son acertadas en el sentido de que, el riesgo es un concepto existente en toda la organización social y de no ser controlado puede derivar en posibles

pérdidas. La finalidad de las organizaciones es la de proveer productos o servicios a la sociedad, este hecho aporta un valor intrínseco, que necesita ser protegido de posibles riesgos y puedan materializarse. Como respuesta a esta necesidad se crea el proceso de Gestión de Riesgos. La Gestión de Riesgos se refiere al desarrollo de actividades con el afán de minimizar las pérdidas ocasionadas debido a la concepción de riesgos en las organizaciones (Soler et al., 2018; Tamayo et al., 2020). La integración de este proceso debe ser una decisión organizacional tomada por la alta dirección para el aseguramiento de la continuidad del ente.

En su estudio desarrollado para el proceso de gestión de riesgos en la industria de la salud, Alam (2016) asegura que la integración del proceso de Gestión de Riesgos, independientemente del tipo de organización, requiere de una serie de cinco pasos descritos en la Figura 7.

Figura 7

Pasos iniciales para la gestión de riesgos



Nota: Elaboración propia a partir de “Steps in the Process of Risk Management in Healthcare” (p.2), por A. Alam, 2016, *Journal of Epidemiology and Preventive Medicine*, 2 (2).

1.1.2. Beneficios e importancia de la gestión de riesgos

Las partes interesadas dentro de las organizaciones están en su mayoría enfocadas en la minimización de costos y tiempos para el desarrollo de actividades relacionadas a sus productos o servicios, Srinivas (2019) considera que, los retrasos en el cumplimiento de estas actividades son debido a riesgos del entorno interno y externo. Para Castro et al. (2020) las razones de que una organización no realice una correcta gestión de los riesgos son: la inmadurez, desinformación o desconocimiento de los beneficios que este proceso conlleva.

En la Figura 8 se recopilan varios de los beneficios que presenta la integración de la Gestión de Riesgos en las organizaciones.

Figura 8

Beneficios de la gestión de riesgos

Nota: Elaboración propia a partir de *Process of Risk Management* (p.13), por K. Srinivasm, 2019, Perspectives on Risk, Assessment and Management Paradigms.

Usualmente, al proceso de Gestión de Riesgos se lo toma como medida preventiva para evitar pérdidas ante afectaciones que pueden llegar a ocurrir; pero, también se lo debería considerar como medida de crecimiento al impulsar la maximización de los objetivos internos de la organización.

Otro de los beneficios a los que se suma la Gestión del Riesgo, es la preparación para auditorías de TI, Imbaquingo et al., (2020) asegura que “la información es poder” y junto con la aplicación de auditorías de TI dentro de las organizaciones, este aspecto de gran importancia estaría asegurado.

1.1.3. Conceptos Relacionados

Para el correcto entendimiento de las actividades pertenecientes a la gestión de riesgos, es necesario la comprensión de conceptos relacionados con este proceso. Estos son:

Activos: considerados todos los objetos que generen valor a la organización. Molina (2015) distingue dos tipos de activos: los activos principales que están fuertemente relacionados con la lógica e información de la institución, y los activos de apoyo, que en su mayoría son los equipos de software, hardware, redes, información, persona e infraestructura de la organización.

Amenazas: Humayun et al. (2020) considera a las amenazas como acciones tomadas para obtener un beneficio de las brechas de seguridad en un sistema e impactarlo negativamente.

Estas amenazas en términos de Tecnología de la Información pueden resultar en afecciones a los sistemas, equipos de cómputo, infraestructura tecnológica y seguridad de la información.

Vulnerabilidad: Se define a la vulnerabilidad como una serie de características de los activos que los predisponen a sufrir daños frente al impacto de un evento, y que dificultan su posterior recuperación (Soler et al., 2018). Las vulnerabilidades dependiendo su tipo pueden afectar a componentes de software, hardware, red y ubicación.

Salvaguardas: también conocidas como contra medidas, son todas aquellas acciones de protecciones establecidas para reducir en el mayor grado posible el efecto de las amenazas (Molina, 2015).

Impacto: magnitud de daño que ocurre a raíz de un ataque a los niveles de seguridad: integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad (Imbaquingo et al., 2017).

Riesgo: posibilidad de que una amenaza se materialice causando daños o beneficios (Imbaquingo et al., 2017).

1.1.4. Riesgos en las IES

Las Instituciones Públicas de Educación Superior son de las organizaciones más importantes dentro de las sociedades, estas aseguran la formación académica de un gran número de personas que significan el futuro de dicha sociedad. Sin embargo, aún existen varias brechas de seguridad que no han sido atendidas y que podrían causar perjuicio en varios aspectos.

Imbaquingo et al. (2020), reconocen varios problemas que enfrentan las IES entorno a la seguridad, estos son:

- Propagación de virus a través de medios tecnológicos y humanos.

- Poco o nulo compromiso en la seguridad de los activos de las IES.
- Dificultades para implementar medidas de seguridad en las IES.

Ante esta problemática se han planteado varias medidas de seguridad, las principales son:

- Evaluación de vulnerabilidades.
- Medidas técnicas.
- Capacitación del personal.
- Políticas de seguridad.

Además, se destaca la implementación de una de las normas internacionales ISO más reconocida para seguridad de la información, la Norma ISO 27002 e ISO 27001.

1.2. Estándares y Metodologías de Gestión de Riesgos

Viguri (2021) asegura que, frente a la presente necesidad de la implementación del proceso de Gestión de Riesgos en las organizaciones, los encargados de estos procesos han visto la necesidad de identificar métodos que faciliten o estandaricen dicho proceso. Por esta razón, varios organismos a nivel internacional han desarrollado distintos estándares y metodologías que permitan de cierta manera homogeneizar lo establecido como “buena calidad ante riesgos”.

En concordancia con Soler et al. (2018), se considera que, el paso más importante y crucial para una correcta gestión de riesgos es la identificación de los tipos de riesgos que afectan a la organización, por esta razón, la selección de la metodología o estándar para el desarrollo del Plan de Gestión de Riesgos es una actividad fundamental.

1.2.1. Normas ISO

Dentro de los esquemas empresariales existe un organismo encargado de desarrollar un conjunto de normas orientadas a la gestión empresarial, la Organización Internacional de Estandarización (ISO) junto con la Comisión de Electrónica Internacional (IEC) proporcionan normas para ser implementadas voluntariamente, aunque, debido a la alta competitividad que existe en el mercado actual, las instituciones toman a estas normas como un referente de reconocimiento y adaptación internacional.

El principal objetivo de las normas ISO es plantear un sistema homogéneo de las características y parámetros de calidad dentro de las empresas (Viguri, 2021).

Las normas ISO contemplan varios aspectos de calidad empresarial, por lo que, es natural encontrarse un amplio abanico de opciones. Dependiendo de su aplicabilidad, las normas han podido ser agrupadas por series o también conocidas familias, por ejemplo, la Serie ISO 9000 para la Gestión de Calidad, ISO 14000 para la Gestión de medio ambiente, ISO 22000, 27000 y 31000; para la Gestión de riesgos (Organización Internacional de Estandarización, 2018).

Cabe mencionar que, existen normas ISO que no son certificables. Guzmán (2019) explica que, para que una de estas sea publicada como certificable, esta debe ser llevada a los organismos miembros de votación y se requieren al menos el 75% de aprobación de dichos organismos.

ISO 27000

La familia de la Norma ISO 27000 es muy conocida a nivel internacional por ser la serie de normas por excelencia para la Gestión de Seguridad de los Sistemas de Información (SGSI) dentro de las organizaciones (Organización Internacional de Estandarización, 2018).

Imbaquingo et al. (2020) asegura que la información es uno de los activos fundamentales para la organización. Por lo que la existencia de esta familia de normas se vería directamente influenciada por la necesidad de garantizar el aseguramiento de la información con los SGSI de las áreas de TI.

En la Tabla 1 se describe de manera rápida cada una de las normas pertenecientes a la familia ISO 27000.

Tabla 1

Descripción de las Normas pertenecientes a la Serie ISO 27000

Norma	Descripción
ISO 27000:2016	Tecnologías de la información, técnicas de seguridad, gestión de la seguridad de los sistemas de información, visión general y vocabulario.
ISO 27001:2013	Tecnologías de la información, técnicas de seguridad, gestión de la seguridad de los sistemas de información, requerimientos.
ISO 27002:2013	Tecnologías de la información, técnicas de seguridad, código de prácticas para los controles de seguridad de la información.

ISO 27003:2010	Tecnologías de la información, técnicas de seguridad, guía de implementación para la gestión de la seguridad de los sistemas de información.
ISO 27004:2009	Tecnologías de la información, técnicas de seguridad, gestión de la seguridad de los sistemas de información, medición.
ISO 27005:2011	Tecnologías de la información, técnicas de seguridad, gestión de riesgos de la seguridad de la información,
ISO 27006:2015	Tecnologías de la información, técnicas de seguridad, requerimientos necesarios para la auditoría y certificación de la gestión de sistemas de información.
ISO 27007:2011	Tecnologías de la información, técnicas de seguridad, guía para la auditoría de la gestión de los sistemas de información.
ISO 27008:2011	Tecnologías de la información, técnicas de seguridad, guía para los auditores en los controles de la seguridad de la información.
ISO 27009:2016	Tecnologías de la información, técnicas de seguridad, aplicación específica de los requerimientos de la norma ISO/IEC 27001

Nota: Elaboración propia a partir de *La Familia de Normas ISO 27000*, por ISOTools, 2015, Blog Calidad y Excelencia (https://www.isotools.org/2015/01/21/familia-normas-iso-27000/).

ISO 27005

"Es la norma que proporciona directrices para la gestión del riesgo de la seguridad de la información, sin proporcionar metodologías específicas para tal fin" (Valencia, 2021).

Esta norma en específico está conformada por 14 secciones en las que se detalla diversas recomendaciones para que las organizaciones mantengan un buen Sistema de Gestión de Seguridad de la Información. La estructura es representada en la Figura 9.

Figura 9

Secciones que conforman la estructura de la Norma ISO 27005

Nota: Elaboración propia a partir de *ISO/IEC 27005:2018 Information technology-Security techniques-Information security risk management*, por Organización Internacional de Estandarización, 2018, (https://dgn.isolutions.iso.org/obp/ui#iso:std:iso-iec:27005:ed-3:v1:en).

ISO 31000.

Bonet et al. (2019) asegura que la norma está enfocada en la gestión de riesgo, sin importar el tamaño, tipo o naturaleza de la organización, a diferencia de las normas ISO de la serie 27000, que solamente están enfocadas en la gestión de riesgos alineados a la seguridad de la información.

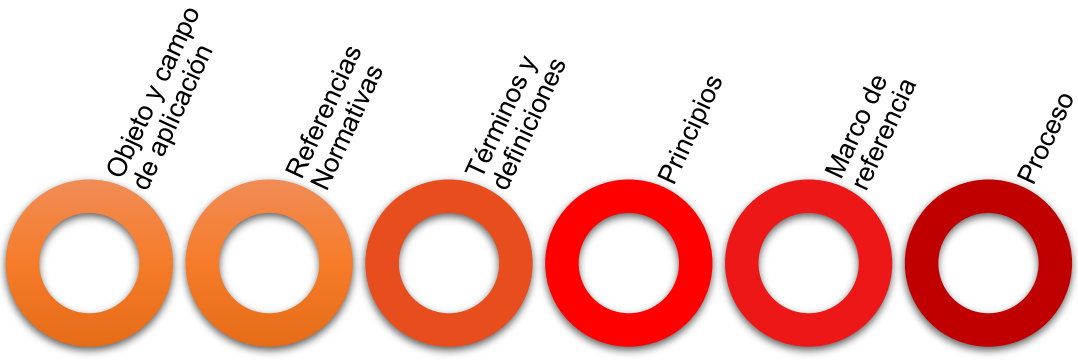
El principal factor que se puede considerar como desfavorable para la Norma ISO 31000, es su no-certificación por parte del comité responsable de las normas referentes a la Gestión de Riesgos ISO/TC 262.

La Organización Internacional de Estandarización (2018) presenta dos versiones, la primera lanzada en el año 2009 y la segunda que se utilizó como reemplazo en el año 2018. Esta última considerada una versión mejorada en ciertos aspectos deficientes de su predecesora, tales como: revisión de los principios de gestión de riesgos, mayor énfasis en el liderazgo y alta dirección, mayor importancia a la naturaleza iterativa de la gestión del riesgo y la simplificación del proceso.

La Figura 10 presenta las seis secciones que conforman la Norma ISO 31000.

Figura 10

Secciones que conforman la estructura de la Norma ISO 31000



Nota: Elaboración propia a partir de *ISO 31000 Risk management*, por Organización Internacional de Estandarización, 2018, (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es).

Si bien la norma cuenta con seis secciones, las tres primeras son meramente secciones informativas que pueden ser despreciadas al momento de tomar en cuenta la alineación de la norma.

1.2.2. Comparación Normas ISO

La selección de las Normas Internacionales ISO resulta muchas veces complicado debido a la amplia gama de opciones existentes. En la Tabla 2 se presenta una comparación en varias métricas, entre las dos principales normas referentes a la Gestión de Riesgos, estas son las Normas ISO 27005 e ISO 31000.

Tabla 2

Comparación Normas ISO 27005 e ISO 31000

Campo de comparación	ISO 27005	ISO 31000
Certificable	Consta como una norma certificable	No es una norma certificable
Última modificación	2018	2018
Herramientas de apoyo	No	Puede hacer uso de la Norma ISO 31010
Disponibilidad	Al ser una norma certificable, tiene un costo dependiendo del ente certificador	Está disponible en la página oficial de la Organización Internacional de Normalización
Aplicabilidad	Su principal campo de aplicación son los Sistemas de Gestión de Seguridad de la Información	Tiene una visión mucho más macro del Sistema de Gestión de Riesgos, por lo que es aplicable a cualquier tipo de riesgos
Alcance	Está diseñada para organizaciones de cualquier tipo	Está diseñada para organizaciones de cualquier tipo
Extensión	Consta de 24 secciones	Consta de 6 secciones
Relación con la alta dirección	Opcional	Si
Identificación de riesgos e impactos	Si	Si
Metodología	Incluye una metodología definida para la gestión de riesgos de los sistemas de información.	No, esta norma no incluye el “cómo hacer”, pero puede adoptar una metodología externa
Guía de aplicación	Si, la norma posee anexos con distintos ejemplos de conceptos relacionados a la gestión de riesgos.	No, pero posee un glosario de términos
Proceso de gestión de riesgos	Se basa en la norma ISO 31000	Tiene un proceso bien definido: identificación, análisis y valoración de riesgos.
Mejora continua	No	Si, hace énfasis en el proceso de mejora continua
Conciencia de uso	Es utilizada cuando se asimila que la información en los sistemas informáticos es importante	Es utilizada en cualquier caso que se desee tener un marco apropiado para la gestión de todo tipo de riesgos.

Nota: Elaboración propia.

Como se aprecia en la tabla comparativa, mientras que la Norma ISO 27005:2018 es una norma mucho más específica en el campo de “Sistema de Gestión de Seguridad de la Información”, la Norma ISO 31000:2018 es una norma mucho más amplia en su campo de aplicación. Esta última puede ser utilizada para todo tipo de riesgo dentro de la organización, y al no estar limitada a un método específico, puede hacer uso de una metodología existente dependiendo de las necesidades.

Además, en acuerdo con Olechowski et al. (2016), la aplicación de la Norma ISO 31000, presenta diversos beneficios:

- Promueve la correcta relación y comunicación entre los gestores de riesgo y la alta dirección.
- Incluye la integración de los objetivos organizacionales con los objetivos de la gestión de riesgos.
- Promueve la mejora en la cultura organizacional.
- Minimiza las pérdidas ocasionadas a raíz de la materialización de las amenazas.
- Promueve la mejora de la toma de decisiones a nivel interno de la organización.

1.2.3. Metodologías de Gestión de Riesgos

Las normas establecidas por la Organización Internacional de Normalización proponen una forma de identificar el estado de calidad en el que se encuentra la organización, pero, no brindan un método con pasos específicos para poder llegar a cumplir con los objetivos que se busca.

Muchos autores desarrollan sus propias metodologías para la gestión de riesgos, tal es el caso de Ay et al. (2022) que desarrolló la metodología ARAMIS, la cual tiene un enfoque en los riesgos industriales. Mientras que muchos otros prefieren utilizar alguna de las ya existentes.

Dentro de las Instituciones Públicas de Educación Superior revisadas, se han implementado metodologías de gestión de riesgos, ya sea de manera interna o a manera de trabajos de integración curricular a organizaciones externas, las más destacables son: OCTAVE, CRAMM y MAGERIT.

OCTAVE

La metodología Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) para la Gestión de Riesgos se enfoca en la Evaluación de amenazas, activos y vulnerabilidades operativamente críticas. Fue desarrollada por el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon, con la finalidad de brindar un nivel de análisis estructurado, enfocado en los activos y la mitigación de amenazas (Gartner Research, 2010).

Alberts et al. (2003) explica que la metodología OCTAVE se divide en tres fases.

I. Se reconoce los elementos necesarios para la gestión. Estos son: los activos, amenazas, vulnerabilidades, exigencias y normas de seguridad. Esta fase a su vez consta de cuatro pasos.

    1. Se identifica la directiva y su conocimiento del tema de seguridad.
    2. Se identifica la directiva y su conocimiento a nivel operacional.
    3. Se identifica al personal y su conocimiento sobre seguridad.
    4. Se identifica las posibles amenazas con base en la información recaudada en pasos anteriores.

II. Se clasifican los componentes y vulnerabilidades técnicas. Esta fase consta de dos pasos.

    1. Identificación de componentes clave para la evaluación de vulnerabilidades tecnológicas.
    2. Evaluación de los componentes clave.

III. Se planifica las medidas de mitigación de riesgos mediante la evaluación de los riesgos. Esta fase consta de dos pasos.

    1. Análisis de riesgos.
    2. Definición de estrategias para la mitigación.

CRAMM

CRAMM es una metodología de análisis y gestión de riesgos desarrollada en 1985 por la Agencia Central de Informática y Telecomunicaciones (CCTA), perteneciente al gobierno de Reino Unido, sus siglas corresponden a CCTA Risk Analysis and Management Method (Crespo & Cordero, 2018).

CRAMM fue diseñada principalmente como metodología de apoyo para los analistas de sistemas con el fin de cumplir los intereses de protección referentes a confidencialidad, integridad y disponibilidad de la información y activos relacionados (Crespo & Cordero, 2018).

La metodología CRAMM comprende 3 fases bien definidas.

I. Se definen los objetivos globales de seguridad para la organización. Además de establecer el alcance, identificación y evaluación de activos asociados.

II. Se analiza las amenazas y vulnerabilidades para definir los riesgos y su posibilidad de materialización.

III. Se identifica posibles salvaguardas para la mitigación de riesgos. En muchos casos que no se elimina el riesgo, se considera la opción de tener riesgos residuales.

MAGERIT

El ministerio de Hacienda y Administraciones Públicas de España define a la metodología a MAGERIT como:

> Una metodología que ha sido elaborada como respuesta a la percepción de la administración pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. Así, menciona que el uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

La metodología MAGERIT persigue los siguientes objetivos:

- Crear conciencia en los encargados de los sistemas de información sobre la necesidad del tratamiento de los riesgos.
- Ofrecer una metodología para el análisis y gestión de riesgos.
- Determinar las mejores medidas para mantener los riesgos mitigados.
- De manera indirecta, mantener a la organización lista para procesos de certificación y acreditación.

La metodología MAGERIT consta de los siguientes pasos:

I. Identificación de activos de TI relevantes a la organización.

II. Identificación de las amenazas a los que los activos están expuestos.

III. Identificación de las posibles salvaguardas efectivas para la mitigación del riesgo.

IV. Definición del impacto que tiene la materialización de una amenaza sobre los activos.

V. Definición de los riesgos, que son el impacto ponderado con la tasa de ocurrencia de las amenazas.

Un detalle para tener en cuenta es que, si bien en el modelo no se aprecia el término "Vulnerabilidad", MAGERIT lo evidencia en su implementación; Ruge (2012) asegura que, dentro de esta se toma a la Vulnerabilidad como "La potencialidad o posibilidad de ocurrencia de una amenaza sobre un activo" (p.27).

MAGERIT en su versión 3 cuenta con tres libros:

I. Método

II. Catálogo de Elementos

III. Guía de Técnicas

1.2.4. Comparación Metodologías de Gestión de Riesgos

La creación de las metodologías para la gestión de riesgos ha sido beneficioso para las distintas organizaciones, que les permite tener un mejor sistema para salvaguardar sus activos, ya sean tecnológicos, informáticos, personales y otros. Pero, el basto número de metodologías muchas veces puede significar confusión e indecisión para la correcta selección de esta.

García & Moreta (2018) desarrollan una comparativa entre 3 metodologías de gestión de riesgos (MAGERIT, OCTAVE, MEHARI) con base en criterios de evaluación relacionados a la Norma ISO 31000. En la Tabla 3 se presenta dicha comparación, pero intercambiando la metodología MEHARI por la metodología CRAMM.

Tabla 3

Comparación Metodologías MAGERIT, OCTAVE, CRAMM

Parámetro ISO 31000	Categoría para evaluar	Mejores prácticas	MAGERIT	OCTAVE	CRAMM
Marco de Referencia	Política de Riesgos	Existe una política formal y actualizada de riesgo aprobada por la autoridad responsable y que transciende a pesar de cambios de personal en la alta dirección.	X	X	X
		La política es revisada y comunicada a toda la organización.	X		
	Responsabilidad	La organización posee un departamento de TI con un equipo de análisis de riesgo.	X		X
		Los roles del equipo de TI están claramente definidos, aceptados y documentados.	X		X
	Compromiso de la Alta Dirección	La alta dirección es un apoyo activo para el equipo de análisis de riesgo.		X	
	Comunicación	Existen programas de capacitación formalizada para establecer una cultura de riesgo.	X		
Identificación y valoración de activos	Determinación y valoración de activos	Los activos/recursos TI han sido clasificados según una perspectiva de: servicios, datos/información, aplicaciones, equipos informáticos, redes de comunicación, soporte de información, equipamiento auxiliar, instalaciones y personal.	X	X	X
Determinar las amenazas de los activos	Identificación y estimación de amenazas	La empresa analiza exhaustivamente las amenazas externas e internas a los que pueden verse afectados los activos de información.	X	X	X
		Por cada amenaza identificada se ha definido la dimensión de disponibilidad, integridad, y confidencialidad; que puede resultar afectada en el activo de información.	X	X	X
Estimar el impacto de la amenaza	Estimación del impacto	Se ha ponderado el impacto acumulado tomando en cuenta la degradación causada por la amenaza, y el impacto repercutido teniendo en cuenta el valor propio del activo y las amenazas a los que está expuesto.	X		

Determinación del riesgo	Evaluación del riesgo	Se ha definido el riesgo acumulado considerando la degradación causada y la frecuencia de la amenaza; y se ha definido el riesgo repercutido calculando el daño en los activos explícitamente valorados.	X		
		Los riesgos son clasificados a partir de una escala que considera la probabilidad e impacto, con la finalidad de priorizar los más significativos.	X	X	
Plan de Acción	Respuesta a los riesgos	Se determina una respuesta por cada riesgo identificado.	X	X	
		Cada respuesta al riesgo está perfectamente desplegada, configurada, mantenida y recaerá en una de estas categorías: Mitigar, Aceptar, Transferir, Eliminar.	X	X	
		Se ha definido el riesgo residual que permanecerá cuando una respuesta al riesgo se implemente.	X	X	
Monitoreo y Dirección	Actividades de control	Se definen indicadores de desempeño sobre la respuesta a los riesgos para determinar su validez.	X		X
		Se evalúa el riesgo residual una vez aplicada la respuesta al riesgo.	X	X	
	Mejora Continua	Exhaustiva recopilación de información para el seguimiento, revisión y aprendizaje del análisis de riesgo.	X		X
		La presencia de nuevos riesgos se identifica sistemáticamente de manera oportuna y proactiva.	X	X	X

Nota: Elaboración propia adaptada de “Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies” (pp.36-37), por García & Moreta, 2018, 7th International Conference on Software Process Improvement (CIMPS).

Con base en la comparación realizada por García & Moreta (2018), se observa varios puntos positivos para la Metodología MAGERIT, entre los cuales el más destacable es la alineación que tiene con las secciones de la ISO 31000 que va a ser aplicada en este estudio.

Esta afirmación también es fundamentada en el estudio “Comparing IT Risk Assessment and Analysis Methods” desarrollada por los Investigadores de Gartner Research, Ben Tomhave, Erik Heidt, Julia H. Allen. En este estudio se elaboró una comparación entre varias metodologías de análisis de riesgos para IT, algunas de las atribuciones brindadas a MAGERIT son: su alto índice de alineamiento con la Norma ISO 31000, su beneficio de poseer un binario ejecutable, su serie de ejemplos de métodos de análisis de riesgos y su mediano tiempo de aceleración.

En concordancia con lo expuesto por Crespo & Cordero (2018), se asimila algunos de los beneficios presentes en la aplicación de MAGERIT como metodología para la gestión de riesgos:

- La metodología MAGERIT, al ser desarrollada por el Ministerio de Hacienda de España, esta contiene sus 3 escritos en español e inglés, mientras que las metodologías OCTAVE y CRAMM solo poseen sus secciones en inglés.
- La metodología MAGERIT cuenta con un software especializado para su proceso, PILAR, que en su versión “Basic” es totalmente gratuito, lo cual facilitará en gran medida la optimización de los procesos necesarios en MAGERIT.
- La metodología MAGERIT es la metodología más utilizada en países latinoamericanos para la gestión de riesgos referentes a informática.
- La metodología MAGERIT tiene muy presente la importancia de los activos junto a las dimensiones de valoración (disponibilidad, integridad y confidencialidad) presentes en la ISO 31000.

1.2.5. Herramientas para la Gestión de Riesgos

El uso de las normas y metodologías para el análisis de riesgos conlleva una extensa lista de actividades, cada una con grandes cantidades de información para ser tratada; frente a este incidente, se han desarrollado herramientas que faciliten el proceso de aplicación. En el caso de la metodología MAGERIT, existe el software PILAR.

PILAR

El Procedimiento Informático Lógico para el Análisis de Riesgos, también conocido como PILAR, es una herramienta desarrollada por el Centro Nacional de Inteligencia para proveer

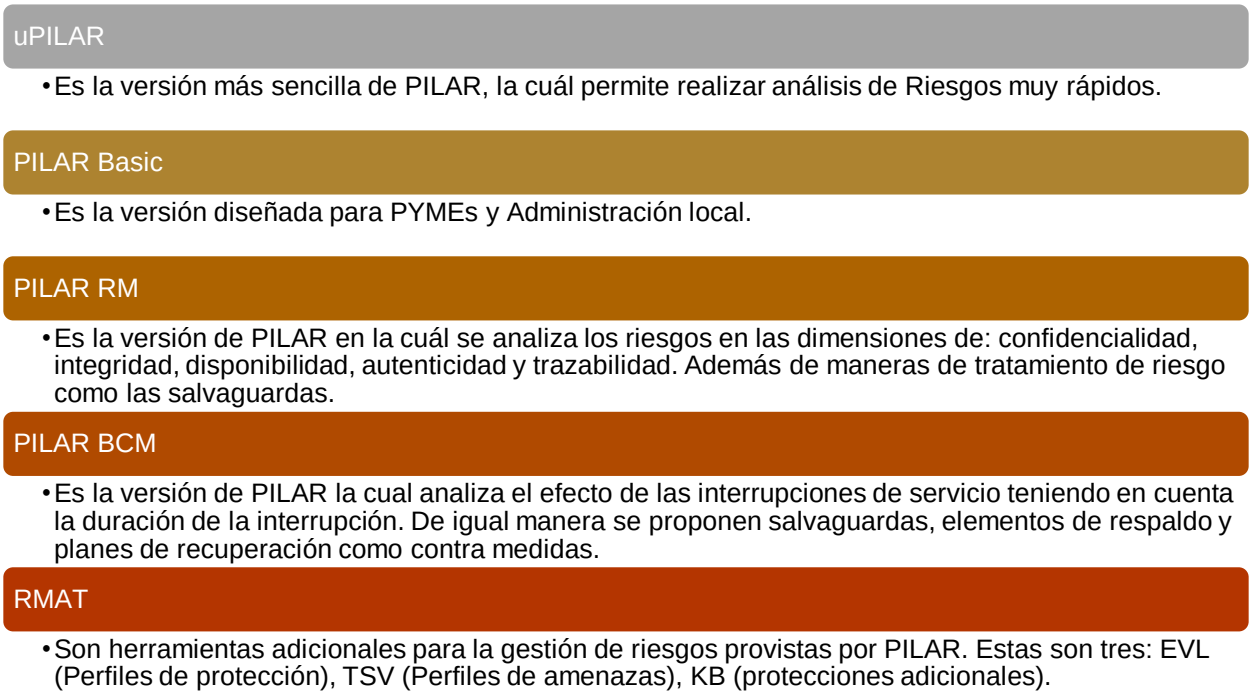
soporte a la aplicación de la metodología MAGERIT dentro de las organizaciones. Esta herramienta analiza las distintas dimensiones del riesgo: confidencialidad, integridad, autenticidad y trazabilidad; para de cierta manera proponer acciones de seguridad como las salvaguardas (Centro Nacional de Inteligencia Española, 2022).

Varios estudios (Vega et al., 2017; Molina, 2015), aseguran que, la herramienta PILAR en la mayoría de sus versiones propone salvaguardas y contramedidas eficientes para tratar los riesgos, a partir del análisis de riesgo residual a lo largo de las distintas fases del proceso.

En la Figura 11 se presenta las distintas versiones de PILAR con sus respectivas características.

Figura 11

Versiones del software PILAR



Nota: Elaboración propia a partir de *Solución PILAR*, por Centro Nacional de Inteligencia Española, 2022, PILAR (https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar).

En la Tabla 4 se presenta una comparación de las distintas versiones para comprender mejor sus diferencias.

Tabla 4

Comparación versiones software PILAR

Aspecto	uPILAR	Basic	RM	BCM	Limitaciones de licencia de evaluación
Análisis de riesgos cualitativo	Si	Si	Si		
Análisis de riesgos cuantitativo			Si		
Análisis de impacto cualitativo				Si	
Análisis de impacto cuantitativo				Si	
Proyecto (fuentes de información)			Si	Si	
Proyecto (dominios de seguridad)	1	Si	Si	Si	
Proyecto (importación)			Si	Si	Bloqueado
Caracterización de activos	Solamente clases	Si	Si	Si	<100
Valoración de activos por dominio	Si	Si	Si	Si	
Dependencia entre activos			Si	Si	
Valoración singular de activos			Si	Si	
Zonas (lógicas, físicas, TEMPEST)	2 estándar	2 estándar	Si		
Caracterización de amenazas	Si	Si	Si	Si	
Elección y valoración de amenazas	tsv	tsv	Manual, opcional, tsv	Manual, opcional, tsv	
Aplicabilidad de salvaguardas	Si	Si	Si	Si	
Valoración de salvaguardas	Si	Si	Si	Si	
Fases del proyecto	Fijas	Manual	Manual	Manual	

Impacto acumulado			Si	Si	
Riesgo acumulado	Top 10	Si	Si	Si	
Impacto repercutido			Si	Si	
Riesgo repercutido	Si	Si	Si	Si	
Perfiles de seguridad	1	Extensible	Extensible		
Informes de tipo patrones	Si	Si	Si	Si	Bloqueado
Informes de texto y gráficos			Si	Si	
Importaciones / exportaciones a CSV	Si	Si	Si	Si	Bloqueado
Importaciones / exportaciones a XML		Si	Si	Si	Bloqueado
Importaciones / exportaciones a SQL	Opcional	Opcional	Opcional	Opcional	Bloqueado

Nota: Tomada de *EAR/PILAR Adquisición*, por A.L.H. J. Mañas S.L, 2022, PILAR (https://www.ar-tools.com/es/tools/compara_es.pdf).

Cada una de estas versiones tiene su descarga disponible en inglés y español para los sistemas operativos Windows, Linux y Mac OS.

Para el uso del software se puede optar por la licencia de evaluación que tiene una duración de 30 días o se puede adquirir una licencia comercial, que, dependiendo del número de personal de la organización, puede variar su precio.

La **licencia de evaluación** contempla todas las tareas de la gestión con las siguientes limitaciones:

- No se permite la generación de informes.
- No se permite la exportación a CSV o XML.
- Número limitado de activos.
- Almacenamiento limitado de salvaguardas.

Las **licencias comerciales** existen de dos tipos, como servicio y como producto.

Las licencias como servicio tienen las siguientes características:

- Pago anual.
- Acceso a todas las versiones de ese año (solamente del tipo de software adquirido).
- Acceso limitado a “solo lectura” si no se renueva.

Tabla 5

Precios Software PILAR como servicio

Herramienta	Micro com	Small com	Big com
Número de usuarios	1	5	10
uPILAR	100 €	200 €	400 €
PILAR Basic	200 €	400 €	800 €
PILAR BCM	350 €	700 €	1.400 €
PILAR RM	500 €	1.000 €	2.000 €
PILAR RM + BCM	700 €	1.400 €	2.800 €
PILAR + BBDD	+30%	+30%	+30%
RMAT	750 €	1.500 €	3.000 €

Nota: Tomada de *EAR/PILAR Adquisición*, por A.L.H. J. Mañas S.L, 2022, PILAR (https://www.ar-tools.com/es/tools/buy.html). Al ser un software original de España, los precios se presentan en Euros.

Las licencias como producto tienen las siguientes características:

- Pago único.
- Acceso a todas las subversiones de la versión adquirida (solamente del tipo de software adquirido).
- 80% de descuento para acceder desde versiones previas.

Tabla 6

Precios Software PILAR como servicio

Herramienta	Micro com	Small com	Big com
Número de usuarios	1	5	10
uPILAR	250 €	500 €	1.000 €
PILAR Basic	500 €	1.000 €	2.000 €
PILAR BCM	1.000 €	2.000 €	4.000 €
PILAR RM	1.500 €	3.000 €	6.000 €
PILAR RM + BCM	2.000 €	4.000 €	8.000 €
PILAR + BBDD	+30%	+30%	+30%
RMAT	2.250 €	4.500 €	9.000 €

Nota: Al ser un software original de España, los precios se presentan en Euros. Tomada de EAR/PILAR Adquisición, por A.L.H. J. Mañas S.L, 2022, PILAR (https://www.ar-tools.com/es/tools/buy.html).

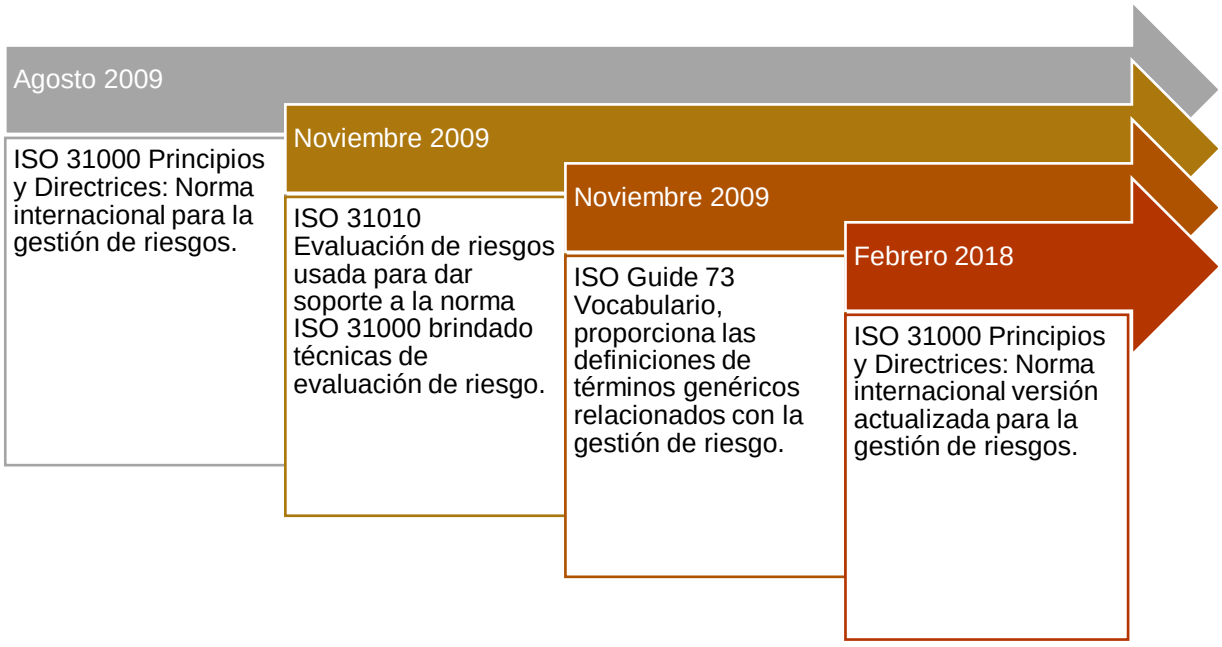
1.3. Norma Internacional para la Gestión de Riesgos ISO/IEC 31000

La Norma Internacional ISO/IEC 31000 surge en el año 2009 como solución a las organizaciones para el análisis y gestión de riesgo de cualquier tipo. El grupo ISO/TC 262 Risk Management ha trabajado desde 2014 para poder obtener una actualización de dicha norma, logrando obtener una segunda versión en el año 2018, siendo esta la norma vigente (Organización Internacional de Estandarización, 2018).

La Norma ISO 31000 se ha convertido en uno de los estándares más sustentables al ser respaldada por diversas normas de apoyo dentro de su serie. Estas son presentadas en la Figura 12.

Figura 12

Normas que apoyan a la Norma ISO 31000



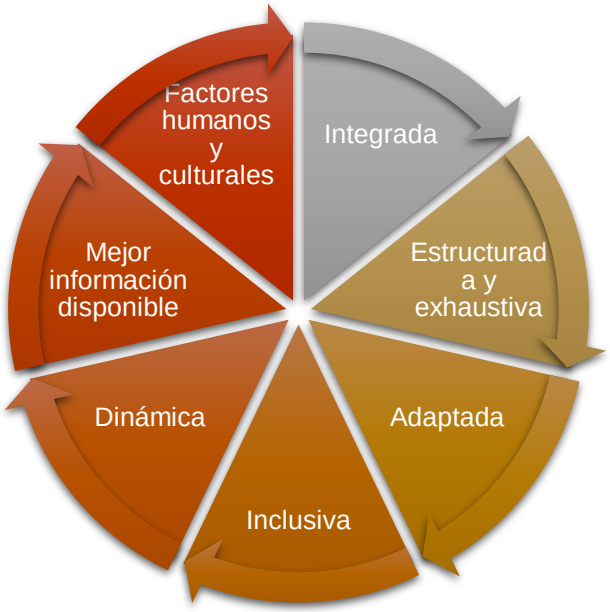
Nota: Tomado de “Diseño de un modelo de sistema para la Gestión de Riesgo con base a la Norma ISO 31000 y MAGERIT Versión 3.0 en la empresa BLUEBOX” (p.22), por O. Guzmán, 2019, *Universidad de Guayaquil*.

1.3.1. Principios

Para la aplicación de la norma ISO 31000 dentro de las organizaciones es necesario tener en cuenta que existe una lista de principios necesarios a tomar en cuenta para una gestión del riesgo eficiente y eficaz. En la Figura 14 se presentan los diferentes principios para la Creación y Protección del valor.

Figura 13

Principios de la Norma ISO 31000



Nota: Tomado de *ISO 31000:2018*, por Organización Internacional de Estandarización, 2018, ISO (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es).

Para una mejor comprensión de cada uno de los principios se presenta a continuación la Tabla 7 con sus definiciones.

Tabla 7

Definición de Principios de la Norma ISO 31000

Principio	Definición
Integrada	"Una organización, debe integrar sus esfuerzos de gestión de riesgos en todas las partes y actividades de la organización."[a]
Estructurada y exhaustiva	"Creación y seguimiento de un riesgo integral y estructurado."[a]
Adaptada	"La gestión del riesgo debe adaptarse a la situación de la organización."[b]

Inclusiva	“La gestión de riesgos debe involucrar a todas las partes interesadas de manera adecuada y oportuna para ser más eficaz.”[a]
Dinámica	“A medida que cambia la organización, incluido su contexto externo e interno, su riesgo el programa de gestión y los esfuerzos también deberían cambiar.”[a]
Mejor información posible	“La gestión eficaz del riesgo se realiza considerando información del pasado y presente y anticipar el futuro.”[a]
Factores humanos y culturales	“La gestión de riesgo debe reconocer las capacidades e intereses de los involucrados en la organización.”[b]
Mejora continua	“A través de la experiencia y el aprendizaje, los gestores de riesgos deben esforzarse continuamente para mejorar.”[a]

Nota: [a]Hardjomidjojo et al. (2022, p.4). [b]Bonet et al. (2019, p.34).

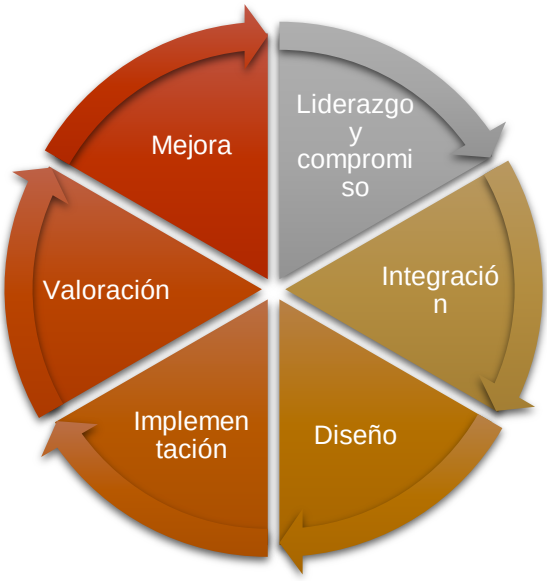
1.3.2. Marco de Referencia

El marco de referencia sirve como asistente en la integración de la gestión de riesgos dentro de la organización, por esta razón es importante una correcta integración con la gobernanza y alta dirección correspondiente (Organización Internacional de Estandarización, 2018).

En la Figura 14, se presentan los componentes del Marco de Referencia.

Figura 14

Marco de Referencia de la Norma ISO 31000



Nota: Tomado de *ISO 31000:2018*, por Organización Internacional de Estandarización, 2018, ISO (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es).

Para una mejor comprensión de cada uno de los elementos del Marco de Referencia se presenta a continuación la Tabla 8 con sus definiciones.

Tabla 8

Definición Elementos del Marco de Referencia de la Norma ISO 31000

Elemento	Definición
Liderazgo y Compromiso	"Es necesaria el interés de la alta dirección y gobernanza de la organización o departamento pertinente al que se aplicará la gestión de riesgos, con la finalidad de procurar la correcta integración de las actividades y funciones dispuestas para el análisis y gestión de riesgos."[a]
Integración	"La integración hace referencia a la fusión de las necesidades y cultura organizacional, con los objetivos propuestos para el Plan de Gestión de Riesgos."[a]
Diseño	"La gestión de riesgos debe tener un diseño adaptado a los procesos organizacionales de la institución."[a]
Implementación	"Para la implementación es necesaria la gestión del riesgo tomando en cuenta un plan que aborde plazos y recursos."[a]
Valoración	"La valoración se puede realizar mediante la comparación del desempeño actual con el plan estratégico a largo plazo, también se puede realizar con una evaluación al nivel madurez en la gestión de riesgos de la organización."[a]
Mejora	"El marco de referencia también debe incluir la Mejora; a consecuencia de grandes cambios organizacionales, de productos, de personal, de estructura, es necesaria la actividad de revisión y seguimiento para asegurar una adaptación continua."[b]

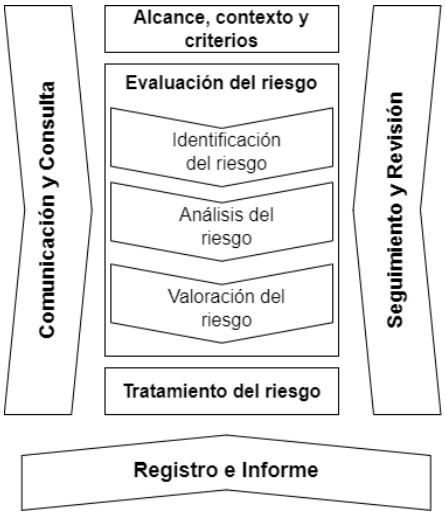
Nota: La tabla presenta las definiciones del marco de referencia de la norma ISO 31000 según dos autores, [a]Organización Internacional de Estandarización (2018). [b]Bonet et al. (2019, p.100). Elaboración propia.

1.3.3. Proceso

El proceso de gestión de riesgo abarca diversos tópicos: establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, comunicación y consulta, seguimiento, revisión y aplicación de políticas. La Figura 15 represente este proceso.

Figura 15

Proceso de la Norma ISO 31000



Nota: Tomado de *ISO 31000:2018*, por Organización Internacional de Estandarización, 2018, ISO (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es).

Comunicación y Consulta

En la primera fase del proceso, la Comunicación y consulta se basa en el proceso de asistencia a las partes interesadas para que se pueda comprender la definición del riesgo y las decisiones a tomar frente a este. Además de poder recaudar la mayor cantidad de información sobre la organización y las partes interesadas para desarrollar una correcta gestión del riesgo (Organización Internacional de Estandarización, 2018).

Alcance, contexto y criterios

Debido a que la gestión de riesgos puede ser aplicable a distintos campos, es importante definir su alcance. Parviainen et al. (2021) definen esta actividad como el establecimiento de los objetivos y decisiones que se deben tomar, especificando el marco temporal y la zona geográfica, alcance del estudio, las fuentes de riesgos, la naturaleza y tipo de consecuencias potenciales, así como, el tipo de método de evaluación a utilizar.

Evaluación del riesgo

Comprende los pasos de identificación, análisis y valoración del riesgo. Este proceso se lo debe llevar de manera sistemática, iterativa y colaborativa con ayuda de las partes interesadas (Organización Internacional de Estandarización, 2018).

El detalle de este análisis dependerá de la cantidad de información recaudada, recursos provistos, confiabilidad de la alta dirección y del alcance propuesto.

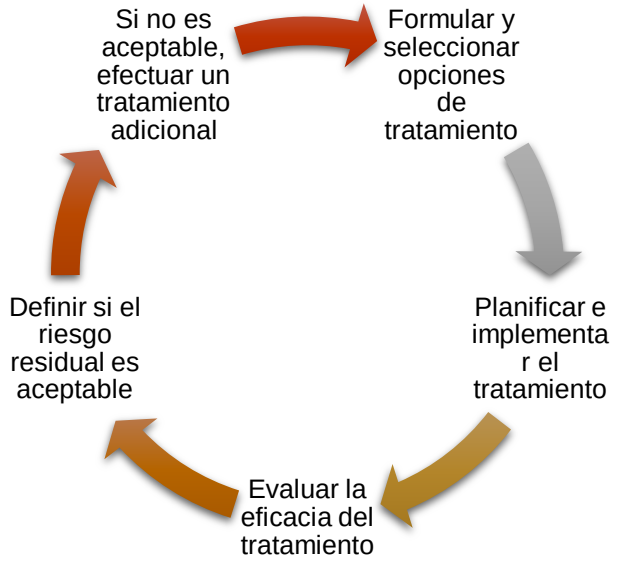
Dali & Lajtha (2012) afirman que, la valoración del riesgo se la puede desarrollar mediante la comparación de los resultados del análisis con los criterios de estos. Junto con esta valoración se puede mejorar la toma de decisiones para el futuro tratamiento.

Tratamiento del riesgo

La esencia del tratamiento del riesgo es minimizar su impacto, para lograr este objetivo, se lleva a cabo una serie de actividades iterativas presentadas en la Figura 16.

Figura 16

Proceso Tratamiento de Riesgos según la Norma ISO 31000



Nota: Elaboración propia a partir de *ISO 31000:2018*, por Organización Internacional de Estandarización, 2018, ISO (https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es).

Seguimiento y revisión

El seguimiento y revisión es una actividad necesaria en todas las etapas del proceso de la gestión del riesgo para poder garantizar una óptima calidad en los resultados esperados.

Guzmán (2019) en su trabajo científico presenta a la etapa de Seguimiento y revisión como una retroalimentación de todo el proceso de gestión de riesgos, reafirma lo expuesto por Parviainen et al. (2021) en su artículo como la confirmación de que, el proceso de gestión de riesgos está funcionando, para así determinar en qué partes se requiere hacer modificaciones.

Registro e informe

Una vez concluido el proceso de gestión de riesgos es necesaria la documentación apropiada, mediante registros e informes, con el fin de presentar los resultados obtenidos, comunicación de los resultados, costos, tiempos, sugerencias para mejorar la toma de decisiones y la rendición de cuentas (Organización Internacional de Estandarización, 2018).

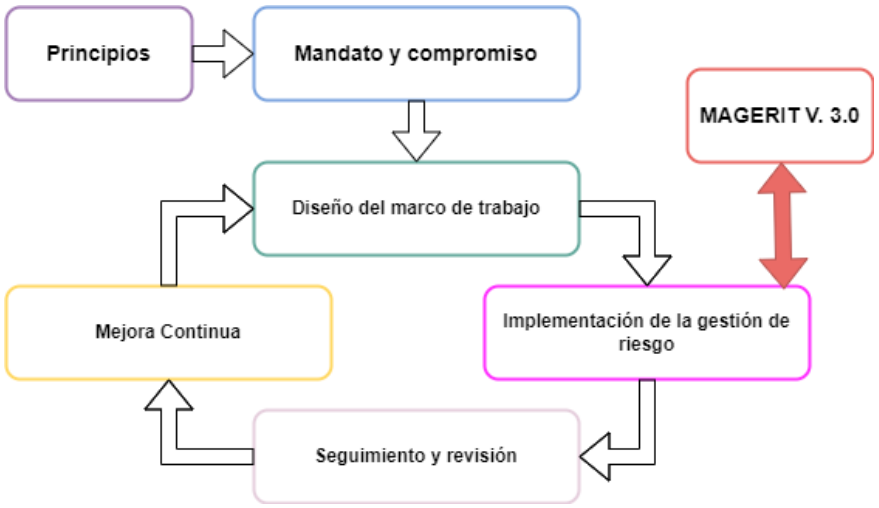
1.4. Metodología para la Gestión de Riesgos MAGERIT versión 3

"MAGERIT permite conocer el estado de la seguridad de los sistemas de información desde el punto de vista de los activos, para de esta manera proporcionar una profunda mitigación de las vulnerabilidades" (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

En la Figura 17 se presenta la relación directa que tiene la metodología MAGERIT con la Norma ISO 31000 en su apartado de Proceso "Evaluación y Tratamiento de Riesgos".

Figura 17

Relación directa de la metodología MAGERIT con la Norma ISO 31000

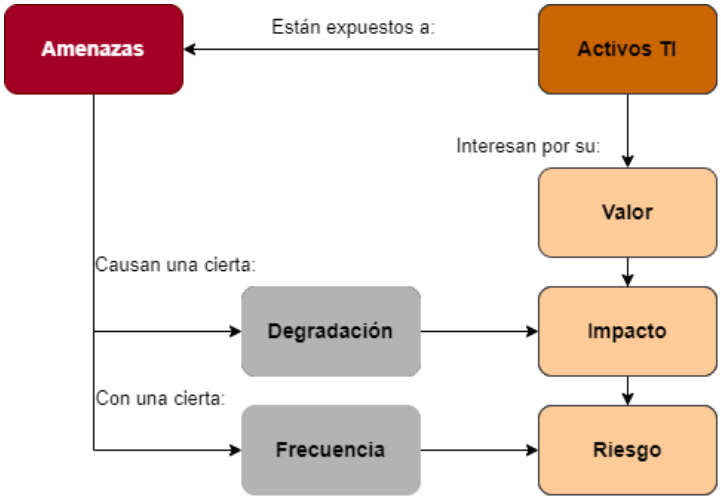


Nota: Elaboración propia a partir de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 Método* (p.7), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

Dentro del modelo que trabaja la metodología MAGERIT, se encuentran todos los conceptos relacionados con la Gestión de Riesgos, esto se aprecia en la Figura 18.

Figura 18

Modelo bajo el que trabaja la Metodología MAGERIT versión 3

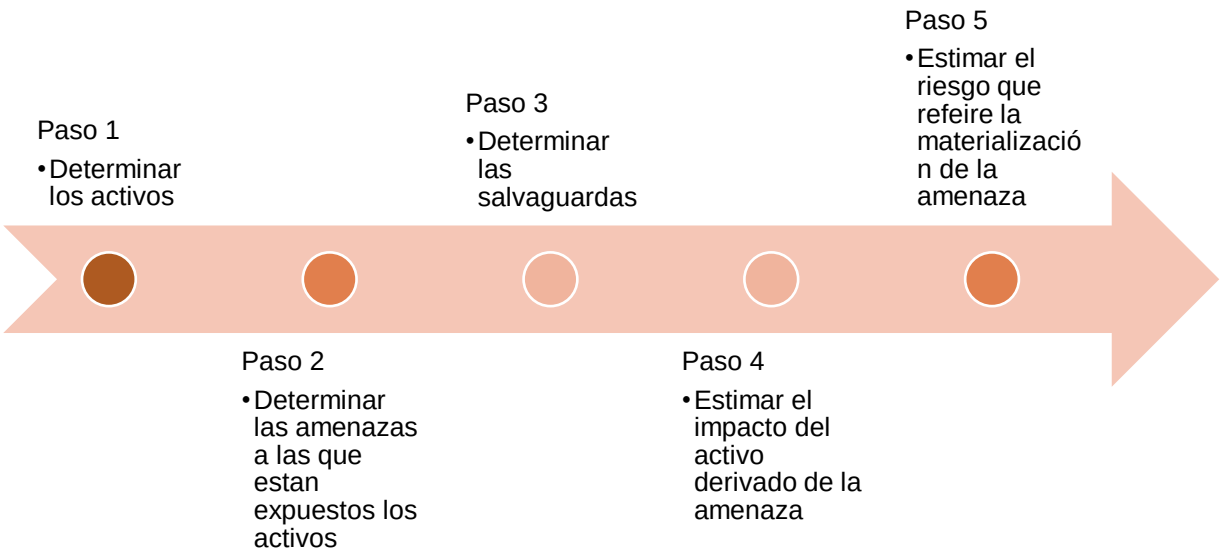


Nota: Tomado de "Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica" (p.27), por J. Ruge, *Universidad Piloto de Colombia*.

Bajo este modelo se definen cinco pasos que propone la metodología MAGERIT para el análisis de riesgos. Se aprecia en la Figura 19.

Figura 19

Pasos de la Metodología MAGERIT



Nota: Tomado de "Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies" (p.32), por Garía & Moreta, 2018, 7th International Conference On Software Process Improvement (CIMPS).

1.4.1. Método

El primer Libro desarrollado por la Dirección General de Modernización Administrativa de España incluye varios apartados importantes para la Gestión de Riesgos con la Metodología MAGERIT, el más relevante es el Método de análisis de riesgos; este capítulo describe una serie de pasos para el cumplimiento de la metodología MAGERIT, que son:

I. Identificación de activos.

II. Dependencia entre activos.

III. Valoración de activos.

IV. Identificación de amenazas.

V. Valoración de amenazas.

VI. Determinación del impacto potencial.

VII. Determinación del riesgo potencial.

VIII. Identificación de salvaguardas.

IX. Valoración de salvaguardas.

X. Estimación del impacto residual.

XI. Estimación del riesgo residual.

1.4.2. Catálogo de elementos

Su principal objetivo es poder brindar a las personas encargadas de la gestión de riesgos una base de datos con elementos estándar, para de esta manera llegar tener resultados mucho más homogéneos entre análisis. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

El libro consta de una lista de secciones presentadas en la Tabla 9.

Tabla 9

Contenido de las Secciones presentes en el Catálogo de Elementos de MAGERIT

Sección	Contenido
Tipos de activos	Estos activos representan en su mayoría la información y los servicios que maneja la organización.
Dimensiones de valoración	Las dimensiones de valoración permiten conocer la importancia de un activo para la organización, para

	posteriormente poder brindarle las correctas medidas de protección en base a su nivel de valoración.
Amenazas	Se refiere a las afectaciones negativas y perjudiciales que les pueden suceder a los activos.
Salvaguardas	Se refiere a las actividades o mecanismos que ayudan a reducir las probabilidades de amenazas o limitar el daño originado por el riesgo presente. Las salvaguardas dependerán de: el tipo de activo, las amenazas presentes y la dimensión de valoración.

Nota: Elaboración propia a partir de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 Catálogo de Elementos* (pp. 7-58), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

1.4.3. Guía Técnica

Brinda diversas técnicas que son comúnmente aplicadas en el análisis y gestión de riesgos. Estas son:

- Técnicas específicas
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas

CAPÍTULO 2

Plan de Gestión de Riesgos

2.1. Metodología de investigación

2.1.1. Tipo de investigación

Investigación Descriptiva: se realizó a través de la observación directa y recolección de información, enfocándose principalmente en el análisis de la información existente para llegar a establecer la situación actual de los laboratorios de informática FICA-UTN.

2.1.2. Métodos de investigación

Deductivo: se inició en el problema general que es el bajo nivel de identificación, análisis y gestión de riesgos en los laboratorios de informática FICA-UTN, para de esta manera, analizar sus distintos elementos como activos, amenazas y salvaguardas.

Analítico: al hacer el análisis de los riesgos se pudo determinar las salvaguardas necesarias a ser implementadas, como meta la de minimizar las afectaciones negativas por la materialización de amenazas.

2.2. Técnicas de investigación

2.2.1. Técnicas de recolección de información

Para el Desarrollo de este estudio se utilizarán varias técnicas para la recolección de información, tales como: revisión de documentos, encuestas, entrevistas y observación de campo.

- **Revisión de documentos:** se solicitó distintos documentos considerados importantes en los procesos internos relacionados a los riegos dentro de los laboratorios de informática FICA-UTN. Los documentos revisados serán el

  fichaje de inventario de los distintos bienes fijos, manual de procedimientos de los laboratorios, reglamentos internos, plan de mantenimiento y plan de contingencia.

- **Encuesta:** Se desarrolló diferentes tipos de encuestas destinadas a dos grupos de personas.

- ✓ La primera encuesta dirigida a los usuarios de los laboratorios de informática FICA-UTN, con finalidad recabar información sobre la conciencia que tienen los mismos en relación con los riesgos presentados durante el uso de los laboratorios. Las preguntas de la encuesta se encuentran en el Anexo A.
- ✓ Las otras dos encuestas serán de tipo “Encuestas con el método Delphi” de validación a expertos para evaluar la efectividad del Plan de Gestión de Riesgos desarrollados en este estudio. Esta técnica fue escogida debido a que los expertos tienen la capacidad de tener un juicio aceptable en el tema de Gestión de Riesgos de TI. Las preguntas de las encuestas se encuentran en el Anexo O y en el Anexo P, respectivamente.

- **Entrevista:** Se desarrolló dos entrevistas a las personas relacionadas con la administración del área de tecnología de los laboratorios de informática FICA-UTN, la primera entrevista realizada a la Jefe de Laboratorios de Informática FICA-UTN, que se desarrolló con un enfoque dirigido al proceso administrativo, operacional, y de gestión dentro de los laboratorios, la segunda entrevista fue realizada al Director de la Dirección de Desarrollo Tecnológico e Informático (DDTI) UTN con preguntas altamente relacionadas con el ámbito de infraestructura tecnológica manejada en la Universidad. Las preguntas de las entrevistas se encuentran en el Anexo B y Anexo C respectivamente.
- **Observación de campo:** La técnica de observación de campo fue utilizada para recolectar información de primera mano acerca de los activos pertenecientes a los laboratorios de informática FICA-UTN, además de, identificar posibles incidentes, peligros y circunstancias negativas que puedan afectar negativamente a la organización.

  Esta técnica se desarrolló por un periodo de siete días, en los que se realizó distintas visitas presenciales a las instalaciones físicas de los laboratorios.

2.2.2. Población y muestra

Para el desarrollo de esta encuesta se determinó como primer paso, definir el tamaño de la muestra, pues esta representará a la población total de estudio. Para el cálculo de este tamaño de la población se consideró 3 factores esenciales.

- Población o Universo
- Margen de error
- Nivel de Confianza

El tamaño de la muestra se lo tomó de manera representativa, pues todas las personas de la población pueden tener la oportunidad de participar en los resultados de la encuesta.

Al ser una población finita, se utilizó la siguiente fórmula para determinar el tamaño de la muestra:

$$n = \frac{N \times Z^2 \times p \times q}{e^2 \times (N-1) + Z^2 \times p \times q}$$

En la cual:

n= Tamaño de muestra buscado

N= Tamaño de la Población o Universo

Z= Parámetro estadístico que depende del Nivel de Confianza (NC)

e= Error de estimación máximo aceptado

p= Probabilidad de que ocurra el evento estudiado (éxito)

q= Probabilidad de que no ocurra el evento estudiado (fracaso) = (1-p)

Para el presente caso de estudio se determinó como Población o Universo al número total de estudiantes que hacen uso de los laboratorios de informática FICA-UTN en el periodo académico actual octubre 2022-febrero 2023. En la Tabla 10 se muestra como a la Población se la dividió de tal manera que se pueda obtener el número representativo de estudiantes que hacen uso de los laboratorios de informática FICA-UTN, seccionados carrera.

Tabla 10

División de la Población finita de estudiantes usuarios de los laboratorios de informática FICA-UTN por carreras.

	CARRERA	ESTUDIANTES
1	Software	249
2	Telecomunicaciones	186
3	Mecatrónica	75
4	Industrial	141
5	Electricidad	18
6	Automotriz	88

	TOTAL	**757**

Nota: Elaboración propia.

Para calcular el tamaño de la muestra se optó por utilizar un Nivel de Confianza del 95% que equivale a 1.96, al igual que un máximo de estimación de error del 10%. Aplicando la fórmula de la muestra para población finita, el resultado fue el presentado en la Tabla 11.

Tabla 11

Muestra calculada para los laboratorios de informática FICA-UTN

Nivel de confianza	Z	95%	1.96
Probabilidad de ocurrencia	p	50%	0.5
Probabilidad de no ocurrencia	q	50%	0.5
Error de muestreo	e	10%	0.1
Tamaño de la población		N	757
Tamaño de la muestra		n	**85**

Nota: Elaboración propia.

Aplicando la ecuación para obtener la muestra de una población finita, se obtuvo un resultado de 85 sujetos; para poder hacer la selección de los sujetos a los que se aplicó la encuesta, se utilizó la tabla de división por carreras y dependiendo de la frecuencia se obtuvo el número de encuestas que se debió realizar por carrera. El resultado se presenta en la Tabla 12.

Tabla 12

Distribución de muestra de estudiantes usuarios de los laboratorios de informática FICA-UTN por carrera

	CARRERA	**ESTUDIANTES**	**f**	**n**
1	Software	249	33%	28
2	Telecomunicaciones	186	25%	21
3	Mecatrónica	75	10%	8
4	Industrial	141	19%	16
5	Electricidad	18	2%	2
6	Automotriz	88	12%	10
	TOTAL	757	100%	**85**

Nota: Elaboración propia.

Las preguntas que componen la encuesta se encuentran en el Anexo A.

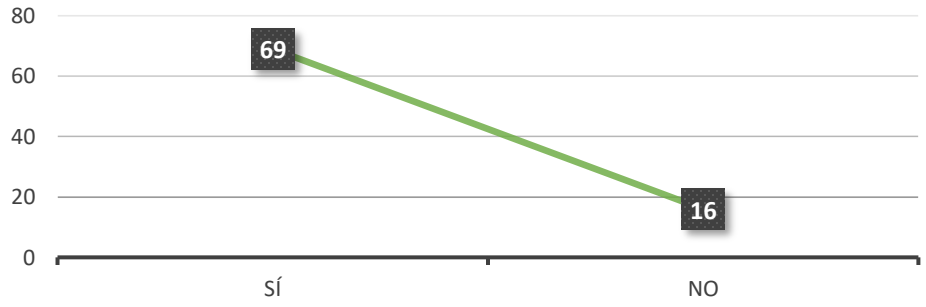
2.2.3. Análisis de resultados de la encuesta

La aplicación de la encuesta se la realizó con el método de Muestreo Aleatorio Simple, en el cual se escogió de las distintas carreras de la Facultad a estudiantes que hagan uso de los laboratorios de informática FICA-UTN, los resultados obtenidos fueron los siguientes:

1. ¿Utiliza usted los equipos (computadores) disponibles en los laboratorios de informática FICA?

Figura 20

Resultados primera pregunta encuesta conciencia de gestión de riesgos



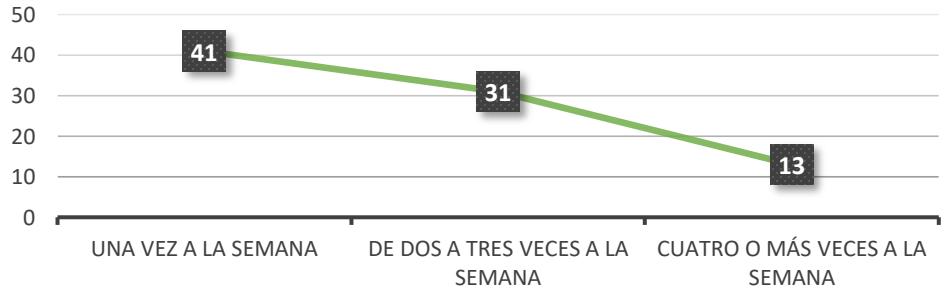
Nota: Elaboración propia.

En los resultados obtenidos de la primera pregunta, se puede observar que el 81% equivalente a 69 de los encuestados hacen uso de los laboratorios de informática FICA, ya sea dentro de horas académicas o de horas autónomas. Mientras que el 19% referente a 16 encuestados no hace uso actualmente de los laboratorios.

2. ¿Con qué frecuencia usted utiliza los laboratorios de Informática FICA?

Figura 21

Resultados segunda pregunta encuesta conciencia de gestión de riesgos



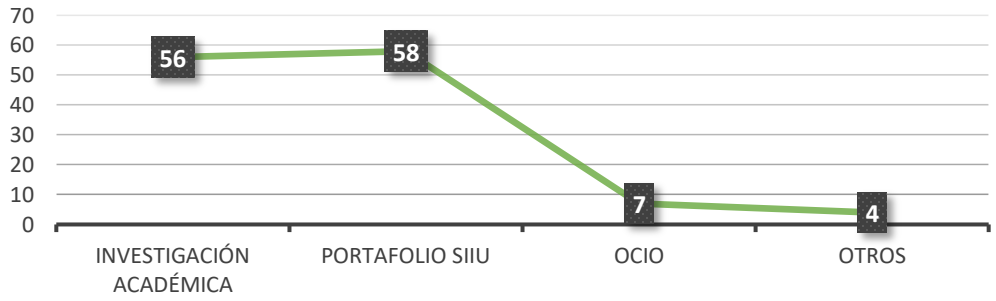
Nota: Elaboración propia.

Los resultados arrojados por la segunda preguntan son, el 48% equivalente a 41 encuestados hace uso de los laboratorios de informática FICA por lo menos una vez a la semana, el 37% referente a 31 encuestados utiliza los laboratorios de informática de dos a tres veces por semana, y el 13% que representa 13 encuestados hace uso de los laboratorios cuatro veces o más por semana. Se concluye que los resultados obtenidos para esta pregunta varían dependiendo de la carrera a la que pertenezcan los encuestados.

3. ¿Qué actividades realiza en los equipos?

Figura 22

Resultados tercera pregunta encuesta conciencia de gestión de riesgos



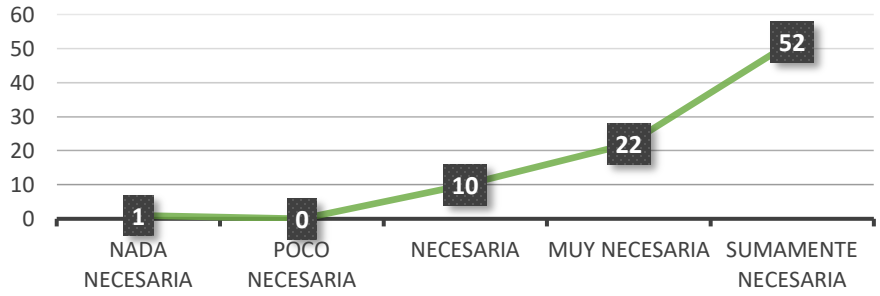
Nota: Elaboración propia.

En los resultados obtenidos por la tercera pregunta se pueden ver las siguientes observaciones, el 46% equivalente a 58 de los encuestados utilizan los equipos (computadores) disponibles en los laboratorios de informática para actividades relacionadas con el servicio de Portafolio Académico SIIU en el cual pueden desarrollar distintas actividades como subir tareas al aula virtual, descargar material necesario para las horas académicas, realizar evaluaciones en línea, realizar la evaluación docente, entre otros. El 45% equivalente a 56 de los encuestados utiliza los equipos (computadores) para la Investigación académica, esta actividad toma en cuenta distintos enfoques como: la investigación científica, desarrollo de tareas, desarrollo de talleres, etc. Inclusive en los resultados se observa que el 6% referente a 7 de los encuestados utiliza los equipos para actividades de ocio y relajación cuando tienen tiempo libre, mientras que el 3% equivalente a 4 encuestados desarrolla otras actividades como programas multimedia, simulación, software; estas actividades tienen cabida en el apartado de Investigación Académica, por lo que el porcentaje inicial de esta actividad aumentaría a 48%, siendo esta la actividad más desarrollada dentro de los laboratorios de informática FICA-UTN.

4. En una escala del 1 al 5 ¿qué tan necesarios son los equipos en los laboratorios de informática FICA?

Figura 23

Resultados cuarta pregunta encuesta conciencia de gestión de riesgos



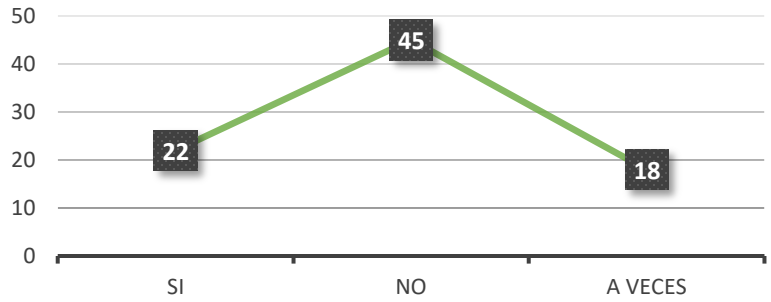
Nota: Elaboración propia.

De los resultados obtenidos en la cuarta pregunta se observa que el 1% equivalente a 1 encuestado considera la existencia de los equipos en los laboratorios de informática FICA-UTN nada necesaria, ningún encuestado considera la existencia de los equipos como poco necesaria, el 12% equivalente a 10 encuestados considera necesaria la existencia de los equipos, el 26% equivalente a 22 encuestados considera muy necesaria la existencia de los equipos y el 61% equivalente a 52 encuestados considera sumamente necesaria la existencia de los equipos en los laboratorios de informática FICA-UTN. Con estos resultados se puede inferir que esta pregunta está altamente relacionada con la pregunta dos, ya que dependiendo las necesidades de la carrera se va a ver afectado la percepción de necesidad de los laboratorios, por ejemplo, la carrera de Software considerará Sumamente necesaria la existencia de los laboratorios porque la mayoría de las asignaturas requieren el uso de equipos de cómputo.

5. ¿Almacena su información en los equipos del laboratorio de Informática FICA?

Figura 24

Resultados quinta pregunta encuesta conciencia de gestión de riesgos



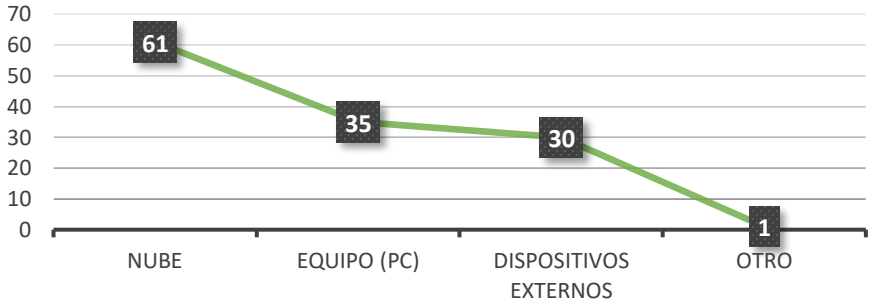
Nota: Elaboración propia.

Los resultados obtenidos en la quinta pregunta fueron, el 26% referente a 22 de los encuestados almacenan su información en los equipos físicos de los laboratorios de informática FICA-UTN, el 53% equivalente a 45 de los encuestados no almacena su información en los equipos físicos, y el 21% que se refiere a 18 d ellos encuestados a veces almacena su información en los equipos físicos. Esto refleja que los estudiantes que “Sí” y “A veces” almacenan su información (47%) no conocen acerca de las políticas de mantenimiento de los equipos dentro de los laboratorios, ya que cuando se realizan estos, se elimina la información de los estudiantes almacenada en ellos.

6. ¿Cuándo hace uso de los equipos del laboratorio de Informática FICA ¿en qué lugar almacena su información?

Figura 25

Resultados sexta pregunta encuesta conciencia de gestión de riesgos



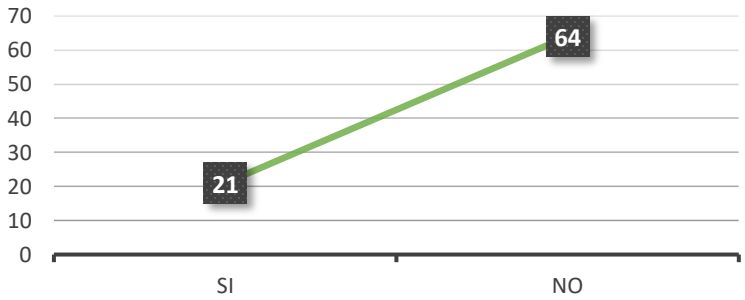
Nota: Elaboración propia.

Los resultados obtenidos de la sexta pregunta son, el 48% equivalente a 61 de los encuestados almacenan su información en servicios de Nube como OneDrive, Google Drive, etc., el 27% referente a 35 encuestados almacena su información en los discos duros internos de los equipos de los laboratorios de informática, el 24% que equivale a 30 de los encuestados almacena su información en Dispositivos de almacenamiento externos tales como, Memorias Flash, Disco duro externo, etc., y el 1% equivalente a 1 encuestado almacena su información en otros lugares. Con estos resultados se observa que la mayoría de encuestados utiliza servicios que garantizan la seguridad de la información como son: la Nube y Almacenamiento externo a los equipos de informática.

7. Si la respuesta a la pregunta anterior fue "Equipo (PC)" ¿cuándo ha vuelto a usar el mismo equipo, ¿su información guardada permanecía vigente?

Figura 26

Resultados séptima pregunta encuesta conciencia de gestión de riesgos



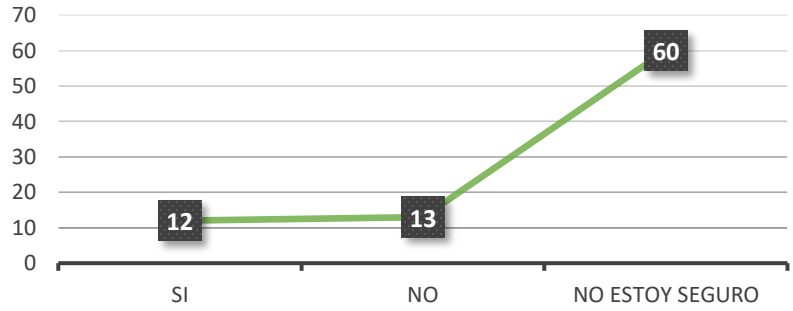
Nota: Elaboración propia.

Los encuestados que escogieron "Equipo (PC)" como medio de almacenamiento respondieron la séptima pregunta y se obtuvieron los siguientes resultados. El 25% equivalente a 21 encuestados, sí encontraron su información vigente en los equipos de informática; pero el 75% referente a 64 de los encuestados no encontraron su información en los equipos de informática, esto debido al desconocimiento por parte de los estudiantes a los protocolos de limpieza de información de los equipos de los laboratorios durante su proceso de mantenimiento.

8. ¿El equipo que utiliza en los laboratorios de informática FICA, cuenta con antivirus?

Figura 27

Resultados octava pregunta encuesta conciencia de gestión de riesgos



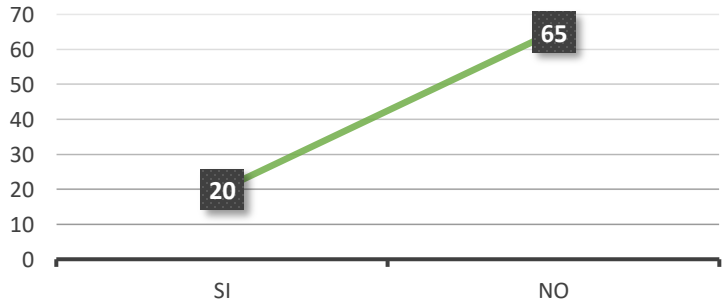
Nota: Elaboración propia.

Los resultados obtenidos para la octava pregunta fueron los siguientes, el 14% equivalente a 12 encuestados aseguran que los equipos dentro de los laboratorios de informática cuentan con antivirus, el 15% equivalente a 13 encuestados afirman que los equipos no cuentan con antivirus, mientras que el 71% que equivale a 60 de los encuestados no están seguros. Estos resultados nos permiten concluir que los usuarios de los laboratorios de informática FICA-UTN no conocen acerca de las seguridades que se ofrecen al hacer uso de los equipos.

9. ¿Conoce usted los riesgos presentes en los laboratorios de informática FICA?

Figura 28

Resultados novena pregunta encuesta conciencia de gestión de riesgos



Nota: Elaboración propia.

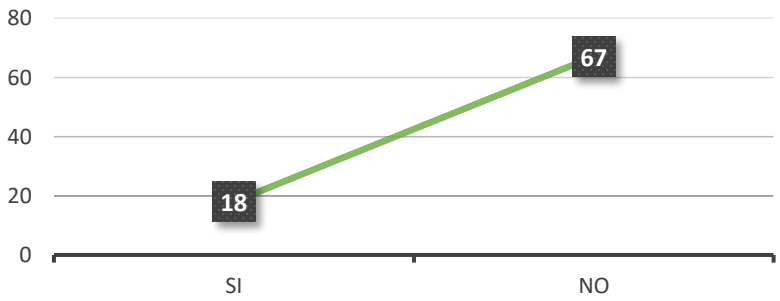
En la novena pregunta se obtuvo resultados de la siguiente manera, el 24% que equivale a 20 de los encuestados si consideran a los riesgos que presenta el uso de los equipos en los laboratorios de informática FICA-UTN, por otro lado, el 76% equivalente a 65 de los encuestados

no consideran los riesgos presentes en el uso de los laboratorios. Estos resultados son preocupantes porque los estudiantes no sabrían cómo actuar frente a la materialización de alguno de los tantos riesgos que existe. Los resultados también permiten asegurar que no existe un buen nivel de conciencia sobre los riesgos por parte de los usuarios de los laboratorios frente a los riesgos tecnológicos.

10. ¿Conoce usted las políticas ante daño o hurto de equipos de los laboratorios de informática FICA?

Figura 29

Resultados décima pregunta encuesta conciencia de gestión de riesgos



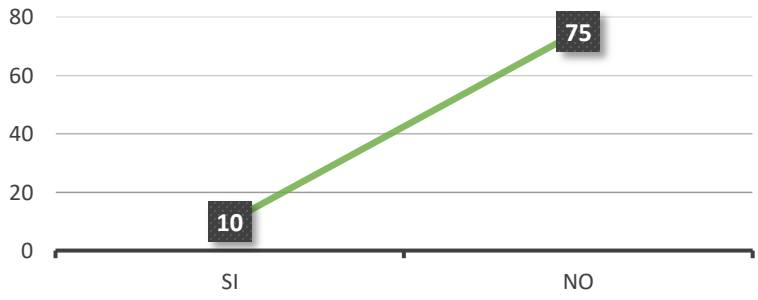
Nota: Elaboración propia.

Los resultados arrojados por la décima pregunta son los siguientes, el 21% referente a 18 de los encuestados asegura conocer las políticas a seguir ante cualquier tipo de daño o hurto de los componentes de los equipos pertenecientes a los laboratorios de informática FICA-UTN, mientras que el 79% equivalente a 67 de los encuestados no conocen dichas políticas.

11. ¿Conoce uste el procedimiento a seguir en caso incendios o fallas eléctricas dentro de los laboratorios de informática FICA?

Figura 30

Resultados onceava pregunta encuesta conciencia de gestión de riesgos



Nota: Elaboración propia.

Los resultados arrojados por la décima pregunta son los siguientes, el 12% referente a 10 de los encuestados asegura conocer las políticas a seguir ante riesgos como incendios o fallas eléctricas que puedan afectar a los equipos pertenecientes a los laboratorios de informática FICA-UTN, mientras que el 88% equivalente a 75 de los encuestados no conocen dichas políticas.

2.3. Nivel de Madurez de Gestión de Riesgos

Para definir el nivel de Madurez en la Gestión de Riesgos de los laboratorios de informática FICA-UTN, se utilizó el Risk Maturity Model (RMM).

El RMM fue desarrollado por la Sociedad de Gestión de Riesgos (RIMS) en 2006 y actualizado por la Empresa Logic Manager en 2020. Este cubre las normas ISO 31000, OCEG Red Book, BS 31100, COSO, FERMA, y Colvencia II (Comunidad de Gestión de Riesgos, 2020).

Este modelo comprende los indicadores clave y las actividades correspondientes a un plan de Gestión de Riesgos en las organizaciones.

Al desarrollar la autoevaluación se obtendrá una puntuación referente al nivel de gestión de riesgos; estos pueden ir desde la etapa más temprana Ad-Hoc (Nivel 1) a la etapa más avanzada Liderazgo (Nivel 5).

La tabla 13 muestra como la Comunidad de Gestión de Riesgos (2020) define los cinco niveles.

Tabla 13

Definición de los niveles de madurez en gestión de riesgos

Nivel de Madurez en Gestión de Riesgos	Definición
Ad Hoc	La organización posee conciencia mínima o nula sobre la gestión de riesgos, en caso de existir, estos procesos son muy rudimentarios y ambiguos, tratan los riesgos de manera ajena a los procesos internos de la organización.
Inicial	La organización cuenta con un proceso para la gestión de riesgos, pero este es aplicado de manera inconstante, por lo que cumple con lo mínimo para la mitigación de perdidas.
Repetible	La organización ya comienza a implementar constantemente los procesos para la gestión de riesgos. No se mantiene la buena comunicación entre los encargados de la gestión de riesgos y la alta dirección.

Gestionado	La organización procura tomar un estándar para el proceso de gestión de riesgos, se desarrollan prácticas de concientización sobre la importancia de estos procesos a todos los miembros de la organización. Se empieza a pensar en un proceso de mejora continua.
Liderazgo	El proceso de gestión de riesgos es aceptado como un proceso integral de la organización, se tiene presente todas sus actividades y se tiene como punto clave la mejora continua mediante actividades de concientización y comunicación.

Nota: Elaboración propia.

Para determinar en qué nivel se encuentra una organización, el RMM establece tres dimensiones de evaluación, estas son:

- Efectividad: Mide si las actividades son capaces de producir los resultados deseados.
- Proactividad: Mide la naturaleza de la gestión de riesgos.
- Cobertura: Mide la amplitud y profundidad de la gestión de riesgos.

Estas dimensiones son evaluadas en siete factores establecidos por el RMM. Estos son:

- Adopción del proceso basado en la Gestión de Riesgo.
- Descubrimiento del riesgo.
- Gestión de procesos de Gestión de Riesgo.
- Gestión del Apetito de Riesgo.
- Disciplina de causa raíz.
- Resiliencia y sostenibilidad empresarial.
- Gestión del rendimiento.

Cada uno de estos factores cuenta con distintos requerimientos y tareas o formas de brindar una calificación cuantitativa de 0 a 10 de las tres dimensiones anteriormente expuestas. Todos los factores, requerimiento y tareas se encuentran en el Anexo D.

Con ayuda de la información recolectada por las entrevistas realizadas a las dos personas relevantes en el campo tecnológico del estudio presente, la Jefe de Laboratorios de informática FICA-UTN, y el Director de la Dirección de Desarrollo Tecnológico e Informático (DDTI) se pudo establecer una valoración a dichas dimensiones de evaluación necesarias para el cálculo del nivel de madurez de gestión de riesgos con el RMM.

Las preguntas referentes a la encuesta realizada a la Jefe de Laboratorios de Informática FICA-UTN se encuentra en el Anexo B, mientras que las preguntas referentes a la encuesta realizada al director del DDT se encuentran en el Anexo C.

Los resultados obtenidos se encuentran en la Tabla 14.

Tabla 14

Resultados Risk Maturity Model aplicado a los laboratorios de informática FICA-UTN

Factor	Requerimiento	Efectividad	Proactividad	Cobertura
Adopción del proceso basado en ERM	Definición de procesos comerciales y propiedad del riesgo	1	1	3
	Propietario del proceso de soporte y de primera línea Participar	0	0	0
	Visión previsora de gestión de riesgos	0	0	0
	Soporte ejecutivo de ERM	2	1	0
Descubrir el riesgo	Propiedad del riesgo por área de negocio	3	3	1
	Indicadores y Medidas de Riesgo Formalizados	0	0	0
	Informes de seguimiento	0	0	0
	Eventos adversos como oportunidades	0	0	0
Gestión de procesos ERM	Supervisión del programa ERM	2	1	2
	Pasos del proceso ERM	0	0	0
	Cultura de Riesgo, Rendición de Cuentas y Comunicación	0	0	0
	Informes de gestión de riesgos	0	0	0
	Repetibilidad y Escalabilidad	2	2	3
Gestión del apetito de riesgo	Vista de la cartera de riesgos	1	3	3
	Compensaciones de riesgo-recompensa	3	1	1
Disciplina de causa raíz	Consideración de la causa raíz	1	3	3
	Recopilación de información sobre riesgos y oportunidades	3	3	0

	Clasificación de la información	0	2	2
	Dependencias y Consecuencias	1	1	0
Resiliencia y sostenibilidad empresarial	Planificación basada en riesgos	0	0	0
	Comprender las consecuencias	3	2	0
	Resiliencia y planificación operativa	0	0	0
Gestión del rendimiento	Comunicación de metas	7	6	4
	Información y planificación de ERM	0	0	0
	Objetivos y actividades del proceso de ERM	0	0	0
TOTAL		**29**	**29**	**22**

Nota: Elaboración propia.

Para determinar el nivel de madurez de gestión de riesgos es necesario sumar los resultados obtenidos en las tres dimensiones de evaluación, a continuación, según la Tabla 15 de niveles de gestión de riesgos, determinar en cuál se encuentran los laboratorios de informática FICA-UTN.

Tabla 15

Puntaje referente para la determinación de niveles de madurez de gestión de riesgos

Nivel	Desde	Hasta
Ad-Hoc	1	150
Inicial	151	300
Repetible	301	450
Gestionado	451	600
Liderazgo	601	750

Nota: Elaboración propia.

La suma de los tres valores de las dimensiones obtenidas para los laboratorios de informática FICA-UTN es de 80 puntos, por lo que según la Tabla 15, se encuentra en el nivel "Ad-Hoc" que es el nivel más bajo en cuanto a madurez de gestión de riesgos se refiere.

2.4. Plan de Gestión de Riesgos

El Plan de Gestión de Riesgos se realizó con apartados seleccionados de la estructura de informes para Procedimientos de Gestión de Riesgos para la Mejora Continua, desarrollado por la firma de Consultores Piffault, encargada de brindar asesoría remota para la gestión de riesgos. Estos apartados son:

1) Propósito
2) Alcance
3) Usuarios
4) Documentos de referencia
5) Proceso de Gestión del riesgo

El Proceso de Gestión del Riesgo consta de tres fases que responden a las recomendaciones dictadas por la Norma ISO 31000. Estas fases son:

- Fase 1 "Comunicación y consulta, Establecimiento del contexto": se desarrolla distintas actividades referentes al apartado de "Comunicación y Consulta" y

"Establecimiento de Contexto" de la Norma ISO 31000:2018 para una buena Gestión del Riesgo, entre estas se encuentran:

I. Principios: determinación de principios que rijan el comportamiento del Plan de Gestión de Riesgos.

II. Compromiso: determinación de las actividades facilitadas por el equipo de encargado de los laboratorios para una eficaz gestión del riesgo.

III. Contexto actual: planteamiento de la situación actual de los laboratorios, comprende elementos como: estructura organizacional, personal encargado, infraestructura física, infraestructura tecnológica, servicios, seguridad y control de acceso, incidentes pasados, contexto interno y externo.

Esta fase se llevó a cabo con ayuda de la técnica de observación de campo, visitas técnicas a los laboratorios de informática FICA-UTN, y con ayuda de entrevistas a la Jefe de Laboratorios y al Director del DDTI.

- Fase 2 "Evaluación y Tratamiento del Riesgo": se realiza todas las actividades pertenecientes al proceso de la metodología MAGERIT, estos son:

I. Identificación de activos: recopilación, análisis y sintetización de los bienes y servicios que generan valor a los laboratorios.

II. Identificación de dependencia entre activos: determinación de las relaciones que existe entre los activos y su posible propagación de daño.

III. Valoración de activos: asignación de un valor cuantitativo para cada activo en distintas dimensiones de valoración (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) referentes a la seguridad.

IV. Identificación de amenazas: recopilación y análisis de las amenazas que pueden afectar a cada uno de los activos identificados en los laboratorios.

V. Valoración de amenazas: asignación de valores cuantitativos a cada una de las posibles amenazas que pueden afectar a los activos en cada dimensión de valoración (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).

VI. Determinación del impacto potencial: cálculo del daño ocasionado en caso de materialización de una amenaza sobre un activo.

VII. Determinación del riesgo potencial: cálculo de la relación existente entre la probabilidad de ocurrencia de una amenaza y el impacto negativo que esta tendría sobre un activo.

VIII. Identificación de salvaguardas: determinación del tipo de medidas de reducción de los riesgos calculados y propuesta de tareas que pueden ser implantadas.

IX. Valoración de salvaguardas: asignación de un valor cuantitativo a cada una de las tareas propuestas y tipos de salvaguardas que pueden ser aplicados para minimizar el riesgo.

X. Estimación del impacto residual: simulación del cálculo del impacto residual asumiendo que las tareas de salvaguardas fueron aplicadas.

XI. Estimación del riesgo residual: simulación del cálculo de reducción del riesgo residual asumiendo que las tareas de salvaguardas fueron aplicadas.

Todas estas actividades se desarrollan con ayuda del software PILAR provisto por el Centro Nacional de Inteligencia Española.

- Fase 3 “Seguimiento y Revisión del riesgo”: se propone actividades de:

I. Monitoreo: propuesta de actividades para el seguimiento de incidentes ocurrido desde la implementación del Plan de Gestión de Riesgos.

II. Validación de la Gestión del Riesgo: propuesta de un método de validación de los resultados.

III. Mejora Continua: comprensión de la definición de la mejora continua en los Planes de Gestión de Riesgos.

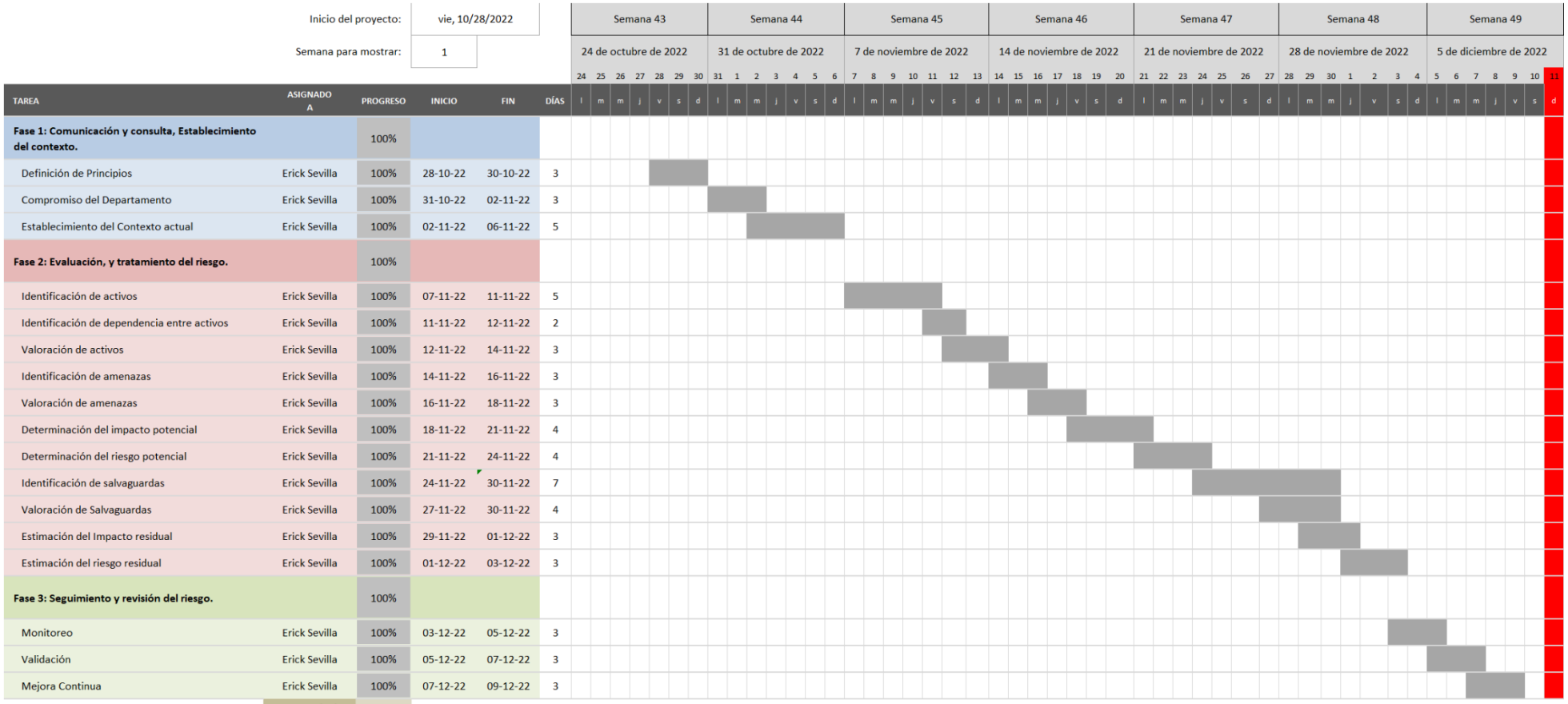
Estas tendrán parte en trabajos futuros con el fin de garantizar la buena Gestión del Riesgo.

Las fases y actividades fueron planificadas con ayuda de la herramienta “Diagrama de Gannt”, la cual es muy útil al momento de planificar actividades con duración de tiempo

establecidas, además, es muy efectivo en el control de progreso de las fases. La planificación se encuentra presente en la Tabla 16.

Tabla 16

Diagrama de Gannt para la Planificación del Plan de Gestión de Riesgos en los laboratorios de informática FICA-UTN



Inicio del proyecto: vie, 10/28/2022

Semana para mostrar: 1

TAREA	ASIGNADO A	PROGRESO	INICIO	FIN	DÍAS
Fase 1: Comunicación y consulta, Establecimiento del contexto.		100%			
Definición de Principios	Erick Sevilla	100%	28-10-22	30-10-22	3
Compromiso del Departamento	Erick Sevilla	100%	31-10-22	02-11-22	3
Establecimiento del Contexto actual	Erick Sevilla	100%	02-11-22	06-11-22	5
Fase 2: Evaluación, y tratamiento del riesgo.		100%			
Identificación de activos	Erick Sevilla	100%	07-11-22	11-11-22	5
Identificación de dependencia entre activos	Erick Sevilla	100%	11-11-22	12-11-22	2
Valoración de activos	Erick Sevilla	100%	12-11-22	14-11-22	3
Identificación de amenazas	Erick Sevilla	100%	14-11-22	16-11-22	3
Valoración de amenazas	Erick Sevilla	100%	16-11-22	18-11-22	3
Determinación del impacto potencial	Erick Sevilla	100%	18-11-22	21-11-22	4
Determinación del riesgo potencial	Erick Sevilla	100%	21-11-22	24-11-22	4
Identificación de salvaguardas	Erick Sevilla	100%	24-11-22	30-11-22	7
Valoración de Salvaguardas	Erick Sevilla	100%	27-11-22	30-11-22	4
Estimación del Impacto residual	Erick Sevilla	100%	29-11-22	01-12-22	3
Estimación del riesgo residual	Erick Sevilla	100%	01-12-22	03-12-22	3
Fase 3: Seguimiento y revisión del riesgo.		100%			
Monitoreo	Erick Sevilla	100%	03-12-22	05-12-22	3
Validación	Erick Sevilla	100%	05-12-22	07-12-22	3
Mejora Continua	Erick Sevilla	100%	07-12-22	09-12-22	3
	Porcentaje de avance	100%			

Nota: Elaboración propia

CAPÍTULO 3

Implementación

Propósito

El propósito de este informe es describir el proceso de Gestión de Riesgos establecido para los Laboratorios de Informática de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte (UTN), para aumentar la probabilidad de éxito en el logro de los siguientes objetivos:

- Fortalecer la capacidad de gestión de riesgos dentro de los laboratorios de informática FICA-UTN.
- Establecer el contexto actual de los laboratorios de informática FICA-UTN.
- Identificar los activos, amenazas, riesgos y salvaguardas dentro de los laboratorios de informática FICA-UTN.
- Proponer tareas a manera de salvaguardas para que, en caso de implantarlas, estas minimicen las pérdidas o efectos negativos causados por la materialización de riesgos.
- Redactar una propuesta de monitoreo del Plan de Gestión de Riesgos.

Alcance

Este procedimiento se aplica para realizar El Plan de Gestión de Riesgos con la Metodología MAGERIT en su versión 3, que tiene sus bases en la Norma Internacional ISO 31000:2018 para la gestión de riesgos. El proceso de Análisis y Gestión de Riesgos será desarrollado con apoyo del software Procedimiento Informático Lógico para el Análisis de Riesgos (PILAR). La identificación de activos se efectuará de manera general con el método de observación y con los documentos de inventario que cuentan los laboratorios. Las salvaguardas serán consideradas guías debido a que el caso de estudio es parte de una Institución Pública que está sometida a regulaciones financieras, de personal y de tiempo. Motivo por el cual, estas deberán ser analizadas y evaluadas en un futuro por parte de los encargados de los laboratorios para decidir implementarlas o modificarlas según sea necesario.

Usuarios

Los usuarios de este procedimiento son todo el personal que realiza labores para los Laboratorios de Informática FICA-UTN dentro del alcance definido.

3.1. Fase 1: Comunicación y consulta, Establecimiento del contexto

3.1.1. Comunicación y consulta

La comunicación y consulta es una parte esencial en la gestión del riesgo, ya que permite el intercambio de información entre las partes interesadas. Gracias a este proceso se puede tener presente que actividades tomar frente a los riesgos, además mejora la toma de decisiones y comprensión del riesgo.

Respecto a los riesgos tecnológicos presentes en los laboratorios de Informática FICA-UTN se identificaron como partes interesadas a los siguientes individuos.

- Director de la Dirección de Desarrollo Tecnológico e Informático UTN.
- Jefe de Laboratorios de Informática FICA-UTN.
- Asistentes de Laboratorios de Informática FICA-UTN.
- Tesista autor del Plan de Gestión de Riesgos.

El proceso de comunicación y consulta se lo desarrolló con ayuda de herramientas de recolección de información como entrevistas y encuestas. Estas se llevaron a cabo de manera presencial y virtual.

La comunicación y consulta permitió establecer 8 principios dictados en la Norma ISO 31000:2018 para el Plan de Gestión de Riesgos, estos son los siguientes:

Integrada

El departamento de Laboratorios de Informática FICA-UTN no dejará aislada al proceso de gestión de riesgos de las demás actividades integrales del departamento.

Estructurada y exhaustiva

El departamento de Laboratorios de Informática FICA-UTN efectuará la gestión de riesgos de manera sistemática y ordenada, de forma que se puede llevar un correcto proceso iterativo.

Adaptada

El departamento de Laboratorios de Informática FICA-UTN adaptará el proceso de gestión de riesgos de tal forma que se alinee a los objetivos, contexto y perfil de riesgos del departamento.

Inclusiva

El departamento de los Laboratorios de Informática FICA-UTN tendrá una participación apropiada y oportuna en las actividades relacionadas con la gestión del riesgo.

Dinámica

El departamento de los Laboratorios de Informática FICA-UTN responderá de manera oportuna a los cambios que puedan existir al contexto de la gestión de riesgos.

Mejor información posible

El departamento de los Laboratorios de Informática FICA-UTN brindará la información histórica, actual, experiencia y de retroalimentación necesaria para poder contextualizar y desarrollar correctamente la gestión de riesgos.

Factores humanos y culturales

El departamento de los Laboratorios de Informática FICA-UTN mejorará el nivel de interés y minimizará la resistencia al cambio que presenta la implementación de la gestión de riesgos.

Mejora Continua

El departamento de los Laboratorios de Informática FICA-UTN en un futuro complementará el proceso de gestión de riesgos con revisiones continuas y la implementación de posibles mejoras.

Además, las partes interesadas se comprometen a:

- Aprobar la implementación del plan de gestión de riesgos dentro de los laboratorios.
- Proveer la información necesaria durante el proceso de implementación.
- Proveer los recursos necesarios.
- Proveer de cierto nivel de autoridad al responsable mientras se desarrolle las actividades relacionadas al plan de gestión de riesgos.

- Facilitar la atención necesaria cuando se lo solicite.

3.1.2. Establecimiento del Contexto

Situación Actual

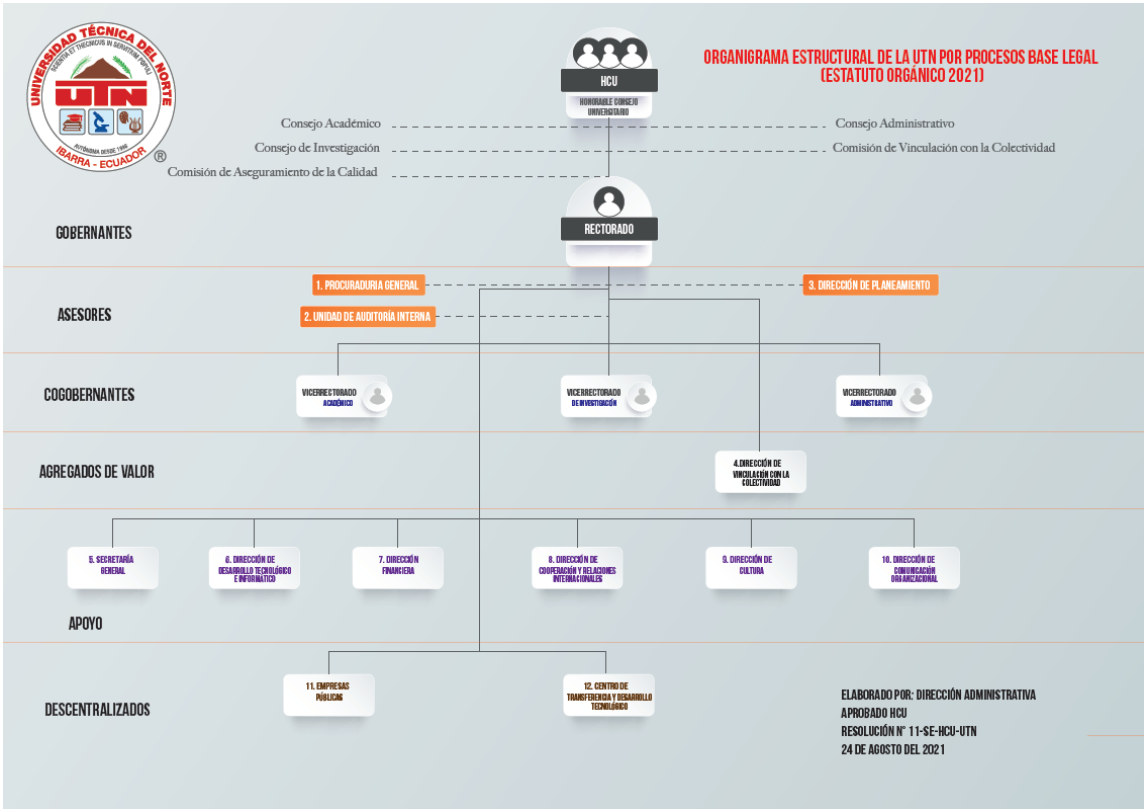
La Universidad Técnica del Norte (UTN) actualmente es un referente en el norte del país en cuanto a Educación Superior se refiere, especialmente reconocida por la calidad de profesionales que forma cada ciclo; ha resaltado enfáticamente en los aspectos tecnológicos, pues está muy bien equipada en cuanto a infraestructura tecnológica.

Para sobrellevar todos los aspectos referentes a la tecnología en la Universidad, se consolidó el Departamento de Desarrollo Tecnológico e Informático (DDTI) UTN, mismo que se encuentra ubicado en el campus principal “El Olivo” de la Institución.

En la Figura 31 se puede observar como el DDTI es uno de los departamentos constituyentes del nivel de apoyo dentro del Organigrama Estructural de la UTN en 2021.

Figura 31

Organigrama Estructural UTN 2021



Nota: Tomado de Estructura Organizacional, por Universidad Técnica del Norte, 2021, UTN (https://www.utn.edu.ec/estructura-organizacional/).

El DDTI comprometido con el apoyo al cumplimiento de los objetivos de la UTN, implementa dos servicios, el primer espacio conocido como “Parque Computacional”, mismo que conforma todos los equipos tecnológicos dentro de la UTN, y el segundo referente a los servicios tecnológicos prestados a los usuarios.

Parte del Parque Computacional son los Laboratorios de Informática de las distintas facultades de la Universidad. En el caso de la Facultad de Ingeniería en Ciencias Aplicadas (FICA), al ser una facultad de carreras muy relacionadas con la tecnología e informática, los laboratorios están destinados a contribuir en el proceso académico de las distintas actividades propuestas por las carreras que conforman esta facultad.

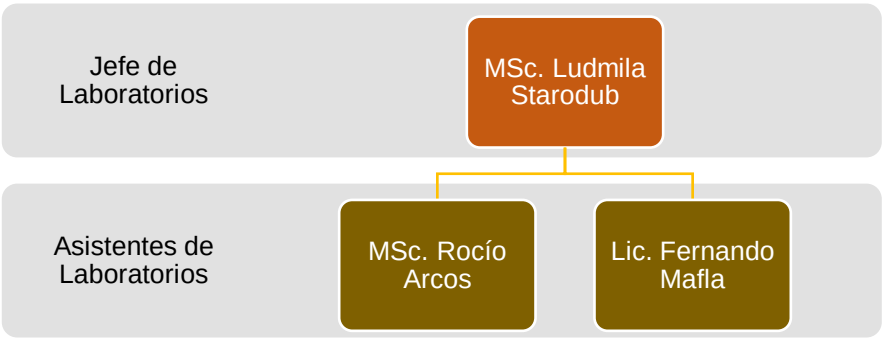
Estructura Organizacional de los Laboratorios de informática FICA-UTN

Los laboratorios de informática son responsabilidad de cada facultad, en este caso, la FICA contempla a los laboratorios de informática como un departamento interno de la facultad, necesario para su correcto funcionamiento.

El alto nivel de importancia de este departamento ha ocasionado la necesidad de designar a un personal con capacidades específicas para cubrir los requerimientos de los laboratorios. En la Figura 32 se aprecia la organización vertical interna de los laboratorios de informática FICA-UTN.

Figura 32

Organigrama Vertical Laboratorios de Informática FICA-UTN



Nota: Elaboración propia.

Cada una de las personas que pertenecen al grupo de encargados de los laboratorios de informática FICA-UTN, tienen designadas diferentes funciones dentro del departamento, en la Tabla 17 se presentan los roles y funciones de cada miembro del personal.

Tabla 17

Roles y Funciones del personal encargado de los Laboratorios de Informática FICA-UTN

ROL	PUESTO	FUNCIONES
Jefe de Laboratorios	Analista de Sistemas 3	• Coordinar y supervisar el trabajo de los asistentes y personal de apoyo, así como también definir sus horarios. • Planificar el trabajo de los encargados de los Laboratorios de informática de la Facultad. • Elaborar plan de contingencia para los Laboratorios de informática de la Facultad. • Elaborar y mantener actualizado el Reglamento del uso de los laboratorios de informática. • Elaborar el POA y PAC de los Laboratorios de informática. • Elaborar el PAC de los Laboratorios de informática. • Elaborar políticas, procedimientos y formularios del uso de laboratorios, control de préstamos, control de mantenimiento de equipos. • Realizar el proceso de bajas de bienes de los Laboratorios de Informática. • Coordinar con los docentes y planificar la distribución de laboratorios para clases prácticas de los programas curriculares: requerimientos de hardware y software, horarios. • Distribución de laboratorios para los cursos de capacitación de la Facultad: requerimientos de hardware y software, horarios. • Realizar los trámites para adecuación y mantenimiento de ambientes físicos, muebles de los laboratorios. • Asesoría informática y soporte técnico a los usuarios de los Laboratorios y personal administrativo de la FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS. • Soporte técnico en los procesos de las pruebas de admisión y matrículas de las careras de la facultad. • Asesoría y soporte técnico en los procesos de adquisición de equipos informáticos a nivel de la Universidad. • Participación en los proyectos académicos y administrativos para la Facultad, relacionados con Tecnologías de información. • Administración y mantenimiento de los equipos de comunicación, cableado estructurado y wireless de la red de la FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS.

Asistente de Laboratorios 1	Asistente de Laboratorio encargado del Área de Mantenimiento de hardware y software de equipos informáticos	• Diagnosticar diariamente el estado de funcionamiento de computadoras de los laboratorios de informática FICA, tomando en cuenta las observaciones de docentes y estudiantes. • Asesoría informática y soporte técnico a los usuarios de los Laboratorios y personal administrativo de la FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS. • Mantenimiento preventivo y correctivo de hardware y software de computadoras y periféricos de los Laboratorios. • Prestar soporte técnico de informática en los eventos de la FICA. • Elaborar y presentar reportes técnicos al Jefe del Laboratorio sobre daños en el hardware para proceder con las bajas y reemplazo de las piezas dañadas. • Elaborar y registrar Actas Entrega recepción de préstamos temporales y permanentes de los bienes previa autorización del Jefe de laboratorio de sistemas. • Administración servidores de instaladores, DHCP, PROXY y ANTIVIRUS. • Inventario de las computadoras, registro de cambio de componentes de hardware. • Soporte técnico en los procesos de las pruebas de admisión y matrículas de las careras de la facultad. • Ayudar en proyectos académicos y administrativos de la Facultad, relacionados con Tecnologías de información. • Más las funciones que le asigne su Jefe inmediato.
Asistente de Laboratorios 2	Asistente de Laboratorio encargado del Área de Desarrollo de Software y Soporte técnico	• Soporte técnico de equipos de proyección, video y sonido del Aula Virtual y pizarras electrónicas de la Facultad. • Asesoría informática y soporte técnico a los usuarios de los Laboratorios y personal administrativo de la FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS. • Diseño, desarrollo e implementación de los sistemas informáticos y aplicaciones web. • Administración y mantenimiento de sistemas informáticos y aplicaciones web de la Facultad. • Soporte técnico, instalación del software para los cursos de capacitación y eventos de la Facultad. • Mantenimiento preventivo y correctivo de hardware y software de computadoras y periféricos instalados en las oficinas administrativas de la FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS. • Soporte técnico en los procesos de las pruebas de admisión y matrículas de las careras de la facultad. • Ayudar en proyectos académicos y administrativos de la Facultad, relacionados con Tecnologías de información. • Más las funciones que le asigne su Jefe inmediato.

Nota: Elaboración propia a partir de “Descripción y perfil de puestos” (pp.107-110), por Honorable Consejo Universitario, 2015, UTN.

Infraestructura física

La Facultad de Ingeniería en Ciencias Aplicadas cuenta con su infraestructura física en el Campus Universitario principal ubicado en “EL Olivo”, dentro de este edificio que compone la facultad se encuentran de forma distribuida los laboratorios de informática.

En la Tabla 18 se presenta la distribución de ambientes físicos pertenecientes a los Laboratorios de Informática FICA-UTN.

Tabla 18

Distribuciones ambientes físicos de los laboratorios de informática FICA-UTN

Ambiente Físico	Descripción
Entrada de laboratorios	En la entrada del área de oficinas y soporte se encuentra un computador y una impresora para uso específico de los estudiantes para consulta de notas e impresión de trabajos en clase.
Área de servidores y desarrollo de sistemas	Conjunto de computadores con servidores como: Servidor proxy y DHCP Servidor de antivirus Instaladores Servidor de base de datos de los sistemas informáticos de la Facultad
Oficinas	Oficinas con computador, impresora, teléfono IP para la persona Jefe de Laboratorios de Sistemas.
Área de soporte y mantenimiento	Área con equipamiento de monitoreo de circuito cerrado con cámaras de video instaladas en el edificio FICA, además cuenta con: Equipos y herramientas para pruebas de mantenimiento. Computador, impresora, teléfono IP del Asistente de Laboratorios.
Cuarto de comunicaciones	Área con rack de conexiones de fibra y cobre, switches de acceso a la red.
Laboratorios de informática	Conjunto de 9 ambientes físicos con equipos de altas prestaciones.
Aula virtual	Área con un computador, proyector, pantalla de proyección, equipo de amplificación que se utiliza para eventos académicos, administrativos y culturales de la facultad.

Nota: Tomada de “Reglamento de Laboratorios de Informática FICA” (pp.1-2), por Honorable Consejo Universitario, 2011, UTN.

Cada uno de los Laboratorios de Informática está dotado de distintos tipos de equipos para procurar cubrir las distintas necesidades académicas de los estudiantes. En la Tabla 19 se presenta los tipos de equipos con los que está provisto cada laboratorio.

Tabla 19

Distribución equipos en los Laboratorios de Informática FICA-UTN

Planta	Laboratorio	Tipo de Equipos	N Equipos
2	Laboratorio de Informática 1	Sistema Operativo Windows	30
	Laboratorio de Informática 2	Sistema Operativo Macintosh	25
	Laboratorio de Informática 3	Sistema Operativo Windows	30
	Laboratorio de Informática 4 / Redes	Sistema Operativo Windows	20
3	Laboratorio de Informática 5 / Software / Base de Datos	Sistema Operativo Windows	31
	Laboratorio de Informática 6 / Software / Multimedia	Sistema Operativo Macintosh	25
	Laboratorio de Informática 7	Sistema Operativo Windows	13
5	Laboratorio de Informática 8 / Software / Programación	Sistema Operativo Windows	18
	Laboratorio de Informática 9 / Software / Sistemas Operativos	Sistema Operativo Windows	30

Nota: Elaboración propia.

Infraestructura Tecnológica

Los laboratorios de Informática FICA son parte integral de la Universidad Técnica del Norte, estos pertenecen al "Parque Computacional" UTN, del cual está encargada cada Facultad.

La tabla 20 presenta la distribución de software utilizada en los laboratorios de informática FICA-UTN.

Tabla 20

Distribución software en los Laboratorios de Informática FICA-UTN

Software	Descripción
Software	Los laboratorios de informática utilizan el software original, así como también el software con las versiones de demostración (demos).
Sistemas Informáticos internos	• Sistema de préstamos y reservaciones de instalaciones • Sistema de administración de biométricos. • Portal Web Academia CISCO • Revista electrónica de la FICA

Nota: Elaboración propia a partir de "Reglamento de Laboratorios de Informática FICA" (p.2), por Honorable Consejo Universitario, 2011, UTN.

En el caso de la FICA, las personas encargadas de la administración y gestión de los equipos computacionales son los 3 laboratoristas. Sin embargo, los servicios presentes en los

laboratorios de informática como: servicio de internet, almacenamiento o nube, son administrados por la Dirección de Desarrollo Tecnológico e Informático (DDTI).

Toda la información referente a los activos fijos en los laboratorios se encuentra debidamente registrada por el Departamento de Almacén y Bodega de la UTN, misma información almacenada en el apartado dirigido al Parque Computacional en la base de datos utilizada por la Universidad.

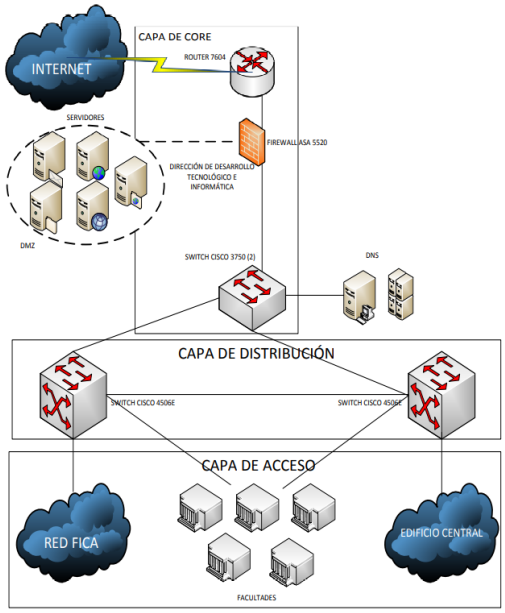
Dentro de los activos físicos también se comprende a los bienes tecnológicos pertenecientes a los laboratorios de informática, estos son debidamente configurados por sus responsables con distintos estándares ya establecidos por el DDTI.

La UTN como en todos sus aspectos ha estado en constante mejora, y el apartado de infraestructura de red no ha sido la excepción. El DDTI ha desarrollado distintas políticas para poder homogeneizar toda la red, además de la implantación de distintas medidas de seguridad, tales como Firewall, Packet Filtering, Mail Security y Antivirus.

La topología de red de la Universidad Técnica del Norte es la presente en Figura 33.

Figura 33

Topología básica de red UTN



Nota: Tomada de “Plan Estratégico UTN”, por Dirección de Desarrollo Tecnológico e Informático UTN, 2021.

En el caso de los laboratorios, la Tabla 21 presenta como están distribuidas las conexiones de red.

Tabla 21

Distribución de equipos de comunicaciones y conexiones de red en los laboratorios de informática FICA-UTN

Ubicación	Rack	Switch CISCO	Puntos de Red
Laboratorio 1	1	1	40
Laboratorio 2	1	1	40
Laboratorio 3	1	2	40
Laboratorio 4	1	2	40
Laboratorio 5	1	2	35
Laboratorio 6	1	1	25 PCs conectadas directamente a un Switch
Laboratorio 7	0	1	12 PCs conectadas directamente a un Switch
Laboratorio 8	0	0	12
Laboratorio 9	1	2	40
Data Center	1	1	Switch Core

Nota: Tomada de "Plan de Mantenimiento de computadoras" (p.4), por Personal Laboratorios de Informática FICA, 2019.

En el caso del Laboratorio 4 que es utilizado para actividades académicas relacionadas con conexiones de red, este cuenta con más equipamiento presentado en la Tabla 22.

Tabla 22

Distribución de equipos de comunicaciones y conexiones de red en el laboratorio de informática 4 FICA-UTN

Ubicación	Rack	Switch	Router
Laboratorio 4	4	15	15

Nota: Tomada de "Plan de Mantenimiento de computadoras" (p.4), por Personal Laboratorios de Informática FICA, 2019.

Servicios

Los laboratorios de Informática FICA-UTN son parte integral de las actividades dentro de la Facultad, debido a que brindan una serie de servicios necesarios tanto para la parte académica, como para la parte administrativa. Estos servicios son:

- Soporte técnico a estudiantes y docentes de la facultad.
- Mantenimiento de hardware y software de índole preventivo y correctivo a los equipos de los laboratorios y a los equipos del personal administrativo que lo solicite.
- Proceso de adquisición de componentes a los laboratorios.

- Administración de servicios: equipos biométricos, software SolidWorks, software FlexSim, sistema de reservación de instalaciones.
- Préstamo internos y externos de insumos.
- Acceso a los equipos a los docentes y estudiantes.

Seguridad y control de acceso

La distribución de los laboratorios se encuentra ubicada de esta manera debido a las disposiciones impuestas por el equipo de infraestructura y electricidad de la Universidad. Además de los laboratorios, existe un espacio creado para el equipo encargado de este departamento, este espacio tiene la finalidad de servir como soporte a las actividades de organización

Debido a la naturaleza del equipamiento de los laboratorios, la directiva institucional optó por el aseguramiento de estos mediante cinco tipos de seguridad:

- Seguridad Biométrica Dactilar
- Seguridad Biométrica Facial
- Seguridad Física
- Vigilancia Humana
- Cámaras de vigilancia

Los laboratorios de Informática cada cierto tiempo optan por solicitar la actualización de los sistemas de vigilancia, más recurrentemente del sistema de seguridad biométrica, por lo que no todos los laboratorios cuentan con todos los sistemas de seguridad. Como se puede observar en la Tabla 23.

Tabla 23

Sistemas de seguridad en los laboratorios de informática FICA-UTN

Laboratorio	Seguridad Biométrica Dactilar	Seguridad Biométrica Facial	Seguridad Física	Cámaras de vigilancia
1	SI	NO	Si	Si
2			Si	Si
3	Si	NO	Si	Si
4	Si	NO	Si	Si
5	SI	SI	Si	Si
6	SI	SI	Si	Si
7	SI	SI	Si	Si

8	NO	SI	Si	Si
9	SI	SI	Si	Si

Nota: Elaboración propia.

Para el acceso a los laboratorios por los sensores biométricos, el departamento almacena los datos biométricos faciales y dactilares de los docentes que durante el periodo académico soliciten el acceso a los laboratorios, para que así puedan acceder con los estudiantes a estos espacios con ayuda del sensor biométrico ubicado junto a la puerta de cada laboratorio.

Además, en el caso de acceso por seguridad física, los docentes podrán requerir, cada vez que lo necesiten, en el área de soporte, una llave para abrir el candado que se encuentra en cada puerta de los laboratorios.

La seguridad interna de los equipos informáticos está de cierta forma controlada gracias al uso de 3 tipos de seguridad implantados:

- Control de acceso a los equipos: Todos los equipos de cómputo poseen dos tipos de usuarios.

  ADMIN-FICA: es el tipo de usuario administrador que puede realizar cualquier acción sin restricción dentro de dicho equipo, se cuenta con una contraseña establecida por los encargados de los laboratorios

  ESTUDIANTE: es el tipo de usuario destinado a los estudiantes, aquí se desarrollarán tareas con menor riesgo de afectaciones negativas a los equipos.

- Firewall: provisto por el equipo encargado de la red en el DDTI, es el dispositivo encargado de monitorear y permitir el tráfico de red establecido como apto para los estudiantes.

- Antivirus: provisto por el equipo de DDTI, es el programa encargado de detectar y eliminar los virus informáticos encontrados en los equipos.

Incidentes pasados

Desde la consolidación de los laboratorios de informática FICA-UTN en el año 1996 han existido una gran cantidad de incidentes relacionados con la pérdida de activos fijos, ya sean por causas naturales o antrópicas, no se ha llevado un registro histórico estricto de estos incidentes, por lo que el conocimiento sobre estos es muy impreciso.

Existen incidentes que ocurren con gran regularidad, por ejemplo, las fallas eléctricas o apagones en los laboratorios presentan un gran peligro para la vida útil de los equipos

electrónicos, debido a los daños que puede causar la gran carga de voltaje con la que regresa la electricidad.

Además, años atrás, existían los incidentes causados por programa maligno. Esto produjo que se presente inconformidad en los usuarios de los laboratorios; ante este problema, el Departamento de Desarrollo Tecnológico e Informático de forma empírica optó por el uso de antivirus a nivel Institucional.

Han existido diversos casos de hurto de componentes pertenecientes a los equipos de los laboratorios, lamentablemente no existen políticas sobre los procedimientos a realizarse en estos casos, si el hurto es menor se solicita la devolución al responsable, pero si es de gran magnitud se realiza una denuncia pública.

Contexto interno y externo

La gestión de riesgos al ser un proceso alineado a los objetivos del departamento se ve afectado por los cambios externos que sufren los laboratorios de informática. Tales son los casos de regulaciones gubernamentales, disposiciones financieras, recomendaciones institucionales; además de cambios internos como la adquisición de nuevos equipos, cambios en los planes estratégicos, cambios tecnológicos, cambios culturales y organizacionales.

Por esta razón es importante realizar un proceso de revisión y seguimiento al Plan de Gestión de Riesgos para asegurar la integridad y alineación con los objetivos del departamento.

3.2. Fase 2: Evaluación, y tratamiento del riesgo.

La evaluación del riesgo es el proceso de identificación del riesgo, análisis del riesgo y valoración del riesgo.

La evaluación del riesgo se desarrolló de manera sistemática, iterativa y colaborativa, basándose en la información obtenida en la fase 1.

Para el desarrollo de la Gestión de Riesgos en los laboratorios de Informática FICA-UTN, se optó por la versión PILAR RM (versión 1.2.2022) con su licenciamiento de evaluación debido a su amplia gama de características en comparación con sus otras versiones.

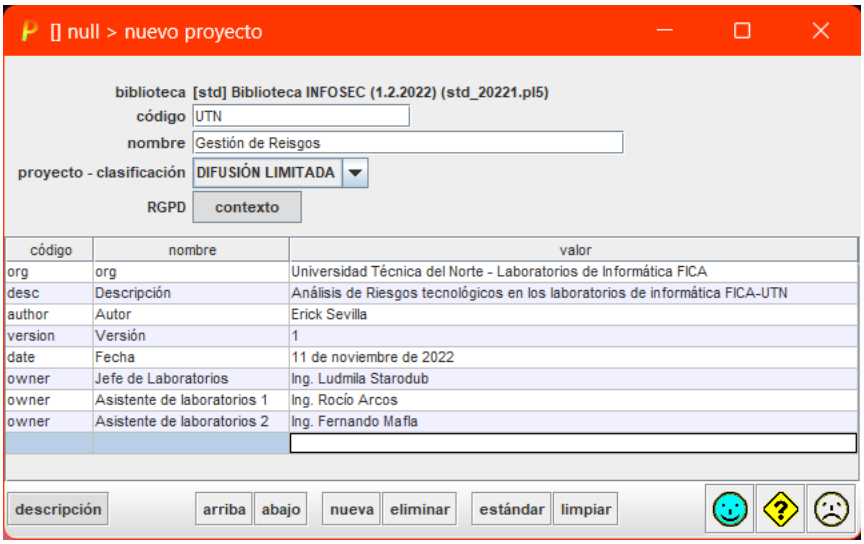
Para facilitar el desarrollo de las actividades de análisis de riesgos, la metodología MAGERIT cuenta con su segundo escrito “Catálogo de Elementos” cuyo fin es poder normalizar y tener un banco de elementos mucho más homogéneo, mediante un listado de tipos de activos, dimensiones y criterios de valoración y tipos de amenazas para cada activo.

Una vez desarrollado este proceso de análisis de riesgos con la herramienta PILAR, se puede obtener una visión sobre el estado que tiene la organización en relación con los riesgos de TI. Para de esta manera proponer soluciones al personal encargado de los laboratorios de informática FICA-UTN.

Para la creación del proyecto en la herramienta PILAR, se inició la aplicación y se ingresó la licencia de evaluación gratuita. Se creó un nuevo proyecto y se rellenó la información conforme fue solicitada. Este proceso se puede apreciar en la Figura 34.

Figura 34

Creación del proyecto en el software PILAR



Nota: Elaboración propia.

3.2.1. Identificación de activos

En esta actividad se desarrolló la identificación de activos relevantes en los procesos internos de la organización. Se considera activo a todo bien que sea valioso para las funciones de la organización y de esta manera garantizar su existencia.

La Tabla 24 presenta la clasificación de activos según el segundo escrito de la metodología MAGERIT “Catálogo de Elementos”.

Tabla 24

Tipos de activos según la Metodología MAGERIT

TIPO DE ACTIVO	DESCRIPCIÓN
Datos / Información	Físicos o digitales, son los datos esenciales para las funciones de la organización. Por ejemplo, documentos, manuales, informes, planes operativos, etc.
Servicios	Se refiere a los servicios técnicos, como los servicios de computación, servicios de mantenimiento y soporte.
Software	Sistemas de información dentro de la organización, tales como: aplicaciones informáticas, software de sistemas, herramientas tecnológicas, bases de datos, virtualizadores, correo electrónico.
Hardware	Referente a los equipos informáticos que facilitan la prestación de servicios de la organización. También comprende los equipos tecnológicos como computadores, servidores y servidores.
Redes de comunicaciones	Comprende las instalaciones para los servicios de comunicaciones, que usualmente son contratados por terceros. Tales como, redes telefónicas, ADSL, comunicación de radio, telefonía móvil, etc.
Soporte de información	Son aquellos dispositivos físicos que permiten el almacenamiento de información de manera extendida. Por ejemplo, discos, memorias USB, DVD, Tarjetas de memoria, etc.
Equipamiento auxiliar	Considera a los equipos que sirven de soporte para los sistemas de información, pero que no están relacionados directamente con los datos. Como, por ejemplo, fuentes de alimentación, generadores eléctricos, cableado, fibra óptica, mobiliario, etc.
Instalaciones	Se refiere a los espacios físicos donde se encuentran los sistemas de información. Tales como, edificios, departamentos, vehículos, contenedores, etc.
Personal	Son las personas relacionadas con los sistemas de información, como, por ejemplo, usuarios externos, usuarios internos, operadores, administradores, desarrolladores, etc.

Nota: Elaboración propia a partir de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 Catálogo de Elementos* (p.7), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

La identificación de activos se desarrolló con ayuda del equipo responsable de los laboratorios de informática FICA-UTN, y con base en la clasificación establecida por la metodología MAGERIT, en la Tabla 25 se describen los 27 activos identificados.

Tabla 25

Identificación de Activos de los Laboratorios de Informática FICA-UTN

CÓDIGO	ACTIVO AGRUPADO	TIPO	ACTIVO
		ESENCIALES	
ESSENTIAL-DATA-001		datos clasificados	Datos de acceso a servidores y sistemas
ESSENTIAL-BDD-001		base de datos	Base de datos de los sistemas informáticos de la Facultad
		DATOS/INFORMACIÓN	
D-INFO-001	Documentos de administración interna	ficheros	Políticas, procedimientos y formularios de uso
		ficheros	Registro de préstamos de equipos
		ficheros	Control de mantenimiento de equipos
		ficheros	Plan Operativo Anual
		ficheros	Plan Anual de Adquisiciones
		ficheros	Reglamentación de Uso
		backup	Copias de seguridad
		ficheros	Plan de Contingencia
D-CONF-001	Datos de configuración	datos de configuración	Configuración de servicios
		datos de gestión interna	Procedimientos administrativos
		código ejecutable	Imágenes ISO de los SO
		datos de credenciales	Claves de instalación de software
		SERVICIOS	
S-INT-001		world wide web	Internet
S-SUPP-001		mantenimiento	Mantenimiento preventivo y correctivo de hardware y software
S-TELF-001		interno	Telefonía
S-SRV-001	Servidores internos	interno	Instaladores
		público en general	Servidor proxy y DHCP
		SOFTWARE	
SW-INST-001		desarrollo propio	Sistema Reserva Instalaciones FICA
SW-BIO-001		desarrollo a medida	Sistema Administración Biométricos
SW-CAP-001	Portal Web para Capacitaciones	desarrollo propio	Portal Web de la Unidad de Capacitación Continua
		desarrollo a medida	Portal Web Academia CISCO

SW-REV-001		desarrollo propio	Revista electrónica de la FICA
SW-OFI-001	Aplicaciones de ofimática / académicas	base de datos	Aplicaciones para la gestión de base de datos
		ofimática	Aplicaciones de ofimática
		estándar	Aplicaciones de académicas
		virtualización	Aplicaciones de virtualización
		servidores	Aplicaciones de servidores web o aplicaciones
		navegación	Navegadores web
		sistemas operativos	Sistemas Operativos
		antivirus	Aplicaciones de antivirus
HARDWARE			
HW-PC-001	Equipos PC y didácticos	informática personal	Equipos PC
		medio de impresión	Impresora
		equipos medios	Proyector Digital
HW-SEG-001		equipos medios	Equipos de seguridad
HW-TELECOM-001	Equipos para redes de telecomunicaciones	soporte de la red	Switch de acceso LAN
		cableado	Cableado estructurado
		encaminadores	Router
		racks	Racks para equipos de telecomunicaciones
		soporte de la red	Patch para panel de red
REDES DE COMUNICACIONES			
COM-REDINT-001	Red interna Laboratorios	red telefónica	Red telefónica
		red Inalámbrica	Red inalámbrica
		WIFI	Internet
EQUIPAMIENTO AUXILIAR			
AUX-EQELEC-001	Equipamiento eléctrico	fuente de alimentación	Reguladores de voltaje
		fuente de alimentación	UPS
		fuente de alimentación	Fuentes de poder
		cableado eléctrico	Cableado eléctrico
		fibra óptica	Fibra óptica
AUX-MOB-001		mobiliario	Mobiliario para los equipos
SOPORTES DE INFORMACIÓN			
MEDIA-INF-001		electrónicos	Nube Microsoft OneDrive
INSTALACIONES			
L-LAB-001	Espacios físicos Laboratorio 1 a 9	cuarto	Espacios físicos Laboratorio 1 a 9
		cuarto	Entrada laboratorios
L-SERV-001	Área de servidores y comunicaciones	cuarto	Área de servidores y desarrollo de sistemas

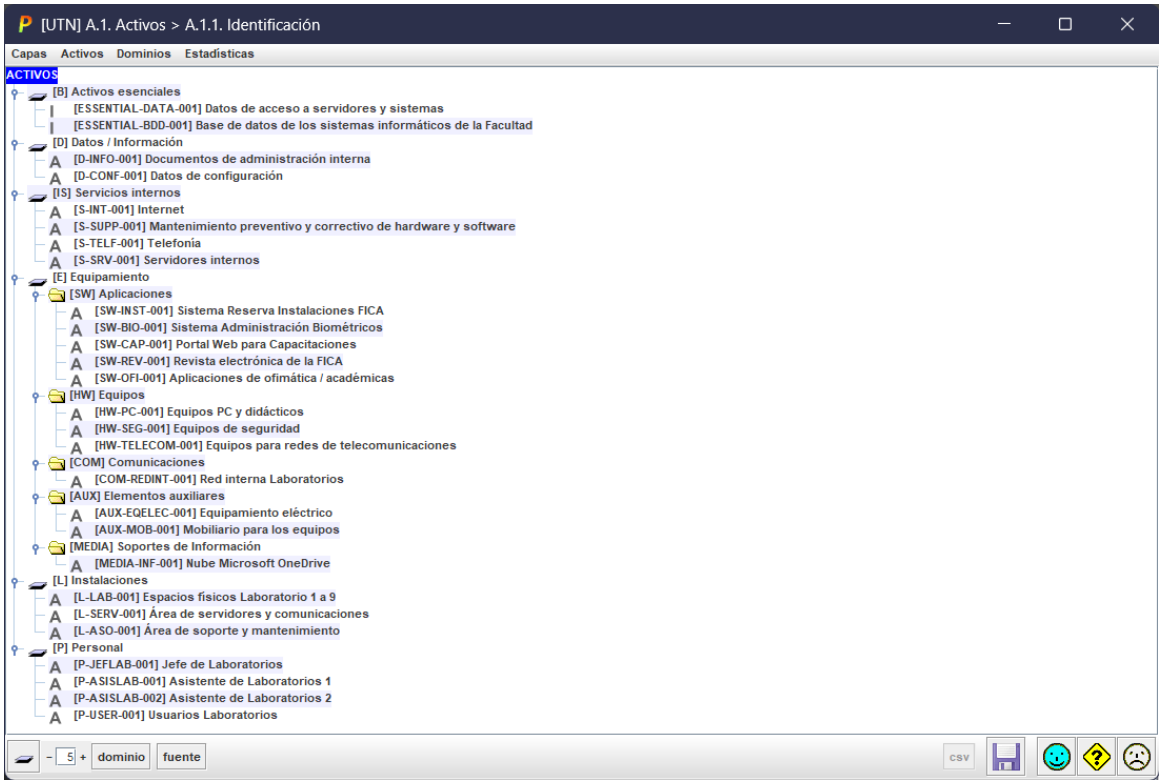
		cuarto	Cuarto de comunicaciones
L-ASO-001		cuarto	Área de soporte y mantenimiento
		PERSONAL	
P-JEFLAB-001		administrador	Jefe de Laboratorios
P-ASISLAB-001		operadores	Asistente de Laboratorios 1
P-ASISLAB-002		operadores	Asistente de Laboratorios 2
P-USER-001	Usuarios Laboratorios	usuarios internos	Docentes
		usuarios internos	Estudiantes

Nota: Elaboración propia.

En la Figura 35 se presenta la identificación de activos en la herramienta PILAR.

Figura 35

Identificación de Activos de los Laboratorios de Informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

3.2.2. Identificación de la dependencia entre activos

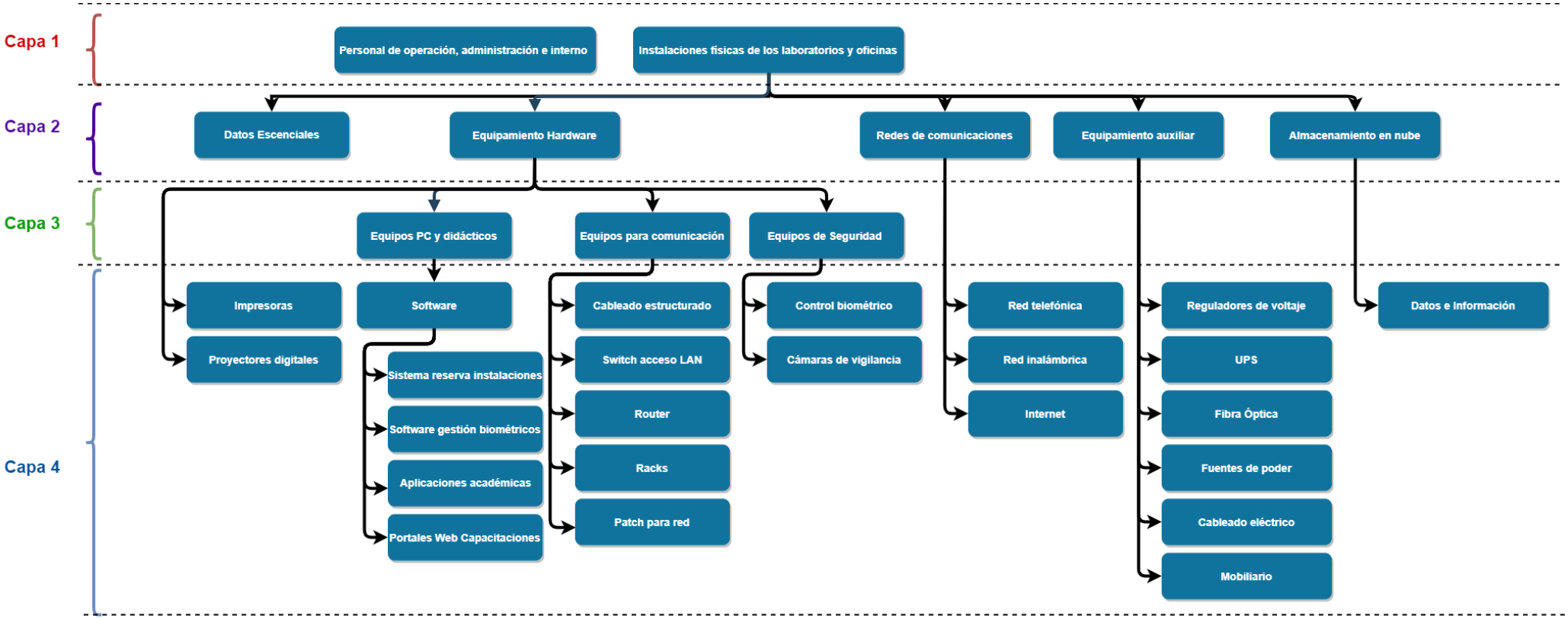
Dentro de las organizaciones los distintos tipos de activos muchas veces tiene relaciones entre sí, a esto se lo denomina dependencia entre activos y es una parte esencial en la gestión de riesgos porque a partir de un “árbol de dependencia” se puede determinar la posible propagación de daños que puede ocurrir a partir de la materialización de las amenazas.

En la parte superior del árbol de dependencia se ubica a los activos “superiores” que dependen de la seguridad de activos “inferiores”.

En la Figura 36 se aprecia el árbol de dependencia de activos.

Figura 36

Árbol de dependencia de activos de los laboratorios de informática FICA-UTN



Nota: Elaboración propia.

El árbol de dependencia representado en la Figura 37 consta de cuatro capas, en las que se encuentran ubicados los activos.

En la Capa 1 se han considerado los activos como la sala de servidores, personal e instalaciones físicas de los laboratorios de informática FICA-UTN. En la Capa 2 se encuentran activos como el equipamiento de hardware, redes de comunicaciones, equipamiento auxiliar y los datos e información. En la Capa 3 se encuentran los equipos necesarios para las actividades de aprendizaje, equipos de comunicaciones, equipos de seguridad y los equipos de cómputo. Para finalmente en la Capa 4 encontrar los activos referentes a las aplicaciones de software.

Los activos que se encuentran en las capas superiores “dependen” de las necesidades de seguridad de los activos de capas inferiores. Por ejemplo, sí el Almacenamiento en nube se ve afectado por una amenaza, los datos e información se verán afectados de alguna u otra forma.

3.2.3. Valoración de los activos

La metodología MAGERIT no toma énfasis en el valor monetario de los activos, más bien desarrolla los procesos de valoración desde una perspectiva de “Necesidad de protección”, esta perspectiva implica que “Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, entonces es algo que vale” (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012). Es decir, cuan más valioso es un activo, necesita un mayor nivel de protección en las dimensiones de valoración correspondientes.

Al igual que la dependencia, la valoración de activos es un paso primordial para la gestión de riesgos, pues en esta actividad se asigna un valor cuantitativo a los activos dependiendo la importancia que tiene para la organización, de esta manera se obtiene una perspectiva de la necesidad de protección que requiere el activo. MAGERIT evalúa la importancia de los activos en distintas dimensiones, estas se presentan en la Tabla 26:

Tabla 26

Definiciones de las dimensiones de valoración de activos según MAGERIT

Dimensión	Definición
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Nota: Elaboración propia a partir *de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 Catálogo de Elementos* (pp.15-16), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

Estas dimensiones funcionan como una faceta o aspecto de los activos, mediante estas se puede posteriormente valorar las consecuencias a raíz de la materialización de las distintas amenazas. Para la valoración de los activos se tomó en cuenta la escala de criterios presentada en la Tabla 27.

Tabla 27

Criterios de Valoración de activos según MAGERIT

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Depreciable	Irrelevante a efectos prácticos

Nota: Tomada de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 Catálogo de Elementos* (p.19), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

Los valores que reciben de esta tabla se refieren a la medida de perjuicio para la organización en caso de que el activo se vea dañado en dicha dimensión.

Junto con el equipo responsable de los Laboratorios de Informática se respondió las preguntas propuestas por MAGERIT con la asignación de valores (Tabla 27) para cada dimensión:

- Disponibilidad [D]: ¿Qué importancia tendría que el activo no estuviera disponible?
- Integridad [I]: ¿Qué importancia tendría que los datos fueran modificados fuera de control?

- Confidencialidad [C]: ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
- Autenticidad [A]: ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
- Trazabilidad [T]: ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

En la Tabla 28 se encuentra la asignación de valoración de cada uno de los activos.

Tabla 28

Valoración de activos de los Laboratorios de Informática FICA-UTN

ACTIVO	D	I	C	A	T	PONDERACIÓN	VALOR
ESENCIALES							
Datos de acceso a servidores y sistemas	9	9	10	10	9	9	Muy Alto
Base de datos de los sistemas informáticos de la Facultad	10	10	8	10	10	10	Extremo
DATOS / INFORMACIÓN							
Documentos de administración interna	8	9	10	10	9	9	Muy Alto
Datos de configuración	8	9	9	8	8	8	Alto
SERVICIO							
Internet	9	7	7	8	8	8	Alto
Mantenimiento preventivo y correctivo de hardware y software	9	7	7	7	8	8	Alto
Telefonía	6	9	8	8	6	7	Alto
Servidores internos	9	9	10	10	9	9	Muy Alto
SOFTWARE							
Sistema Reserva Instalaciones FICA	8	9	6	8	8	8	Alto
Sistema Administración Biométricos	9	10	9	9	9	9	Muy Alto
Portal Web para Capacitaciones	4	9	4	8	8	7	Alto
Revista electrónica de la FICA	4	9	4	8	8	7	Alto
Aplicaciones de ofimática / académicas	8	7	2	6	5	6	Alto
HARDWARE							
Equipos PC y didácticos	10	9	6	9	9	9	Muy Alto
Equipos de seguridad	9	9	7	9	9	9	Muy Alto
Equipos para redes de telecomunicaciones	9	9	6	8	8	8	Alto
REDES DE COMUNICACIONES							
Red interna laboratorios	8	8	8	7	7	8	Alto
EQUIPAMIENTO AUXILIAR							

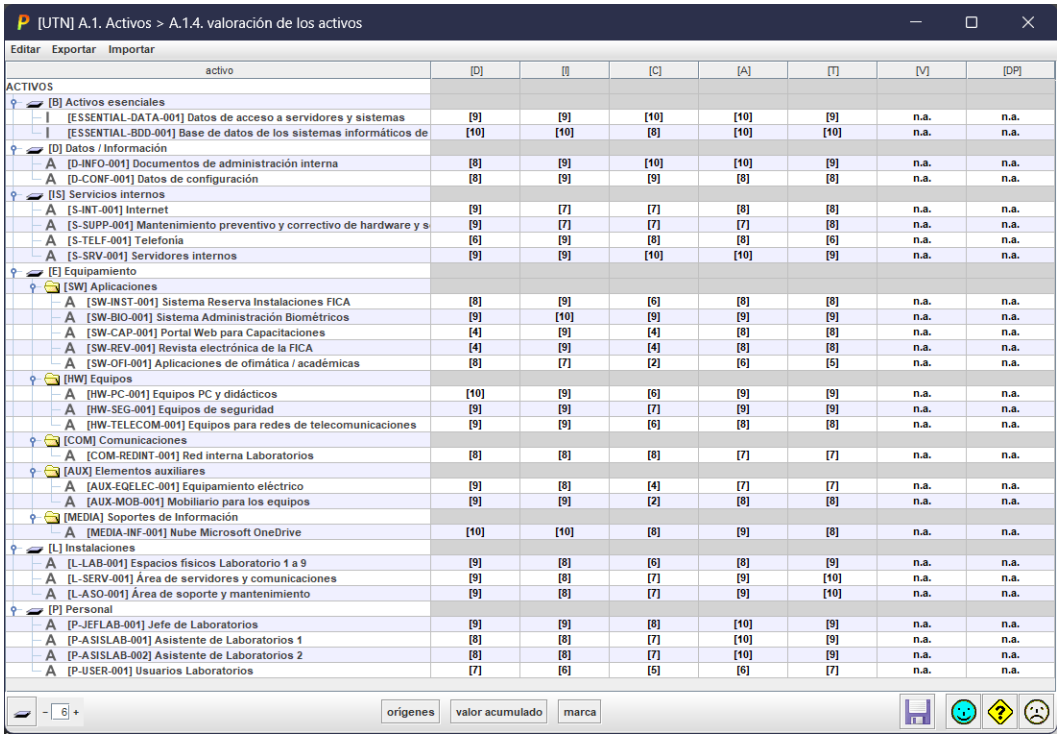
Equipamiento eléctrico	9	8	4	7	7	7	Alto
Mobiliario para los equipos	9	9	2	8	8	7	Alto
SOPORTES DE INFORMACIÓN							
Nube Microsoft OneDrive	10	10	8	9	8	8	Muy Alto
INSTALACIONES							
Espacios físicos Laboratorio 1 a 9	9	8	6	8	9	8	Alto
Área de servidores y desarrollo de sistemas	9	8	7	9	10	9	Muy Alto
Área de soporte y mantenimiento	9	8	7	9	10	9	Muy Alto
PERSONAL							
Jefe de Laboratorios	9	9	8	10	9	9	Muy Alto
Asistente de Enseñanza de los laboratorios 1	8	8	7	10	9	8	Alto
Asistente de Enseñanza de los laboratorios 2	8	8	7	10	9	8	Alto
Usuarios Laboratorios	7	6	5	6	7	6	Alto

Nota: La tabla presenta las distintas valoraciones cuantitativas para cada uno de los activos en sus cinco dimensiones de valoración (D: disponibilidad, I: integridad, C: confidencialidad, A: autenticidad, T: trazabilidad) identificados en los laboratorios de informática FICA-UTN. Elaboración propia.

En la Figura 37 se presenta la identificación de activos en la herramienta PILAR.

Figura 37

Valoración de Activos Software PILAR



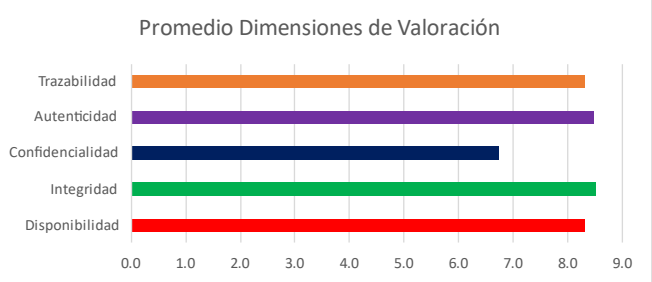
activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS							
[B] Activos esenciales							
[ESSENTIAL-DATA-001] Datos de acceso a servidores y sistemas	[9]	[9]	[10]	[10]	[9]	n.a.	n.a.
[ESSENTIAL-BDD-001] Base de datos de los sistemas informáticos de	[10]	[10]	[8]	[10]	[10]	n.a.	n.a.
[D] Datos / Información							
[D-INFO-001] Documentos de administración interna	[8]	[9]	[10]	[10]	[9]	n.a.	n.a.
[D-CONF-001] Datos de configuración	[8]	[9]	[9]	[8]	[8]	n.a.	n.a.
[IS] Servicios internos							
[S-INT-001] Internet	[9]	[7]	[7]	[8]	[8]	n.a.	n.a.
[S-SUPP-001] Mantenimiento preventivo y correctivo de hardware y s	[9]	[7]	[7]	[7]	[8]	n.a.	n.a.
[S-TELF-001] Telefonía	[6]	[9]	[8]	[8]	[6]	n.a.	n.a.
[S-SRV-001] Servidores internos	[9]	[9]	[10]	[10]	[9]	n.a.	n.a.
[E] Equipamiento							
[SW] Aplicaciones							
[SW-INST-001] Sistema Reserva Instalaciones FICA	[8]	[9]	[6]	[8]	[8]	n.a.	n.a.
[SW-BIO-001] Sistema Administración Biométricos	[9]	[10]	[9]	[9]	[9]	n.a.	n.a.
[SW-CAP-001] Portal Web para Capacitaciones	[4]	[9]	[4]	[8]	[8]	n.a.	n.a.
[SW-REV-001] Revista electrónica de la FICA	[4]	[9]	[4]	[8]	[8]	n.a.	n.a.
[SW-OFI-001] Aplicaciones de ofimática / académicas	[8]	[7]	[2]	[6]	[5]	n.a.	n.a.
[HW] Equipos							
[HW-PC-001] Equipos PC y didácticos	[10]	[9]	[6]	[9]	[9]	n.a.	n.a.
[HW-SEG-001] Equipos de seguridad	[9]	[9]	[7]	[9]	[9]	n.a.	n.a.
[HW-TELECOM-001] Equipos para redes de telecomunicaciones	[9]	[9]	[6]	[8]	[8]	n.a.	n.a.
[COM] Comunicaciones							
[COM-REDINT-001] Red interna Laboratorios	[8]	[8]	[8]	[7]	[7]	n.a.	n.a.
[AUX] Elementos auxiliares							
[AUX-EQELEC-001] Equipamiento eléctrico	[9]	[8]	[4]	[7]	[7]	n.a.	n.a.
[AUX-MOB-001] Mobiliario para los equipos	[9]	[9]	[2]	[8]	[8]	n.a.	n.a.
[MEDIA] Soportes de Información							
[MEDIA-INF-001] Nube Microsoft OneDrive	[10]	[10]	[8]	[9]	[8]	n.a.	n.a.
[L] Instalaciones							
[L-LAB-001] Espacios físicos Laboratorio 1 a 9	[9]	[8]	[6]	[8]	[9]	n.a.	n.a.
[L-SERV-001] Área de servidores y comunicaciones	[9]	[8]	[7]	[9]	[10]	n.a.	n.a.
[L-ASO-001] Área de soporte y mantenimiento	[9]	[8]	[7]	[9]	[10]	n.a.	n.a.
[P] Personal							
[P-JEFLAB-001] Jefe de Laboratorios	[9]	[9]	[8]	[10]	[9]	n.a.	n.a.
[P-ASISLAB-001] Asistente de Laboratorios 1	[8]	[8]	[7]	[10]	[9]	n.a.	n.a.
[P-ASISLAB-002] Asistente de Laboratorios 2	[8]	[8]	[7]	[10]	[9]	n.a.	n.a.
[P-USER-001] Usuarios Laboratorios	[7]	[6]	[5]	[6]	[7]	n.a.	n.a.

Nota: Elaboración propia.

La Figura 38 presenta un promedio de las valoraciones cuantitativas por dimensión de valoración de todos los activos identificados en los laboratorios de informática FICA-UTN.

Figura 38

Promedio dimensiones de valoración activos de los Laboratorio de Informática FICA-UTN

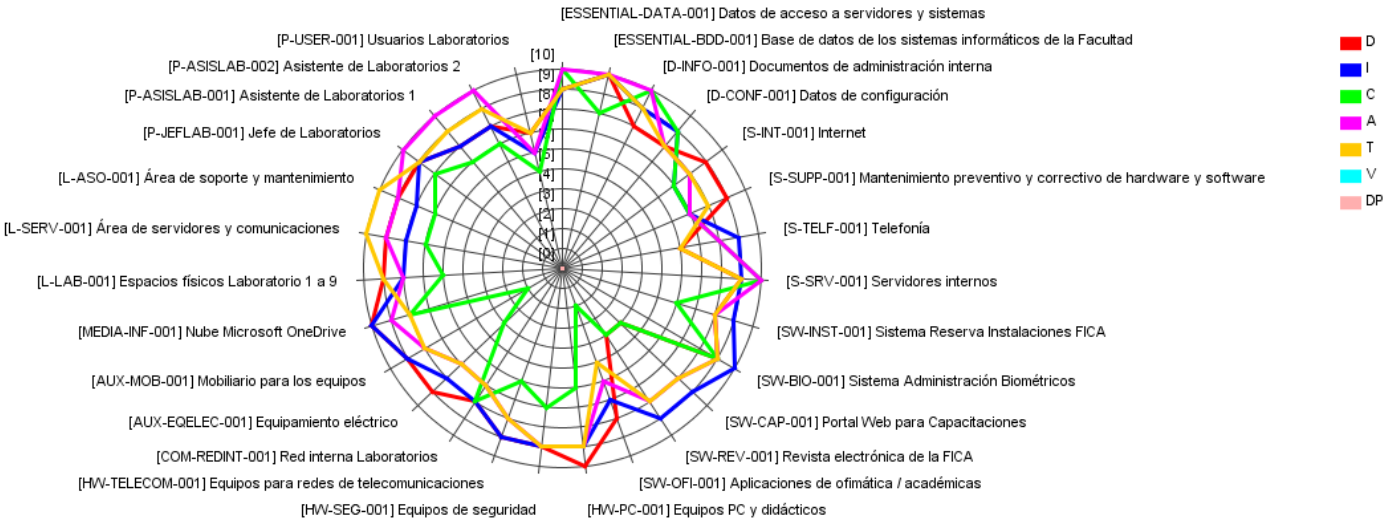


Nota: Elaboración propia.

La Figura 39 presenta en un gráfico de tipo área, el valor de activo en su respectiva dimensión dentro de los laboratorios de informática FICA-UTN.

Figura 39

Valor de activos Laboratorios de Informática FICA-UTN



Nota: Elaboración propia.

3.2.4. Identificación de Amenazas

El paso siguiente a la caracterización de activos, es la identificación de amenazas que pueden afectar a cada uno de ellos. La metodología MAGERIT en su segundo escrito “Catálogo de Elementos” expone cuatro diferentes tipos de amenazas:

- [N] Desastres Naturales
- [I] Origen Industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Dependiendo el tipo de activo, MAGERIT relaciona a cada uno con la posible amenaza que lo podría afectar. Se identificaron un total 286 amenazas distribuidas entre los 27 activos pertenecientes a los laboratorios de informática FICA-UTN, dichas amenazas se encuentran listadas en el Anexo E. La Tabla 29 presenta una muestra de la lista antes mencionada.

Tabla 29

Identificación de amenazas por activos de los Laboratorios de Informática FICA-UTN

ACTIVO	AMENAZAS
ESENCIALES	
Datos de acceso a servidores y sistemas	[A.13] Repudio (negación de actuaciones)
Base de datos de los sistemas informáticos de la Facultad	[A.13] Repudio (negación de actuaciones)
DATOS / INFORMACIÓN	
Documentos de administración interna	[E.15] Alteración de la información
Documentos de administración interna	[E.18] Destrucción de la información
Documentos de administración interna	[E.19] Fugas de información
Documentos de administración interna	[A.5] Suplantación de identidad
Documentos de administración interna	[A.6] Abuso de privilegios de acceso
Documentos de administración interna	[A.11] Acceso no autorizado
Datos de configuración	[E.4] Errores de configuración
Datos de configuración	[E.15] Alteración de la información
Datos de configuración	[E.18] Destrucción de la información
Datos de configuración	[E.19] Fugas de información
Datos de configuración	[A.4] Manipulación de los ficheros de configuración
Datos de configuración	[A.5] Suplantación de identidad
Datos de configuración	[A.6] Abuso de privilegios de acceso
Datos de configuración	[A.11] Acceso no autorizado
SERVICIOS	
Internet	

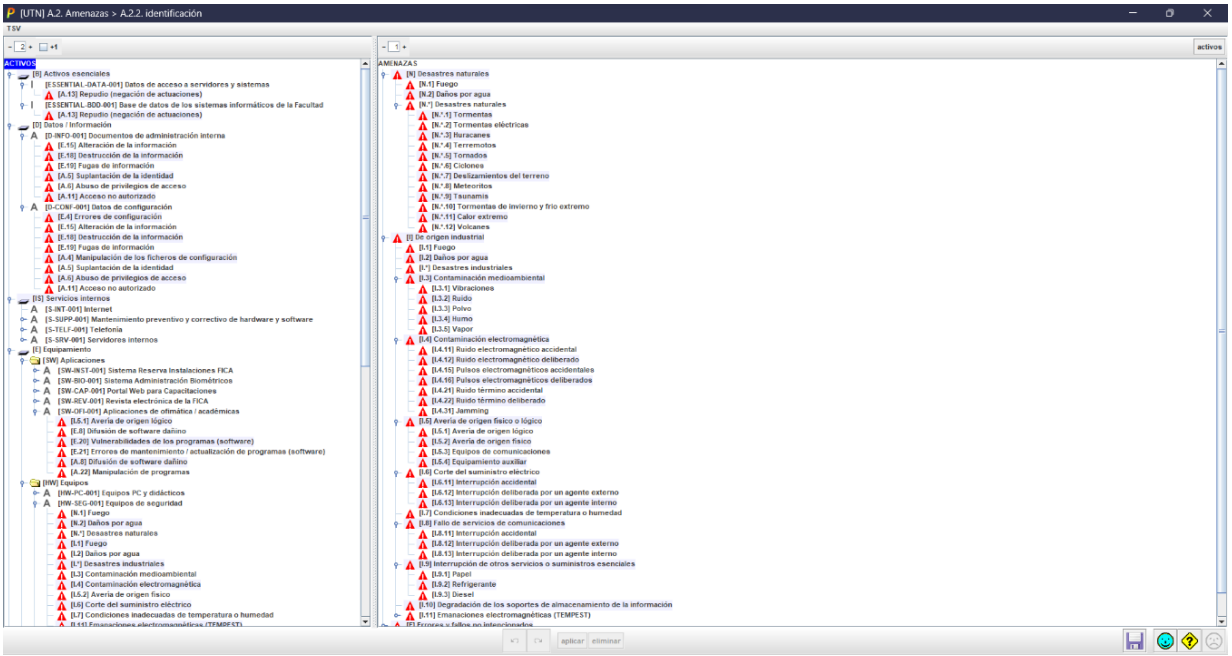
Mantenimiento preventivo y correctivo de hardware y software	[E.1] Errores de los usuarios
Mantenimiento preventivo y correctivo de hardware y software	[E.2] Errores del administrador del sistema / de la seguridad
Mantenimiento preventivo y correctivo de hardware y software	[E.15] Alteración de la información
Mantenimiento preventivo y correctivo de hardware y software	[E.18] Destrucción de la información
Mantenimiento preventivo y correctivo de hardware y software	[E.19] Fugas de información
Mantenimiento preventivo y correctivo de hardware y software	[E.24] Caída del sistema por agotamiento de recursos

Nota: Elaboración propia.

De igual manera, PILAR identifica de manera automática las amenazas en relación de los activos identificados, como se presenta en la Figura 40.

Figura 40

Identificación de amenazas por activos de los Laboratorios de Informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

3.2.5. Valoración de Amenazas

Una vez identificadas las amenazas, el siguiente paso consiste en valorarlas en dos sentidos:

Impacto o Degradación del valor: mide el daño sobre el activo en caso de que la amenaza relacionada se materializase. Para determinarlo se usa la escala presentada en la Tabla 30. Pero para el uso del software PILAR, se necesitan valores numéricos, por lo que se utiliza un porcentaje de 0 a 100.

Tabla 30

Escala Degradación del valor de un activo

MA	100%	Muy alta	Casi seguro	Fácil
A	75%	Alta	Muy alto	Medio
M	50%	Media	Posible	Difícil
B	25%	Baja	Poco probable	Muy difícil
MB	0%	Muy baja	Muy raro	Extremadamente difícil

Nota: Tomada de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 Método* (p.28), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

Frecuencia o Probabilidad de ocurrencia: se refiere a la frecuencia de ocurrencia de materialización de una amenaza. Se utiliza la tasa anual de ocurrencia presentada en la Tabla 31.

Tabla 31

Valores de probabilidad de ocurrencia de una amenaza

MA	100	Muy frecuente	A diario
A	10	frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	siglos

Nota: Tomada de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 Método* (p.28), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

Junto con el equipo encargado de los Laboratorios de Informática FICA-UTN se asignó los valores cuantitativos para el Impacto (Tabla 30) y para la Probabilidad de ocurrencia (Tabla 31) de cada una de las amenazas identificada. Al no contar con un registro de incidentes

ocurridos en los laboratorios, esta valoración fue realizada a manera de suposición e influenciada por los valores por defecto que provee PILAR.

La valoración de todas las amenazas en cada una de sus dimensiones dependiendo su probabilidad de ocurrencia (frecuencia) y degradación de valor (impacto) se encuentran en el Anexo F, mientras que la Tabla 32 presenta una muestra de dicha lista.

Tabla 32

Valoración de amenazas por activos de los Laboratorios de Informática FICA-UTN

ACTIVO	AMENAZAS	F	D	I	C	A	T
ESENCIALES							
Datos de acceso a servidores y sistemas	[A.13] Repudio (negación de actuaciones)	1					50%
Base de datos de los sistemas informáticos de la Facultad	[A.13] Repudio (negación de actuaciones)	1					50%
DATOS / INFORMACIÓN							
Documentos de administración interna	[E.15] Alteración de la información	1		1%			
Documentos de administración interna	[E.18] Destrucción de la información	1	1%				
Documentos de administración interna	[E.19] Fugas de información	1			10%		
Documentos de administración interna	[A.5] Suplantación de identidad	10		10%	50%	100%	
Documentos de administración interna	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Documentos de administración interna	[A.11] Acceso no autorizado	100		10%	50%		
Datos de configuración	[E.4] Errores de configuración	1		1%			
Datos de configuración	[E.15] Alteración de la información	1		1%			
Datos de configuración	[E.18] Destrucción de la información	1	1%				
Datos de configuración	[E.19] Fugas de información	1			10%		
Datos de configuración	[A.4] Manipulación de los ficheros de configuración	10	10 %	10%	10%		
Datos de configuración	[A.5] Suplantación de identidad	10		10%	50%	100%	
Datos de configuración	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Datos de configuración	[A.11] Acceso no autorizado	100		10%	50%		

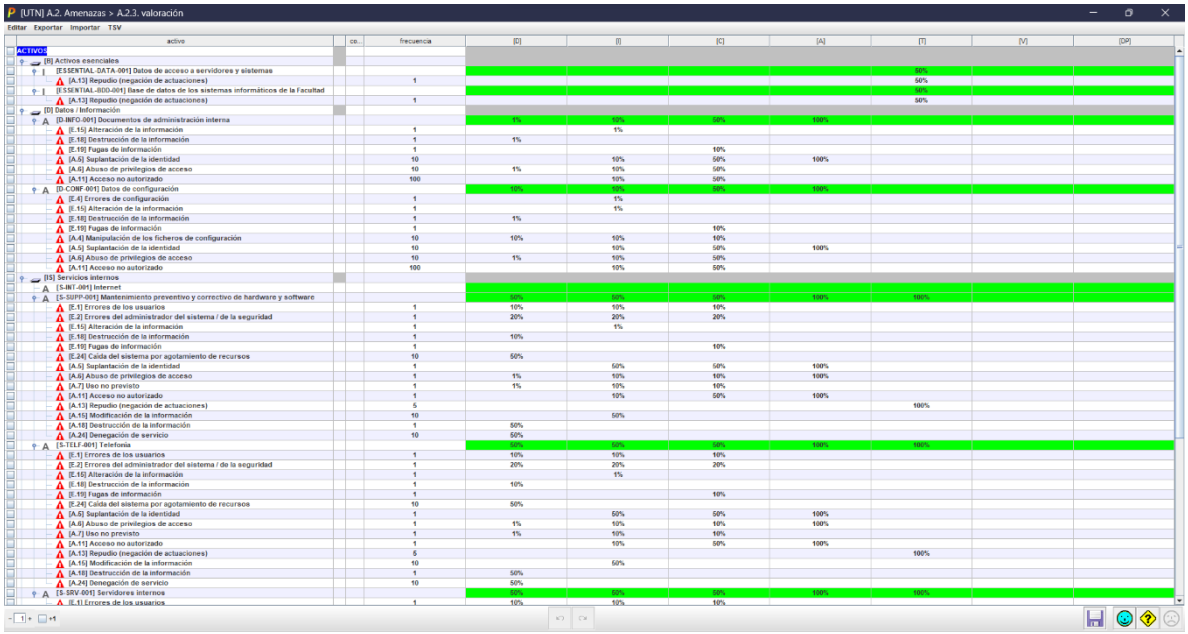
SERVICIOS					
Internet					
Mantenimiento preventivo y correctivo de hardware y software	[E.1] Errores de los usuarios	1	10 %	10%	10%
Mantenimiento preventivo y correctivo de hardware y software	[E.2] Errores del administrador del sistema / de la seguridad	1	20 %	20%	20%
Mantenimiento preventivo y correctivo de hardware y software	[E.15] Alteración de la información	1		1%	
Mantenimiento preventivo y correctivo de hardware y software	[E.18] Destrucción de la información	1	10 %		
Mantenimiento preventivo y correctivo de hardware y software	[E.19] Fugas de información	1			10%

Nota: La tabla presenta una muestra del listado de la valoración de amenazas que podrían afectar a los activos identificados en los laboratorios de informática FICA-UTN. En donde F: frecuencia o probabilidad de ocurrencia, D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

En la Figura 41 se presenta la valoración de las amenazas en función de la degradación de los activos y la probabilidad de ocurrencia provistas por el software PILAR.

Figura 41

Valoración de amenazas por activos de los Laboratorios de Informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

3.2.6. Determinación del impacto potencial

El impacto potencial se refiere al daño ocasionado por la materialización de una amenaza sobre un activo. El impacto potencial es proporcional al valor del activo y su degradación, por lo que es necesario su determinación para establecer las salvaguardas más adecuadas. El cálculo del valor del impacto se lo realizó para cada activo, por cada amenaza y en cada dimensión de valoración en función de la degradación.

Dicho impacto se lo puede realizar desde dos enfoques:

Impacto potencial acumulado: Se tiene en cuenta el valor acumulado del activo (el propio más el acumulado de los activos que dependen de él) y las amenazas a las que está expuesto. La ecuación para su cálculo es el siguiente:

$$Impacto\ potencial\ acumulado = \%\ Degradación\ de\ amenaza\ \times Valor\ acumulado\ del\ activo$$

El cálculo del impacto potencial acumulado se encuentra en el Anexo G, mientras que la Tabla 33 presenta una muestra de dicha lista.

Tabla 33

Impacto potencial acumulado de afectación de activos en los laboratorios de informática FICA-UTN

	IMPACTO POTENCIAL ACUMULADO					PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	**A**	**T**	
ACTIVOS ESENCIALES	**10**	**10**	**10**	**10**	**10**	
Datos de acceso a servidores y sistemas					9	
[A.13] Repudio (negación de actuaciones)					9	9.0
Base de datos biométricos					9	
[A.13] Repudio (negación de actuaciones)					9	9.0
DATOS / INFORMACIÓN	**7**	**7**	**9**	**10**		
Documentos de administración interna	4	7	9	10		
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	4					4.0
[E.19] Fugas de información			7			
[A.5] Suplantación de identidad		7	9	10		8.7
[A.6] Abuso de privilegios de acceso	4	7	9			6.7
[A.11] Acceso no autorizado		7	9			
Datos de configuración	7	7	9	10		
[E.4] Errores de configuración		4				4.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	4					4.0
[E.19] Fugas de información			7			7.0
[A.4] Manipulación de los ficheros de configuración	7	7	7			7.0
[A.5] Suplantación de identidad		7	9	10		8.7
[A.6] Abuso de privilegios de acceso	4	7	9			6.7
[A.11] Acceso no autorizado		7	9			8.0
SERVICIOS	**9**	**9**	**9**	**10**	**10**	
Internet						
Mantenimiento preventivo y correctivo de hardware y software	9	9	9	10	10	
[E.1] Errores de los usuarios	7	7	7			7.0
[E.2] Errores del administrador del sistema / de la seguridad	8	8	8			8.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	7					7.0
[E.19] Fugas de información			7			7.0
[E.24] Caída del sistema por agotamiento de recursos	9					9.0

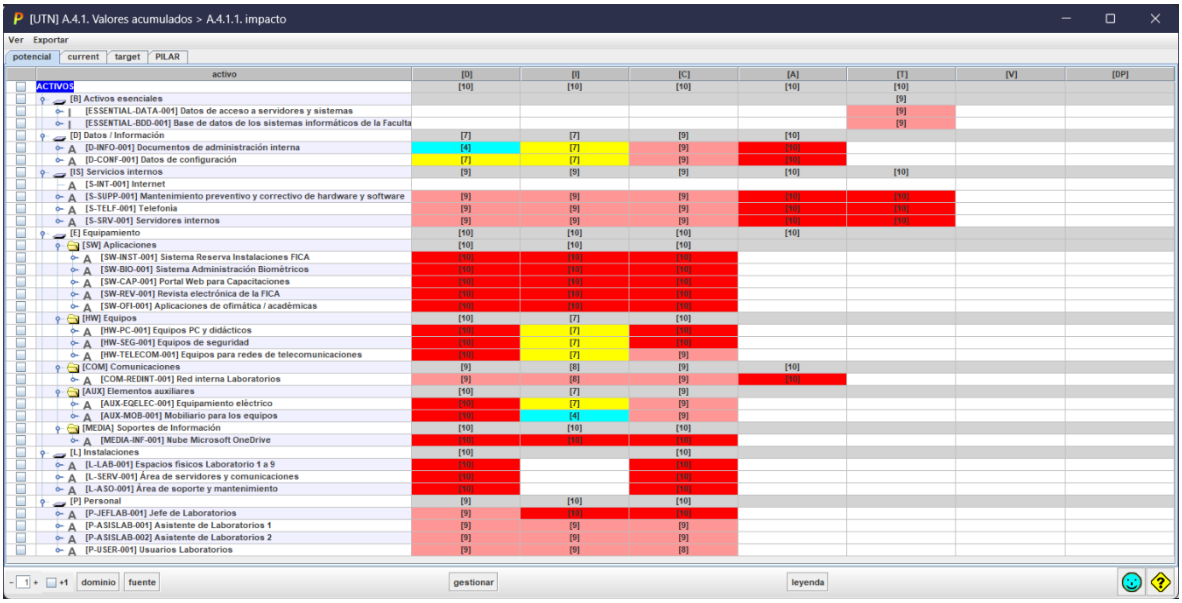
[A.5] Suplantación de identidad		9	9	10		9.3
[A.6] Abuso de privilegios de acceso	4	7	7	10		7.0
[A.7] Uso no previsto	4	7	7			6.0
[A.11] Acceso no autorizado		7	9	10		8.7
[A.13] Repudio (negación de actuaciones)					10	10.0
[A.15] Modificación de la información		9				9.0
[A.18] Destrucción de la información	9					9.0
[A.24] Denegación de servicio	9					9.0
Telefonía	9	9	9	10	10	
[E.1] Errores de los usuarios	7	7	7			7.0
[E.2] Errores del administrador del sistema / de la seguridad	8	8	8			8.0
[E.15] Alteración de la información		4				4.0

Nota: La tabla muestra el impacto acumulado, en donde D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

En la Figura 42 se presenta el impacto potencial acumulado en el software PILAR.

Figura 42

Impacto potencia acumulado de afectación de activos en los laboratorios de informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

Impacto potencial repercutido: Se tiene en cuenta el valor propio del activo y las amenazas a las que están expuestos los activos que dependen de él.

$$Impacto\ potencia\ repercutido = \%\ Degradación\ de\ amenaza\ \times Valor\ propio\ del\ activo$$

El cálculo del impacto potencial repercutido se encuentra en la Tabla 34.

Tabla 34

Impacto potencial repercutido de afectación de activos en los laboratorios de informática FICA-UTN

	IMPACTO POTENCIAL REPERCUTIDO					PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	**A**	**T**	
Datos de acceso a servidores y sistemas	9	9	10	10	9	9.4
Base de datos de los sistemas informáticos de la Facultad	10	10	8	10	10	9.6
Documentos de administración interna	4	7	9	10		7.5
Datos de configuración	7	7	9	10		8.3
Internet						
Mantenimiento preventivo y correctivo de hardware y software	9	9	9	10	10	9.4
Telefonía	9	9	9	10	10	9.4
Servidores internos	9	9	9	10	10	9.4
Sistema reserva instalaciones FICA	10	10	10			10.0
Aplicación para el manejo de biométricos	10	10	10			10.0
Portal Web para Capacitaciones	10	10	10			10.0
Revista electrónica de la FICA	10	10	10			10.0
Aplicaciones de ofimática / académicas	10	10	10			10.0
Equipos PC / didácticos	10	7	10			9.0
Equipos de seguridad	10	7	10			9.0
Equipos para redes de telecomunicaciones	10	7	9			8.7
Red interna laboratorios	9	8	9	10		9.0
Equipamiento eléctrico	10	7	9			8.7
Mobiliario para los equipos	10	4	9			7.7
Nube Microsoft OneDrive	10	10	10			10.0
Espacios físicos Lab 1 a 9	10		10			10.0
Área de servidores y comunicaciones	10		10			10.0
Área de soporte y mantenimiento	10		10			10.0
Jefe de Laboratorios	9	10	10			9.7
Asistente de Laboratorios 1	9	9	9			9.0

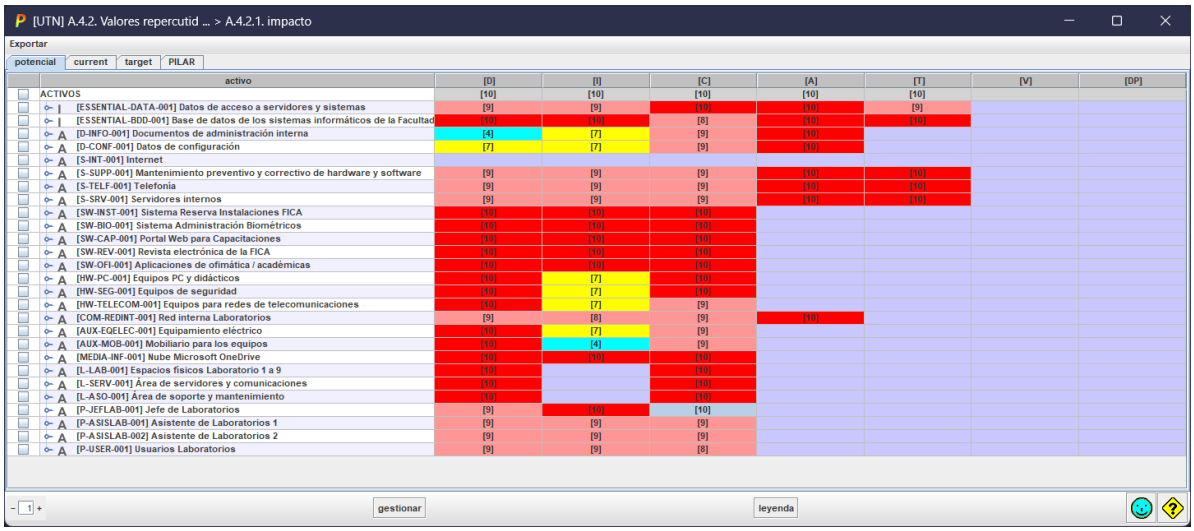
Asistente de Laboratorios 2	9	9	9			9.0
Usuarios Laboratorios	9	9	8			8.7

Nota: La tabla presenta una muestra del listado del impacto potencial repercutido de los activos identificados en los laboratorios de informática FICA-UTN. D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

En la Figura 43 se presenta el impacto potencial repercutido para cada activo de los laboratorios de informática FICA-UTN.

Figura 43

Impacto potencial repercutido de afectación de activos en los laboratorios de informática FICA-UTN en el software PILAR

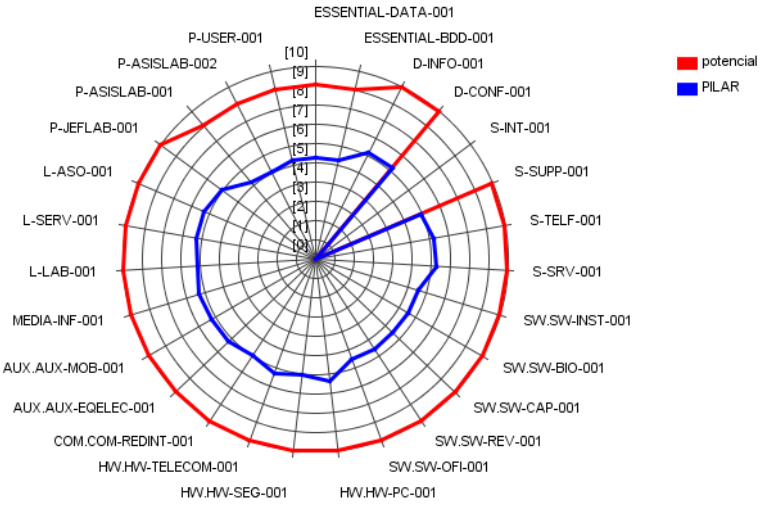


Nota: Elaboración propia.

En la Figura 44 se presenta un gráfico en el cual la línea roja representa los valores de impacto acumulado potencial actual para cada activo, mientras que la línea azul representa los valores recomendados por PILAR.

Figura 44

Gráfico de valores de impacto potencial acumulado de afectación de activos de los laboratorios de informática FICA-UTN



Nota: Elaboración propia

El impacto potencial acumulado al calcularse sobre el valor acumulado de los activos del sistema permite la determinación de las salvaguardas en el proceso de gestión de riesgos. Mientras que el impacto potencial repercutido al calcularse sobre el valor propio de los activos permite determinar solamente las consecuencias de las incidencias de amenazas.

3.2.7. Determinación del riesgo potencial

Una vez calculado el impacto potencial, se determinó el riesgo potencial, el cual es la medida de daño teniendo en cuenta la probabilidad de ocurrencia. El riesgo es proporcional al impacto y probabilidad. Su relación se aprecia en la Tabla 35.

Tabla 35

Niveles de Riesgo

IMPACTO	MA	Media	Alta	Muy alta	Crítico	Crítico
	A	Baja	Media	Alta	Muy alta	Crítico
	M	Muy baja	Baja	Media	Alta	Muy alta
	B	Aceptable	Muy baja	Baja	Media	Alta
	MB	Aceptable	Aceptable	Muy baja	Baja	Media
		MB	B	M	A	M A
	PROBABILIDAD					

Nota: Adaptado de “Risk management methodology in the supply chain: a case study applied” (p.1058), por Hermoso & Garzón, 2021, Annals of Operations Research, 2 (313).

El cálculo del valor del riesgo se lo realizó para cada activo, por cada amenaza y en cada dimensión de valoración.

Dicho riesgo se lo puede realizar desde dos enfoques:

Riesgo potencial acumulado: Se tiene en cuenta el valor acumulado del impacto sobre el activo debido a una amenaza, y la probabilidad de amenaza. La ecuación para su cálculo es el siguiente:

$$Riesgo\ potencial\ acumulado = \ Probabilidad\ \ de\ amenaza\ \times Valor\ acumulado\ del\ impacto$$

El cálculo del riesgo potencial acumulado se encuentra en el Anexo H, mientras que la Tabla 36 presenta una muestra de dicha lista.

Tabla 36

Riesgo potencial acumulado de afectación de activos en los laboratorios de informática FICA-UTN

	IMPACTO POTENCIAL ACUMULADO					PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	**A**	**T**	
ACTIVOS ESENCIALES					**6.3**	
Datos de acceso a servidores y sistemas					**6.3**	
[A.13] Repudio (negación de actuaciones)					6.3	6.3
Base de datos biométricos					**6.3**	
[A.13] Repudio (negación de actuaciones)					6.3	6.3
DATOS / INFORMACIÓN	**5.9**	**6.8**	**8.1**	**7.7**		
Documentos de administración interna	**4.2**	**6.8**	**8.1**	**7.7**		
[E.15] Alteración de la información		3.3				3.3
[E.18] Destrucción de la información	3.3					3.3
[E.19] Fugas de información			5.1			5.1
[A.5] Suplantación de identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			5.8
[A.11] Acceso no autorizado		6.8	8.1			7.5
Datos de configuración	**5.9**	**6.8**	**8.1**	**7.7**		
[E.4] Errores de configuración		3.3				3.3
[E.15] Alteración de la información		3.3				3.3
[E.18] Destrucción de la información	3.3					3.3
[E.19] Fugas de información			5.1			5.1

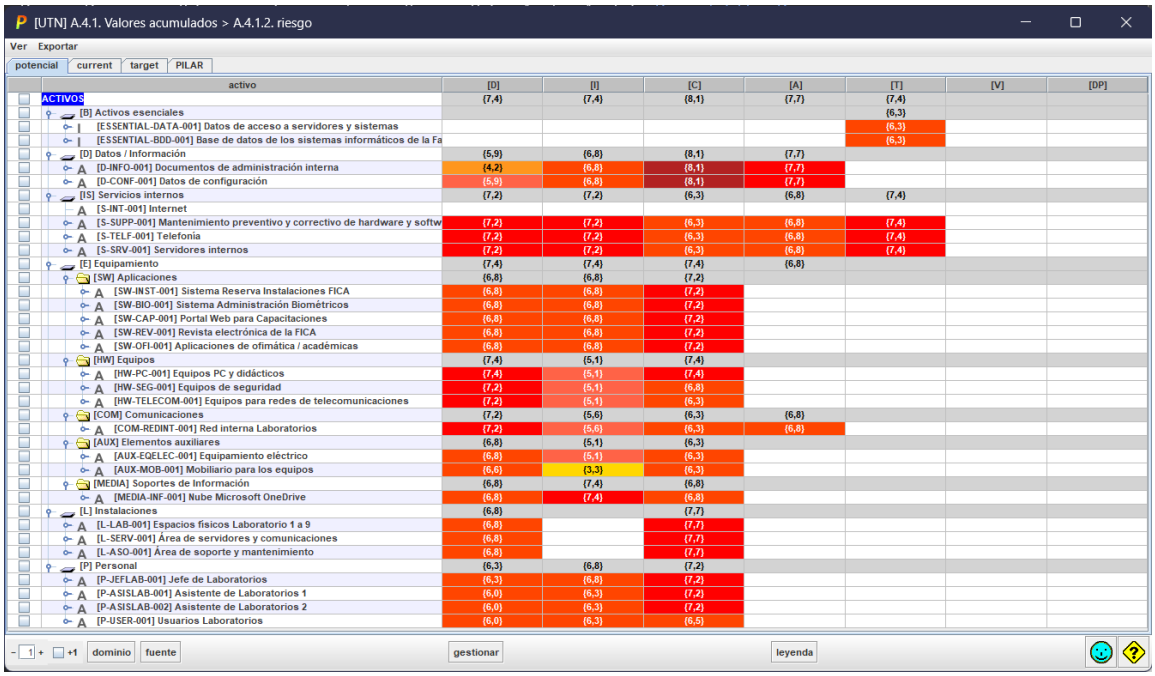
[A.4] Manipulación de los ficheros de configuración	5.9	5.9	5.9			5.9
[A.5] Suplantación de identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			5.8
[A.11] Acceso no autorizado		6.8	8.1			7.5
SERVICIOS	**7.2**	**7.2**	**6.3**	**6.8**	**7.4**	
Internet						
Mantenimiento preventivo y correctivo de hardware y software	**7.2**	**7.2**	**6.3**	**6.8**	**7.4**	
[E.1] Errores de los usuarios	5.1	5.1	5.1			5.1
[E.2] Errores del administrador del sistema / de la seguridad	5.6	5.6	5.6			5.6
[E.15] Alteración de la información		3.3				3.3

Nota: La tabla muestra el cálculo del riesgo potencial acumulado, en donde D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

En la Figura 45 se presenta los valores de riesgo potencial acumulado en el software PILAR para cada activo.

Figura 45

Riesgo potencial acumulado de afectación de activos en los laboratorios de informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

Riesgo potencial repercutido: Se tiene en cuenta el valor repercutido del impacto sobre el activo debido a una amenaza, y la probabilidad de amenaza. La ecuación para su cálculo es el siguiente:

$$Riesgo\ potencial\ repercutido = \ Probabilidad\ \ de\ amenaza\ \times Valor\ repercutido\ del\ impacto$$

El cálculo del riesgo potencial repercutido se encuentra en la Tabla 37.

Tabla 37

Riesgo potencial repercutido de afectación de activos en los laboratorios de informática FICA-UTN

	IMPACTO POTENCIAL REPERCUTIDO					PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	**A**	**T**	
Datos de acceso a servidores y sistemas	6.9	7.1	8.1	7.7	7.1	7.4
Base de datos de los sistemas informáticos de la Facultad	7.4	7.7	6.9	7.7	7.7	7.5
Documentos de administración interna	4.2	6.8	8.1	7.7		6.7
Datos de configuración	5.9	6.8	8.1	7.7		7.1
Internet						
Mantenimiento preventivo y correctivo de hardware y software	7.2	7.2	6.3	6.8	7.4	7.0
Telefonía	7.2	7.2	6.3	6.8	7.4	7.0
Servidores internos	7.2	7.2	6.3	6.8	7.4	7.0
Sistema reserva instalaciones FICA	6.8	6.8	7.2			6.9
Aplicación para el manejo de biométricos	6.8	6.8	7.2			6.9
Portal Web para Capacitaciones	6.8	6.8	7.2			6.9
Revista electrónica de la FICA	6.8	6.8	7.2			6.9
Aplicaciones de ofimática / académicas	6.8	6.8	7.2			6.9
Equipos PC / didácticos	7.4	5.1	7.4			6.6
Equipos de seguridad	7.2	5.1	6.8			6.4
Equipos para redes de telecomunicaciones	7.2	5.1	6.3			6.2
Red interna laboratorios	7.2	5.6	6.3	6.8		6.5
Equipamiento eléctrico	6.8	5.1	6.3			6.1
Mobiliario para los equipos	6.6	3.3	6.3			5.4
Nube Microsoft OneDrive	6.8	7.4	6.8			7.0

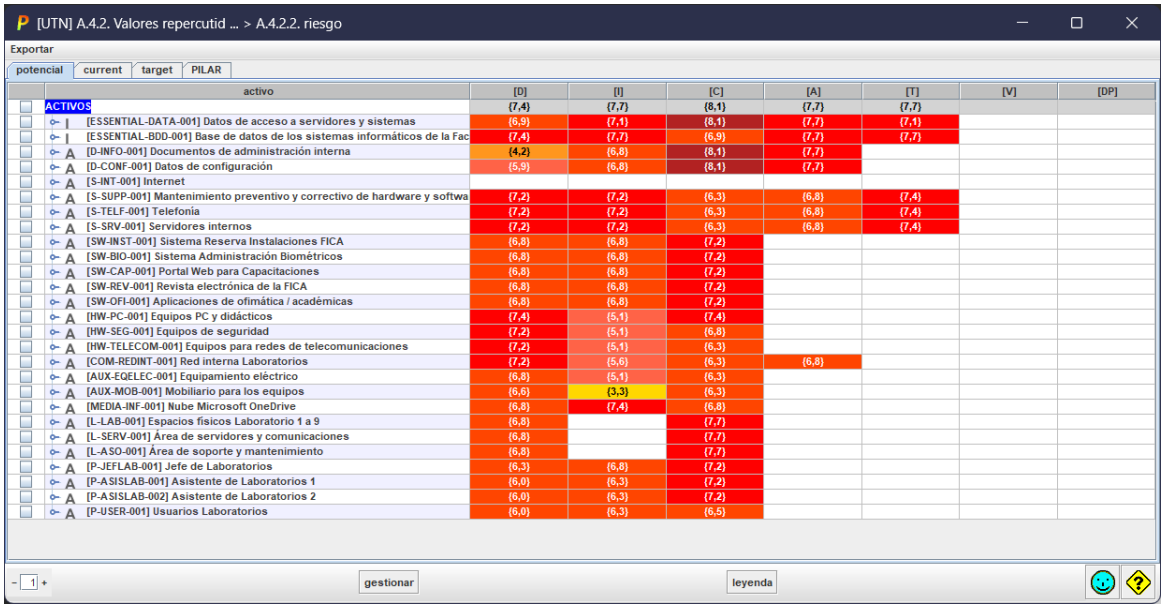
Espacios físicos Lab 1 a 9	6.8		7.7	7.3
Área de servidores y comunicaciones	6.8		7.7	7.3
Área de soporte y mantenimiento	6.8		7.7	7.3
Jefe de Laboratorios	6.3	6.8	7.2	6.8
Asistente de Laboratorios 1	6	6.3	7.2	6.5
Asistente de Laboratorios 2	6	6.3	7.2	6.5
Usuarios Laboratorios	6	6.3	6.5	6.3

Nota: La tabla muestra el cálculo del riesgo potencial repercutido, D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

En la Figura 46 se presenta los valores de riesgo potencial repercutido en el software PILAR para cada activo.

Figura 46

Riesgo potencial repercutido de afectación de activos en los laboratorios de informática FICA-UTN en el software PILAR

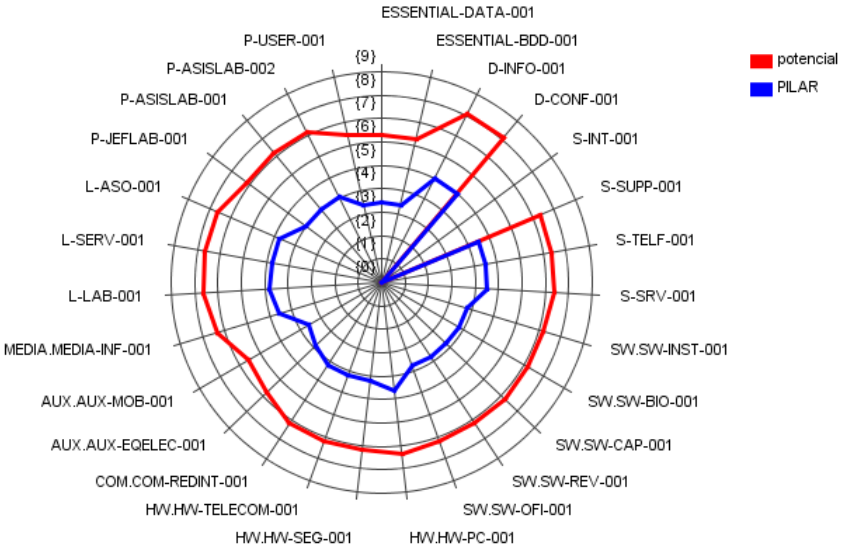


Nota: Elaboración propia.

En la Figura 47 se presenta un gráfico en el cual la línea roja representa los valores de riego potencial acumulado actual para cada activo, mientras que la línea azul representa los valores recomendados por PILAR.

Figura 47

Gráfico valores de riesgo acumulado de afectación de activos de los laboratorios de informática FICA-UTN



Nota: Elaboración propia

El riesgo potencial acumulado al calcularse sobre el valor acumulado de los activos del sistema permite la determinación de las salvaguardas en el proceso de gestión de riesgos. Mientras que el riesgo potencial repercutido al calcularse sobre el valor propio de los activos permite determinar solamente las consecuencias de las incidencias de amenazas.

3.2.8. Identificación de Salvaguardas

El paso previo a la identificación de Salvaguardas es la estandarización de amenazas dependiendo los riesgos potenciales acumulados (Anexo H) de mayor peso identificados. Para este paso se tomó en cuenta el promedio de pesos relacionados con los riesgos tecnológicos como: software malicioso, acceso no autorizado, alteración de la información, etc. El valor establecido fue de 6,5, resultando en una recolección de 97 riesgos. La recopilación se encuentra en el Anexo I. Mientras que la Tabla 38 ya presenta el listado de las amenazas junto con los activos afectados.

Tabla 38

Riesgos de peso mayor identificados en los laboratorios de informática FICA-UTN

# ACTIVO	ACTIVOS	AMENAZA	PESO PONDERADO
1	Espacios físicos Lab 1 a 20	[A.25] Robo de equipos	7.7
2	Área de servidores y comunicaciones	[A.25] Robo de equipos	7.7
3	Área de soporte y mantenimiento	[A.25] Robo de equipos	7.7
4	Documentos de administración interna	[A.11] Acceso no autorizado	7.5
5	Datos de configuración	[A.11] Acceso no autorizado	7.5
6	Mantenimiento preventivo y correctivo de hardware y software	[A.13] Repudio (negación de actuaciones)	7.4
7	Telefonía	[A.13] Repudio (negación de actuaciones)	7.4
8	Servidores internos	[A.13] Repudio (negación de actuaciones)	7.4
9	Equipos PC / didácticos	[E.25] Pérdida de equipos	7.4
10	Equipos PC / didácticos	[A.25] Robo de equipos	7.4
11	Nube Microsoft OneDrive	[A.15] Modificación de la información	7.4
12	Mantenimiento preventivo y correctivo de hardware y software	[E.24] Caída del sistema por agotamiento de recursos	7.2
13	Mantenimiento preventivo y correctivo de hardware y software	[A.15] Modificación de la información	7.2
14	Mantenimiento preventivo y correctivo de hardware y software	[A.24] Denegación de servicio	7.2
15	Telefonía	[E.24] Caída del sistema por agotamiento de recursos	7.2
16	Telefonía	[A.15] Modificación de la información	7.2
17	Telefonía	[E.24] Caída del sistema por agotamiento de recursos	7.2
18	Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	7.2
19	Servidores internos	[A.15] Modificación de la información	7.2
20	Servidores internos	[A.24] Denegación de servicio	7.2
21	Equipos PC / didácticos	[E.24] Caída del sistema por agotamiento de recursos	7.2
22	Equipos de seguridad	[E.24] Caída del sistema por agotamiento de recursos	7.2
23	Equipos para redes de telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	7.2
24	Red interna laboratorios	[A.24] Denegación de servicio	7.2

25	Jefe de Laboratorios	[A.19] Revelación de información	7.2

Nota: Elaboración propia.

De esta manera se redujo de 286 riesgos a 97 que están distribuidos entre 25 tipos.

La Norma ISO 31000 en su apartado de Tratamiento de Riesgos, considera tres opciones de tratamiento, estos se encuentran en la Tabla 39.

Tabla 39

Opciones de Tratamiento del Riesgo según la Norma ISO 31000

Tratamiento	Definición
Evitar	Evitar el riesgo decidiendo eliminar las condiciones que hacen viable su materialización, abarca actividades como: • No iniciar o continuar con la actividad que genera el riesgo • Eliminar la fuente del riesgo (procesos o equipos)
Minimizar	Abarca tareas como: • Modificar la degradación (impacto) o la probabilidad de ocurrencia (frecuencia) • Compartir el riesgo para diversificar el coste de consecuencias
Aceptar o Retener	Significa aceptar o aumentar el riesgo en busca de obtener una oportunidad de solución

Nota: Elaboración propia a partir de *Guía para la aplicación de UNE-ISO 31000:2018 (1st ed.)* (pp.173-175), por Bonet et al, 2019. Asociación Española de Normalización y Certificación.

A los 25 tipos riesgos se asignó una opción de tratamiento según la severidad de su naturaleza. Esta asignación se la puede apreciar en el Anexo J, mientras que la Tabla 40 presenta una muestra de dicho anexo.

Tabla 40

Asignación de opción de tratamiento a los riesgos identificados en los laboratorios de informática FICA-UTN

RIESGO	ACTIVO AFECTADO	TRATAMIENTO
[A.11] Acceso no autorizado	Documentos de administración interna	Minimizar
	Datos de configuración	
[A.13] Repudio (negación de actuaciones)	Mantenimiento preventivo y correctivo de hardware y software	Minimizar
	Telefonía	
	Servidores internos	
[A.15] Modificación de la información	Nube Microsoft OneDrive	Minimizar
	Mantenimiento preventivo y correctivo de hardware y software	
	Telefonía	

	Servidores internos	
[A.18] Destrucción de la información	Nube Microsoft OneDrive	Evitar
[A.19] Revelación de información	Jefe de Laboratorios	Evitar
	Asistente de Enseñanza de los laboratorios 7	
	Asistente de Enseñanza de los laboratorios 8	
	Usuarios Laboratorios	
[A.22] Manipulación de programas	Sistema reserva instalaciones FICA	Minimizar
	Aplicación para el manejo de biométricos	
	Portal Web para Capacitaciones	
	Portal Web para Capacitaciones	
	Aplicaciones de ofimática / académicas	
[A.24] Denegación de servicio	Mantenimiento preventivo y correctivo de hardware y software	Minimizar
	Servidores internos	
	Equipos PC / didácticos	
	Equipos de seguridad	
	Equipos para redes de telecomunicaciones	
[A.25] Robo de equipos	Espacios físicos Lab 1 a 20	Minimizar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
	Equipos PC / didácticos	
	Equipamiento eléctrico	
	Equipos de seguridad	

Nota: Elaboración propia.

Una vez asignadas las opciones de tratamiento de los riesgos, se puede tener presente que salvaguardas tienen prioridad en la gestión de riesgos. Estas salvaguardas son aquellas actividades que minimizan el riesgo. En el segundo escrito “Catálogo de Elementos” se presenta distintos tipos de salvaguardas para cada tipo de activo.

Para determinar las salvaguardas es necesario tener en cuenta varios aspectos como:

- Tipo de activo a proteger
- Amenazas de las que se necesita protección
- Salvaguardas alternativas

Además, se tomó en cuenta el principio de proporcionalidad en cuanto a los valores de los activos y la probabilidad de ocurrencia de las amenazas.

Los tipos de protecciones ofrecidas por las salvaguardas son:

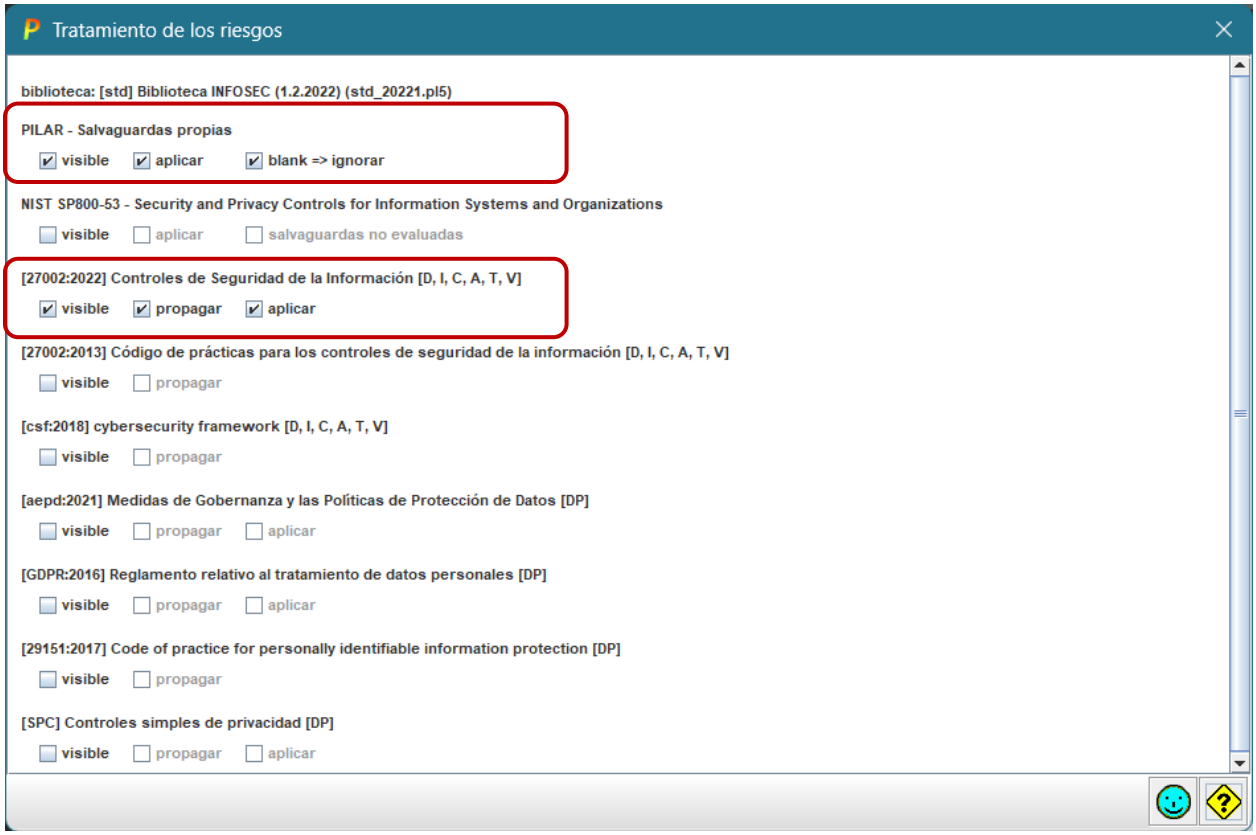
- [PR] Prevención: reduce las oportunidades de que un incidente ocurra.

- [DS] Disuasión: evita que el atacante se atreva a atacar.
- [EL] Eliminación: elimina el incidente impidiendo que este tenga lugar.
- [IM] Minimización del impacto: acota las consecuencias de un incidente.
- [CR] Corrección: repara el daño ya producido.
- [RC] Recuperación: permite regresar al estado anterior al incidente.
- [MN] Monitorización: monitoriza los incidentes ocurridos y que ocurren para anticiparse a los incidentes.
- [DC] Detección: detecta el ataque e informa de que está ocurriendo.
- [AW] Concienciación: formación de personas relacionadas con el sistema.
- [AD] Administración: son los componentes de seguridad del sistema.

La herramienta PILAR permite varias modificaciones en su configuración para modelar la gestión del riesgo según las necesidades de la organización. En este caso, para optar cumplir con la necesidad de un estándar de seguridad, en la configuración de “Tratamiento del Riesgo” (salvaguardas) se hizo uso de las salvaguardas propias de PILAR, además de la Norma ISO/IEC 27002:2022 referente a la Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información en las dimensiones de Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad. Dicha configuración se observa en la Figura 48.

Figura 48

Selección Estándar de Seguridad para el Tratamiento de Riesgos en el software PILAR

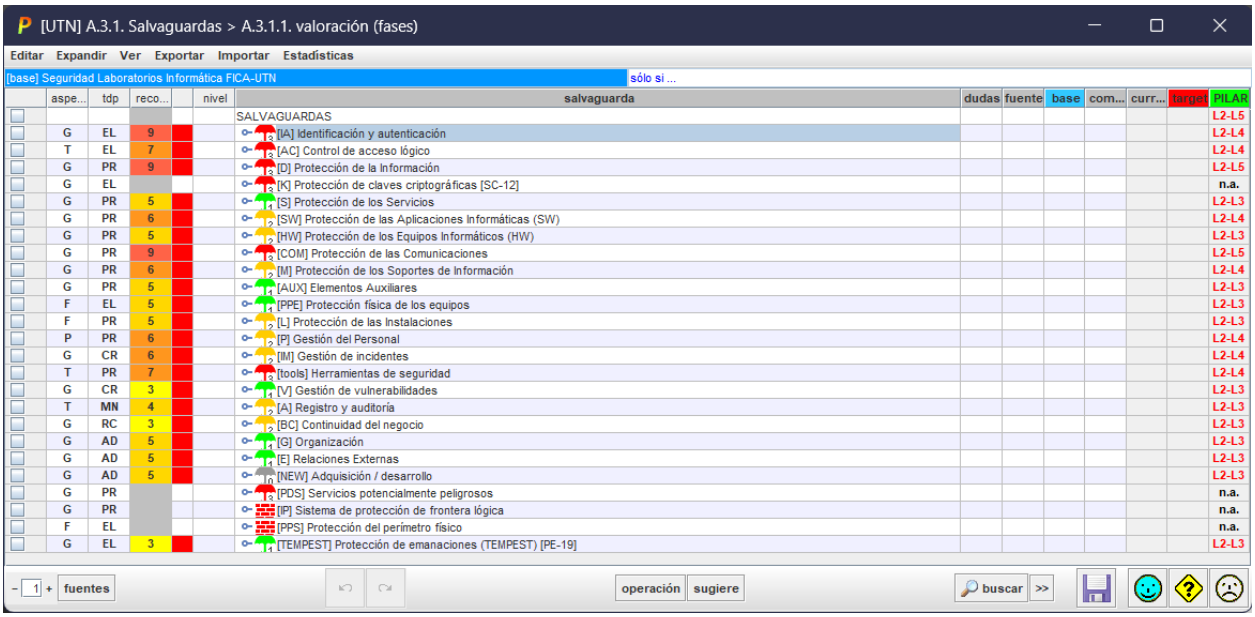


Nota: Elaboración propia.

Dependiendo la selección de los estándares de Seguridad para el tratamiento de riesgos, la metodología MAGERIT propone diversas salvaguardas, en este caso específico se han identificado 25 salvaguardas, estas se aprecian en la Figura 49.

Figura 49

Identificación de salvaguardas para los laboratorios de informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

Una amenaza puede ser controlada por varios tipos de salvaguardas, para el correcto cumplimiento de estas salvaguardas es necesario proponer diversas tareas que mitiguen la amenaza. En el Anexo K se presenta el listado de activos, amenazas, tipo de salvaguarda y tareas propuestas para su cumplimiento, mientras que en la Tabla 41 se presenta una muestra de este listado.

Tabla 41

Identificación de Tareas por Salvaguardas para los laboratorios de informática FICA-UTN

RIESGO	ACTIVO AFECTADO	TRATAMIENTO	SALVAGUARDA	TIPO DE PROTECCIÓN	TAREA PROPUESTA
[A.11] Acceso no autorizado	Documentos de administración interna	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
	Datos de configuración		[IA] Identificación y autenticación	EL	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario
[A.13] Repudio (negación de actuaciones)	Mantenimiento preventivo y correctivo de hardware y software	Minimizar	[G] Organización	AD	Establecimiento de una normativa para el uso de firmas electrónicas en documentos
	Telefonía		[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras
	Servidores internos		[K] Protección de claves criptográficas	EL	Implementación del cifrado hash para el almacenamiento de contraseñas
[A.15] Modificación de la información	Nube Microsoft OneDrive	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN
	Mantenimiento preventivo y correctivo de hardware y software		[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN
	Telefonía		[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN
	Servidores internos		[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN

[A.18] Destrucción de la información	Nube Microsoft OneDrive	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de almacenamiento
[A.19] Revelación de información	Jefe de Laboratorios	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN
	Asistente de Enseñanza de los laboratorios 7		[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN
	Asistente de Enseñanza de los laboratorios 8		[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN
	Usuarios Laboratorios		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos

Nota: Elaboración propia.

Las tareas fueron propuestas a manera de que se pueda atacar a más de una amenaza, se realizó la recopilación de estas obteniendo un total de 33 tareas, distribuidas entre 17 de los 25 tipos de salvaguardas aplicables a este caso de estudio. Estas tareas fueron revisadas por los encargados de los laboratorios de informática FICA-UTN para determinar si alguna de estas tareas ya está implantada. Esta información se la encuentra en la Tabla 42.

Tabla 42

Sintetización de Tareas propuestas para el cumplimiento de salvaguardas en los laboratorios de informática FICA-UTN

SALVAGUARDA	TIPO DE PROTECCIÓN	TAREA PROPUESTA	¿EXISTE?
[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de almacenamiento	SI
[AUX] Elementos auxiliares	PR	Corrección de la carga de dispositivos electrónicos en la distribución de red eléctrica	NO

[V] Gestión de vulnerabilidades	PR	Desarrollar un manual de emergencia para las redes eléctricas	SI
[SW] Protección de las aplicaciones informáticas	CR	Desarrollo de la documentación de programas y archivos	NO
[V] Gestión de vulnerabilidades	MI	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)	NO
[AUX] Elementos auxiliares	IM	Desarrollo de un Plan de Emergencia en caso de fallas eléctricas	NO
[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN	NO
[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos	NO
[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte	NO
[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)	/
[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)	/
[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware	/
[V] Gestión de vulnerabilidades	CR	Establecimiento de políticas de uso para los usuarios de los laboratorios de informática FICA-UTN	SI
[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)	/
[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software	SI
[S] Protección de los servicios	PR	Establecimiento de un Plan de renovación de equipos de hardware por vida útil	NO
[BC] Continuidad del negocio	RC	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques	NO
[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware	/
[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware	/
[G] Organización	AD	Establecimiento de una normativa para el uso de firmas electrónicas en documentos	/

[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos	NO
[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores	SI
[BC] Continuidad del negocio	RC	Implantación de un software de antivirus y antimalware efectivo	/
[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN	NO
[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones	SI
[IP] Sistema de protección de frontera lógica	PR	Implementación de firewall para la red interna de los laboratorios de informática FICA-UTN	SI
[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras	/
[SW] Protección de las aplicaciones informáticas	PR	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)	NO
[AUX] Elementos auxiliares	PR	Implementación de UPS para mantener operativos los servicios	/
[K] Protección de claves criptográficas	EL	Implementación del cifrado hash para el almacenamiento de contraseñas	NO
[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores	/
[PPE] Protección física de los equipos	EL	Instalación de equipo de aire acondicionado para evitar recalentamiento de equipos	NO
[IA] Identificación y autenticación	EL	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario	SI

Nota: Los valores en "¿Existente?" son; Si: Ya existe un proceso relacionado a esa tarea de salvaguarda, No: No existe un proceso relacionado a esa tarea de salvaguarda, /: Existe un proceso que no es óptimo para cumplir con esa tarea de salvaguarda. *Elaboración propia.*

Para finalizar la identificación de salvaguardas, se tomará aquellas que no existan o que tengan un proceso que no sea óptimo, el recuento es de 25 tareas que serán explicadas brevemente en el Anexo L a manera de Tabla con presupuestos, personal y tiempos estimados con base en referencias de consultas de internet.

La implementación de todas estas tareas tendría un costo aproximado $39,100.00, mientras que el tiempo es variable si se decide realizar una implementación con varias tareas a la vez.

3.2.9. Valoración de Salvaguardas

Una vez presentes las tareas propuestas para el cumplimiento de salvaguardas, es necesario determinar la eficiencia que tienen.

La eficacia de las salvaguardas dependerá de que tan idóneas sean y que tan bien implantadas estén. En la Tabla 43 se aprecia el grado de eficacia de las salvaguardas.

Tabla 43

Eficacia de las salvaguardas

Factor	Nivel	Significado
0%	L0	Inexistente
20%	L1	Inicial / ad hoc
40%	L2	Reproducible, pero intuitivo
60%	L3	Proceso definido
80%	L4	Gestionable y medible
100%	L5	Optimizado

Nota: Tomada de *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 Método* (p.34), por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

La valoración de eficacia se realizó en dos dimensiones: actual y proyección. La actual hace referencia al valor actual de la salvaguarda en caso de estar implementada, y la Proyección es el valor que se espera obtener cuando se la implemente. Estas valoraciones fueron determinadas en conjunto con el equipo responsable de los laboratorios de informática FICA-UTN, y se pueden apreciar en la Tabla 44.

Tabla 44

Valoración eficacia de tareas para las salvaguardas en laboratorios de informática FICA-UTN

N	TAREAS PROPUESTAS	ACTUAL	OBJETIVO
1	Aseguramiento de respaldos de información en el servicio de almacenamiento	2	3
2	Corrección de la carga de dispositivos electrónicos en la distribución de red eléctrica	0	3
3	Desarrollar un manual de emergencia para las redes eléctricas	2	3
4	Desarrollo de la documentación de programas y archivos	0	2
5	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)	0	2
6	Desarrollo de un Plan de Emergencia en caso de fallas eléctricas	0	4
7	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN	0	4
8	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos	0	4
9	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte	0	3
10	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)	1	4
11	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)	1	3
12	Establecimiento de buenas prácticas para la adquisición de Hardware	1	4
13	Establecimiento de políticas de uso para los usuarios de los laboratorios de informática FICA-UTN	2	2
14	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)	1	3
15	Establecimiento de un Plan de Mantenimiento de Hardware y Software	2	4
16	Establecimiento de un Plan de renovación de equipos de hardware por vida útil	0	3
17	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques	0	3
18	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware	1	4
19	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware	1	4
20	Establecimiento de una normativa para el uso de firmas electrónicas en documentos	1	3
21	Establecimiento de una normativa para imponer sanciones ante daños a los activos	0	4
22	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores	2	3

23	Implantación de un software de antivirus y antimalware efectivo	1	3
24	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN	0	3
25	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones	2	3
26	Implementación de firewall para la red interna de los laboratorios de informática FICA-UTN	2	3
27	Implementación de registro de actividades mediante bitácoras	1	3
28	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)	0	2
29	Implementación de UPS para mantener operativos los servicios	1	3
30	Implementación del cifrado hash para el almacenamiento de contraseñas	0	3
31	Instalación de detectores de humo, alarmas contra incendios, extintores	1	3
32	Instalación de equipo de aire acondicionado para evitar recalentamiento de equipos	0	2
33	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario	2	3

Nota: Elaboración propia.

Una vez valoradas las tareas propuestas, se puede sacar un promedio de las tareas correspondientes a cada salvaguarda, para obtener la valoración general de estas. Esta valoración se encuentra en la Tabla 45.

Tabla 45

Valoración eficacia las salvaguardas en laboratorios de informática FICA-UTN

N	SALVAGUARDA	ACTUAL	OBJETIVO
1	[A] Registro y auditoría	0	3
2	[AC] Control de acceso lógico	0	3
3	[AUX] Elementos auxiliares	1	3
4	[BC] Continuidad del negocio	1	3
5	[D] Protección de la información	1	4
6	[HW] Protección de los equipos informáticos	0	4
7	[G] Organización	2	2
8	[IA] Identificación y autenticación	2	4
9	[K] Protección de claves criptográficas	3	3
10	[P] Gestión del Personal	0	3

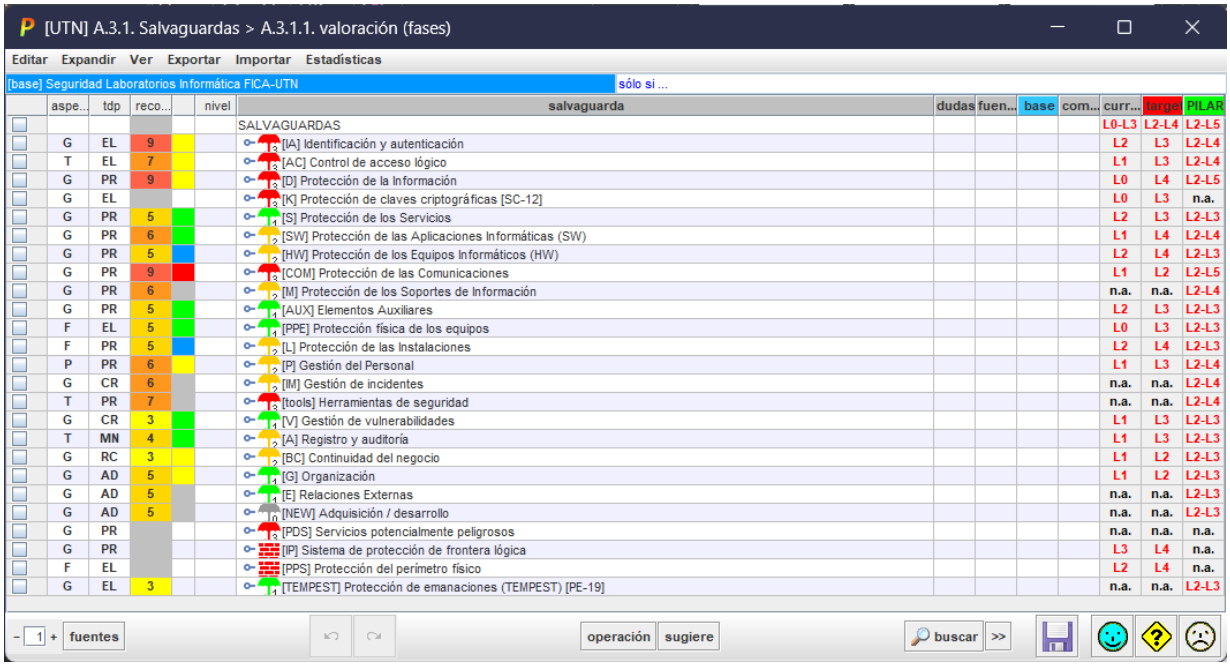
11	[L] Protección de las instalaciones	4	4
12	[IP] Sistema de protección de frontera lógica	0	4
13	[PPW] Protección física de los equipos	1	3
14	[PSS] Protección del perímetro físico	4	4
15	[S] Protección de los servicios	2	3
16	[SW] Protección de las aplicaciones informáticas	0	4
17	[V] Gestión de vulnerabilidades	1	3

Nota: Elaboración propia.

De igual manera, en la Figura 50 se puede observar que el software PILAR permite el ingreso de estos valores, además de proponer uno recomendado, y así poder obtener un resultado a manera de gráfico para el cálculo del impacto y riesgo residual.

Figura 50

Valoración de eficacia de salvaguardas de los laboratorios de informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

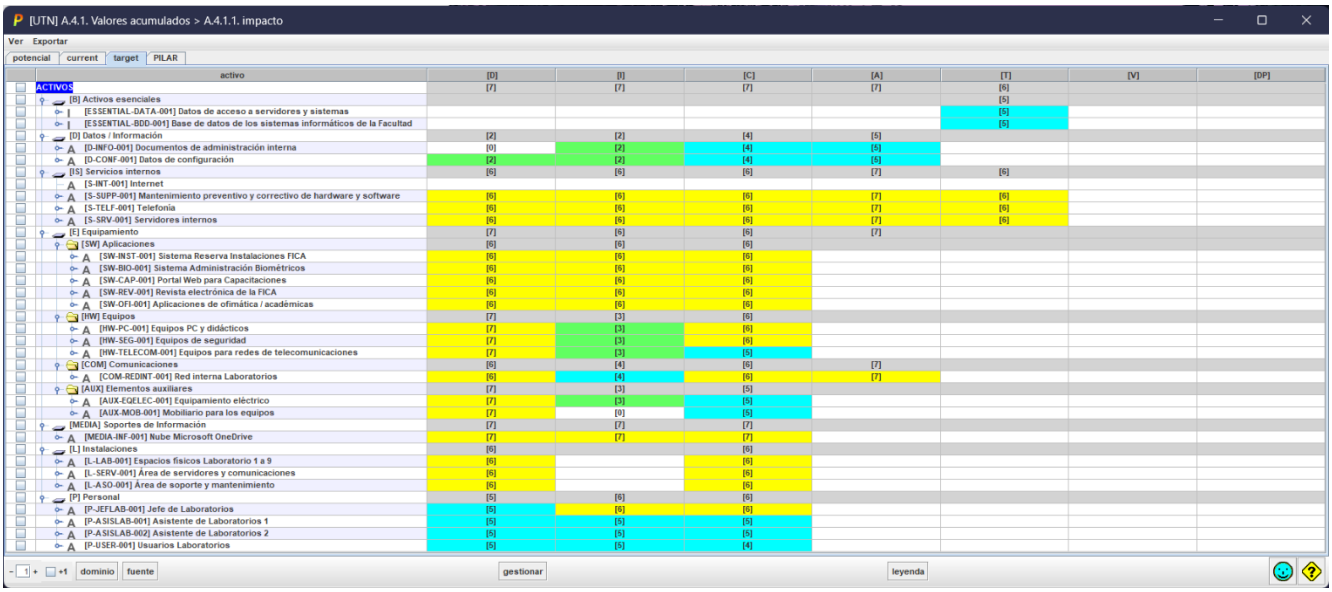
3.2.10. Estimación del Impacto Residual

Si se llega a desplegar las tareas propuestas para el cumplimiento de las salvaguardas, el sistema modifica su impacto potencial (original) a un impacto residual. A razón de que el software PILAR simula que las salvaguardas fueron implementadas, ofreció una valoración del impacto residual acumulado y el impacto residual repercutido.

El impacto residual acumulado se lo presenta en la Figura 51, mientras que el impacto residual repercutido en la Figura 52.

Figura 51

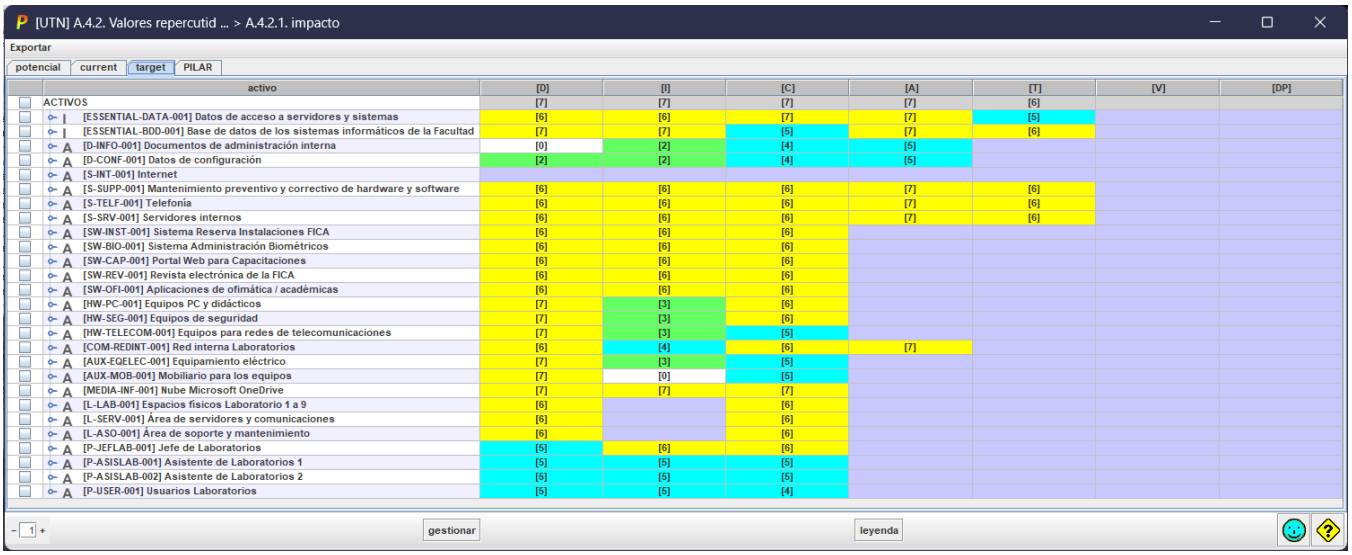
Impacto residual acumulado de afectación de activos de los laboratorios de informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

Figura 52

Impacto residual repercutido de afectación de activos de los laboratorios de informática FICA-UTN en el software PILAR

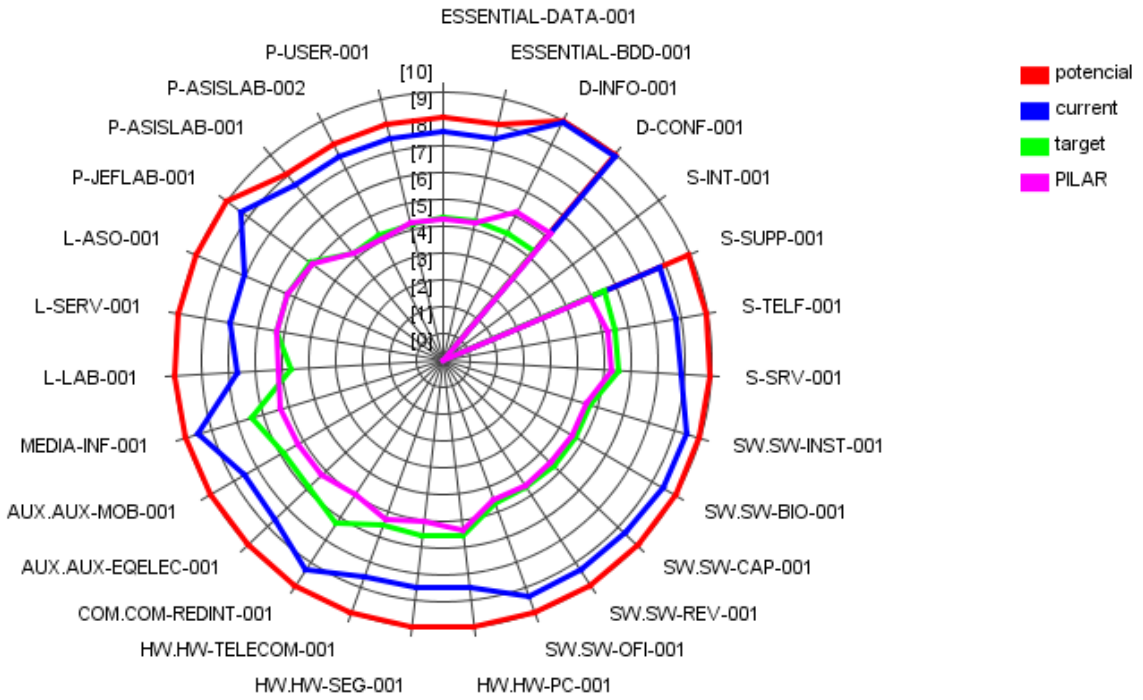


Nota: Elaboración propia.

En la Figura 53 se presenta el gráfico resumen de los impactos potencial, actual, objetivo y recomendado por el software PILAR.

Figura 53

Gráfico valores de impactos de afectación de activos de los laboratorios de informática FICA-UTN



Nota: Elaboración propia

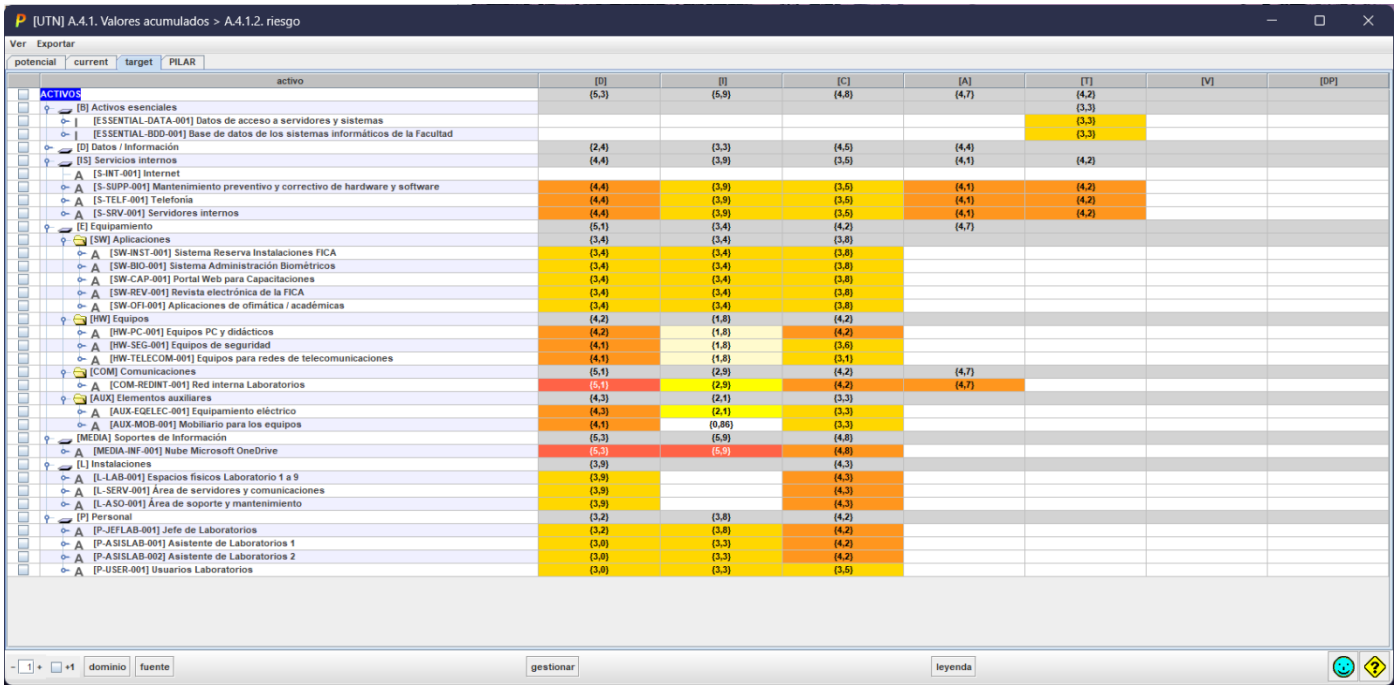
3.2.11. Estimación del Riesgo Residual

Al igual que el impacto residual, el software PILAR simula que las salvaguardas fueron implementadas y ofreció una valoración del riesgo residual acumulado y el riesgo residual repercutido.

El riesgo residual acumulado se lo presenta en la Figura 54, mientras que el riesgo residual repercutido en la Figura 55.

Figura 54

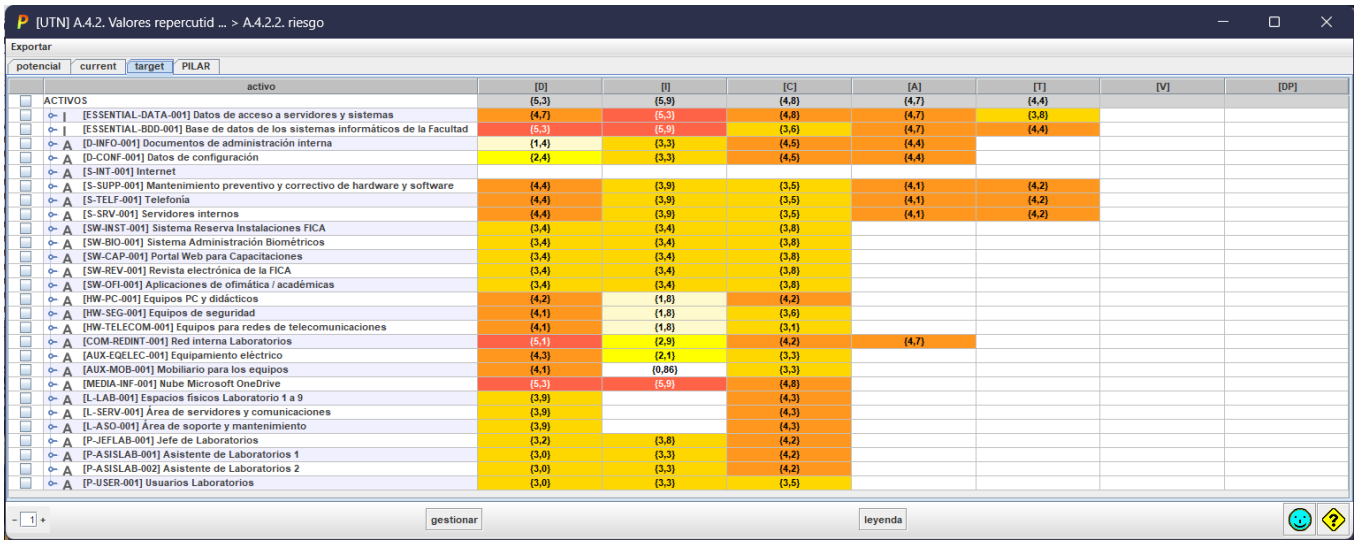
Riesgo residual acumulado de afectación de activos de los laboratorios de informática FICA-UTN en el software PILAR



Nota: Elaboración propia.

Figura 55

Riesgo residual repercutido de afectación de activos de los laboratorios de informática FICA-UTN en el software PILAR

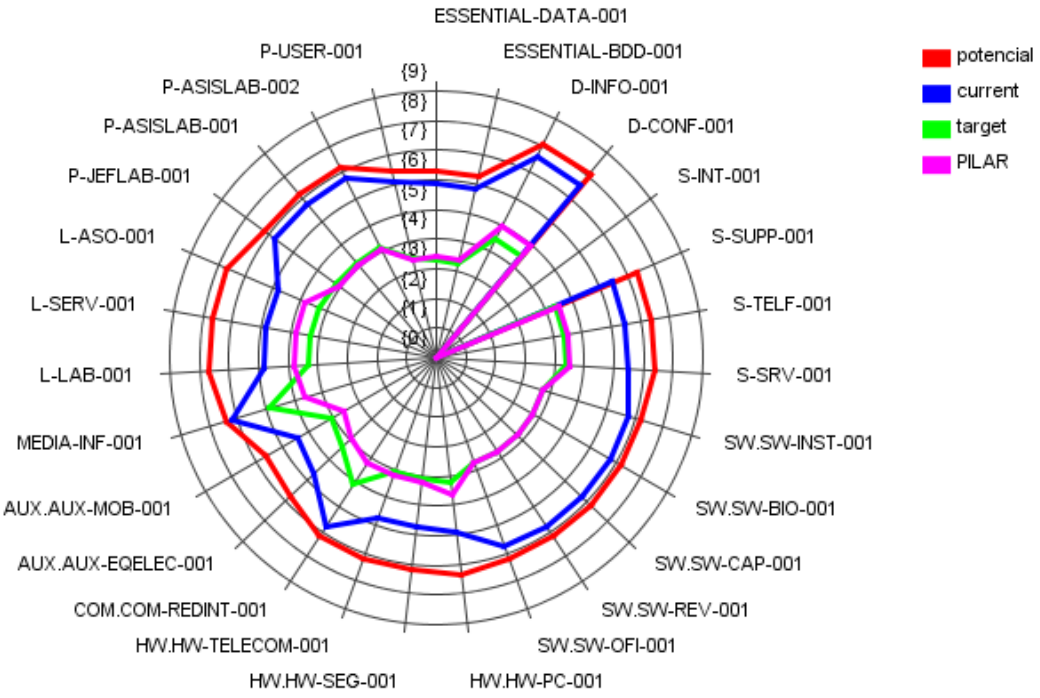


Nota: Elaboración propia.

En la Figura 56 se presenta el gráfico resumen de los riesgo potencial, actual, objetivo y recomendado por el software PILAR.

Figura 56

Gráfico valores de riesgo de afectación de activos de los laboratorios de informática FICA-UTN



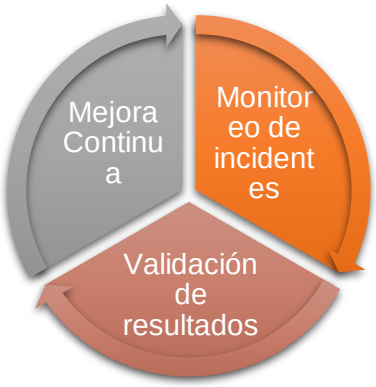
Nota: Elaboración propia

3.3. Fase 3: Seguimiento y Revisión

La fase de Seguimiento y Revisión se desarrolla mediante las etapas de Monitoreo, Validación y Mejora Continua, su finalidad es corroborar el correcto cumplimiento de las funciones para el que fue diseñado el Plan de Gestión de Riesgos (mitigación y reducción del riesgo). El proceso cíclico se lo encuentra en la Figura 57.

Figura 57

Proceso cíclico de Seguimiento y Revisión Plan de Gestión de Riesgos Laboratorios de Informática FICA-UTN.



Nota: Elaboración propia.

Debido a la extensión de tiempo que significaría desarrollar el análisis de factibilidad y la implantación de las salvaguardas, este se propone como desarrollo de un trabajo futuro, mientras que el monitoreo será una propuesta de diseño.

3.3.1. Monitoreo

El Plan de Gestión de Riesgos al estar diseñado para una organización pequeña, con un promedio de 750 usuarios rotativos en un periodo de seis meses, se recomienda realizar el monitoreo dos veces al año.

Para el monitoreo se debe llevar un registro de los incidentes presentados durante los seis meses, esté registro será desarrollado por cualquier miembro del equipo responsable de los laboratorios de informática FICA-UTN con ayuda de una plantilla de ficha elaborada en Microsoft Excel, y almacenada en una carpeta compartida en el servicio de Microsoft One Drive denominada “INC_RIESGOS_2023”.

La plantilla se encuentra en la Tabla 46.

Tabla 46

Plantilla registro de incidentes

Universidad Técnica del Norte
Facultad de Ingeniería en Ciencias Aplicadas
Carrera de Ingeniería de Software
Trabajo de Titulación
RESGISTRO DE INCIDENCIAS Y RIESGOS 2022-2023

Nota: La siguiente tabla tiene el fin de recaudar información acerca de incidentes ocurridos posterior implementación de la gestión de riesgos en los laboratorios de Informática FICA-UTN.
Instrucciones: Por favor ingrese los datos según corresponda, escoger desde la lusta desplegable en los casos que sea posible, caso contrario llenar como se crea c

	Nro	FECHA Y HORA	RESPONSABLE	ACTIVO AFECTADO	AMENAZA IDENTIFICADA	IMPACTO	PROBABILIDAD	SALVAGUARDA	ACCIONES	EFECTIVIDAD (0-10)	COMENTARIO
Ejemplo	X	1/1/2022 10:30	Ludmila Starodub	Equipos PC y didácticos	[A.25] Robo de equipos	100%	1	[PPE] Protección física de los equipos	Establecimiento de una normativa para imponer sanciones ante daños a los activos	8	Con la normativa de sanciones se pudo recuperar parte del dinero por el robo de equipos
	1										
	2										
	3										
	4										
	5										
	6										
	7										
	8										
	9										
	10										

Nota: Elaboración propia.

3.3.2. Valoración

Para la valoración propia del Plan de Gestión de Riesgos se recomienda realizarlo con un método de comparación, para el cual se recomienda el siguiente proceso:

I. Selección de los riesgos de mayor peso en el proceso inicial (este trabajo de titulación) de la Gestión de Riesgos.

II. Implantación de las tareas propuestas para el cumplimiento de las salvaguardas, según los encargados de los laboratorios de informática FICA-UTN consideren factibles en el periodo de seis meses.

III. Determinación del nuevo peso de los riesgos considerados en el paso I.

IV. Análisis y comparación de los pesos en estos riesgos.

Se debe tomar en cuenta que la más mínima reducción del peso de riesgo se considera un éxito en la mitigación de pérdidas causadas a partir de los riesgos.

3.3.3. Mejora Continua

La mejora continua del Plan de Gestión de Riesgos comprende el análisis de resultados obtenidos por la Valoración, para modificar el Plan Actual en el apartado de contramedidas que mitiguen los riesgos residuales (salvaguardas) mediante la propuesta de nuevas tareas y de esta manera reducir aún más los riesgos que queden presentes.

3.4. Socialización

El apartado de socialización es de gran importancia para la finalización de la Implementación del Plan de Gestión de Riesgos, los objetivos de este son:

- Compartir los conocimientos adquiridos durante todo el proceso de desarrollo del Plan de Gestión de Riesgos.
- Informar acerca de todas las actividades que ya se han desarrollado.
- Explicar en qué consiste cada una de las tareas propuestas para el cumplimiento de las salvaguardas.
- Explicar la propuesta de guía para el apartado de Seguimiento y Revisión del Plan de Gestión de Riesgos.
- Aclarar dudas que puedan surgir.

La socialización se desarrolló de manera presencial a manera de exposición con ayuda de material didáctico elaborado con ayuda de la herramienta visual “Canva”, este se encuentra en el Anexo M, el público solicitado para este proceso fueron las personas encargadas de los laboratorios de informática FICA-UTN (Jefe de Laboratorios y Asistentes de Enseñanza de los Laboratorios). La duración estimada de la socialización fue de una hora y media más el tiempo de preguntas y dudas.

De igual manera, se desarrolló un documento entregable denominado “Plan de Gestión de Riesgos Laboratorios de Informática 2022-2023”, en el cual se detalla todas las actividades realizadas a manera de informe. Este documento, junto con los archivos: hojas de cálculo y archivo .mgr referente al software PILAR, se entrega de manera oficial a la persona encargada de los laboratorios (Jefe de Laboratorios).

Además, para contribuir a mejorar la conciencia sobre los riesgos presentes en los laboratorios de informática FICA-UTN, se desarrolló material POP (afiches y trípticos) para los usuarios de los laboratorios (docentes y estudiantes) con información relevante sobre riesgos y formas sencillas de prevenirlos. Este material se encuentra en el Anexo

CAPÍTULO 4

Resultados

4.1. Evaluación del Plan de Gestión de Riesgos con el método Delphi

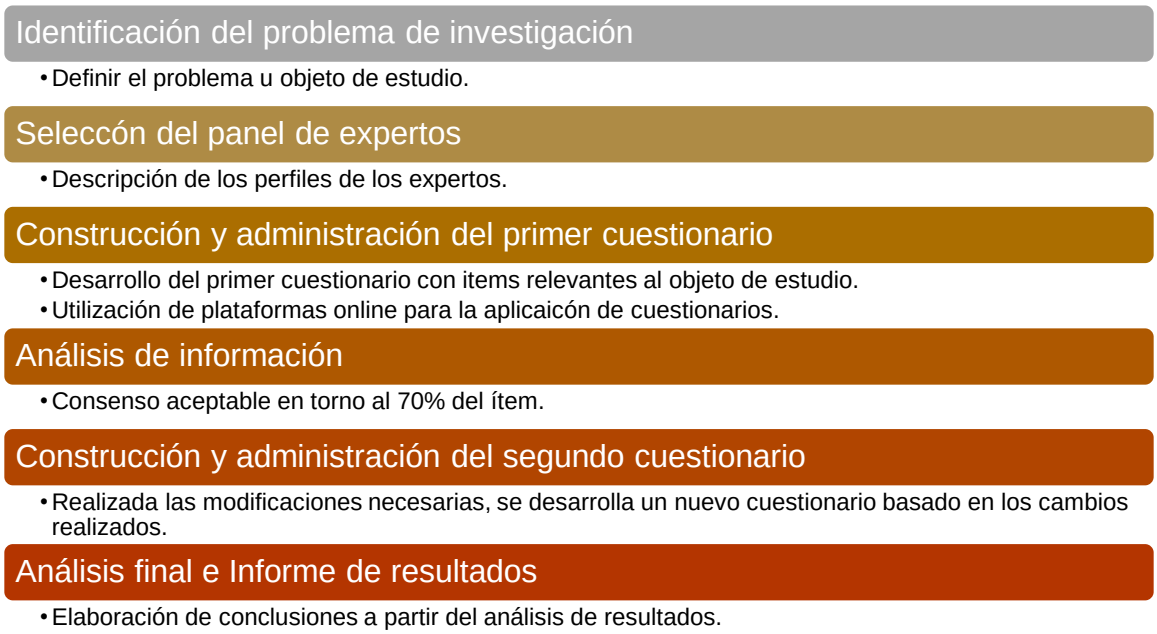
Una vez finalizado el desarrollo e implantación del Plan de Gestión de Riesgos, es importante asegurarse que su elaboración fue exitosa, para poder verificar la validez de este objeto (Plan de Gestión de Riesgos Tecnológicos) se optó por la Evaluación con el método Delphi.

El método Delphi es un método de recopilación de información de manera interactiva e iterativa, en el cual se utiliza la opinión de expertos en el área para lograr el objetivo de una investigación, cada uno de los expertos en diversas rondas responde a un cuestionario desarrollado en relación con el objeto de estudio y la retroalimentación de este (Sterling et al., 2022).

Romero (2021) considera a seis como los elementos pertenecientes al método Delphi de consulta a expertos, estos son presentados en la Figura 58.

Figura 58

Elementos Método Delphi



Nota: Adaptada de “Elementos esenciales para elaborar un estudio con el método (e)Delphi” (p.101), por Romero A., 2021, *Sociedad Española de Enfermería Intensiva y Unidades Coronarias*.

4.1.1. Identificación del Problema de Investigación

Como primer paso del método Delphi, es necesario la identificación del problema u objetivo de investigación, en este caso es evaluar la eficacia del Plan de Gestión de Riesgos Tecnológicos en los Laboratorios de Informática FICA-UTN, un informe elaborado con ayuda de la metodología MAGERIT versión 3 y basado en las consideraciones de la Norma ISO 31000 para el análisis y gestión de riesgos tecnológicos dentro de este departamento.

4.1.2. Selección del panel de expertos

Campos et al. (2014) asegura que el universo que funcionará como participantes del método Delphi son aquellos expertos, estudiosos, interesados y/o afectados por el objetivo de estudio. Dependiendo las necesidades de estudio, estos expertos pueden ser de índole académica, profesional o ambos.

El responsable de cada estudio debe determinar las condiciones que debe tener un experto para poder participar dentro de la validación. En el estudio realizado por Zhang et al. (2020, citados por Romero, 2021, p. 102) se considera varias especificaciones para la selección de expertos, con base en ellas, se definió las siguientes para este específico caso de estudio:

a) Título de licenciatura o superior.

b) Experiencia profesional y comprometida en el campo de la tecnología y/o seguridad informática.

c) Capacidad de proporcionar opiniones y sugerencias integrales.

d) Alta motivación y disposición para participar en el estudio.

El número recomendado de expertos varía según varios autores, Landeta (2002) menciona que el número recomendado es entre 7 y 30, García & Fernández (2008) recomiendan de 15 a 25, pero Cabero & Barroso (2013) aseguran que la selección de expertos es muy variante debido a que muchas veces no se cuenta con la accesibilidad a expertos suficientes relacionados con el objeto de estudio.

Se estableció contacto mediante correo electrónico con un número inicial de 7 expertos de distintas organizaciones, pero se obtuvo respuesta de 4, la información relevante de dichos

expertos se encuentra en la Tabla 47. Además, se realizó la encuesta al grupo de 14 estudiantes de la asignatura de “Auditoría Informática” de sexto nivel de la carrera de Ingeniería de Software de la Universidad Técnica del Norte, debido a que están obteniendo conocimientos relacionados con el tema este trabajo de titulación.

Tabla 47

Expertos seleccionados para la validación con el Método Delphi

N	Institución	Categoría de la Institución	Grado académico
E1	Universidad Técnica del Norte	Institución Pública de Educación Superior	Magíster en Evaluación y Auditoría de Sistemas Tecnológicos
E2	Universidad de las Fuerzas Armadas ESPE	Institución Pública de Educación Superior	Magíster en Evaluación y Auditoría de Sistemas Tecnológicos
E3	Universidad Técnica de Ambato	Institución Pública de Educación Superior	Magíster en Evaluación y Auditoría de Sistemas Tecnológicos
E4	Universidad de las Fuerzas Armadas ESPE	Institución Pública de Educación Superior	Magíster en Sistemas e Informática
E5	Universidad Técnica del Norte	Institución Pública de Educación Superior	Estudiantes Ingeniería de Software

Nota: La tabla muestra la información de los expertos seleccionados, donde E son los expertos. Elaboración propia

Las rondas realizadas en el método Delphi varía dependiendo las necesidades y que tan complejo sea el objeto de estudio, para este caso se utilizará la recomendación expuesta por Enrique & Trujillo (2018) de no utilizar más de dos rondas si se quiere evitar que la validación se extienda mucho.

4.1.3. Construcción y administración del cuestionario inicial

Una vez definido el objetivo de investigación, se desarrolló un cuestionario de 10 ítems, los cuales estarán enfocados al objetivo de investigación, teniendo en cuenta los puntos más importantes del Plan de Gestión de Riesgos. Este cuestionario inicial se encuentra en el Anexo O. Todo el proceso de recolección de datos fue desarrollado vía electrónica. La invitación a la participación se realizó vía e-mail. Se estipuló que el tiempo esperado entre el envío de información y la recepción de respuestas sería de una semana laborable; la información enviada incluyó el documento del informe del Plan de Gestión de Riesgos y un vínculo para el acceso al cuestionario en Google Forms.

A excepción del ítem 10 (argumento personal), para la evaluación de los demás ítems se propuso la escala de Likert de 5 puntos expuesta en la Tabla 48.

Tabla 48

Escala de Likert para la valoración de cuestionarios

Valor	Escala de Likert
1	Totalmente de acuerdo
2	De acuerdo
3	Indiferente o neutro
4	En desacuerdo
5	Totalmente en desacuerdo

Nota: Elaboración propia.

4.1.4. Análisis de información

El análisis de información fue desarrollado con estrategias descriptivas, cualitativas y cuantitativas a razón de interpretar los resultados obtenidos por parte de los cuestionarios.

Para la validez de cada pregunta, Polit & Beck (2006, citados en Silva & Montilha, 2021, p.6), proponen los Índices de Validez de Contenido (CVI) por ítem y total. Las fórmulas para estos índices son las siguientes:

$$CVI = \frac{número\ de\ respuestas\ positivas}{número\ total\ de\ respuestas}$$

$$CVITotal = \frac{número\ de\ respuestas\ positivas}{(número\ de\ expertos\ \times número\ de\ ítems)}$$

De acuerdo con la literatura, para que un instrumento de evaluación se considere válido, su CVI total debe ser mayor o igual que 90%, y para la validez de cada ítem, este debe tener un CVI mayor o igual que 78%. Si estos valores se cumplen, se considera que se ha llegado a un consenso, por otra parte, si no se cumple, se puede solicitar comentarios o propuestas de mejora para modificar y/o remover ítems.

De igual manera, se optó por la utilización de técnicas auxiliares como:

- **Estadística descriptiva:** Es la rama de la estadística que permite resumir de forma clara la información recopilada (Redón et al., 2016). Al utilizar variables cuantitativas como lo es la escala de Likert, se optó por hacer uso de las medidas de tendencia central como lo son: la media aritmética, mediana y moda.

- **Alfa de Cronbach: "**Es un coeficiente estadístico para estimar la confiabilidad de una prueba, o de cualquier compuesto obtenido a partir de la suma de varias mediciones" (Cervantes, 2005). El valor producido por este estadístico varía entre 0 y 1, a lo cual Campo & Oviedo (2008, citados en Tuapanta et al., 2017, p.39), consideran que el valor mínimo aceptable se debe encontrar entre 0,70 y 0,90.

Los resultados obtenidos fueron los siguientes.

Primero se realizó un análisis de las 14 respuestas obtenidas por el cuestionario aplicado a los estudiantes de "Auditoría Informática", estas se muestran en la Tabla 49.

Tabla 49

Resultados primer cuestionario a estudiantes de la asignatura de Auditoría Informática

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
E1	1	3	2	1	1	1	1	1	1	No cambiaría nada
E2	1	2	2	2	1	2	1	2	3	No
E3	1	2	2	2	2	3	2	2	2	Ninguno
E4	2	2	2	2	3	2	2	1	2	No nada
E5	1	3	2	2	1	2	2	1	1	Por el momento no, todo está en base a lo establecido
E6	1	3	2	1	2	2	2	2	2	ninguno
E7	2	2	1	1	2	1	2	3	3	No sería necesario
E8	1	3	3	2	2	1	3	1	1	No, porque me parece que está acertados, debido a que se enfoca en los riesgos inherentes que prestan los laboratorios de la FICA.
E9	1	2	3	2	2	2	1	2	1	.
E10	2	2	1	2	1	2	2	2	2	Ninguno
E11	1	1	1	1	1	1	1	1	1	Todo está correcto
E12	2	3	3	2	2	2	2	2	2	No
E13	3	4	1	2	2	2	3	2	3	En el proceso de ejecución y reconocimiento de riesgos, se debería poner mayor enfoque en la evaluación y revisión de campo.
E14	3	3	3	3	2	2	2	2	2	No
Moda	1	3	2	2	2	2	2	2	2	No

Nota: La tabla muestra los datos tabulados, donde P son las preguntas y E son los estudiantes. Elaboración propia.

Con estadística descriptiva se realizó el cálculo de la Moda de las respuestas para determinar el valor típico del grupo en cada ítem, de esta manera se generaliza las respuestas de los estudiantes para poder colocarlas como un experto más en el análisis posterior.

Los resultados obtenidos por parte de los expertos se presentan en la Tabla 50.

Tabla 50

Resultados primer cuestionario a expertos

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
E1	1	2	2	2	2	2	2	2	2	No, no tengo sugerencias
E2	1	2	2	2	1	1	2	2	1	Actualizar estándares de seguridad
E3	1	2	2	1	3	2	2	1	1	Explicar cómo se desarrolló las diferentes valoraciones.
E4	1	2	1	1	1	2	1	1	1	Le agregaría de forma más específica el control de las licencias de su software y su respectiva renovación.
E5	1	3	2	2	2	2	2	2	2	No

Nota: La tabla muestra los datos tabulados, donde P son las preguntas y E son los expertos. Elaboración propia.

Para realizar el cálculo de los índices de validez de contenido, es necesario la tabulación de respuestas por pregunta y valor en la escala de Likert. Dicha tabulación se encuentra en la Tabla 51, y de forma gráfica en la Figura 59.

Tabla 51

Tabulación respuestas del primer cuestionario a expertos por pregunta y valor en la escala de Likert

	TD	D	N	A	TA
P1	0	0	0	0	5
P2	0	0	1	4	0
P3	0	0	0	4	1
P4	0	0	0	3	2
P5	0	0	1	2	2
P6	0	0	0	4	1
P7	0	0	0	4	1
P8	0	0	0	3	2
P9	0	0	0	2	3
P10					

Nota: TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente o neutro, A: De acuerdo, TA: Totalmente de acuerdo. P: preguntas del cuestionario. Elaboración propia.

Figura 59

Respuestas por ítem del primer cuestionario a expertos

Nota: TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente o neutro, A: De acuerdo, TA: Totalmente de acuerdo. P: preguntas del cuestionario. Elaboración propia.

Una vez tabuladas las respuestas se puede hacer los cálculos de Índice de Validez de Contenido con las fórmulas anteriormente mencionadas. Estos se presentan en la Tabla 52

Tabla 52

Índice de Validez de Contenido (CVI) del primer cuestionario a expertos

Pregunta	TD	D	N	A	TA	IVC ÍTEM
1. Considera usted, ¿qué es necesario el desarrollo de un Plan de Gestión de Riesgos Tecnológicos en departamentos de tecnologías como los “Laboratorios de Informática FICA-UTN”?	-	-	-	-	100%	100%
2. ¿En su opinión, el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología “Laboratorios de Informática FICA-UTN” es un informe fácil de comprender?	-	-	20%	80%	-	80%
3. ¿A su juicio, el informe de Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología “Laboratorios de Informática FICA-UTN” cuenta con la información necesaria?	-	-	-	80%	20%	100%
4. ¿En su opinión, la selección de la metodología MAGERIT versión 3 y la norma ISO 31000 para el desarrollo del Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología “Laboratorios de Informática FICA-UTN” fue acertada?	-	-	-	60%	40%	100%
5. ¿Considera usted, que los pasos desarrollados en el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología “Laboratorios de Informática FICA-UTN” fueron los necesarios?	-	-	20%	40%	40%	80%
6. ¿A su juicio, la utilización del software PILAR y las hojas de cálculo de Excel fueron acertadas para el manejo de la información relevante en el desarrollo del Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología “Laboratorios de Informática FICA-UTN”?	-	-	-	80%	20%	100%
7. ¿En su opinión, las tareas propuestas a manera de salvaguardas para la mitigación de riesgos en el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología “Laboratorios de Informática FICA-UTN” fueron las idóneas?	-	-	-	80%	20%	100%
8. Considera usted, ¿qué el Plan de Gestión de Riesgos cumplió con su objetivo de identificación, análisis y mitigación de riesgos en el departamento de tecnología “Laboratorios de Informática FICA-UTN”?	-	-	-	60%	40%	100%
9. A su juicio, el Plan de Gestión de Riesgos Tecnológicos desarrollado para el departamento de tecnología “Laboratorios de Informática FICA-UTN”, ¿puede ser aplicado en otras Instituciones de Educación Superior?	-	-	-	40%	60%	100%

10. Cambiaría usted algún elemento presentado en el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología “Laboratorios de Informática FICA-UTN”, ¿cuál sería?	
IVC TOTAL	95.56%

Nota: TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente o neutro, A: De acuerdo, TA: Totalmente de acuerdo, IVC: Índice de validez de contenido. Elaboración Propia.

Dentro de la primera ronda de cuestionarios se obtuvo un índice de Validez de Contenido (IVC) Total de 95.56%, lo que según la literatura es un buen puntaje para permitir como válido el cuestionario. Todas las preguntas cuentan con un IVC de ítem mayor o igual a 80%, por lo que se considera que existe un consenso en los resultados y no es necesario el cambio o eliminación de los ítems.

Para corroborar la validez del cuestionario también se aplicó la técnica de estadística Alfa de Cronbach a todo el cuestionario, la fórmula para el alfa de Cronbach es la siguiente:

$$\alpha = \frac{K}{K-1} \times \left[1 - \frac{\sum Vi}{Vt}\right]$$

En donde,

$\alpha = Alfa\ de\ Cronbach$

$K = Número\ de\ ítems$

$Vi = Varianza\ de\ cada\ ítem$

$Vt = Varianza\ total$

Los valores de varianza se encuentran en la Tabla 53, mientras que los cálculos del alfa de Cronbach en la Tabla 54.

Tabla 53

Varianza de ítems del primer cuestionario a expertos

	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**Sumatoria**
E1	1	2	2	2	2	2	2	2	2	17
E2	1	2	2	2	1	1	2	2	1	14
E3	1	2	2	1	3	2	2	1	1	15
E4	1	2	1	1	1	2	1	1	1	11
E5	1	3	2	2	2	2	2	2	2	18
Varianza	0	0.16	0.16	0.24	0.56	0.16	0.16	0.24	0.24	6

Nota: P: Número de pregunta, E: Número de Experto. Elaboración propia

Tabla 54

Alfa de Cronbach del primer cuestionario a expertos

K	9
Suma Varianzas (Vi)	1.920
Varianza Total (Vt)	6.00

Parte 1	1.125
Parte2	0.680
Cronbach	**0.765**

Nota: Elaboración propia.

El Alfa de Cronbach arroja un resultado de 0.765 lo cual se encuentra en el rango aceptable para la validez interna del cuestionario.

A pesar de ello, el ítem 10 considera una pregunta argumentativa referente a si se optaría por algún cambio o mejora en el Plan de Gestión de Riesgos realizado. Estas sugerencias fueron tomadas en cuenta para la modificación del Informe y las preguntas de la segunda ronda del método Delphi.

4.1.5. Construcción y administración del segundo cuestionario

Previa la construcción del segundo cuestionario, es necesario tomar en cuenta las respuestas obtenidas en el ítem número 10 del primer cuestionario referentes a si se optaría por algún cambio al informe actual de Gestión de Riesgos realizado.

La recapitulación de las respuestas se presenta en la tabla 55.

Tabla 55

Recapitulación de respuestas al ítem 10 del primer cuestionario

P10. ¿Cambiaría usted algún elemento presentado en el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "¿Laboratorios de Informática FICA-UTN", cuál sería?	
Expertos	**Respuesta**
E1	No, no tengo sugerencias
E2	Actualizar estándares de seguridad
E3	Explicar cómo se desarrolló las diferentes valoraciones.
E4	Le agregaría de forma más específica el control de las licencias de su software y su respectiva renovación.
E5	No

Nota: E: Número de Experto. Elaboración propia

Tanto el experto 1 como 5 no presentan sugerencias de modificaciones al Informe desarrollado, mientras que los tres restantes brindan comentarios que maximizarían la eficacia del Plan de Gestión de Riesgos.

Para atender de manera adecuada cada uno de estos comentarios, se desarrollaron las siguientes adecuaciones:

1. **Actualización Estándares de Seguridad**

   Para el desarrollo de este trabajo se utilizó la Norma ISO 31000:2018 como estándar para la gestión de riesgos, aun así este no se lo considera estándar de seguridad. Por lo que al momento de realizar el proceso de gestión de riesgos en el software PILAR RM (versión 1.2.2022) se configuró que para las actividades relacionadas con el "Tratamiento del Riesgo" (salvaguardas) se utilice el estándar ISO/IEC 27002:2022 referente a la Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información en las dimensiones de Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

2. **Técnicas de valoración**

   Las técnicas de valoración para los activos, amenazas y salvaguardas están expuestas en el Plan de Gestión de Riesgos, estas fueron desarrolladas con las métricas explícitas por MAGERIT en sus escritos "Método" y "Catálogo de Elementos", esta vez se incluyó una mejor explicación de la integración del equipo responsable de los laboratorios en la valoración en cada una de las dimensiones de los activos (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad), los dos sentidos de valoración de amenazas (Degradación del activo y Probabilidad de Ocurrencia de la amenaza) y la valoración de proyección de salvaguardas (Estado actual y objetivo).

3. **Licencias de software**

   Dentro del Informe del Plan de Gestión de Riesgos se incluyó información sobre las versiones disponibles del software PILAR, al igual que la comparación de características que ofrece cada una. Se añadió información sobre los dos tipos de licenciamiento del software y el precio que correspondiente a cada una de las licencias.

Una vez desarrolladas las adecuaciones en el Informe se desarrolló el segundo cuestionario para la validación con el método Delphi. El formato será el mismo utilizado para el primer cuestionario, este constará de 5 ítems relacionados directamente con los cambios sugeridos como respuesta del primer cuestionario. Estas preguntas se encuentran en el Anexo P.

4.1.6. Análisis final de información

De la misma manera en la que se desarrolló el análisis del primer cuestionario, es necesario condensar las respuestas de los 14 estudiantes de Auditoría Informática en una sola para poder analizarla después junto con las respuestas de los cuatro expertos. Este primer análisis se presenta en la Tabla 56.

Tabla 56

Resultados segundo cuestionario a estudiantes de la asignatura de Auditoría Informática

	P1	P2	P3	P4	P5
E1	2	2	2	2	2
E2	2	2	2	1	2
E3	2	1	2	2	2
E4	1	2	2	2	2
E5	2	2	2	2	2
E6	1	1	2	2	2
E7	2	2	2	2	2
E8	2	2	2	2	3
E9	1	1	1	1	1
E10	2	2	2	3	2
E11	2	2	2	1	2
E12	2	2	2	2	2
E13	1	1	2	2	2
E14	2	1	2	2	2
Moda	2	2	2	2	2

Nota: La tabla muestra los datos tabulados, donde P son las preguntas y E son los estudiantes. Elaboración propia.

Con estadística descriptiva se realizó el cálculo de la Moda de las respuestas para determinar el valor típico del grupo en cada ítem, de esta manera se generaliza las respuestas de los estudiantes para poder colocarlas como un experto más en el análisis posterior.

Los resultados obtenidos por parte de los expertos se presentan en la Tabla 57.

Tabla 57

Resultados segundo cuestionario a expertos

	P1	P2	P3	P4	P5
E1	1	2	2	2	1
E2	1	1	2	1	2
E3	2	2	2	2	2

E4	1	2	1	1	1
E5	2	2	2	2	2

Nota: La tabla muestra los datos tabulados, donde P son las preguntas y E son los expertos. Elaboración propia.

Para realizar el cálculo de los índices de validez de contenido, es necesario la tabulación de respuestas por pregunta y valor en la escala de Likert. Dicha tabulación se encuentra en la Tabla 58, y de forma gráfica en la Figura 60.

Tabla 58

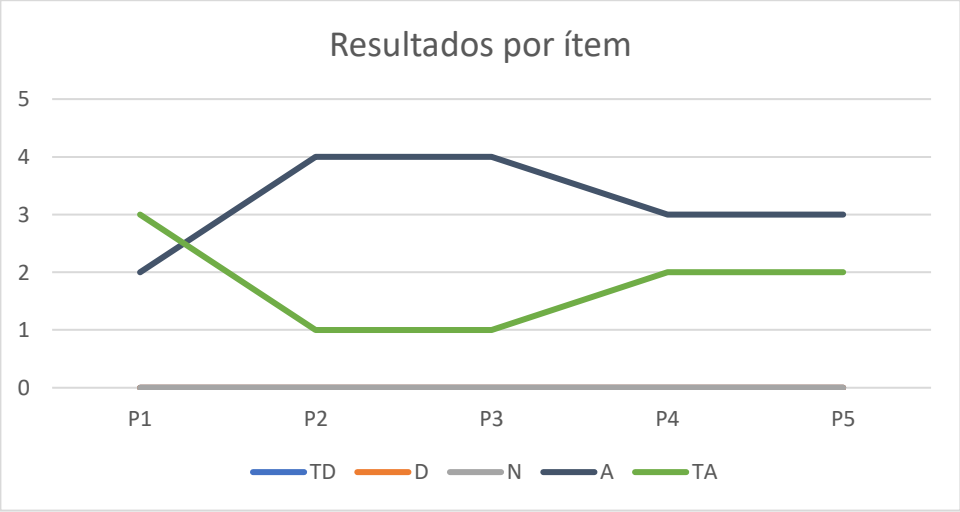
Tabulación respuestas del segundo cuestionario a expertos por pregunta y valor en la escala de Likert

	TD	**D**	**N**	**A**	**TA**
P1	0	0	0	2	3
P2	0	0	0	4	1
P3	0	0	0	4	1
P4	0	0	0	3	2
P5	0	0	0	3	2

Nota: TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente o neutro, A: De acuerdo, TA: Totalmente de acuerdo. P: preguntas del cuestionario. Elaboración propia.

Figura 60

Respuestas por ítem del segundo cuestionario a expertos



Nota: TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente o neutro, A: De acuerdo, TA: Totalmente de acuerdo. P: preguntas del cuestionario. Elaboración propia.

Una vez tabuladas las respuestas se puede realizar nuevamente los cálculos de Índice de Validez de Contenido al igual que en el análisis del primer cuestionario. Estos se presentan en la Tabla 59

Tabla 59

Índice de Validez de Contenido (CVI) del segundo cuestionario a expertos

Pregunta	TD	D	N	A	TA	IVC ÍTEM
1. ¿A su juicio, el estándar de seguridad ISO/IEC 27002 en su versión actualizada de 2022 utilizado por MAGERIT mediante su herramienta PILAR RM (v.1.2.2022) para el tratamiento de los riesgos es el más acertado respecto a este proceso de Gestión de Riesgos Tecnológicos desarrollado para los Laboratorios de Informática FICA-UTN?	-	-	-	40%	60%	100%
2. ¿Considera usted que, debido al beneficio de amplia gama de características y funcionalidades provistas en su licenciamiento de prueba, la herramienta PILAR en su versión RM (1.2.2022) fue la mejor opción para desarrollar el proceso de Gestión de Riesgos Tecnológicos en los Laboratorios de Informática FICA-UTN?	-	-	-	80%	20%	100%
3. ¿Estaría usted de acuerdo con, que al no contar con registro de incidentes ocurridos en los laboratorios de informática FICA-UTN, fue acertado a valorar la frecuencia de amenazas en base a los valores asignados por el software PILAR?	-	-	-	80%	20%	100%
4. ¿Considera usted que, en respuesta al enfoque de Mejora Continua, fue acertada el planteamiento de realizar una revisión de la Gestión de Riesgos Tecnológicos en los laboratorios de informática FICA-UTN una vez hayan trascurridos seis meses del desarrollo de esta?	-	-	-	60%	40%	100%
5. ¿En su opinión, los cambios implementados en el Informe del Plan de Gestión de Riesgos Tecnológicos desarrollados para los Laboratorios de Informática FICA-UTN mejoraron la calidad de este a raíz de las consideraciones tomadas del análisis del primer cuestionario?	-	-	-	60%	40%	100%
IVC TOTAL				100.00%		

Nota: TD: Totalmente desacuerdo, D: Desacuerdo, N: Indiferente o neutro, A: De acuerdo, TA: Totalmente de acuerdo, IVC: índice de validez de contenido. Elaboración Propia.

Referente a la segunda ronda de cuestionarios se obtuvo un índice de Validez de Contenido (IVC) Total de 100%, lo que significa que todas las respuestas fueron positivas y válidas para el cuestionario. Igualmente, todas las preguntas cuentan con un IVC de ítem del 100%, por lo que se considera que existe un consenso en los resultados y no es necesario el cambio o eliminación de los ítems.

Una vez más, para corroborar la validez del cuestionario se aplicó la técnica de estadística Alfa de Cronbach a todo el cuestionario.

Los valores de varianza se encuentran en la Tabla 60, mientras que los cálculos del alfa de Cronbach en la Tabla 61.

Tabla 60

Varianza de ítems del segundo cuestionario a expertos

	P1	**P2**	**P3**	**P4**	**P5**	**Sumatoria**
E1	1	2	2	2	1	8
E2	1	1	2	1	2	7
E3	2	2	2	2	2	10
E4	1	2	1	1	1	6
E5	2	2	2	2	2	10
Varianza	0.24	0.16	0.16	0.24	0.24	2.56

Nota: P: Número de pregunta, E: Número de experto. Elaboración propia

Tabla 61

Alfa de Cronbach del segundo cuestionario a expertos

K	5
Suma Varianzas (Vi)	1.04
Varianza Total (Vt)	2.56
Parte 1	1.25
Parte2	0.593
Cronbach	**0.742**

Nota: Elaboración propia.

El Alfa de Cronbach arroja un resultado de 0.742 lo cual se encuentra en el rango aceptable para la validez interna del cuestionario.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La revisión de bibliografía fue un proceso de gran ayuda para tener claros los conceptos relacionados a la gestión de riesgos tecnológicos en las áreas de TI, esto fue de gran utilidad para realizar la comparación y selección de Norma y Metodología para el desarrollo de este trabajo de titulación.

2. El Plan de Gestión de Riesgos permitió reconocer riesgos tecnológicos relacionados a la seguridad de la información como: modificación, destrucción, y acceso no autorizado. Sin embargo, también se identificó riesgos tecnológicos con otros enfoques como: robo de equipos, desastres naturales e industriales, denegación de servicios, difusión de software dañino. Con esta base y la comparación realizada en el capítulo 1, se concluye que, la selección de la Norma ISO/IEC 31000:2018 fue la ideal para el proceso de Gestión de Riesgos, debido a que no se limita a un solo tipo de riesgos.

3. La propuesta de distintas tareas a manera de salvaguardas para la minimización del impacto negativo de los riesgos, junto con la simulación de implantación desarrollada por el software PILAR, permitió observar una presunta reducción de hasta un 40% en los valores concernientes al impacto de los distintos riesgos, lo cual se traduce en un evidente beneficio dentro del departamento y sus usuarios.

4. La validación del Plan de Gestión de Riesgos con el método Delphi permitió apreciar la opinión de varios expertos en relación con el informe desarrollado. Estos lo definieron como un informe necesario, justificado, comprensible, replicable, con la selección de normas, metodologías y herramientas de software acertadas.

5. La implantación del Plan de Gestión de riesgos tuvo un impacto positivo en el personal responsable de los Laboratorios, ya que, gracias al informe desarrollado, estos pueden desarrollar actividades como: reconocer los activos más importantes, identificar amenazas y riesgos presentes, y tener opciones de tratamiento para minimizar el impacto de estos con la ayuda de tareas propuestas a manera de salvaguardas.

6. Se tuvo una muy buena experiencia con el uso de la norma ISO/IEC 31000:2018, tiene un muy buen rendimiento al poder ser utilizada en cualquier organización, además de acoplarse muy fácilmente a diferentes metodologías de gestión de riesgos. De igual manera la experiencia con el uso de la Metodología MAGERIT resulto placentera al permitir la optimización de tiempos y esfuerzos gracias a sus beneficios de: disponibilidad de idioma español e inglés, tres escritos digitales gratuitos y la herramienta de software “PILAR”.

Recomendaciones

1. Se recomienda designar a un miembro del personal de los Laboratorios de Informática FICA-UTN a ser el responsable del registro y revisión de incidentes relacionados al riesgo con ayuda de la Plantilla propuesta en el apartado de Monitoreo referente a la Fase 3 de “Seguimiento y Revisión”.

2. Se recomienda realizar un análisis y evaluación de factibilidad de las 33 tareas propuestas a manera de salvaguardas para la minimización del impacto de riesgos presentes en los Laboratorios de Informática FICA-UTN.

3. Se recomienda que, una vez transcurridos los seis meses del desarrollo del Plan de Gestión de Riesgos Tecnológicos, y que se hayan implantado por lo menos 5 tareas propuestas a manera de salvaguardas, evaluar nuevamente el nivel de gestión de riesgos con ayuda del Modelo Risk Managmenet Model (RMM) para verificar que ha existido un aumento en el puntaje inicial obtenido.

4. Se recomienda desarrollar un trabajo futuro relacionado al análisis de riesgos con un enfoque cuantitativo orientado a aspectos de pérdidas económicas por afectación de activos debido a la materialización de amenazas en los Laboratorios de Informática.

5. Se recomienda replicar este proceso de Gestión de Riesgos en los demás Laboratorios de Informática de otras Facultades dentro la Universidad Técnica del Norte y presentarla como una metodología estándar para la Institución y así servir de ejemplo para otras Instituciones Públicas de Educación Superior.

REFERENCIAS Y BIBLIOGRAFÍA

Bibliografia

Alam, A. (2016). Steps in the Process of Risk Management in Healthcare. Journal Of Epidemiology And Preventive Medicine, 02(02). doi: 10.19104/jepm.2016.118

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE Approach. https://doi.org/10.21236/ada634134

Ay, C., Güler, T., & Bal Beşikçi, E. (2022). Implementation of ARAMIS methodology in the risk assessment of chemical tankers: The case of loading operation. Ocean Engineering, 261, 112211. https://doi.org/10.1016/j.oceaneng.2022.112211

Bitrix. (2021). Diagrama de Gantt Para Proyectos. Diagrama de Gantt. Recuperado el 5 de octubre de 2022, desde https://www.bitrix24.es/uses/Diagrama-de-Gantt-Para-Proyectos.php?gclid=CjwKCAiA24SPBhB0EiwAjBgkhrPDpqt4Z0aJey15h_Im0JUMWBld-doVBeGJZbpTc2AZsOSZmrYUAhoCW-AQAvD_BwE

Bonet, Á., Alcázar, J., Quintana, S., & Méndez, J. (2019). Guía para la aplicación de UNE-ISO 31000:2018 (1st ed.). Asociación Española de Normalización y Certificación.

Cabero Almenara, J. y Barroso, J. (2013). La utilización del juicio de experto para la evaluación de TIC: el coeficiente de competencia experta. Bordón, 65(2), 25-38.

Campos, V., Melián, A., & Sanchis, J. R. (2014). El método Delphi como técnica de Diagnóstico Estratégico. Estudio Empírico Aplicado a Las Empresas de inserción en España. Revista Europea De Dirección y Economía De La Empresa, 23(2), 72–81. https://doi.org/10.1016/j.redee.2013.06.002

Castro-Rivera, V., Herrera-Acuña, R., & Villalobos-Abarca, M. (2020). Desarrollo de un software web para la generación de planes de gestión de riesgos de software. Información Tecnológica, 31(3), 135-148. doi: 10.4067/s0718-07642020000300135

Centro Nacional de Inteligencia Española. (2022). PILAR. Pilar.ccn-cert.cni.es. Recuperado el 5 de octubre de 2022, desde https://pilar.ccn-cert.cni.es/.

Cervantes, V. (2005). Interpretaciones del Coeficiente Alpha de Cronbach.

Consejo Nacional de Planificación. (2021). Plan de Creación de Oportunidades 2021-2025. Quito, Pichincha; Secretaría Nacional de Planificación.

Crespo, E., & Cordero, G. (2018). Estudio Comparativo entre las metodologías CRAMM y MAGERIT para la gestión de riesgos de TI en las MPYMES. UDA AKADEM, (1), 38-47. https://doi.org/10.33324/udaakadem.vi1.129

Dali, A., & Lajtha, C. (2012). ISO 31000 Risk Management— "The Gold Standard". EDPACS, 45(5), 1-8. https://doi.org/10.1080/07366981.2012.682494

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 Método (1st ed.). Ministerio de Hacienda y Administraciones Públicas.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 Catálogo de Elementos (1st ed.). Ministerio de Hacienda y Administraciones Públicas.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 3 Guía de Técnica (1st ed.). Ministerio de Hacienda y Administraciones Públicas.

Enrique, C., & Trujillo, L. (2018). Aplicación del Método Delphi modificado para la validación de un cuestionario de incorporación del tic en la Práctica Docente. Revista Iberoamericana De Evaluación Educativa, 11(1), 113–135. https://doi.org/10.15366/riee2018.11.1.007

García, F., & Moreta, L. (2018). Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies. 2018 7Th International Conference On Software Process Improvement (CIMPS). https://doi.org/10.1109/cimps.2018.8625848

García, L., & Fernández, S. (2008). Procedimiento de aplicación del trabajo creativo en grupo de expertos. Ingeniería Energética, 29(2), 46–50.

Gartner Research. (2010). The OCTAVE Risk Assessment Methodologies [Blog]. Recuperado el 5 de octubre de 2022, desde https://www.gartner.com/en/documents/1405794.

Guzmán, O. (2019). Diseño de un modelo de sistema para la Gestión de Riesgo con base a la Norma ISO 31000 y MAGERIT Versión 3.0 en la empresa BLUEBOX. Universidad De Guayaquil. Recuperado el 3 de octubre de 2022, desde http://repositorio.ug.edu.ec/bitstream/redug/44421/1/Tesis-Dise%C3%B1o%20de%20un%20modelo%20de%20sistema%20para%20la%20gesti%C3%B3n%20de%20riesgos%20con%20base%20a%20la%20norma%20ISO%2031000%20y%20M.pdf.

Hardjomidjojo, H., Pranata, C., & Baigorria, G. (2022). Rapid assessment model on risk management based on ISO 31000:2018. IOP Conference Series: Earth And Environmental Science, 1063(1), 012043. https://doi.org/10.1088/1755-1315/1063/1/012043

Hermoso, M., & Garzón, J. (2021). Risk management methodology in the supply chain: a case study applied. Annals Of Operations Research, 313(2), 1051-1075. https://doi.org/10.1007/s10479-021-04220-y

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal For Science And Engineering, 45(4), 3171-3189. https://doi.org/10.1007/s13369-019-04319-2.

Imbaquingo, D., Bernabé, M., Cajas, F., Luje, R. (2020). Evaluación de metodologías de auditoría informática basado en su riesgo inherente. Universidad De Las Fuerzas Armadas.

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De la Torre, J., Jácome, J. (2020). Análisis de las principales dificultades en la Auditoría Informática: Una revisión sistemática de literatura. Revista Ibérica De Sistemas e Tecnologías De Información, 427–440.

Imbaquingo, D., Saltos, T., Arciniega, S., León, D., Ordoñez, A. (2020). Problemas de seguridad de la información en Instituciones de Educación Superior. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). https://doi.org/10.23919/cisti49556.2020.9141014.

Imbaquingo, D., Jácome, J. y Pusdá, M. (2017). Fundamentos de Auditoría Informática basada en riesgos. Ibarra, Ecuador: Universidad Técnica del Norte.

ISOTools. (2015, April 10). La Familia de Normas ISO 27000. Software ISO. Recuperado el 8 de febrero de 2022, desde https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

Jaramillo, E., & Sevilla, E. (2021, Diciembre 16). Distribución aulas y laboratorios FICA. personal.

Landeta, J. (1999). El método delphi: Una técnica de previsión para la incertidumbre (1st ed., Vol. 1). Ariel.

Manterola, C., Astudillo, P., Arias, E., & Claros, N. (2013). Revisiones Sistemáticas de la literatura. Qué Se Debe saber acerca de ellas. Cirugía Española, 91(3), 149–155. https://doi.org/10.1016/j.ciresp.2011.07.009

Molina, M. (2015). Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral. Universidad Politécnica De Madrid. Recuperado el 5 de octubre de 2022, desde dehttp://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Olechowski, A., Oehmen, J., Seering, W., & Ben, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play?. International Journal Of Project Management, 34(8), 1568-1578. https://doi.org/10.1016/j.ijproman.2016.08.002

Organización de las Naciones Unidas. (2020). Objetivos y Metas de Desarrollo Sostenible Recuperado el 20 de febrero de 2020 desde https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

Organización Internacional de Estandarización. (2018). ISO 31000:2018. Organización Internacional de Estandarización, 2. Recuperado el 3 de octubre de 2022, desde https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

Parviainen, T., Goerlandt, F., Helle, I., Haapasaari, P., & Kuikka, S. (2021). Implementing Bayesian networks for ISO 31000:2018-based Maritime Oil Spill Risk Management: State-of-art, implementation benefits and challenges, and future research directions. Journal of

Environmental Management, 278, 111520. https://doi.org/10.1016/j.jenvman.2020.111520

Redón, M., Villasis, M., & Miranda, M. (2016). Estadística descriptiva. Revista Alegría México, 63(4), 397–407.

Risk Management Community, (2020) What is the risk maturity model for ERM?, The Risk Maturity Model. RIMS. Recuperado el 5 de octubre de 2022, desde https://www.riskmaturitymodel.org/about-the-risk-maturity-model-for-erm/

Allen, J., Robins, A., Tomhave, B., & Heidt, E. (2014, March). Comparing Methodologies for IT Risk Assessment and Analysis. CERT's Podcast Series. other. Recuperado en 2021, desde Comparing Methodologies for IT Risk Assessment and Analysis.

Romero, A. (2021). Elementos Esenciales para elaborar un estudio con El Método (e)delphi. Enfermería Intensiva, 32(2), 100–104. https://doi.org/10.1016/j.enfi.2020.09.001

Ruge, J. (2012). Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Universidad Piloto De Colombia. Recuperado el 5 de octubre de 2022, desde http://polux.unipiloto.edu.co:8080/00000744.pdf.

Samblás, A. (2014, February 21). Gestión del Riesgo. Recuperado el 22 de noviembre de 2021, desde http://calidadtic.blogspot.com/2014/02/gestion-del-riesgo.html.

Silva, M. R., & Montilha, R. de. (2021). Aportes de la Técnica Delphi a la validación de una Evaluación de Terapia Ocupacional para la discapacidad visual. Cadernos Brasileiros De Terapia Ocupacional, 29. https://doi.org/10.1590/2526-8910.ctoao2163

Soler González, R., Varela-Lorenzo, P., Oñate-Andino, A., & Naranjo-Silva, E. (2018). La gestión de riesgo: el ausente recurrente de la administración de empresas. CIENCIA UNEMI, 11(26), 51-62. https://doi.org/10.29076/issn.2528-7737vol11iss26.2018pp51-62p

Srinivas, K. (2019). Process of Risk Management. Perspectives on Risk, Assessment and Management Paradigms. https://doi.org/10.5772/intechopen.80804

Starodub, L., & Sevilla, E. (2021, Noviembre 10). Distributivo de equipos tecnológicos de los laboratorios de informática FICA. personal.

Sterling, S., Plonsky, L., Larsson, T., Kytö, M., & Yaw, K. (2022). Introducing and illustrating the Delphi Method for Applied Linguistics Research. Research Methods in Applied Linguistics, 2(1), 2–4. https://doi.org/10.1016/j.rmal.2022.100040

Tamayo, M., González, D., De la Caridad, M., Fornet, J., & Cabrera, E. (2020). La gestión de riesgos (1st ed.). Universo Sur.

Tuapanta, J., Duque, M., & Mena, A. (2017). Alfa de Cronbach para validar un cuestionario de uso de Tic en Docentes Universitarios (thesis). ESPOCH, Riobamba.

Universidad Técnica del Norte. (2013). Plan de Desarrollo Informático UTN 2013- 2017.

Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000. RISTI - Revista Ibérica De Sistemas e Tecnologias De Informação, (22), 73–88. https://doi.org/10.17013/risti.22.73-88.

Vega, R., Arroyo, R., & Guun, S. (2017). Experience in Applying the Analysis and Risk Management Methodology called MAGERIT to Identify Threats and Vulnerabilities in an Agro-industrial Company. International Journal Of Applied Engineering Research, 12(17). Recuperado el 11 de octubre de 2022, desde https://repositorio.espe.edu.ec/handle/21000/19672.

Viguri, J. (2021). Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. IDP. Revista De Internet Derecho Y Política, (33). https://doi.org/10.7238/idp.v0i33.376366

Anexos

Anexo A: Encuesta sobre conciencia de gestión de riesgos

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC

Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Encuesta sobre la Conciencia en la Gestión de Riesgos

La presente encuesta tiene como finalidad recolectar información sobre el conocimiento y conciencia que se tiene acerca de la gestión de riesgos. La información recolectada será de carácter privada y los datos del encuestado no serán revelados.

Facultad: FICA

Carrera: _____

1. **¿Utiliza o a utilizado usted los equipos (computadores) disponibles en los laboratorios de informática FICA?**
   Si
   No

2. **¿Con qué frecuencia usted utiliza los laboratorios de Informática FICA?**
   Una vez a la semana
   De dos a tres veces a la semana
   Cuatro o más veces a la semana

3. **¿Qué actividades realiza en los equipos?**
   Investigación académica
   Uso de software educativo (programas o aplicaciones)
   Portafolio SIIU
   Ocio
   Otro

4. **En una escala del 1 al 5 ¿qué tan necesarios considera a los equipos en los laboratorios de informática FICA?**
   1) Nada necesaria
   2) Poco necesaria
   3) Necesaria
   4) Muy necesaria
   5) Sumamente necesaria

5. **¿Almacena su información en los equipos del laboratorio de Informática FICA?**
   Si
   No

A veces

6. **Cuando hace uso de los equipos del laboratorio de Informática FICA ¿en qué lugar almacena su información?**
   Nube
   Equipo (PC)
   Dispositivos externos físicos (Flash Memory, Disco externo)
   Otros (especifique)

7. **Si la respuesta a la pregunta anterior fue "Equipo (PC)" ¿cuándo ha vuelto a usar el mismo equipo, ¿su información guardada permanecía vigente?**
   Si
   No

8. **¿El equipo que utiliza en los laboratorios de informática FICA, cuenta con antivirus?**
   Si
   No
   No estoy seguro

9. **¿Conoce usted los riesgos presentes en los laboratorios de informática FICA?**
   Si
   No

10. **¿Conoce usted las políticas ante daño o hurto de equipos de los laboratorios de informática FICA?**
    Si
    No

11. **¿Conoce uste el procedimiento a seguir en caso incendios o fallas eléctricas dentro de los laboratorios de informática FICA?**
    Si
    No

Anexo B: Entrevista jefe Laboratorios informática FICA-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC

Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Trabajo de Titulación

Entrevista sobre la Gestión de Riesgos

La presente entrevista tiene como finalidad recolectar información necesaria acerca de la gestión de riesgos en los laboratorios de informática de la FICA-UTN.

Para esta entrevista se tomó en consideración a la responsable de los laboratorios de informática FICA-UTN, Ingeniera Ludmila Starodub. La transcripción de la entrevista es la siguiente.

1. **Dentro de la organización de los laboratorios de informática. ¿Existe algún tipo de Organigrama Estructural Interno? ¿Cuál es?**
2. **¿Cuál es el número total de laboratorios de informática en la FICA?**
3. **¿Qué cursos hacen uso de los laboratorios de informática FICA?**
4. **¿Cuál es el promedio ocupacional de equipos en los laboratorios?**
5. **¿Cuál es el proceso para poder acceder a los laboratorios?**
6. **¿Cuál es el proceso de mantenimiento que se les da a los equipos?**
7. **Dentro del personal vigente de los laboratorios de informática ¿Existen responsables sobre los activos como: computadores, proyectores, mouse?**
8. **¿Se cuenta con algún tipo de control o firewall para restringir el acceso hacia redes privadas por parte de los estudiantes?**
9. **¿Los equipos (computadoras) solicitan el inicio de sesión a todos los usuarios?**
10. **¿Se cuenta con algún tipo de servicio para mantener respaldos de la información en los equipos?**
11. **¿Se maneja de alguna forma el control de acceso a internet para los estudiantes?**
12. **¿Existen políticas de gestión de riesgos en los laboratorios, como, por ejemplo, que hacer ante incendios, fallos eléctricos, robo, programa maligno?**
13. **¿Qué sucede cuando algún activo se daña o está defectuoso?**

14. **¿Existe algún tipo de rendición de cuenta de activos al final de cada ciclo académico?**

15. **¿Se ha desarrollado capacitaciones al personal de los laboratorios sobre la gestión de riesgos?**

16. **¿Cuál ha sido el principal origen para perdida de activos? (Natural, antrópico)**

17. **¿Los activos cuentan con algún tipo de aseguramiento?**

18. **¿Cómo es el fichaje de los activos?**

19. **¿Cómo funciona la seguridad en los laboratorios?**

20. **¿Es permitido almacenar la información personal en los equipos de los laboratorios?**

21. **¿Se puede instalar software en los equipos de los laboratorios?**

Anexo C: Entrevista director Dirección de Desarrollo Tecnológico e Informático (DDTI)

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC

Resolución No 001-073 CEAACES – 2013 – 13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Trabajo de Titulación

Entrevista la Infraestructura Tecnológica UTN

La presente entrevista tiene como finalidad recolectar información necesaria acerca de la Infraestructura tecnológica dentro de la UTN, con el fin de tener un conocimiento más amplio sobre del contexto actual de los laboratorios de informática FICA.

Para esta entrevista se tomó en consideración al responsable de la Dirección de Desarrollo Tecnológico e Informático (DDTI), Ingeniero Jorge Caraguay. Las interrogantes de la entrevista son la siguiente.

1. **¿Los laboratorios de informática, son parte del DDTI o son responsabilidad de cada facultad?**

2. **¿Qué bases de datos se utilizan?**

3. **¿Existe un apartado en la base de datos para los datos de los laboratorios de informática?**

4. **¿Qué sistemas operativos utilizan los servidores de aplicaciones?**

5. **¿Qué marcas de dispositivos son utilizados en la red? (Cisco, Alcatel, 3Com, etc.)**

6. **¿Se tiene estándares de configuraciones para los equipos?**

7. **¿Se cuenta con políticas o procedimientos para actividades críticas? (respaldo de información, incidentes de seguridad, etc.)**

8. **Por favor, indique que elementos de seguridad tiene la red**
   - Firewall
   - Proxy
   - Packet filtering
   - IPS o IDS
   - Mail security -> Microsoft
   - Control de contenido
   - Gateway Antivirus
   - Antispyware
   - VPN
   - Antivirus PC

9. **En cuanto al internet,**
    - **El tipo de enlace a internet es: dedicado, ADSL, institucional u otro**:
    - **Velocidad de transmisión del enlace a internet es:**

10. **¿Se cuenta con respaldo de energía eléctrica?**

11. **¿Se tiene un diagrama de la topología de red? (Facilitar una imagen de ser posible)**

12. **¿A nivel Institucional se han realizado análisis de riesgos sobre TI?**

13. **¿Se han desarrollado capacitaciones sobre riesgos de TI?**

Anexo D: Modelo de Madurez de Riesgos (RMM)

FACTOR	DEFINICIÓN	REQUEIMIENTO	TAREA
Adopción del proceso basado en ERM	Mide la cultura de riesgo de la organización y considera el grado de apoyo ejecutivo o de la junta directiva para la gestión de riesgos empresariales	Definición de procesos comerciales y propiedad del riesgo	¿Están definidas formalmente las funciones y los procesos en toda la organización?
			¿Cada funcionario identifica sus propios riesgos en el contexto de un lenguaje de riesgo común?
			¿Los funcionarios de los procesos de negocio evalúan los riesgos de forma recurrente?
			¿Los funcionarios valoran y evalúan sus oportunidades con una frecuencia recurrente?
			¿Los funcionarios utilizan los resultados de las evaluaciones y el seguimiento de riesgos para identificar y actuar en las áreas de mejora?
			¿Los problemas de riesgo que enfrenta la organización están formalmente documentados, escalados y priorizados para su corrección oportuna?
		Propietario del proceso de soporte y de primera línea Participar	¿Se realizan evaluaciones de riesgos en todas las áreas?
			¿Son explícitas y bien comprendidas las relaciones entre los problemas, los hallazgos y sus riesgos?
		Visión previsora de gestión de riesgos	¿Los funcionarios crean planes de acción a largo plazo para cumplir con los objetivos de gestión de riesgos?
		Soporte ejecutivo de ERM	¿La organización promueve la rendición de cuentas al hacer que la gerencia de primera línea identifique, posea, evalúe y revise los riesgos de manera recurrente?
			¿Se requieren evaluaciones de riesgo cualitativas para cada gran proyecto, nuevo producto, cambio de modelo de negocio, etc.?
			¿Existe evidencia de las prioridades de riesgo hechas por el Comité de Riesgos?
			¿La competencia en gestión de riesgos es parte de las revisiones de desempeño en todos los niveles de la organización?

Descubrir el riesgo	Mide la calidad y la cobertura de sus evaluaciones de riesgos. Examina el método de recopilación de información sobre riesgos, el proceso de evaluación de riesgos y si se pueden descubrir tendencias y correlaciones en toda la empresa a partir de la información de riesgos.	Propiedad del riesgo por área de negocio	¿La identificación de riesgos está descentralizada y distribuida en cascada a los funcionarios más familiarizados con el riesgo y las actividades de mitigación correspondientes?
		Indicadores y Medidas de Riesgo Formalizados	¿Se utilizan criterios de evaluación estandarizados para el impacto del riesgo, la probabilidad y la eficacia del control para clasificar y priorizar objetivamente activos?
			Además de las evaluaciones a nivel empresarial, ¿los funcionarios llevan a cabo, análisis y evaluaciones de riesgos específicos (p. ej., procesos críticos y proyectos de alto riesgo)?
		Informes de seguimiento	¿La organización considera tanto las ventajas como las desventajas de los riesgos identificados en sus informes de ERM?
			¿Se prueban regularmente las actividades de mitigación y control para garantizar que estén implementadas y reduzcan el riesgo de manera efectiva?
		Eventos adversos como oportunidades	¿Se identifican y evalúan las oportunidades y los objetivos estratégicos como parte del proceso de gestión de riesgos?
Gestión de procesos ERM	Mide el grado en que la organización ha adoptado una metodología ERM a lo largo de su cultura y decisiones organizacionales, y qué tan bien el programa de gestión de riesgos sigue los pasos de mejores prácticas para identificar, evaluar, evaluar, mitigar y monitorear los riesgos.	Supervisión del programa ERM	¿Cada área tiene una persona designada responsable de identificar vulnerabilidades de riesgo, mantener el cumplimiento normativo y alcanzar los objetivos de desempeño?
			¿Se delega la responsabilidad de la gestión de riesgos en toda la estructura organizativa (p. ej., procesos comerciales, líneas de productos, etc.)
			¿Los gerentes participan activamente en el programa Gestión de Riesgos Empresarial?
		Pasos del proceso ERM	¿Hay un marco común de gestión de riesgos (p. ej., biblioteca de riesgos de causa raíz, criterios de evaluación de riesgos, etc.) disponible y utilizado por todas las áreas?
			¿Se utilizan pasos secuenciales e iterativos de identificación, evaluación, evaluación, mitigación y monitoreo de riesgos para mejorar el desempeño, la toma de decisiones y la asignación de presupuesto?
			¿Las evaluaciones cualitativas determinan la necesidad y la prioridad de más análisis o modelos cuantitativos?

		Cultura de Riesgo, Rendición de Cuentas y Comunicación	¿Se comprenden e integran los procedimientos de gestión de riesgos y la cultura de riesgos en todos los niveles de la organización?
			¿Se evalúan las oportunidades estratégicas en múltiples dimensiones, como el impacto, el momento y la confianza en que se pueden lograr los resultados positivos?
		Informes de gestión de riesgos	¿Los informes que miden el progreso del programa y las actividades de la Gestión de Riesgos se proporcionan a las partes interesadas con una frecuencia establecida?
		Repetibilidad y Escalabilidad	¿Las evaluaciones de riesgos son agregadas y revisadas periódicamente por un comité de riesgos corporativos?
			¿Se revisan y actualizan periódicamente los criterios y supuestos utilizados al realizar evaluaciones de riesgos?
Gestión del apetito de riesgo	Evalúa el nivel de conciencia sobre las compensaciones riesgo-recompensa, la responsabilidad por el riesgo, la definición de tolerancias al riesgo y si la organización es efectiva para cerrar la brecha entre el riesgo potencial y el real	Vista de la cartera de riesgos	¿La visión organizativa del riesgo es dinámica (p. ej., por proceso empresarial, categoría de riesgo y objetivo estratégico)?
			¿La tolerancia al riesgo está formalmente definida para cada área y categoría de riesgo?
			¿Se agrega y analiza la información de la evaluación de riesgos y se abordan las dependencias?
			¿Se abordan periódicamente las diferencias entre la tolerancia al riesgo definida y los riesgos materializados?
		Compensaciones de riesgo-recompensa	¿Se entienden las compensaciones riesgo-recompensa y los líderes las utilizan para impulsar sus acciones?
			¿Se consideran el apetito por el riesgo y las compensaciones riesgo-recompensa a lo largo de cada paso iterativo del proceso Gestión de Riesgo?
			Cuando ocurre un evento de riesgo, ¿se evalúa el riesgo para determinar si el evento se identificó previamente y si la evaluación fue precisa?
			¿Se vuelven a evaluar los riesgos cuando cambian las métricas clave de riesgo y rendimiento?
			¿La asignación de recursos se basa en un análisis de riesgo-recompensa?

			¿Se miden las evaluaciones de riesgos que consideran los efectos de las actividades de mitigación frente a la tolerancia al riesgo de la organización?
Disciplina de causa raíz	Evalúa el grado en que una organización identifica el riesgo por fuente, o causa raíz, frente a los síntomas y resultados que producen. Centrarse en la causa raíz de un riesgo y clasificarlos en consecuencia fortalecerá los esfuerzos de respuesta y mitigación	Consideración de la causa raíz	¿Se identifican todos los riesgos utilizando un enfoque de causa raíz para garantizar que se aborde el problema y no el síntoma?
			¿Se utilizan categorías de causa raíz para distinguir entre riesgos dentro de las evaluaciones de riesgos? (por ejemplo, fraude externo versus interno)
			¿Se comprenden las causas y efectos de los riesgos?
		Recopilación de información sobre riesgos y oportunidades	¿Se desarrollan evaluaciones de riesgos y planes de acción en el contexto de ejemplos y escenarios concretos?
			¿Se rastrean y utilizan las causas fundamentales de los incidentes o eventos de pérdida para determinar la eficacia de los controles?
		Clasificación de la información	¿Se identifican, evalúan, mitigan, controlan y notifican a lo largo del tiempo los riesgos financieros específicos (p. ej., crédito, liquidez, capital, etc.)?
			¿Se identifican, evalúan y monitorean las causas fundamentales de los riesgos operativos?
			¿Se documentan, miden, informan y gestionan los objetivos de la organización?
			¿Todos los departamentos utilizan un vocabulario uniforme de gestión de riesgos empresariales y una clasificación de la información?
		Dependencias y Consecuencias	¿Se utilizan evaluaciones de riesgos para determinar los efectos potenciales (es decir, pérdidas y ganancias) sobre los objetivos?
			¿Se utilizan las causas fundamentales de todos los incidentes y eventos de pérdida para impulsar la asignación de recursos para implementar controles más estrictos?
			¿Está claro cómo el riesgo de un departamento podría afectar a otros departamentos, así como a toda la organización?
Resiliencia y sostenibilidad empresarial	Evalúa el grado en que la continuidad del negocio, la planificación	Planificación basada en riesgos	¿Las evaluaciones de riesgos impulsan el equilibrio entre los resultados diarios y las prioridades a largo plazo?
		Comprender las consecuencias	¿Las evaluaciones de riesgos realizadas por los propietarios de riesgos de primera línea impulsan el análisis y la planificación de la continuidad?

	operativa y otras actividades de sostenibilidad se abordan con una metodología basada en el riesgo		¿Las dependencias ascendentes y descendentes de los recursos clave (personas, proveedores, aplicaciones de TI) se entienden en todas las áreas y se consideran durante el proceso de ERM?
		Resiliencia y planificación operativa	¿Se consideran las categorías de riesgo de causa raíz (personas, procesos, entorno externo, relaciones, sistemas, etc.) en la planificación?
			¿Están las evaluaciones, políticas y procedimientos bien documentados, fácilmente disponibles y actualizados regularmente?
			¿Las unidades de negocios informan sobre cómo los eventos externos e internos impactan sus modelos de negocios y objetivos estratégicos?
			¿La identificación y evaluación de múltiples escenarios juega un papel en la planificación estratégica?
Gestión del rendimiento	Determina el grado en que una organización ejecuta sus visiones y estrategia. Evalúa la fortaleza en la planificación, comunicación y medición de los objetivos centrales de la empresa con un proceso basado en el riesgo, y la medida en que el progreso se desvía de las expectativas	Comunicación de metas	¿Los objetivos de la organización están vinculados a medidas de desempeño específicas?
			¿Son los empleados de todos los niveles responsables de comprender y tomar medidas sobre los riesgos que pueden impedirles alcanzar sus objetivos?
			¿Todos los empleados entienden cómo la evaluación de las compensaciones riesgo-recompensa les ayuda a alcanzar los objetivos?
			¿Entienden los empleados los efectos potenciales de los principales riesgos de la organización, en caso de que se materialicen?
			¿Las decisiones de asignación de recursos se basan en criterios de evaluación formalizados, como el impacto en el desempeño, el momento de los beneficios y la garantía de que se pueden lograr los resultados positivos?
		Información y planificación de ERM	Al establecer prioridades para la planificación estratégica, ¿se tiene en cuenta la gestión de riesgos empresariales?
			¿La competencia en gestión de riesgos es parte de las discusiones sobre compensación y desarrollo profesional en toda la organización?
			¿Es la gestión de riesgos empresariales una parte formal del establecimiento de objetivos?

	Objetivos y actividades del proceso de ERM	Al evaluar nuevas oportunidades, ¿la organización mide e informa la efectividad de sus esfuerzos de gestión de riesgos?
		¿Las áreas consideran su impacto en otras áreas de la organización al determinar sus objetivos (por ejemplo, finanzas, cumplimiento y otras implicaciones estratégicas)?
		¿Utilizan los empleados de todos los niveles un enfoque basado en el riesgo (es decir, evaluaciones, controles y seguimiento de riesgos regulares) para alcanzar los objetivos departamentales y corporativos?
		¿Se evalúan las desviaciones en las expectativas frente a los resultados de los proyectos, iniciativas e hitos operativos en el contexto de las metas?

Nota: La tabla muestra los siete factores, con sus requerimientos y tareas específicas para el Medición de la madurez de Gestión de Riesgos en una organización. Elaboración propia a partir de The Risk Maturity Model, por Risk Management Community, 2020, (https://rmm.my.logicmanager.com/).

Anexo E: Identificación de Amenazas en los laboratorios de informática FICA-UTN

ACTIVO	AMENAZAS
ESENCIALES	
Datos de acceso a servidores y sistemas	[A.13] Repudio (negación de actuaciones)
Base de datos de los sistemas informáticos de la Facultad	[A.13] Repudio (negación de actuaciones)
DATOS / INFORMACIÓN	
Documentos de administración interna	[E.15] Alteración de la información
Documentos de administración interna	[E.18] Destrucción de la información
Documentos de administración interna	[E.19] Fugas de información
Documentos de administración interna	[A.5] Suplantación de identidad
Documentos de administración interna	[A.6] Abuso de privilegios de acceso
Documentos de administración interna	[A.11] Acceso no autorizado
Datos de configuración	[E.4] Errores de configuración
Datos de configuración	[E.15] Alteración de la información
Datos de configuración	[E.18] Destrucción de la información
Datos de configuración	[E.19] Fugas de información
Datos de configuración	[A.4] Manipulación de los ficheros de configuración
Datos de configuración	[A.5] Suplantación de identidad
Datos de configuración	[A.6] Abuso de privilegios de acceso
Datos de configuración	[A.11] Acceso no autorizado
SERVICIOS	
Internet	
Mantenimiento preventivo y correctivo de hardware y software	[E.1] Errores de los usuarios
Mantenimiento preventivo y correctivo de hardware y software	[E.2] Errores del administrador del sistema / de la seguridad
Mantenimiento preventivo y correctivo de hardware y software	[E.15] Alteración de la información
Mantenimiento preventivo y correctivo de hardware y software	[E.18] Destrucción de la información
Mantenimiento preventivo y correctivo de hardware y software	[E.19] Fugas de información
Mantenimiento preventivo y correctivo de hardware y software	[E.24] Caída del sistema por agotamiento de recursos
Mantenimiento preventivo y correctivo de hardware y software	[A.5] Suplantación de identidad

Mantenimiento preventivo y correctivo de hardware y software	[A.6] Abuso de privilegios de acceso
Mantenimiento preventivo y correctivo de hardware y software	[A.7] Uso no previsto
Mantenimiento preventivo y correctivo de hardware y software	[A.11] Acceso no autorizado
Mantenimiento preventivo y correctivo de hardware y software	[A.13] Repudio (negación de actuaciones)
Mantenimiento preventivo y correctivo de hardware y software	[A.15] Modificación de la información
Mantenimiento preventivo y correctivo de hardware y software	[A.18] Destrucción de la información
Mantenimiento preventivo y correctivo de hardware y software	[A.24] Denegación de servicio
Telefonía	[E.1] Errores de los usuarios
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad
Telefonía	[E.15] Alteración de la información
Telefonía	[E.18] Destrucción de la información
Telefonía	[E.19] Fugas de información
Telefonía	[E.24] Caída del sistema por agotamiento de recursos
Telefonía	[A.5] Suplantación de identidad
Telefonía	[A.6] Abuso de privilegios de acceso
Telefonía	[A.7] Uso no previsto
Telefonía	[A.11] Acceso no autorizado
Telefonía	[A.13] Repudio (negación de actuaciones)
Telefonía	[A.15] Modificación de la información
Telefonía	[A.16]
Telefonía	[A.18] Destrucción de la información
Servidores internos	[E.1] Errores de los usuarios
Servidores internos	[E.2] Errores del administrador del sistema / de la seguridad
Servidores internos	[E.15] Alteración de la información
Servidores internos	[E.18] Destrucción de la información
Servidores internos	[E.19] Fugas de información
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos
Servidores internos	[A.5] Suplantación de identidad
Servidores internos	[A.6] Abuso de privilegios de acceso
Servidores internos	[A.7] Uso no previsto
Servidores internos	[A.11] Acceso no autorizado
Servidores internos	[A.13] Repudio (negación de actuaciones)
Servidores internos	[A.15] Modificación de la información
Servidores internos	[A.18] Destrucción de la información
Servidores internos	[A.24] Denegación de servicio

SOFTWARE	
Sistema reserva instalaciones FICA	[I.5.1.] Avería de origen lógico
Sistema reserva instalaciones FICA	[E.8] Difusión de software dañino
Sistema reserva instalaciones FICA	[E.20] Vulnerabilidades de los programas (software)
Sistema reserva instalaciones FICA	[E.21] Errores de mantenimiento / actualización de programas
Sistema reserva instalaciones FICA	[A.8] Difusión de software dañino
Sistema reserva instalaciones FICA	[A.22] Manipulación de programas
Aplicación para el manejo de biométricos	[I.5.1.] Avería de origen lógico
Aplicación para el manejo de biométricos	[E.8] Difusión de software dañino
Aplicación para el manejo de biométricos	[E.20] Vulnerabilidades de los programas (software)
Aplicación para el manejo de biométricos	[E.21] Errores de mantenimiento / actualización de programas
Aplicación para el manejo de biométricos	[A.8] Difusión de software dañino
Aplicación para el manejo de biométricos	[A.22] Manipulación de programas
Portal Web para Capacitaciones	[I.5.1.] Avería de origen lógico
Portal Web para Capacitaciones	[E.8] Difusión de software dañino
Portal Web para Capacitaciones	[E.20] Vulnerabilidades de los programas (software)
Portal Web para Capacitaciones	[E.21] Errores de mantenimiento / actualización de programas
Portal Web para Capacitaciones	[A.8] Difusión de software dañino
Portal Web para Capacitaciones	[A.22] Manipulación de programas
Revista electrónica de la FICA	[I.5.1.] Avería de origen lógico
Revista electrónica de la FICA	[E.8] Difusión de software dañino
Revista electrónica de la FICA	[E.20] Vulnerabilidades de los programas (software)
Revista electrónica de la FICA	[E.21] Errores de mantenimiento / actualización de programas
Revista electrónica de la FICA	[A.8] Difusión de software dañino
Revista electrónica de la FICA	[A.22] Manipulación de programas
Aplicaciones de ofimática / académicas	[I.5.1.] Avería de origen lógico
Aplicaciones de ofimática / académicas	[E.8] Difusión de software dañino
Aplicaciones de ofimática / académicas	[E.20] Vulnerabilidades de los programas (software)
Aplicaciones de ofimática / académicas	[E.21] Errores de mantenimiento / actualización de programas

Aplicaciones de ofimática / académicas	[A.8] Difusión de software dañino
Aplicaciones de ofimática / académicas	[A.22] Manipulación de programas
HARDWARE	
Equipos PC / didácticos	[N.1] Fuego
Equipos PC / didácticos	[N.2] Daños por agua
Equipos PC / didácticos	[N.] Desastres naturales
Equipos PC / didácticos	[I.1] Fuego
Equipos PC / didácticos	[I.2] Daños por agua
Equipos PC / didácticos	[I.] Desastres industriales
Equipos PC / didácticos	[I.3] Contaminación medioambiental
Equipos PC / didácticos	[I.4] Contaminación electromagnética
Equipos PC / didácticos	[I.5.2] Avería de origen físico
Equipos PC / didácticos	[I.6] Corte de suministro eléctrico
Equipos PC / didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad
Equipos PC / didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipos PC / didácticos	[E.23] Errores de mantenimiento (actualización de equipos (hardware)
Equipos PC / didácticos	[E.24] Caída del sistema por agotamiento de recursos
Equipos PC / didácticos	[E.25] Pérdida de equipos
Equipos PC / didácticos	[A.7] Uso no previsto
Equipos PC / didácticos	[A.11] Acceso no autorizado
Equipos PC / didácticos	[A.23] Manipulación del hardware
Equipos PC / didácticos	[A.24] Denegación de servicio
Equipos PC / didácticos	[A.25] Robo de equipos
Equipos PC / didácticos	[A.26] Ataque destructivo
Equipos de seguridad	[N.1] Fuego
Equipos de seguridad	[N.2] Daños por agua
Equipos de seguridad	[N.] Desastres naturales
Equipos de seguridad	[I.1] Fuego
Equipos de seguridad	[I.2] Daños por agua
Equipos de seguridad	[I.] Desastres industriales
Equipos de seguridad	[I.3] Contaminación medioambiental
Equipos de seguridad	[I.4] Contaminación electromagnética
Equipos de seguridad	[I.5.2] Avería de origen físico

Equipos de seguridad	[I.6] Corte de suministro eléctrico
Equipos de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad
Equipos de seguridad	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipos de seguridad	[E.23] Errores de mantenimiento (actualización de equipos (hardware)
Equipos de seguridad	[E.24] Caída del sistema por agotamiento de recursos
Equipos de seguridad	[E.25] Pérdida de equipos
Equipos de seguridad	[A.7] Uso no previsto
Equipos de seguridad	[A.11] Acceso no autorizado
Equipos de seguridad	[A.23] Manipulación del hardware
Equipos de seguridad	[A.24] Denegación de servicio
Equipos de seguridad	[A.25] Robo de equipos
Equipos de seguridad	[A.26] Ataque destructivo
Equipos para redes de telecomunicaciones	[N.1] Fuego
Equipos para redes de telecomunicaciones	[N.2] Daños por agua
Equipos para redes de telecomunicaciones	[N.] Desastres naturales
Equipos para redes de telecomunicaciones	[I.1] Fuego
Equipos para redes de telecomunicaciones	[I.2] Daños por agua
Equipos para redes de telecomunicaciones	[I.] Desastres industriales
Equipos para redes de telecomunicaciones	[I.3] Contaminación medioambiental
Equipos para redes de telecomunicaciones	[I.4] Contaminación electromagnética
Equipos para redes de telecomunicaciones	[I.5.2] Avería de origen físico
Equipos para redes de telecomunicaciones	[I.6] Corte de suministro eléctrico
Equipos para redes de telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad
Equipos para redes de telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipos para redes de telecomunicaciones	[E.23] Errores de mantenimiento (actualización de equipos (hardware)
Equipos para redes de telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos
Equipos para redes de telecomunicaciones	[E.25] Pérdida de equipos

Equipos para redes de telecomunicaciones	[A.7] Uso no previsto
Equipos para redes de telecomunicaciones	[A.11] Acceso no autorizado
Equipos para redes de telecomunicaciones	[A.23] Manipulación del hardware
Equipos para redes de telecomunicaciones	[A.24] Denegación de servicio
Equipos para redes de telecomunicaciones	[A.25] Robo de equipos
Equipos para redes de telecomunicaciones	[A.26] Ataque destructivo
REDES DE COMUNICACIONES	
Red interna laboratorios	[I.8] Fallo de servicios de comunicaciones
Red interna laboratorios	[E.2] Errores del administrador del sistema / de la seguridad
Red interna laboratorios	[E.9] Errores de [re-]encadenamiento
Red interna laboratorios	[E.10] Errores de secuencia
Red interna laboratorios	[E.15] Alteración de la información
Red interna laboratorios	[E.19] Fugas de información
Red interna laboratorios	[E.24] Caída del sistema por agotamiento de recursos
Red interna laboratorios	[A.5] Suplantación de identidad
Red interna laboratorios	[A.7] Uso no previsto
Red interna laboratorios	[A.9] [Re-]encaminamiento de mansajes
Red interna laboratorios	[A.10] Alteración de secuencias
Red interna laboratorios	[A.11] Acceso no autorizado
Red interna laboratorios	[A.12] Análisis de tráfico
Red interna laboratorios	[A.14] Interceptación de información (escucha)
Red interna laboratorios	[A.15] Modificación de la información
Red interna laboratorios	[A.18] Destrucción de la información
Red interna laboratorios	[A.24] Denegación de servicio
EQUIPAMIENTO AUXILIAR	
Equipamiento eléctrico	[N.1] Fuego
Equipamiento eléctrico	[N.2] Daño por agua
Equipamiento eléctrico	[N.] Desastres naturales
Equipamiento eléctrico	[I.1] Fuego
Equipamiento eléctrico	[I.2] Daños por agua
Equipamiento eléctrico	[I.] Desastres industriales
Equipamiento eléctrico	[I.3] Contaminación medioambiental
Equipamiento eléctrico	[I.4] Contaminación electromagnética
Equipamiento eléctrico	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipamiento eléctrico	[E.23] Errores de mantenimiento (actualización de equipos (hardware)
Equipamiento eléctrico	[A.7] Uso no previsto

Equipamiento eléctrico	[A.11] Acceso no autorizado
Equipamiento eléctrico	[A.23] Manipulación del hardware
Equipamiento eléctrico	[A.25] Robo de equipos
Equipamiento eléctrico	[A.26] Ataque destructivo
Mobiliario para los equipos	[N.1] Fuego
Mobiliario para los equipos	[N.2] Daño por agua
Mobiliario para los equipos	[N.] Desastres naturales
Mobiliario para los equipos	[I.1] Fuego
Mobiliario para los equipos	[I.2] Daños por agua
Mobiliario para los equipos	[I.] Desastres industriales
Mobiliario para los equipos	[I.3] Contaminación medioambiental
Mobiliario para los equipos	[E.23] Errores de mantenimiento (actualización de equipos (hardware)
Mobiliario para los equipos	[A.7] Uso no previsto
Mobiliario para los equipos	[A.23] Manipulación del hardware
Mobiliario para los equipos	[A.25] Robo de equipos
Mobiliario para los equipos	[A.26] Ataque destructivo
SOPORTES DE INFORMACIÓN	
Nube Microsoft OneDrive	[N.1] Fuego
Nube Microsoft OneDrive	[N.2] Daño por agua
Nube Microsoft OneDrive	[N.] Desastres naturales
Nube Microsoft OneDrive	[I.1] Fuego
Nube Microsoft OneDrive	[I.2] Daños por agua
Nube Microsoft OneDrive	[I.] Desastres industriales
Nube Microsoft OneDrive	[I.3] Contaminación medioambiental
Nube Microsoft OneDrive	[I.4] Contaminación electromagnética
Nube Microsoft OneDrive	[I.5.2] Avería de origen físico
Nube Microsoft OneDrive	[I.6] Corte del suministro eléctrico
Nube Microsoft OneDrive	[I.7] Condiciones inadecuadas de temperatura o humedad
Nube Microsoft OneDrive	[I.10] Degradación de los soportes de almacenamiento de la información
Nube Microsoft OneDrive	[I.11] Emanaciones electromagnéticas (TEMPEST)
Nube Microsoft OneDrive	[E.1] Errores de los usuarios
Nube Microsoft OneDrive	[E.15] Alteración de la información
Nube Microsoft OneDrive	[E.18] Destrucción de la información
Nube Microsoft OneDrive	[E.19] Fugas de información
Nube Microsoft OneDrive	[E.23] Errores de mantenimiento (actualización de equipos (hardware)
Nube Microsoft OneDrive	[E.25] Pérdida de equipos
Nube Microsoft OneDrive	[A.7] Uso no previsto
Nube Microsoft OneDrive	[A.11] Acceso no autorizado
Nube Microsoft OneDrive	[A.15] Modificación de la información

Nube Microsoft OneDrive	[A.18] Destrucción de la información
Nube Microsoft OneDrive	[A.23] Manipulación del hardware
Nube Microsoft OneDrive	[A.25] Robo de equipos
Nube Microsoft OneDrive	[A.26] Ataque destructivo
INSTALACIONES	
Espacios físicos Lab 1 a 9	[N.1] Fuego
Espacios físicos Lab 1 a 10	[N.2] Daño por agua
Espacios físicos Lab 1 a 11	[N.] Desastres naturales
Espacios físicos Lab 1 a 12	[I.1] Fuego
Espacios físicos Lab 1 a 13	[I.2] Daños por agua
Espacios físicos Lab 1 a 14	[I.] Desastres industriales
Espacios físicos Lab 1 a 15	[I.3] Contaminación medioambiental
Espacios físicos Lab 1 a 16	[I.4] Contaminación electromagnética
Espacios físicos Lab 1 a 17	[E.25] Pérdida de equipos
Espacios físicos Lab 1 a 18	[A.6] Abuso de privilegios de acceso
Espacios físicos Lab 1 a 19	[A.7] Uso no previsto
Espacios físicos Lab 1 a 20	[A.25] Robo de equipos
Espacios físicos Lab 1 a 21	[A.26] Ataque destructivo
Espacios físicos Lab 1 a 22	[A.27] Ocupación enemiga
Área de servidores y comunicaciones	[N.1] Fuego
Área de servidores y comunicaciones	[N.2] Daño por agua
Área de servidores y comunicaciones	[N.] Desastres naturales
Área de servidores y comunicaciones	[I.1] Fuego
Área de servidores y comunicaciones	[I.2] Daños por agua
Área de servidores y comunicaciones	[I.] Desastres industriales
Área de servidores y comunicaciones	[I.3] Contaminación medioambiental
Área de servidores y comunicaciones	[I.4] Contaminación electromagnética
Área de servidores y comunicaciones	[E.25] Pérdida de equipos
Área de servidores y comunicaciones	[A.6] Abuso de privilegios de acceso
Área de servidores y comunicaciones	[A.7] Uso no previsto
Área de servidores y comunicaciones	[A.25] Robo de equipos
Área de servidores y comunicaciones	[A.26] Ataque destructivo

Área de servidores y comunicaciones	[A.27] Ocupación enemiga
Área de soporte y mantenimiento	[N.1] Fuego
Área de soporte y mantenimiento	[N.2] Daño por agua
Área de soporte y mantenimiento	[N.] Desastres naturales
Área de soporte y mantenimiento	[I.1] Fuego
Área de soporte y mantenimiento	[I.2] Daños por agua
Área de soporte y mantenimiento	[I.] Desastres industriales
Área de soporte y mantenimiento	[I.3] Contaminación medioambiental
Área de soporte y mantenimiento	[I.4] Contaminación electromagnética
Área de soporte y mantenimiento	[E.25] Pérdida de equipos
Área de soporte y mantenimiento	[A.6] Abuso de privilegios de acceso
Área de soporte y mantenimiento	[A.7] Uso no previsto
Área de soporte y mantenimiento	[A.25] Robo de equipos
Área de soporte y mantenimiento	[A.26] Ataque destructivo
Área de soporte y mantenimiento	[A.27] Ocupación enemiga
PERSONAL	
Jefe de Laboratorios	[E.15] Alteración de la información
Jefe de Laboratorios	[E.18] Destrucción de la información
Jefe de Laboratorios	[E.19] Fugas de información
Jefe de Laboratorios	[E.28] Indisponibilidad del personal
Jefe de Laboratorios	[A.15] Modificación de la información
Jefe de Laboratorios	[A.18] Destrucción de la información
Jefe de Laboratorios	[A.19] Revelación de información
Jefe de Laboratorios	[A.28] Indisponibilidad del personal
Jefe de Laboratorios	[A.29] Extorsión
Jefe de Laboratorios	[A.30] Ingeniería social (picaresca)
Asistente de Laboratorios 1	[E.15] Alteración de la información
Asistente de Laboratorios 1	[E.18] Destrucción de la información
Asistente de Laboratorios 1	[E.19] Fugas de información
Asistente de Laboratorios 1	[E.28] Indisponibilidad del personal
Asistente de Laboratorios 1	[A.15] Modificación de la información
Asistente de Laboratorios 1	[A.18] Destrucción de la información
Asistente de Laboratorios 1	[A.19] Revelación de información
Asistente de Laboratorios 1	[A.28] Indisponibilidad del personal
Asistente de Laboratorios 1	[A.29] Extorsión
Asistente de Laboratorios 1	[A.30] Ingeniería social (picaresca)
Asistente de Laboratorios 2	[E.15] Alteración de la información
Asistente de Laboratorios 2	[E.18] Destrucción de la información
Asistente de Laboratorios 2	[E.19] Fugas de información
Asistente de Laboratorios 2	[E.28] Indisponibilidad del personal
Asistente de Laboratorios 2	[A.15] Modificación de la información
Asistente de Laboratorios 2	[A.18] Destrucción de la información

Asistente de Laboratorios 2	[A.19] Revelación de información
Asistente de Laboratorios 2	[A.28] Indisponibilidad del personal
Asistente de Laboratorios 2	[A.29] Extorsión
Asistente de Laboratorios 2	[A.30] Ingeniería social (picaresca)
Usuarios Laboratorios	[E.15] Alteración de la información
Usuarios Laboratorios	[E.18] Destrucción de la información
Usuarios Laboratorios	[E.19] Fugas de información
Usuarios Laboratorios	[A.13] Repudio (negación de actuaciones)
Usuarios Laboratorios	[A.15] Modificación de la información
Usuarios Laboratorios	[A.18] Destrucción de la información
Usuarios Laboratorios	[A.19] Revelación de información
Usuarios Laboratorios	[A.28] Indisponibilidad del personal
Usuarios Laboratorios	[A.29] Extorsión
Usuarios Laboratorios	[A.30] Ingeniería social (picaresca)

Nota: Elaboración propia

Anexo F: Valoración de Amenazas en los laboratorios de informática FICA-UTN

ACTIVO	AMENAZAS	FRECUENCIA	D	I	C	A	T
ESENCIALES							
Datos de acceso a servidores y sistemas	[A.13] Repudio (negación de actuaciones)	1					50%
Base de datos de los sistemas informáticos de la Facultad	[A.13] Repudio (negación de actuaciones)	1					50%
DATOS / INFORMACIÓN							
Documentos de administración interna	[E.15] Alteración de la información	1		1%			
Documentos de administración interna	[E.18] Destrucción de la información	1	1%				
Documentos de administración interna	[E.19] Fugas de información	1			10%		
Documentos de administración interna	[A.5] Suplantación de identidad	10		10%	50%	100%	
Documentos de administración interna	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Documentos de administración interna	[A.11] Acceso no autorizado	100		10%	50%		
Datos de configuración	[E.4] Errores de configuración	1		1%			
Datos de configuración	[E.15] Alteración de la información	1		1%			
Datos de configuración	[E.18] Destrucción de la información	1	1%				
Datos de configuración	[E.19] Fugas de información	1			10%		
Datos de configuración	[A.4] Manipulación de los ficheros de configuración	10	10%	10%	10%		
Datos de configuración	[A.5] Suplantación de identidad	10		10%	50%	100%	
Datos de configuración	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Datos de configuración	[A.11] Acceso no autorizado	100		10%	50%		
SERVICIOS							
Internet							

Mantenimiento preventivo y correctivo de hardware y software	[E.1] Errores de los usuarios	1	10%	10%	10%		
Mantenimiento preventivo y correctivo de hardware y software	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%		
Mantenimiento preventivo y correctivo de hardware y software	[E.15] Alteración de la información	1		1%			
Mantenimiento preventivo y correctivo de hardware y software	[E.18] Destrucción de la información	1	10%				
Mantenimiento preventivo y correctivo de hardware y software	[E.19] Fugas de información	1			10%		
Mantenimiento preventivo y correctivo de hardware y software	[E.24] Caída del sistema por agotamiento de recursos	10	50%				
Mantenimiento preventivo y correctivo de hardware y software	[A.5] Suplantación de identidad	1		50%	50%	100%	
Mantenimiento preventivo y correctivo de hardware y software	[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	100%	
Mantenimiento preventivo y correctivo de hardware y software	[A.7] Uso no previsto	1	1%	10%	10%		
Mantenimiento preventivo y correctivo de hardware y software	[A.11] Acceso no autorizado	1		10%	50%	100%	
Mantenimiento preventivo y correctivo de hardware y software	[A.13] Repudio (negación de actuaciones)	5					100%
Mantenimiento preventivo y correctivo de hardware y software	[A.15] Modificación de la información	10		50%			

Mantenimiento preventivo y correctivo de hardware y software	[A.18] Destrucción de la información	1	50%				
Mantenimiento preventivo y correctivo de hardware y software	[A.24] Denegación de servicio	10	50%				
Telefonía	[E.1] Errores de los usuarios	1	10%	10%	10%		
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%		
Telefonía	[E.15] Alteración de la información	1		1%			
Telefonía	[E.18] Destrucción de la información	1	10%				
Telefonía	[E.19] Fugas de información	1			10%		
Telefonía	[E.24] Caída del sistema por agotamiento de recursos	10	50%				
Telefonía	[A.5] Suplantación de identidad	1		50%	50%	100%	
Telefonía	[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	100%	
Telefonía	[A.7] Uso no previsto	1	1%	10%	10%		
Telefonía	[A.11] Acceso no autorizado	1		10%	50%	100%	
Telefonía	[A.13] Repudio (negación de actuaciones)	5					100%
Telefonía	[A.15] Modificación de la información	10		50%			
Telefonía	[A.18] Destrucción de la información	1	50%				
Telefonía	[E.24] Caída del sistema por agotamiento de recursos	10	50%				
Servidores internos	[E.1] Errores de los usuarios	1	10%	10%	10%		
Servidores internos	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%		
Servidores internos	[E.15] Alteración de la información	1		1%			
Servidores internos	[E.18] Destrucción de la información	1	10%				
Servidores internos	[E.19] Fugas de información	1			10%		
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	10	50%				
Servidores internos	[A.5] Suplantación de identidad	1		50%	50%	100%	

Servidores internos	[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	100%	
Servidores internos	[A.7] Uso no previsto	1	1%	10%	10%		
Servidores internos	[A.11] Acceso no autorizado	1		10%	50%	100%	
Servidores internos	[A.13] Repudio (negación de actuaciones)	5					100%
Servidores internos	[A.15] Modificación de la información	10		50%			
Servidores internos	[A.18] Destrucción de la información	1	50%				
Servidores internos	[A.24] Denegación de servicio	10	50%				
SOFTWARE							
Sistema reserva instalaciones FICA	[I.5.1.] Avería de origen lógico	1	50%				
Sistema reserva instalaciones FICA	[E.8] Difusión de software dañino	1	10%	10%	10%		
Sistema reserva instalaciones FICA	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%		
Sistema reserva instalaciones FICA	[E.21] Errores de mantenimiento / actualización de programas	10	1%	10%	50%		
Sistema reserva instalaciones FICA	[A.8] Difusión de software dañino	1	100%	100%	100%		
Sistema reserva instalaciones FICA	[A.22] Manipulación de programas	1	50%	100%	100%		
Aplicación para el manejo de biométricos	[I.5.1.] Avería de origen lógico	1	50%				
Aplicación para el manejo de biométricos	[E.8] Difusión de software dañino	1	10%	10%	10%		
Aplicación para el manejo de biométricos	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%		
Aplicación para el manejo de biométricos	[E.21] Errores de mantenimiento / actualización de programas	10	1%	10%	50%		
Aplicación para el manejo de biométricos	[A.8] Difusión de software dañino	1	100%	100%	100%		
Aplicación para el manejo de biométricos	[A.22] Manipulación de programas	1	50%	100%	100%		

Portal Web para Capacitaciones	[I.5.1.] Avería de origen lógico	1	50%		
Portal Web para Capacitaciones	[E.8] Difusión de software dañino	1	10%	10%	10%
Portal Web para Capacitaciones	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Portal Web para Capacitaciones	[E.21] Errores de mantenimiento / actualización de programas	10	1%	10%	50%
Portal Web para Capacitaciones	[A.8] Difusión de software dañino	1	100%	100%	100%
Portal Web para Capacitaciones	[A.22] Manipulación de programas	1	50%	100%	100%
Revista electrónica de la FICA	[I.5.1.] Avería de origen lógico	1	50%		
Revista electrónica de la FICA	[E.8] Difusión de software dañino	1	10%	10%	10%
Revista electrónica de la FICA	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Revista electrónica de la FICA	[E.21] Errores de mantenimiento / actualización de programas	10	1%	10%	50%
Revista electrónica de la FICA	[A.8] Difusión de software dañino	1	100%	100%	100%
Revista electrónica de la FICA	[A.22] Manipulación de programas	1	50%	100%	100%
Aplicaciones de ofimática / académicas	[I.5.1.] Avería de origen lógico	1	50%		
Aplicaciones de ofimática / académicas	[E.8] Difusión de software dañino	1	10%	10%	10%
Aplicaciones de ofimática / académicas	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Aplicaciones de ofimática / académicas	[E.21] Errores de mantenimiento / actualización de programas	10	1%	10%	50%
Aplicaciones de ofimática / académicas	[A.8] Difusión de software dañino	1	100%	100%	100%
Aplicaciones de ofimática / académicas	[A.22] Manipulación de programas	1	50%	100%	100%
HARDWARE					
Equipos PC / didácticos	[N.1] Fuego	0,1	100%		

Equipos PC / didácticos	[N.2] Daños por agua	0,1	50%		
Equipos PC / didácticos	[N.] Desastres naturales	0,1	100%		
Equipos PC / didácticos	[I.1] Fuego	0,5	100%		
Equipos PC / didácticos	[I.2] Daños por agua	0,5	50%		
Equipos PC / didácticos	[I.] Desastres industriales	0,5	100%		
Equipos PC / didácticos	[I.3] Contaminación medioambiental	0,1	50%		
Equipos PC / didácticos	[I.4] Contaminación electromagnética	1	10%		
Equipos PC / didácticos	[I.5.2] Avería de origen físico	1	50%		
Equipos PC / didácticos	[I.6] Corte de suministro eléctrico	1	100%		
Equipos PC / didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
Equipos PC / didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipos PC / didácticos	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	1	10%		
Equipos PC / didácticos	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Equipos PC / didácticos	[E.25] Pérdida de equipos	5	100%		100%
Equipos PC / didácticos	[A.7] Uso no previsto	1	10%	1%	10%
Equipos PC / didácticos	[A.11] Acceso no autorizado	1	10%	10%	50%
Equipos PC / didácticos	[A.23] Manipulación del hardware	0,5	50%		50%
Equipos PC / didácticos	[A.24] Denegación de servicio	2	100%		
Equipos PC / didácticos	[A.25] Robo de equipos	5	100%		100%
Equipos PC / didácticos	[A.26] Ataque destructivo	1	100%		
Equipos de seguridad	[N.1] Fuego	0,1	100%		
Equipos de seguridad	[N.2] Daños por agua	0,1	50%		
Equipos de seguridad	[N.] Desastres naturales	0,1	100%		

Equipos de seguridad	[I.1] Fuego	0,5	100%		
Equipos de seguridad	[I.2] Daños por agua	0,5	50%		
Equipos de seguridad	[I.] Desastres industriales	0,5	100%		
Equipos de seguridad	[I.3] Contaminación medioambiental	0,1	50%		
Equipos de seguridad	[I.4] Contaminación electromagnética	1	10%		
Equipos de seguridad	[I.5.2] Avería de origen físico	1	50%		
Equipos de seguridad	[I.6] Corte de suministro eléctrico	1	100%		
Equipos de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
Equipos de seguridad	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipos de seguridad	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	1	10%		
Equipos de seguridad	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Equipos de seguridad	[E.25] Pérdida de equipos	1	100%		100%
Equipos de seguridad	[A.7] Uso no previsto	1	1%	1%	10%
Equipos de seguridad	[A.11] Acceso no autorizado	1	10%	10%	50%
Equipos de seguridad	[A.23] Manipulación del hardware	0,5	50%		50%
Equipos de seguridad	[A.24] Denegación de servicio	2	100%		
Equipos de seguridad	[A.25] Robo de equipos	0,5	100%		100%
Equipos de seguridad	[A.26] Ataque destructivo	1	100%		
Equipos para redes de telecomunicaciones	[N.1] Fuego	0,1	100%		
Equipos para redes de telecomunicaciones	[N.2] Daños por agua	0,1	50%		
Equipos para redes de telecomunicaciones	[N.] Desastres naturales	0,1	100%		

Equipos para redes de telecomunicaciones	[I.1] Fuego	0,5	100%		
Equipos para redes de telecomunicaciones	[I.2] Daños por agua	0,5	50%		
Equipos para redes de telecomunicaciones	[I.] Desastres industriales	0,5	100%		
Equipos para redes de telecomunicaciones	[I.3] Contaminación medioambiental	0,1	50%		
Equipos para redes de telecomunicaciones	[I.4] Contaminación electromagnética	1	10%		
Equipos para redes de telecomunicaciones	[I.5.2] Avería de origen físico	1	50%		
Equipos para redes de telecomunicaciones	[I.6] Corte de suministro eléctrico	1	100%		
Equipos para redes de telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
Equipos para redes de telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipos para redes de telecomunicaciones	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	1	10%		
Equipos para redes de telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Equipos para redes de telecomunicaciones	[E.25] Pérdida de equipos	1	20%		50%
Equipos para redes de telecomunicaciones	[A.7] Uso no previsto	1	10%		10%
Equipos para redes de telecomunicaciones	[A.11] Acceso no autorizado	1	10%	10%	50%
Equipos para redes de telecomunicaciones	[A.23] Manipulación del hardware	0,5	100%		50%
Equipos para redes de telecomunicaciones	[A.24] Denegación de servicio	2	100%		
Equipos para redes de telecomunicaciones	[A.25] Robo de equipos	0,5	20%		50%
Equipos para redes de telecomunicaciones	[A.26] Ataque destructivo	1	100%		

REDES DE COMUNICACIONES						
Red interna laboratorios	[I.8] Fallo de servicios de comunicaciones	1	50%			
Red interna laboratorios	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	
Red interna laboratorios	[E.9] Errores de [re-]encadenamiento	1			10%	
Red interna laboratorios	[E.10] Errores de secuencia	1		10%		
Red interna laboratorios	[E.15] Alteración de la información	1		1%		
Red interna laboratorios	[E.19] Fugas de información	1			10%	
Red interna laboratorios	[E.24] Caída del sistema por agotamiento de recursos	1	50%			
Red interna laboratorios	[A.5] Suplantación de identidad	1		10%	50%	100%
Red interna laboratorios	[A.7] Uso no previsto	1	10%	10%	10%	
Red interna laboratorios	[A.9] [Re-]encaminamiento de mansajes	1			10%	
Red interna laboratorios	[A.10] Alteración de secuencias	1		10%		
Red interna laboratorios	[A.11] Acceso no autorizado	1		10%	50%	100%
Red interna laboratorios	[A.12] Análisis de tráfico	1			2%	
Red interna laboratorios	[A.14] Interceptación de información (escucha)	1			10%	
Red interna laboratorios	[A.15] Modificación de la información	1		10%		
Red interna laboratorios	[A.18] Destrucción de la información	1	50%			
Red interna laboratorios	[A.24] Denegación de servicio	10	50%			
EQUIPAMIENTO AUXILIAR						
Equipamiento eléctrico	[N.1] Fuego	0,1	100%			
Equipamiento eléctrico	[N.2] Daño por agua	0,1	50%			
Equipamiento eléctrico	[N.] Desastres naturales	0,1	100%			
Equipamiento eléctrico	[I.1] Fuego	0,5	100%			
Equipamiento eléctrico	[I.2] Daños por agua	0,5	50%			

Equipamiento eléctrico	[I.] Desastres industriales	0,5	100%		
Equipamiento eléctrico	[I.3] Contaminación medioambiental	0,1	50%		
Equipamiento eléctrico	[I.4] Contaminación electromagnética	0,5	10%		
Equipamiento eléctrico	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipamiento eléctrico	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	1	10%		
Equipamiento eléctrico	[A.7] Uso no previsto	1	50%	1%	1%
Equipamiento eléctrico	[A.11] Acceso no autorizado	1		10%	50%
Equipamiento eléctrico	[A.23] Manipulación del hardware	1	50%		50%
Equipamiento eléctrico	[A.25] Robo de equipos	0,8	100%		0
Equipamiento eléctrico	[A.26] Ataque destructivo	1	100%		
Mobiliario para los equipos	[N.1] Fuego	0,1	100%		
Mobiliario para los equipos	[N.2] Daño por agua	0,1	50%		
Mobiliario para los equipos	[N.] Desastres naturales	0,1	100%		
Mobiliario para los equipos	[I.1] Fuego	0,5	100%		
Mobiliario para los equipos	[I.2] Daños por agua	0,5	50%		
Mobiliario para los equipos	[I.] Desastres industriales	0,5	100%		
Mobiliario para los equipos	[I.3] Contaminación medioambiental	0,1	50%		
Mobiliario para los equipos	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	1	10%		
Mobiliario para los equipos	[A.7] Uso no previsto	1	50%	1%	1%
Mobiliario para los equipos	[A.23] Manipulación del hardware	1	50%		50%
Mobiliario para los equipos	[A.25] Robo de equipos	0,5	10%		50%
Mobiliario para los equipos	[A.26] Ataque destructivo	1	10%		
SOPORTES DE INFORMACIÓN					
Nube Microsoft OneDrive	[N.1] Fuego	0,1	100%		
Nube Microsoft OneDrive	[N.2] Daño por agua	0,1	50%		
Nube Microsoft OneDrive	[N.] Desastres naturales	0,1	100%		
Nube Microsoft OneDrive	[I.1] Fuego	0,5	100%		
Nube Microsoft OneDrive	[I.2] Daños por agua	0,5	50%		

Nube Microsoft OneDrive	[I.] Desastres industriales	0,5	100%		
Nube Microsoft OneDrive	[I.3] Contaminación medioambiental	1	50%		
Nube Microsoft OneDrive	[I.4] Contaminación electromagnética	1	10%		
Nube Microsoft OneDrive	[I.5.2] Avería de origen físico	1	50%		
Nube Microsoft OneDrive	[I.6] Corte del suministro eléctrico	1	100%		
Nube Microsoft OneDrive	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
Nube Microsoft OneDrive	[I.10] Degradación de los soportes de almacenamiento de la información	1	100%		
Nube Microsoft OneDrive	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Nube Microsoft OneDrive	[E.1] Errores de los usuarios	1	1%	5%	10%
Nube Microsoft OneDrive	[E.15] Alteración de la información	1		1%	
Nube Microsoft OneDrive	[E.18] Destrucción de la información	1	100%		
Nube Microsoft OneDrive	[E.19] Fugas de información	1			10%
Nube Microsoft OneDrive	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	1	100%	10%	50%
Nube Microsoft OneDrive	[E.25] Pérdida de equipos	1	10%		50%
Nube Microsoft OneDrive	[A.7] Uso no previsto	1	1%		1%
Nube Microsoft OneDrive	[A.11] Acceso no autorizado	1		1%	50%
Nube Microsoft OneDrive	[A.15] Modificación de la información	5		100%	
Nube Microsoft OneDrive	[A.18] Destrucción de la información	1	100%		
Nube Microsoft OneDrive	[A.23] Manipulación del hardware	0,1	50%		50%
Nube Microsoft OneDrive	[A.25] Robo de equipos	1	10%		100%
Nube Microsoft OneDrive	[A.26] Ataque destructivo	1	10%		
INSTALACIONES					
Espacios físicos Lab 1 a 9	[N.1] Fuego	1	100%		
Espacios físicos Lab 1 a 10	[N.2] Daño por agua	1	100%		
Espacios físicos Lab 1 a 11	[N.] Desastres naturales	0,5	100%		
Espacios físicos Lab 1 a 12	[I.1] Fuego	1	100%		
Espacios físicos Lab 1 a 13	[I.2] Daños por agua	1	100%		
Espacios físicos Lab 1 a 14	[I.] Desastres industriales	1	100%		

Espacios físicos Lab 1 a 15	[I.3] Contaminación medioambiental	1	10%	
Espacios físicos Lab 1 a 16	[I.4] Contaminación electromagnética	0,1	10%	
Espacios físicos Lab 1 a 17	[E.25] Pérdida de equipos	10		10%
Espacios físicos Lab 1 a 18	[A.6] Abuso de privilegios de acceso	1	10%	
Espacios físicos Lab 1 a 19	[A.7] Uso no previsto	1	10%	
Espacios físicos Lab 1 a 20	[A.25] Robo de equipos	10		100%
Espacios físicos Lab 1 a 21	[A.26] Ataque destructivo	0,1	100%	
Espacios físicos Lab 1 a 22	[A.27] Ocupación enemiga	1	100%	
Área de servidores y comunicaciones	[N.1] Fuego	1	100%	
Área de servidores y comunicaciones	[N.2] Daño por agua	1	100%	
Área de servidores y comunicaciones	[N.] Desastres naturales	0,5	100%	
Área de servidores y comunicaciones	[I.1] Fuego	1	100%	
Área de servidores y comunicaciones	[I.2] Daños por agua	1	100%	
Área de servidores y comunicaciones	[I.] Desastres industriales	1	100%	
Área de servidores y comunicaciones	[I.3] Contaminación medioambiental	1	10%	
Área de servidores y comunicaciones	[I.4] Contaminación electromagnética	0,1	10%	
Área de servidores y comunicaciones	[E.25] Pérdida de equipos	10		10%
Área de servidores y comunicaciones	[A.6] Abuso de privilegios de acceso	1	10%	
Área de servidores y comunicaciones	[A.7] Uso no previsto	1	10%	
Área de servidores y comunicaciones	[A.25] Robo de equipos	10		100%
Área de servidores y comunicaciones	[A.26] Ataque destructivo	0,1	100%	

Área de servidores y comunicaciones	[A.27] Ocupación enemiga	1	100%	
Área de soporte y mantenimiento	[N.1] Fuego	1	100%	
Área de soporte y mantenimiento	[N.2] Daño por agua	1	100%	
Área de soporte y mantenimiento	[N.] Desastres naturales	0,5	100%	
Área de soporte y mantenimiento	[I.1] Fuego	1	100%	
Área de soporte y mantenimiento	[I.2] Daños por agua	1	100%	
Área de soporte y mantenimiento	[I.] Desastres industriales	1	100%	
Área de soporte y mantenimiento	[I.3] Contaminación medioambiental	1	10%	
Área de soporte y mantenimiento	[I.4] Contaminación electromagnética	0,1	10%	
Área de soporte y mantenimiento	[E.25] Pérdida de equipos	10		10%
Área de soporte y mantenimiento	[A.6] Abuso de privilegios de acceso	1	10%	
Área de soporte y mantenimiento	[A.7] Uso no previsto	1	10%	
Área de soporte y mantenimiento	[A.25] Robo de equipos	10		100%
Área de soporte y mantenimiento	[A.26] Ataque destructivo	0,1	100%	
Área de soporte y mantenimiento	[A.27] Ocupación enemiga	1	100%	
PERSONAL				
Jefe de Laboratorios	[E.15] Alteración de la información	1	10%	
Jefe de Laboratorios	[E.18] Destrucción de la información	1	1%	
Jefe de Laboratorios	[E.19] Fugas de información	1		10%
Jefe de Laboratorios	[E.28] Indisponibilidad del personal	1	10%	

Jefe de Laboratorios	[A.15] Modificación de la información	1		50%	
Jefe de Laboratorios	[A.18] Destrucción de la información	1	10%		
Jefe de Laboratorios	[A.19] Revelación de información	10			50%
Jefe de Laboratorios	[A.28] Indisponibilidad del personal	0,5	20%		
Jefe de Laboratorios	[A.29] Extorsión	0,9	50%	100%	100%
Jefe de Laboratorios	[A.30] Ingeniería social (picaresca)	0,5	50%	100%	100%
Asistente de Laboratorios 1	[E.15] Alteración de la información	1		10%	
Asistente de Laboratorios 1	[E.18] Destrucción de la información	1	1%		
Asistente de Laboratorios 1	[E.19] Fugas de información	1			10%
Asistente de Laboratorios 1	[E.28] Indisponibilidad del personal	1	30%		
Asistente de Laboratorios 1	[A.15] Modificación de la información	1		50%	
Asistente de Laboratorios 1	[A.18] Destrucción de la información	1	10%		
Asistente de Laboratorios 1	[A.19] Revelación de información	10			50%
Asistente de Laboratorios 1	[A.28] Indisponibilidad del personal	0,5	50%		
Asistente de Laboratorios 1	[A.29] Extorsión	0,9	20%	10%	50%
Asistente de Laboratorios 1	[A.30] Ingeniería social (picaresca)	0,5	20%	20%	20%
Asistente de Laboratorios 2	[E.15] Alteración de la información	1		10%	
Asistente de Laboratorios 2	[E.18] Destrucción de la información	1	1%		
Asistente de Laboratorios 2	[E.19] Fugas de información	1			10%
Asistente de Laboratorios 2	[E.28] Indisponibilidad del personal	1	30%		
Asistente de Laboratorios 2	[A.15] Modificación de la información	1		50%	
Asistente de Laboratorios 2	[A.18] Destrucción de la información	1	10%		
Asistente de Laboratorios 2	[A.19] Revelación de información	10			50%
Asistente de Laboratorios 2	[A.28] Indisponibilidad del personal	0,5	50%		
Asistente de Laboratorios 2	[A.29] Extorsión	0,9	20%	10%	50%
Asistente de Laboratorios 2	[A.30] Ingeniería social (picaresca)	0,5	20%	20%	20%
Usuarios Laboratorios	[E.15] Alteración de la información	1		10%	
Usuarios Laboratorios	[E.18] Destrucción de la información	1	1%		
Usuarios Laboratorios	[E.19] Fugas de información	1			10%
Usuarios Laboratorios	[A.13] Repudio (negación de actuaciones)	1	10%		

Usuarios Laboratorios	[A.15] Modificación de la información	1		50%	
Usuarios Laboratorios	[A.18] Destrucción de la información	1	10%		
Usuarios Laboratorios	[A.19] Revelación de información	10			20%
Usuarios Laboratorios	[A.28] Indisponibilidad del personal	0,5	50%		
Usuarios Laboratorios	[A.29] Extorsión	0,9	10%	20%	20%
Usuarios Laboratorios	[A.30] Ingeniería social (picaresca)	0,5	10%	20%	20%

Nota: La tabla presenta una muestra del listado de la valoración de amenazas que podrían afectar a los activos identificados en los laboratorios de informática FICA-UTN. En donde F: frecuencia o probabilidad de ocurrencia, D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

Anexo G: Impacto potencial acumulado de afectación de activos en los laboratorios de informática FICA-UTN

	IMPACTO POTENCIAL ACUMULADO					PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	**A**	**T**	
ACTIVOS ESENCIALES	**10**	**10**	**10**	**10**	**10**	
Datos de acceso a servidores y sistemas					9	
[A.13] Repudio (negación de actuaciones)					9	9.0
Base de datos biométricos					9	
[A.13] Repudio (negación de actuaciones)					9	9.0
DATOS / INFORMACIÓN	**7**	**7**	**9**	**10**		
Documentos de administración interna	4	7	9	10		
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	4					4.0
[E.19] Fugas de información			7			
[A.5] Suplantación de identidad		7	9	10		8.7
[A.6] Abuso de privilegios de acceso	4	7	9			6.7
[A.11] Acceso no autorizado		7	9			
Datos de configuración	7	7	9	10		
[E.4] Errores de configuración		4				4.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	4					4.0
[E.19] Fugas de información			7			7.0
[A.4] Manipulación de los ficheros de configuración	7	7	7			7.0
[A.5] Suplantación de identidad		7	9	10		8.7
[A.6] Abuso de privilegios de acceso	4	7	9			6.7
[A.11] Acceso no autorizado		7	9			8.0
SERVICIOS	**9**	**9**	**9**	**10**	**10**	
Internet						

Mantenimiento preventivo y correctivo de hardware y software	9	9	9	10	10	
[E.1] Errores de los usuarios	7	7	7			7.0
[E.2] Errores del administrador del sistema / de la seguridad	8	8	8			8.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	7					7.0
[E.19] Fugas de información			7			7.0
[E.24] Caída del sistema por agotamiento de recursos	9					9.0
[A.5] Suplantación de identidad		9	9	10		9.3
[A.6] Abuso de privilegios de acceso	4	7	7	10		7.0
[A.7] Uso no previsto	4	7	7			6.0
[A.11] Acceso no autorizado		7	9	10		8.7
[A.13] Repudio (negación de actuaciones)					10	10.0
[A.15] Modificación de la información		9				9.0
[A.18] Destrucción de la información	9					9.0
[A.24] Denegación de servicio	9					9.0
Telefonía	9	9	9	10	10	
[E.1] Errores de los usuarios	7	7	7			7.0
[E.2] Errores del administrador del sistema / de la seguridad	8	8	8			8.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	7					7.0
[E.19] Fugas de información			7			7.0
[E.24] Caída del sistema por agotamiento de recursos	9					9.0
[A.5] Suplantación de identidad		9	9	10		9.3
[A.6] Abuso de privilegios de acceso	4	7	7	10		7.0
[A.7] Uso no previsto	4	7	7			6.0
[A.11] Acceso no autorizado		7	9	10		8.7
[A.13] Repudio (negación de actuaciones)					10	10.0
[A.15] Modificación de la información		9				9.0
[A.18] Destrucción de la información	9					9.0

[E.24] Caída del sistema por agotamiento de recursos	9					9.0
Servidores internos	9	9	9	10	10	
[E.1] Errores de los usuarios	7	7	7			7.0
[E.2] Errores del administrador del sistema / de la seguridad	8	8	8			8.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	7					7.0
[E.19] Fugas de información			7			7.0
[E.24] Caída del sistema por agotamiento de recursos	9					9.0
[A.5] Suplantación de identidad		9	9	10		9.3
[A.6] Abuso de privilegios de acceso	4	7	7	10		7.0
[A.7] Uso no previsto	4	7	7			6.0
[A.11] Acceso no autorizado		7	9	10		8.7
[A.13] Repudio (negación de actuaciones)					10	10.0
[A.15] Modificación de la información		9				9.0
[A.18] Destrucción de la información	9					9.0
[A.24] Denegación de servicio	9					9.0
SOFTWARE	**10**	**10**	**10**			
Sistema reserva instalaciones FICA	10	10	10			
[I.5.1.] Avería de origen lógico	9					9.0
[E.8] Difusión de software dañino	7	7	7			7.0
[E.20] Vulnerabilidades de los programas (software)	4	8	8			6.7
[E.21] Errores de mantenimiento / actualización de programas	4	7	9			6.7
[A.8] Difusión de software dañino	10	10	10			10.0
[A.22] Manipulación de programas	9	10	10			9.7
Aplicación para el manejo de biométricos	10	10	10			
[I.5.1.] Avería de origen lógico	9					9.0
[E.8] Difusión de software dañino	7	7	7			7.0
[E.20] Vulnerabilidades de los programas (software)	4	8	8			6.7
[E.21] Errores de mantenimiento / actualización de programas	4	7	9			6.7

[A.8] Difusión de software dañino	10	10	10		10.0
[A.22] Manipulación de programas	9	10	10		9.7
Portal Web para Capacitaciones	10	10	10		
[I.5.1.] Avería de origen lógico	9				9.0
[E.8] Difusión de software dañino	7	7	7		7.0
[E.20] Vulnerabilidades de los programas (software)	4	8	8		6.7
[E.21] Errores de mantenimiento / actualización de programas	4	7	9		6.7
[A.8] Difusión de software dañino	10	10	10		10.0
[A.22] Manipulación de programas	9	10	10		9.7
Portal Web para Capacitaciones	10	10	10		
[I.5.1.] Avería de origen lógico	9				9.0
[E.8] Difusión de software dañino	7	7	7		7.0
[E.20] Vulnerabilidades de los programas (software)	4	8	8		6.7
[E.21] Errores de mantenimiento / actualización de programas	4	7	9		6.7
[A.8] Difusión de software dañino	10	10	10		10.0
[A.22] Manipulación de programas	9	10	10		9.7
Aplicaciones de ofimática / académicas	10	10	10		
[I.5.1.] Avería de origen lógico	9				9.0
[E.8] Difusión de software dañino	7	7	7		7.0
[E.20] Vulnerabilidades de los programas (software)	4	8	8		6.7
[E.21] Errores de mantenimiento / actualización de programas	4	7	9		6.7
[A.8] Difusión de software dañino	10	10	10		10.0
[A.22] Manipulación de programas	9	10	10		9.7
HARDWARE	**10**	**7**	**10**		
Equipos PC / didácticos	10	7	10		
[N.1] Fuego	10				10.0
[N.2] Daños por agua	9				9.0
[N.] Desastres naturales	10				10.0
[I.1] Fuego	10				10.0

[I.2] Daños por agua	9				9.0
[I.] Desastres industriales	10				10.0
[I.3] Contaminación medioambiental	9				9.0
[I.4] Contaminación electromagnética	7				7.0
[I.5.2] Avería de origen físico	9				9.0
[I.6] Corte de suministro eléctrico	10				10.0
[I.7] Condiciones inadecuadas de temperatura o humedad	10				10.0
[I.11] Emanaciones electromagnéticas (TEMPEST)			4		4.0
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	7				7.0
[E.24] Caída del sistema por agotamiento de recursos	9				9.0
[E.25] Pérdida de equipos	10		10		10.0
[A.7] Uso no previsto	7	4	7		6.0
[A.11] Acceso no autorizado	7	7	9		7.7
[A.23] Manipulación del hardware	9		9		9.0
[A.24] Denegación de servicio	10				10.0
[A.25] Robo de equipos	10		10		10.0
[A.26] Ataque destructivo	10				10.0
Equipos de seguridad	10	7	10		
[N.1] Fuego	10				10.0
[N.2] Daños por agua	9				9.0
[N.] Desastres naturales	10				10.0
[I.1] Fuego	10				10.0
[I.2] Daños por agua	9				9.0
[I.] Desastres industriales	10				10.0
[I.3] Contaminación medioambiental	9				9.0
[I.4] Contaminación electromagnética	7				7.0
[I.5.2] Avería de origen físico	9				9.0
[I.6] Corte de suministro eléctrico	10				10.0
[I.7] Condiciones inadecuadas de temperatura o humedad	10				10.0

[I.11] Emanaciones electromagnéticas (TEMPEST)			4		4.0
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	7				7.0
[E.24] Caída del sistema por agotamiento de recursos	9				9.0
[E.25] Pérdida de equipos	10		10		10.0
[A.7] Uso no previsto	4	4	7		5.0
[A.11] Acceso no autorizado	7	7	9		7.7
[A.23] Manipulación del hardware	9		9		9.0
[A.24] Denegación de servicio	10				10.0
[A.25] Robo de equipos	10		10		10.0
[A.26] Ataque destructivo	10				10.0
Equipos para redes de telecomunicaciones	10	7	9		
[N.1] Fuego	10				10.0
[N.2] Daños por agua	9				9.0
[N.] Desastres naturales	10				10.0
[I.1] Fuego	10				10.0
[I.2] Daños por agua	9				9.0
[I.] Desastres industriales	10				10.0
[I.3] Contaminación medioambiental	9				9.0
[I.4] Contaminación electromagnética	7				7.0
[I.5.2] Avería de origen físico	9				9.0
[I.6] Corte de suministro eléctrico	10				10.0
[I.7] Condiciones inadecuadas de temperatura o humedad	10				10.0
[I.11] Emanaciones electromagnéticas (TEMPEST)			4		4.0
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	7				7.0
[E.24] Caída del sistema por agotamiento de recursos	9				9.0
[E.25] Pérdida de equipos	8		9		8.5
[A.7] Uso no previsto	7		7		7.0
[A.11] Acceso no autorizado	7	7	9		7.7
[A.23] Manipulación del hardware	10		9		9.5

[A.24] Denegación de servicio	10					10.0
[A.25] Robo de equipos	8		9			8.5
[A.26] Ataque destructivo	10					10.0
REDES DE COMUNICACIONES	**9**	**8**	**9**	**10**		
Red interna laboratorios	9	8	9	10		
[I.8] Fallo de servicios de comunicaciones	9					9.0
[E.2] Errores del administrador del sistema / de la seguridad	8	8	8			8.0
[E.9] Errores de [re-]encadenamiento			7			7.0
[E.10] Errores de secuencia		7				7.0
[E.15] Alteración de la información		4				4.0
[E.19] Fugas de información			7			7.0
[E.24] Caída del sistema por agotamiento de recursos	9					9.0
[A.5] Suplantación de identidad		7	9	10		8.7
[A.7] Uso no previsto	7	7	7			7.0
[A.9] [Re-]encaminamiento de mansajes			7			7.0
[A.10] Alteración de secuencias		7				7.0
[A.11] Acceso no autorizado		7	9	10		8.7
[A.12] Análisis de tráfico			5			5.0
[A.14] Interceptación de información (escucha)			7			7.0
[A.15] Modificación de la información		7				7.0
[A.18] Destrucción de la información	9					9.0
[A.24] Denegación de servicio	9					9.0
EQUIPAMINETO AUXILIAR	**10**	**7**	**9**			
Equipamiento eléctrico	10	7	9			
[N.1] Fuego	10					10.0
[N.2] Daño por agua	9					9.0
[N.] Desastres naturales	10					10.0
[I.1] Fuego	10					10.0
[I.2] Daños por agua	9					9.0

[I.] Desastres industriales	10				10.0
[I.3] Contaminación medioambiental	9				9.0
[I.4] Contaminación electromagnética	7				7.0
[I.11] Emanaciones electromagnéticas (TEMPEST)			4		4.0
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	7				7.0
[A.7] Uso no previsto	9	4	4		5.7
[A.11] Acceso no autorizado		7	9		8.0
[A.23] Manipulación del hardware	9		9		9.0
[A.25] Robo de equipos	10				10.0
[A.26] Ataque destructivo	10				10.0
Mobiliario para los equipos	10	4	9		
[N.1] Fuego	10				10.0
[N.2] Daño por agua	9				9.0
[N.] Desastres naturales	10				10.0
[I.1] Fuego	10				10.0
[I.2] Daños por agua	9				9.0
[I.] Desastres industriales	10				10.0
[I.3] Contaminación medioambiental	9				9.0
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	7				7.0
[A.7] Uso no previsto	9	4	4		5.7
[A.23] Manipulación del hardware	9		9		9.0
[A.25] Robo de equipos	7		9		8.0
[A.26] Ataque destructivo	7				7.0
SOPORTES DE INFORMACIÓN	**10**	**10**	**10**		10.0
Nube Microsoft OneDrive	10	10	10		
[N.1] Fuego	10				10.0
[N.2] Daño por agua	9				9.0
[N.] Desastres naturales	10				10.0
[I.1] Fuego	10				10.0

[I.2] Daños por agua	9							9.0
[I.] Desastres industriales	10							10.0
[I.3] Contaminación medioambiental	9							9.0
[I.4] Contaminación electromagnética	7							7.0
[I.5.2] Avería de origen físico	9							9.0
[I.6] Corte del suministro eléctrico	10							10.0
[I.7] Condiciones inadecuadas de temperatura o humedad	10							10.0
[I.10] Degradación de los soportes de almacenamiento de la información	10							10.0
[I.11] Emanaciones electromagnéticas (TEMPEST)				4				4.0
[E.1] Errores de los usuarios	4	6		7				5.7
[E.15] Alteración de la información		4						4.0
[E.18] Destrucción de la información	10							10.0
[E.19] Fugas de información				7				7.0
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	10	7		9				8.7
[E.25] Pérdida de equipos	7			9				8.0
[A.7] Uso no previsto	4			4				4.0
[A.11] Acceso no autorizado		4		9				6.5
[A.15] Modificación de la información		10						10.0
[A.18] Destrucción de la información	10							10.0
[A.23] Manipulación del hardware	9			9				9.0
[A.25] Robo de equipos	7			10				8.5
[A.26] Ataque destructivo	7							7.0
INSTALACIONES	**10**			**10**				
Espacios físicos Lab 1 a 9	10			10				
[N.1] Fuego	10							10.0
[N.2] Daño por agua	10							10.0
[N.] Desastres naturales	10							10.0
[I.1] Fuego	10							10.0
[I.2] Daños por agua	10							10.0

[I.] Desastres industriales	10		10.0
[I.3] Contaminación medioambiental	7		7.0
[I.4] Contaminación electromagnética	7		7.0
[E.25] Pérdida de equipos		7	7.0
[A.6] Abuso de privilegios de acceso	7		7.0
[A.7] Uso no previsto	7		7.0
[A.25] Robo de equipos		10	10.0
[A.26] Ataque destructivo	10		10.0
[A.27] Ocupación enemiga	10		10.0
Área de servidores y comunicaciones	10	10	
[N.1] Fuego	10		10.0
[N.2] Daño por agua	10		10.0
[N.] Desastres naturales	10		10.0
[I.1] Fuego	10		10.0
[I.2] Daños por agua	10		10.0
[I.] Desastres industriales	10		10.0
[I.3] Contaminación medioambiental	7		7.0
[I.4] Contaminación electromagnética	7		7.0
[E.25] Pérdida de equipos		7	7.0
[A.6] Abuso de privilegios de acceso	7		7.0
[A.7] Uso no previsto	7		7.0
[A.25] Robo de equipos		10	10.0
[A.26] Ataque destructivo	10		10.0
[A.27] Ocupación enemiga	10		10.0
Área de soporte y mantenimiento	10	10	
[N.1] Fuego	10		10.0
[N.2] Daño por agua	10		10.0
[N.] Desastres naturales	10		10.0
[I.1] Fuego	10		10.0

[I.2] Daños por agua	10			10.0
[I.] Desastres industriales	10			10.0
[I.3] Contaminación medioambiental	7			7.0
[I.4] Contaminación electromagnética	7			7.0
[E.25] Pérdida de equipos			7	7.0
[A.6] Abuso de privilegios de acceso	7			7.0
[A.7] Uso no previsto	7			7.0
[A.25] Robo de equipos			10	10.0
[A.26] Ataque destructivo	10			10.0
[A.27] Ocupación enemiga	10			10.0
PERSONAS	**9**	**10**	**10**	
Jefe de Laboratorios	9	10	10	
[E.15] Alteración de la información		7		7.0
[E.18] Destrucción de la información	4			4.0
[E.19] Fugas de información			7	7.0
[E.28] Indisponibilidad del personal	7			7.0
[A.15] Modificación de la información		9		9.0
[A.18] Destrucción de la información	7			7.0
[A.19] Revelación de información			9	9.0
[A.28] Indisponibilidad del personal	8			8.0
[A.29] Extorsión	9	10	10	9.7
[A.30] Ingeniería social (picaresca)	9	10	10	9.7
Asistente de Enseñanza de los laboratorios 1	9	9	9	
[E.15] Alteración de la información		7		7.0
[E.18] Destrucción de la información	4			4.0
[E.19] Fugas de información			7	7.0
[E.28] Indisponibilidad del personal	8			8.0
[A.15] Modificación de la información		9		9.0
[A.18] Destrucción de la información	7			7.0

[A.19] Revelación de información			9	9.0
[A.28] Indisponibilidad del personal	9			9.0
[A.29] Extorsión	8	7	9	8.0
[A.30] Ingeniería social (picaresca)	8	8	8	8.0
Asistente de Enseñanza de los laboratorios 2	9	9	9	
[E.15] Alteración de la información		7		7.0
[E.18] Destrucción de la información	4			4.0
[E.19] Fugas de información			7	7.0
[E.28] Indisponibilidad del personal	8			8.0
[A.15] Modificación de la información		9		9.0
[A.18] Destrucción de la información	7			7.0
[A.19] Revelación de información			9	9.0
[A.28] Indisponibilidad del personal	9			9.0
[A.29] Extorsión	8	7	9	8.0
[A.30] Ingeniería social (picaresca)	8	8	8	8.0
Usuarios Laboratorios	9	9	8	
[E.15] Alteración de la información		7		7.0
[E.18] Destrucción de la información	4			4.0
[E.19] Fugas de información			7	7.0
[A.13] Repudio (negación de actuaciones)	7			7.0
[A.15] Modificación de la información		9		9.0
[A.18] Destrucción de la información	7			7.0
[A.19] Revelación de información			8	8.0
[A.28] Indisponibilidad del personal	9			9.0
[A.29] Extorsión	7	8	8	7.7
[A.30] Ingeniería social (picaresca)	7	8	8	7.7

Nota: La tabla muestra el impacto potencial acumulado, en donde D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

Anexo H: Riesgo potencial acumulado de Amenazas en laboratorios de informática FICA-UTN

	RIESGO POTENCIAL ACUMULADO					PESO PONDERADO
ACTIVOS	**D**	**I**	**C**	**A**	**T**	
ACTIVOS ESENCIALES					6.3	
Datos de acceso a servidores y sistemas					6.3	
[A.13] Repudio (negación de actuaciones)					6.3	6.3
Base de datos biométricos					6.3	
[A.13] Repudio (negación de actuaciones)					6.3	6.3
DATOS / INFORMACIÓN	5.9	6.8	8.1	7.7		
Documentos de administración interna	4.2	6.8	8.1	7.7		
[E.15] Alteración de la información		3.3				3.3
[E.18] Destrucción de la información	3.3					3.3
[E.19] Fugas de información			5.1			5.1
[A.5] Suplantación de identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			5.8
[A.11] Acceso no autorizado		6.8	8.1			7.5
Datos de configuración	5.9	6.8	8.1	7.7		
[E.4] Errores de configuración		3.3				3.3
[E.15] Alteración de la información		3.3				3.3
[E.18] Destrucción de la información	3.3					3.3
[E.19] Fugas de información			5.1			5.1
[A.4] Manipulación de los ficheros de configuración	5.9	5.9	5.9			5.9
[A.5] Suplantación de identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			5.8
[A.11] Acceso no autorizado		6.8	8.1			7.5
SERVICIOS	7.2	7.2	6.3	6.8	7.4	
Internet						

Mantenimiento preventivo y correctivo de hardware y software	7.2	7.2	6.3	6.8	7.4	
[E.1] Errores de los usuarios	5.1	5.1	5.1			5.1
[E.2] Errores del administrador del sistema / de la seguridad	5.6	5.6	5.6			5.6
[E.15] Alteración de la información		3.3				3.3
[E.18] Destrucción de la información	5.1					5.1
[E.19] Fugas de información			5.1			5.1
[E.24] Caída del sistema por agotamiento de recursos	7.2					7.2
[A.5] Suplantación de identidad		6.3	6.3	6.8		6.5
[A.6] Abuso de privilegios de acceso	3.3	5.1	5.1	6.8		5.1
[A.7] Uso no previsto	3.3	5.1	5.1			4.5
[A.11] Acceso no autorizado		5.1	6.3	6.8		6.1
[A.13] Repudio (negación de actuaciones)					7.4	7.4
[A.15] Modificación de la información		7.2				7.2
[A.18] Destrucción de la información	6.3					6.3
[A.24] Denegación de servicio	7.2					7.2
Telefonía	7.2	7.2	6.3	6.8	7.4	
[E.1] Errores de los usuarios	5.1	5.1	5.1			5.1
[E.2] Errores del administrador del sistema / de la seguridad	5.6	5.6	5.6			5.6
[E.15] Alteración de la información		3.3				3.3
[E.18] Destrucción de la información	5.1					5.1
[E.19] Fugas de información			5.1			5.1
[E.24] Caída del sistema por agotamiento de recursos	7.2					7.2
[A.5] Suplantación de identidad		6.3	6.3	6.8		6.5
[A.6] Abuso de privilegios de acceso	3.3	5.1	5.1	6.8		5.1
[A.7] Uso no previsto	3.3	5.1	5.1			4.5
[A.11] Acceso no autorizado		5.1	6.3	6.8		6.1
[A.13] Repudio (negación de actuaciones)					7.4	7.4
[A.15] Modificación de la información		7.2				7.2
[A.18] Destrucción de la información	6.3					6.3

[E.24] Caída del sistema por agotamiento de recursos	7.2					7.2
Servidores internos	7.2	7.2	6.3	6.8	7.4	
[E.1] Errores de los usuarios	5.1	5.1	5.1			5.1
[E.2] Errores del administrador del sistema / de la seguridad	5.6	5.6	5.6			5.6
[E.15] Alteración de la información		3.3				3.3
[E.18] Destrucción de la información	5.1					5.1
[E.19] Fugas de información			5.1			5.1
[E.24] Caída del sistema por agotamiento de recursos	7.2					7.2
[A.5] Suplantación de identidad		6.3	6.3	6.8		6.5
[A.6] Abuso de privilegios de acceso	3.3	5.1	5.1	6.8		5.1
[A.7] Uso no previsto	3.3	5.1	5.1			4.5
[A.11] Acceso no autorizado		5.1	6.3	6.8		6.1
[A.13] Repudio (negación de actuaciones)					7.4	7.4
[A.15] Modificación de la información		7.2				7.2
[A.18] Destrucción de la información	6.3					6.3
[A.24] Denegación de servicio	7.2					7.2
SOFTWARE	6.8	6.8	7.2			
Sistema reserva instalaciones FICA	6.8	6.8	7.2			
[I.5.1.] Avería de origen lógico	6.3					6.3
[E.8] Difusión de software dañino	5.1	5.1	5.1			5.1
[E.20] Vulnerabilidades de los programas (software)	3.3	5.6	5.6			4.8
[E.21] Errores de mantenimiento / actualización de programas	4.2	5.9	7.2			5.8
[A.8] Difusión de software dañino	6.8	6.8	6.8			6.8
[A.22] Manipulación de programas	6.3	6.8	6.8			6.6
Aplicación para el manejo de biométricos	6.8	6.8	7.2			
[I.5.1.] Avería de origen lógico	6.3					6.3
[E.8] Difusión de software dañino	5.1	5.1	5.1			5.1
[E.20] Vulnerabilidades de los programas (software)	3.3	5.6	5.6			4.8
[E.21] Errores de mantenimiento / actualización de programas	4.2	5.9	7.2			5.8

[A.8] Difusión de software dañino	6.8	6.8	6.8	6.8
[A.22] Manipulación de programas	6.3	6.8	6.8	6.6
Portal Web para Capacitaciones	6.8	6.8	7.2	
[I.5.1.] Avería de origen lógico	6.3			6.3
[E.8] Difusión de software dañino	5.1	5.1	5.1	5.1
[E.20] Vulnerabilidades de los programas (software)	3.3	5.6	5.6	4.8
[E.21] Errores de mantenimiento / actualización de programas	4.2	5.9	7.2	5.8
[A.8] Difusión de software dañino	6.8	6.8	6.8	6.8
[A.22] Manipulación de programas	6.3	6.8	6.8	6.6
Portal Web para Capacitaciones	6.8	6.8	7.2	
[I.5.1.] Avería de origen lógico	6.3			6.3
[E.8] Difusión de software dañino	5.1	5.1	5.1	5.1
[E.20] Vulnerabilidades de los programas (software)	3.3	5.6	5.6	4.8
[E.21] Errores de mantenimiento / actualización de programas	4.2	5.9	7.2	5.8
[A.8] Difusión de software dañino	6.8	6.8	6.8	6.8
[A.22] Manipulación de programas	6.3	6.8	6.8	6.6
Aplicaciones de ofimática / académicas	6.8	6.8	7.2	
[I.5.1.] Avería de origen lógico	6.3			6.3
[E.8] Difusión de software dañino	5.1	5.1	5.1	5.1
[E.20] Vulnerabilidades de los programas (software)	3.3	5.6	5.6	4.8
[E.21] Errores de mantenimiento / actualización de programas	4.2	5.9	7.2	5.8
[A.8] Difusión de software dañino	6.8	6.8	6.8	6.8
[A.22] Manipulación de programas	6.3	6.8	6.8	6.6
HARDWARE	7.4	5.1	7.4	
Equipos PC / didácticos	7.4	5.1	7.4	
[N.1] Fuego	5.9			5.9
[N.2] Daños por agua	5.4			5.4
[N.] Desastres naturales	5.9			5.9
[I.1] Fuego	6.6			6.6

[I.2] Daños por agua	6			6.0
[I.] Desastres industriales	6.6			6.6
[I.3] Contaminación medioambiental	5.4			5.4
[I.4] Contaminación electromagnética	5.1			5.1
[I.5.2] Avería de origen físico	6.3			6.3
[I.6] Corte de suministro eléctrico	6.8			6.8
[I.7] Condiciones inadecuadas de temperatura o humedad	6.8			6.8
[I.11] Emanaciones electromagnéticas (TEMPEST)			3.3	3.3
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1			5.1
[E.24] Caída del sistema por agotamiento de recursos	7.2			7.2
[E.25] Pérdida de equipos	7.4		7.4	7.4
[A.7] Uso no previsto	5.1	3.3	5.1	4.5
[A.11] Acceso no autorizado	5.1	5.1	6.3	5.5
[A.23] Manipulación del hardware	6		6	6.0
[A.24] Denegación de servicio	7.1			7.1
[A.25] Robo de equipos	7.4		7.4	7.4
[A.26] Ataque destructivo	6.8			6.8
Equipos de seguridad	7.2	5.1	6.8	
[N.1] Fuego	5.9			5.9
[N.2] Daños por agua	5.4			5.4
[N.] Desastres naturales	5.9			5.9
[I.1] Fuego	6.6			6.6
[I.2] Daños por agua	6			6.0
[I.] Desastres industriales	6.6			6.6
[I.3] Contaminación medioambiental	5.4			5.4
[I.4] Contaminación electromagnética	5.1			5.1
[I.5.2] Avería de origen físico	6.3			6.3
[I.6] Corte de suministro eléctrico	6.8			6.8
[I.7] Condiciones inadecuadas de temperatura o humedad	6.8			6.8

[I.11] Emanaciones electromagnéticas (TEMPEST)			3.3	3.3
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1			5.1
[E.24] Caída del sistema por agotamiento de recursos	7.2			7.2
[E.25] Pérdida de equipos	6.8		6.8	6.8
[A.7] Uso no previsto	3.3	3.3	5.1	3.9
[A.11] Acceso no autorizado	5.1	5.1	6.3	5.5
[A.23] Manipulación del hardware	6		6	6.0
[A.24] Denegación de servicio	7.1			7.1
[A.25] Robo de equipos	6.6		6.6	6.6
[A.26] Ataque destructivo	6.8			6.8
Equipos para redes de telecomunicaciones	7.2	5.1	6.3	
[N.1] Fuego	5.9			5.9
[N.2] Daños por agua	5.4			5.4
[N.] Desastres naturales	5.9			5.9
[I.1] Fuego	6.6			6.6
[I.2] Daños por agua	6			6.0
[I.] Desastres industriales	6.6			6.6
[I.3] Contaminación medioambiental	5.4			5.4
[I.4] Contaminación electromagnética	5.1			5.1
[I.5.2] Avería de origen físico	6.3			6.3
[I.6] Corte de suministro eléctrico	6.8			6.8
[I.7] Condiciones inadecuadas de temperatura o humedad	6.8			6.8
[I.11] Emanaciones electromagnéticas (TEMPEST)			3.3	3.3
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1			5.1
[E.24] Caída del sistema por agotamiento de recursos	7.2			7.2
[E.25] Pérdida de equipos	5.6		6.3	6.0
[A.7] Uso no previsto	5.1		5.1	5.1
[A.11] Acceso no autorizado	5.1	5.1	6.3	5.5

[A.23] Manipulación del hardware	6.6		6		6.3
[A.24] Denegación de servicio	7.1				7.1
[A.25] Robo de equipos	5.3		6		5.7
[A.26] Ataque destructivo	6.8				6.8
REDES DE COMUNICACIONES	7.2	5.6	6.3	6.8	
Red interna laboratorios	7.2	5.6	6.3	6.8	
[I.8] Fallo de servicios de comunicaciones	6.3				6.3
[E.2] Errores del administrador del sistema / de la seguridad	5.6	5.6	5.6		5.6
[E.9] Errores de [re-]encadenamiento			5.1		5.1
[E.10] Errores de secuencia		5.1			5.1
[E.15] Alteración de la información		3.3			3.3
[E.19] Fugas de información			5.1		5.1
[E.24] Caída del sistema por agotamiento de recursos	6.3				6.3
[A.5] Suplantación de identidad		5.1	6.3	6.8	6.1
[A.7] Uso no previsto	5.1	5.1	5.1		5.1
[A.9] [Re-]encaminamiento de mansajes			5.1		5.1
[A.10] Alteración de secuencias		5.1			5.1
[A.11] Acceso no autorizado		5.1	6.3	6.8	6.1
[A.12] Análisis de tráfico			3.8		3.8
[A.14] Interceptación de información (escucha)			5.1		5.1
[A.15] Modificación de la información		5.1			5.1
[A.18] Destrucción de la información	6.3				6.3
[A.24] Denegación de servicio	7.2				7.2
EQUIPAMINETO AUXILIAR	6.8	5.1	6.3		
Equipamiento eléctrico	6.8	5.1	6.3		
[N.1] Fuego	5.9				5.9
[N.2] Daño por agua	5.4				5.4
[N.] Desastres naturales	5.9				5.9
[I.1] Fuego	6.6				6.6

[I.2] Daños por agua	6			6.0
[I.] Desastres industriales	6.6			6.6
[I.3] Contaminación medioambiental	5.4			5.4
[I.4] Contaminación electromagnética	4.8			4.8
[I.11] Emanaciones electromagnéticas (TEMPEST)			3.3	3.3
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1			5.1
[A.7] Uso no previsto	6.3	3.3	3.3	4.3
[A.11] Acceso no autorizado		5.1	6.3	5.7
[A.23] Manipulación del hardware	6.3		6.3	6.3
[A.25] Robo de equipos	6.7			6.7
[A.26] Ataque destructivo	6.8			6.8
Mobiliario para los equipos	6.6	3.3	6.3	
[N.1] Fuego	5.9			5.9
[N.2] Daño por agua	5.4			5.4
[N.] Desastres naturales	5.9			5.9
[I.1] Fuego	6.6			6.6
[I.2] Daños por agua	6			6.0
[I.] Desastres industriales	6.6			6.6
[I.3] Contaminación medioambiental	5.4			5.4
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1			5.1
[A.7] Uso no previsto	6.3	3.3	3.3	4.3
[A.23] Manipulación del hardware	6.3		6.3	6.3
[A.25] Robo de equipos	4.8		6	5.4
[A.26] Ataque destructivo	5.1			5.1
SOPORTES DE INFORMACIÓN	6.8	7.4	6.8	
Nube Microsoft OneDrive	6.8	7.4	6.8	
[N.1] Fuego	5.9			5.9
[N.2] Daño por agua	5.4			5.4

[N.] Desastres naturales	5.9			5.9
[I.1] Fuego	6.6			6.6
[I.2] Daños por agua	6			6.0
[I.] Desastres industriales	6.6			6.6
[I.3] Contaminación medioambiental	6.3			6.3
[I.4] Contaminación electromagnética	5.1			5.1
[I.5.2] Avería de origen físico	6.3			6.3
[I.6] Corte del suministro eléctrico	6.8			6.8
[I.7] Condiciones inadecuadas de temperatura o humedad	6.8			6.8
[I.10] Degradación de los soportes de almacenamiento de la información	6.8			6.8
[I.11] Emanaciones electromagnéticas (TEMPEST)			3.3	3.3
[E.1] Errores de los usuarios	3.3	4.5	5.1	4.3
[E.15] Alteración de la información		3.3		3.3
[E.18] Destrucción de la información	6.8			6.8
[E.19] Fugas de información			5.1	5.1
[E.23] Errores de mantenimiento (actualización de equipos (hardware)	6.8	5.1	6.3	6.1
[E.25] Pérdida de equipos	5.1		6.3	5.7
[A.7] Uso no previsto	3.3		3.3	3.3
[A.11] Acceso no autorizado		3.3	6.3	4.8
[A.15] Modificación de la información		7.4		7.4
[A.18] Destrucción de la información	6.8			6.8
[A.23] Manipulación del hardware	5.4		5.4	5.4
[A.25] Robo de equipos	5.1		6.8	6.0
[A.26] Ataque destructivo	5.1			5.1
INSTALACIONES	6.8		7.7	
Espacios físicos Lab 1 a 9	6.8		7.7	
[N.1] Fuego	6.8			6.8
[N.2] Daño por agua	6.8			6.8

[N.] Desastres naturales	6.6		6.6
[I.1] Fuego	6.8		6.8
[I.2] Daños por agua	6.8		6.8
[I.] Desastres industriales	6.8		6.8
[I.3] Contaminación medioambiental	5.1		5.1
[I.4] Contaminación electromagnética	4.2		4.2
[E.25] Pérdida de equipos		5.9	5.9
[A.6] Abuso de privilegios de acceso	5.1		5.1
[A.7] Uso no previsto	5.1		5.1
[A.25] Robo de equipos		7.7	7.7
[A.26] Ataque destructivo	5.9		5.9
[A.27] Ocupación enemiga	6.8		6.8
Área de servidores y comunicaciones	6.8	7.7	
[N.1] Fuego	6.8		6.8
[N.2] Daño por agua	6.8		6.8
[N.] Desastres naturales	6.6		6.6
[I.1] Fuego	6.8		6.8
[I.2] Daños por agua	6.8		6.8
[I.] Desastres industriales	6.8		6.8
[I.3] Contaminación medioambiental	5.1		5.1
[I.4] Contaminación electromagnética	4.2		4.2
[E.25] Pérdida de equipos		5.9	5.9
[A.6] Abuso de privilegios de acceso	5.1		5.1
[A.7] Uso no previsto	5.1		5.1
[A.25] Robo de equipos		7.7	7.7
[A.26] Ataque destructivo	5.9		5.9
[A.27] Ocupación enemiga	6.8		6.8
Área de soporte y mantenimiento	6.8	7.7	
[N.1] Fuego	6.8		6.8

[N.2] Daño por agua	6.8			6.8
[N.] Desastres naturales	6.6			6.6
[I.1] Fuego	6.8			6.8
[I.2] Daños por agua	6.8			6.8
[I.] Desastres industriales	6.8			6.8
[I.3] Contaminación medioambiental	5.1			5.1
[I.4] Contaminación electromagnética	4.2			4.2
[E.25] Pérdida de equipos			5.9	5.9
[A.6] Abuso de privilegios de acceso	5.1			5.1
[A.7] Uso no previsto	5.1			5.1
[A.25] Robo de equipos			7.7	7.7
[A.26] Ataque destructivo	5.9			5.9
[A.27] Ocupación enemiga	6.8			6.8
PERSONAS	6.3	6.8	7.2	
Jefe de Laboratorios	6.3	6.8	7.2	
[E.15] Alteración de la información		5.1		5.1
[E.18] Destrucción de la información	3.3			3.3
[E.19] Fugas de información			5.1	5.1
[E.28] Indisponibilidad del personal	5.1			5.1
[A.15] Modificación de la información		6.3		6.3
[A.18] Destrucción de la información	5.1			5.1
[A.19] Revelación de información			7.2	7.2
[A.28] Indisponibilidad del personal	5.3			5.3
[A.29] Extorsión	6.3	6.8	6.8	6.6
[A.30] Ingeniería social (picaresca)	6	6.6	6.6	6.4
Asistente de Enseñanza de los laboratorios 1	6	6.3	7.2	
[E.15] Alteración de la información		5.1		5.1
[E.18] Destrucción de la información	3.3			3.3
[E.19] Fugas de información			5.1	5.1
[E.28] Indisponibilidad del personal	5.9			5.9

[A.15] Modificación de la información		6.3		6.3
[A.18] Destrucción de la información	5.1			5.1
[A.19] Revelación de información			7.2	7.2
[A.28] Indisponibilidad del personal	6			6.0
[A.29] Extorsión	5.6	5	6.3	5.6
[A.30] Ingeniería social (picaresca)	5.3	5.3	5.3	5.3
Asistente de Enseñanza de los laboratorios 2	6	6.3	7.2	
[E.15] Alteración de la información		5.1		5.1
[E.18] Destrucción de la información	3.3			3.3
[E.19] Fugas de información			5.1	5.1
[E.28] Indisponibilidad del personal	5.9			5.9
[A.15] Modificación de la información		6.3		6.3
[A.18] Destrucción de la información	5.1			5.1
[A.19] Revelación de información			7.2	7.2
[A.28] Indisponibilidad del personal	6			6.0
[A.29] Extorsión	5.6	5	6.3	5.6
[A.30] Ingeniería social (picaresca)	5.3	5.3	5.3	5.3
Usuarios Laboratorios	6	6.3	6.5	
[E.15] Alteración de la información		5.1		5.1
[E.18] Destrucción de la información	3.3			3.3
[E.19] Fugas de información			5.1	5.1
[A.13] Repudio (negación de actuaciones)	5.1			5.1
[A.15] Modificación de la información		6.3		6.3
[A.18] Destrucción de la información	5.1			5.1
[A.19] Revelación de información			6.5	6.5
[A.28] Indisponibilidad del personal	6			6.0
[A.29] Extorsión	5	5.6	5.6	5.4
[A.30] Ingeniería social (picaresca)	4.8	5.3	5.3	5.1

Nota: La tabla muestra el riesgo potencial acumulado, en donde D: degradación en la dimensión de disponibilidad, I: degradación en la dimensión de integridad, C: degradación en la dimensión de confidencialidad, A: degradación en la dimensión de autenticidad, T: degradación en la dimensión de trazabilidad. Elaboración propia.

Anexo I: Recopilación Riesgos de mayor peso en laboratorios de informática FICA-UTN

ACTIVOS	AMENAZA	PESO PONDERADO
Documentos de administración interna	[A.11] Acceso no autorizado	7.5
Datos de configuración	[A.11] Acceso no autorizado	7.5
Mantenimiento preventivo y correctivo de hardware y software	[A.11] Acceso no autorizado	6.1
Telefonía	[A.11] Acceso no autorizado	6.1
Servidores internos	[A.11] Acceso no autorizado	6.1
Equipamiento eléctrico	[A.11] Acceso no autorizado	5.7
Equipos PC / didácticos	[A.11] Acceso no autorizado	5.5
Equipos de seguridad	[A.11] Acceso no autorizado	5.5
Equipos para redes de telecomunicaciones	[A.11] Acceso no autorizado	5.5
Nube Microsoft OneDrive	[A.11] Acceso no autorizado	4.8
Mantenimiento preventivo y correctivo de hardware y software	[A.13] Repudio (negación de actuaciones)	7.4
Telefonía	[A.13] Repudio (negación de actuaciones)	7.4
Servidores internos	[A.13] Repudio (negación de actuaciones)	7.4
Datos de acceso a servidores y sistemas	[A.13] Repudio (negación de actuaciones)	6.3
Base de datos biométricos	[A.13] Repudio (negación de actuaciones)	6.3
Usuarios Laboratorios	[A.13] Repudio (negación de actuaciones)	5.1
Nube Microsoft OneDrive	[A.15] Modificación de la información	7.4
Mantenimiento preventivo y correctivo de hardware y software	[A.15] Modificación de la información	7.2
Telefonía	[A.15] Modificación de la información	7.2
Servidores internos	[A.15] Modificación de la información	7.2
Jefe de Laboratorios	[A.15] Modificación de la información	6.3
Asistente de Enseñanza de los laboratorios 5	[A.15] Modificación de la información	6.3
Asistente de Enseñanza de los laboratorios 6	[A.15] Modificación de la información	6.3
Usuarios Laboratorios	[A.15] Modificación de la información	6.3
Nube Microsoft OneDrive	[A.18] Destrucción de la información	6.8
Mantenimiento preventivo y correctivo de hardware y software	[A.18] Destrucción de la información	6.3
Telefonía	[A.18] Destrucción de la información	6.3
Servidores internos	[A.18] Destrucción de la información	6.3
Jefe de Laboratorios	[A.18] Destrucción de la información	5.1

Asistente de Enseñanza de los laboratorios 6	[A.18] Destrucción de la información	5.1
Asistente de Enseñanza de los laboratorios 7	[A.18] Destrucción de la información	5.1
Usuarios Laboratorios	[A.18] Destrucción de la información	5.1
Jefe de Laboratorios	[A.19] Revelación de información	7.2
Asistente de Enseñanza de los laboratorios 7	[A.19] Revelación de información	7.2
Asistente de Enseñanza de los laboratorios 8	[A.19] Revelación de información	7.2
Usuarios Laboratorios	[A.19] Revelación de información	6.5
Sistema reserva instalaciones FICA	[A.22] Manipulación de programas	6.6
Aplicación para el manejo de biométricos	[A.22] Manipulación de programas	6.6
Portal Web para Capacitaciones	[A.22] Manipulación de programas	6.6
Portal Web para Capacitaciones	[A.22] Manipulación de programas	6.6
Aplicaciones de ofimática / académicas	[A.22] Manipulación de programas	6.6
Equipos para redes de telecomunicaciones	[A.23] Manipulación del hardware	6.3
Equipamiento eléctrico	[A.23] Manipulación del hardware	6.3
Mobiliario para los equipos	[A.23] Manipulación del hardware	6.3
Equipos PC / didácticos	[A.23] Manipulación del hardware	6.0
Equipos de seguridad	[A.23] Manipulación del hardware	6.0
Nube Microsoft OneDrive	[A.23] Manipulación del hardware	5.4
Mantenimiento preventivo y correctivo de hardware y software	[A.24] Denegación de servicio	7.2
Servidores internos	[A.24] Denegación de servicio	7.2
Equipos PC / didácticos	[A.24] Denegación de servicio	7.1
Equipos de seguridad	[A.24] Denegación de servicio	7.1
Equipos para redes de telecomunicaciones	[A.24] Denegación de servicio	7.1
Espacios físicos Lab 1 a 20	[A.25] Robo de equipos	7.7
Área de servidores y comunicaciones	[A.25] Robo de equipos	7.7
Área de soporte y mantenimiento	[A.25] Robo de equipos	7.7
Equipos PC / didácticos	[A.25] Robo de equipos	7.4
Equipamiento eléctrico	[A.25] Robo de equipos	6.7
Equipos de seguridad	[A.25] Robo de equipos	6.6
Nube Microsoft OneDrive	[A.25] Robo de equipos	6.0
Equipos para redes de telecomunicaciones	[A.25] Robo de equipos	5.7

Mobiliario para los equipos	[A.25] Robo de equipos	5.4
Equipos PC / didácticos	[A.26] Ataque destructivo	6.8
Equipos de seguridad	[A.26] Ataque destructivo	6.8
Equipos para redes de telecomunicaciones	[A.26] Ataque destructivo	6.8
Equipamiento eléctrico	[A.26] Ataque destructivo	6.8
Espacios físicos Lab 1 a 21	[A.26] Ataque destructivo	5.9
Área de servidores y comunicaciones	[A.26] Ataque destructivo	5.9
Área de soporte y mantenimiento	[A.26] Ataque destructivo	5.9
Mobiliario para los equipos	[A.26] Ataque destructivo	5.1
Nube Microsoft OneDrive	[A.26] Ataque destructivo	5.1
Espacios físicos Lab 1 a 22	[A.27] Ocupación enemiga	6.8
Área de servidores y comunicaciones	[A.27] Ocupación enemiga	6.8
Área de soporte y mantenimiento	[A.27] Ocupación enemiga	6.8
Asistente de Enseñanza de los laboratorios 8	[A.28] Indisponibilidad del personal	6.0
Asistente de Enseñanza de los laboratorios 9	[A.28] Indisponibilidad del personal	6.0
Usuarios Laboratorios	[A.28] Indisponibilidad del personal	6.0
Jefe de Laboratorios	[A.28] Indisponibilidad del personal	5.3
Jefe de Laboratorios	[A.29] Extorsión	6.6
Asistente de Enseñanza de los laboratorios 9	[A.29] Extorsión	5.6
Asistente de Enseñanza de los laboratorios 10	[A.29] Extorsión	5.6
Usuarios Laboratorios	[A.29] Extorsión	5.4
Jefe de Laboratorios	[A.30] Ingeniería social (picaresca)	6.4
Asistente de Enseñanza de los laboratorios 10	[A.30] Ingeniería social (picaresca)	5.3
Asistente de Enseñanza de los laboratorios 11	[A.30] Ingeniería social (picaresca)	5.3
Usuarios Laboratorios	[A.30] Ingeniería social (picaresca)	5.1
Datos de configuración	[A.4] Manipulación de los ficheros de configuración	5.9
Documentos de administración interna	[A.5] Suplantación de identidad	6.9
Datos de configuración	[A.5] Suplantación de identidad	6.9
Mantenimiento preventivo y correctivo de hardware y software	[A.5] Suplantación de identidad	6.5
Telefonía	[A.5] Suplantación de identidad	6.5
Servidores internos	[A.5] Suplantación de identidad	6.5

Documentos de administración interna	[A.6] Abuso de privilegios de acceso	5.8
Datos de configuración	[A.6] Abuso de privilegios de acceso	5.8
Espacios físicos Lab 1 a 18	[A.6] Abuso de privilegios de acceso	5.1
Área de servidores y comunicaciones	[A.6] Abuso de privilegios de acceso	5.1
Área de soporte y mantenimiento	[A.6] Abuso de privilegios de acceso	5.1
Mantenimiento preventivo y correctivo de hardware y software	[A.6] Abuso de privilegios de acceso	5.1
Telefonía	[A.6] Abuso de privilegios de acceso	5.1
Servidores internos	[A.6] Abuso de privilegios de acceso	5.1
Equipos para redes de telecomunicaciones	[A.7] Uso no previsto	5.1
Espacios físicos Lab 1 a 19	[A.7] Uso no previsto	5.1
Área de servidores y comunicaciones	[A.7] Uso no previsto	5.1
Área de soporte y mantenimiento	[A.7] Uso no previsto	5.1
Mantenimiento preventivo y correctivo de hardware y software	[A.7] Uso no previsto	4.5
Telefonía	[A.7] Uso no previsto	4.5
Servidores internos	[A.7] Uso no previsto	4.5
Equipos PC / didácticos	[A.7] Uso no previsto	4.5
Equipamiento eléctrico	[A.7] Uso no previsto	4.3
Mobiliario para los equipos	[A.7] Uso no previsto	4.3
Equipos de seguridad	[A.7] Uso no previsto	3.9
Nube Microsoft OneDrive	[A.7] Uso no previsto	3.3
Sistema reserva instalaciones FICA	[A.8] Difusión de software dañino	6.8
Aplicación para el manejo de biométricos	[A.8] Difusión de software dañino	6.8
Portal Web para Capacitaciones	[A.8] Difusión de software dañino	6.8
Portal Web para Capacitaciones	[A.8] Difusión de software dañino	6.8
Aplicaciones de ofimática / académicas	[A.8] Difusión de software dañino	6.8
Mantenimiento preventivo y correctivo de hardware y software	[E.1] Errores de los usuarios	5.1
Telefonía	[E.1] Errores de los usuarios	5.1
Servidores internos	[E.1] Errores de los usuarios	5.1
Nube Microsoft OneDrive	[E.1] Errores de los usuarios	4.3
Jefe de Laboratorios	[E.15] Alteración de la información	5.1

Asistente de Enseñanza de los laboratorios 1	[E.15] Alteración de la información	5.1
Asistente de Enseñanza de los laboratorios 2	[E.15] Alteración de la información	5.1
Usuarios Laboratorios	[E.15] Alteración de la información	5.1
Documentos de administración interna	[E.15] Alteración de la información	3.3
Datos de configuración	[E.15] Alteración de la información	3.3
Mantenimiento preventivo y correctivo de hardware y software	[E.15] Alteración de la información	3.3
Telefonía	[E.15] Alteración de la información	3.3
Servidores internos	[E.15] Alteración de la información	3.3
Red interna laboratorios	[E.15] Alteración de la información	3.3
Nube Microsoft OneDrive	[E.15] Alteración de la información	3.3
Nube Microsoft OneDrive	[E.18] Destrucción de la información	6.8
Mantenimiento preventivo y correctivo de hardware y software	[E.18] Destrucción de la información	5.1
Telefonía	[E.18] Destrucción de la información	5.1
Servidores internos	[E.18] Destrucción de la información	5.1
Documentos de administración interna	[E.18] Destrucción de la información	3.3
Datos de configuración	[E.18] Destrucción de la información	3.3
Jefe de Laboratorios	[E.18] Destrucción de la información	3.3
Asistente de Enseñanza de los laboratorios 2	[E.18] Destrucción de la información	3.3
Asistente de Enseñanza de los laboratorios 3	[E.18] Destrucción de la información	3.3
Usuarios Laboratorios	[E.18] Destrucción de la información	3.3
Documentos de administración interna	[E.19] Fugas de información	5.1
Datos de configuración	[E.19] Fugas de información	5.1
Mantenimiento preventivo y correctivo de hardware y software	[E.19] Fugas de información	5.1
Telefonía	[E.19] Fugas de información	5.1
Servidores internos	[E.19] Fugas de información	5.1
Nube Microsoft OneDrive	[E.19] Fugas de información	5.1
Jefe de Laboratorios	[E.19] Fugas de información	5.1
Asistente de Enseñanza de los laboratorios 3	[E.19] Fugas de información	5.1
Asistente de Enseñanza de los laboratorios 4	[E.19] Fugas de información	5.1
Usuarios Laboratorios	[E.19] Fugas de información	5.1

Mantenimiento preventivo y correctivo de hardware y software	[E.2] Errores del administrador del sistema / de la seguridad	5.6
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad	5.6
Servidores internos	[E.2] Errores del administrador del sistema / de la seguridad	5.6
Sistema reserva instalaciones FICA	[E.20] Vulnerabilidades de los programas (software)	4.8
Aplicación para el manejo de biométricos	[E.20] Vulnerabilidades de los programas (software)	4.8
Portal Web para Capacitaciones	[E.20] Vulnerabilidades de los programas (software)	4.8
Portal Web para Capacitaciones	[E.20] Vulnerabilidades de los programas (software)	4.8
Aplicaciones de ofimática / académicas	[E.20] Vulnerabilidades de los programas (software)	4.8
Sistema reserva instalaciones FICA	[E.21] Errores de mantenimiento / actualización de programas	5.8
Aplicación para el manejo de biométricos	[E.21] Errores de mantenimiento / actualización de programas	5.8
Portal Web para Capacitaciones	[E.21] Errores de mantenimiento / actualización de programas	5.8
Portal Web para Capacitaciones	[E.21] Errores de mantenimiento / actualización de programas	5.8
Aplicaciones de ofimática / académicas	[E.21] Errores de mantenimiento / actualización de programas	5.8
Nube Microsoft OneDrive	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	6.1
Equipos PC / didácticos	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1
Equipos de seguridad	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1
Equipos para redes de telecomunicaciones	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1
Equipamiento eléctrico	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1
Mobiliario para los equipos	[E.23] Errores de mantenimiento (actualización de equipos (hardware)	5.1
Mantenimiento preventivo y correctivo de hardware y software	[E.24] Caída del sistema por agotamiento de recursos	7.2
Telefonía	[E.24] Caída del sistema por agotamiento de recursos	7.2
Telefonía	[E.24] Caída del sistema por agotamiento de recursos	7.2
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	7.2
Equipos PC / didácticos	[E.24] Caída del sistema por agotamiento de recursos	7.2

Equipos de seguridad	[E.24] Caída del sistema por agotamiento de recursos	7.2
Equipos para redes de telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	7.2
Equipos PC / didácticos	[E.25] Pérdida de equipos	7.4
Equipos de seguridad	[E.25] Pérdida de equipos	6.8
Equipos para redes de telecomunicaciones	[E.25] Pérdida de equipos	6.0
Espacios físicos Lab 1 a 17	[E.25] Pérdida de equipos	5.9
Área de servidores y comunicaciones	[E.25] Pérdida de equipos	5.9
Área de soporte y mantenimiento	[E.25] Pérdida de equipos	5.9
Nube Microsoft OneDrive	[E.25] Pérdida de equipos	5.7
Asistente de Enseñanza de los laboratorios 4	[E.28] Indisponibilidad del personal	5.9
Asistente de Enseñanza de los laboratorios 5	[E.28] Indisponibilidad del personal	5.9
Jefe de Laboratorios	[E.28] Indisponibilidad del personal	5.1
Datos de configuración	[E.4] Errores de configuración	3.3
Sistema reserva instalaciones FICA	[E.8] Difusión de software dañino	5.1
Aplicación para el manejo de biométricos	[E.8] Difusión de software dañino	5.1
Portal Web para Capacitaciones	[E.8] Difusión de software dañino	5.1
Portal Web para Capacitaciones	[E.8] Difusión de software dañino	5.1
Aplicaciones de ofimática / académicas	[E.8] Difusión de software dañino	5.1
Espacios físicos Lab 1 a 14	[I.] Desastres industriales	6.8
Área de servidores y comunicaciones	[I.] Desastres industriales	6.8
Área de soporte y mantenimiento	[I.] Desastres industriales	6.8
Equipos PC / didácticos	[I.] Desastres industriales	6.6
Equipos de seguridad	[I.] Desastres industriales	6.6
Equipos para redes de telecomunicaciones	[I.] Desastres industriales	6.6
Equipamiento eléctrico	[I.] Desastres industriales	6.6
Mobiliario para los equipos	[I.] Desastres industriales	6.6
Nube Microsoft OneDrive	[I.] Desastres industriales	6.6
Espacios físicos Lab 1 a 12	[I.1] Fuego	6.8
Área de servidores y comunicaciones	[I.1] Fuego	6.8
Área de soporte y mantenimiento	[I.1] Fuego	6.8

Equipos PC / didácticos	[I.1] Fuego	6.6
Equipos de seguridad	[I.1] Fuego	6.6
Equipos para redes de telecomunicaciones	[I.1] Fuego	6.6
Equipamiento eléctrico	[I.1] Fuego	6.6
Mobiliario para los equipos	[I.1] Fuego	6.6
Nube Microsoft OneDrive	[I.1] Fuego	6.6
Nube Microsoft OneDrive	[I.10] Degradación de los soportes de almacenamiento de la información	6.8
Equipos PC / didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)	3.3
Equipos de seguridad	[I.11] Emanaciones electromagnéticas (TEMPEST)	3.3
Equipos para redes de telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)	3.3
Equipamiento eléctrico	[I.11] Emanaciones electromagnéticas (TEMPEST)	3.3
Nube Microsoft OneDrive	[I.11] Emanaciones electromagnéticas (TEMPEST)	3.3
Espacios físicos Lab 1 a 13	[I.2] Daños por agua	6.8
Área de servidores y comunicaciones	[I.2] Daños por agua	6.8
Área de soporte y mantenimiento	[I.2] Daños por agua	6.8
Equipos PC / didácticos	[I.2] Daños por agua	6.0
Equipos de seguridad	[I.2] Daños por agua	6.0
Equipos para redes de telecomunicaciones	[I.2] Daños por agua	6.0
Equipamiento eléctrico	[I.2] Daños por agua	6.0
Mobiliario para los equipos	[I.2] Daños por agua	6.0
Nube Microsoft OneDrive	[I.2] Daños por agua	6.0
Nube Microsoft OneDrive	[I.3] Contaminación medioambiental	6.3
Equipos PC / didácticos	[I.3] Contaminación medioambiental	5.4
Equipos de seguridad	[I.3] Contaminación medioambiental	5.4
Equipos para redes de telecomunicaciones	[I.3] Contaminación medioambiental	5.4
Equipamiento eléctrico	[I.3] Contaminación medioambiental	5.4
Mobiliario para los equipos	[I.3] Contaminación medioambiental	5.4
Espacios físicos Lab 1 a 15	[I.3] Contaminación medioambiental	5.1
Área de servidores y comunicaciones	[I.3] Contaminación medioambiental	5.1
Área de soporte y mantenimiento	[I.3] Contaminación medioambiental	5.1
Equipos PC / didácticos	[I.4] Contaminación electromagnética	5.1
Equipos de seguridad	[I.4] Contaminación electromagnética	5.1
Equipos para redes de telecomunicaciones	[I.4] Contaminación electromagnética	5.1

Nube Microsoft OneDrive	[I.4] Contaminación electromagnética	5.1
Equipamiento eléctrico	[I.4] Contaminación electromagnética	4.8
Espacios físicos Lab 1 a 16	[I.4] Contaminación electromagnética	4.2
Área de servidores y comunicaciones	[I.4] Contaminación electromagnética	4.2
Área de soporte y mantenimiento	[I.4] Contaminación electromagnética	4.2
Sistema reserva instalaciones FICA	[I.5.1.] Avería de origen lógico	6.3
Aplicación para el manejo de biométricos	[I.5.1.] Avería de origen lógico	6.3
Portal Web para Capacitaciones	[I.5.1.] Avería de origen lógico	6.3
Portal Web para Capacitaciones	[I.5.1.] Avería de origen lógico	6.3
Aplicaciones de ofimática / académicas	[I.5.1.] Avería de origen lógico	6.3
Equipos PC / didácticos	[I.5.2] Avería de origen físico	6.3
Equipos de seguridad	[I.5.2] Avería de origen físico	6.3
Equipos para redes de telecomunicaciones	[I.5.2] Avería de origen físico	6.3
Nube Microsoft OneDrive	[I.5.2] Avería de origen físico	6.3
Equipos PC / didácticos	[I.6] Corte de suministro eléctrico	6.8
Equipos de seguridad	[I.6] Corte de suministro eléctrico	6.8
Equipos para redes de telecomunicaciones	[I.6] Corte de suministro eléctrico	6.8
Nube Microsoft OneDrive	[I.6] Corte del suministro eléctrico	6.8
Equipos PC / didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Equipos de seguridad	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Equipos para redes de telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Nube Microsoft OneDrive	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Espacios físicos Lab 1 a 11	[N.] Desastres naturales	6.6
Área de servidores y comunicaciones	[N.] Desastres naturales	6.6
Área de soporte y mantenimiento	[N.] Desastres naturales	6.6
Equipos PC / didácticos	[N.] Desastres naturales	5.9
Equipos de seguridad	[N.] Desastres naturales	5.9
Equipos para redes de telecomunicaciones	[N.] Desastres naturales	5.9
Equipamiento eléctrico	[N.] Desastres naturales	5.9
Mobiliario para los equipos	[N.] Desastres naturales	5.9
Nube Microsoft OneDrive	[N.] Desastres naturales	5.9

Espacios físicos Lab 1 a 9	[N.1] Fuego	6.8
Área de servidores y comunicaciones	[N.1] Fuego	6.8
Área de soporte y mantenimiento	[N.1] Fuego	6.8
Equipos PC / didácticos	[N.1] Fuego	5.9
Equipos de seguridad	[N.1] Fuego	5.9
Equipos para redes de telecomunicaciones	[N.1] Fuego	5.9
Equipamiento eléctrico	[N.1] Fuego	5.9
Mobiliario para los equipos	[N.1] Fuego	5.9
Nube Microsoft OneDrive	[N.1] Fuego	5.9
Espacios físicos Lab 1 a 10	[N.2] Daño por agua	6.8
Área de servidores y comunicaciones	[N.2] Daño por agua	6.8
Área de soporte y mantenimiento	[N.2] Daño por agua	6.8
Equipamiento eléctrico	[N.2] Daño por agua	5.4
Mobiliario para los equipos	[N.2] Daño por agua	5.4
Nube Microsoft OneDrive	[N.2] Daño por agua	5.4
Equipos PC / didácticos	[N.2] Daños por agua	5.4
Equipos de seguridad	[N.2] Daños por agua	5.4
Equipos para redes de telecomunicaciones	[N.2] Daños por agua	5.4

Nota: Elaboración propia.

Anexo J: Asignación de opción de tratamiento a los riesgos identificados en los laboratorios de informática FICA-UTN

RIESGO	ACTIVO AFECTADO	TRATAMIENTO
[A.11] Acceso no autorizado	Documentos de administración interna	Minimizar
	Datos de configuración	
[A.13] Repudio (negación de actuaciones)	Mantenimiento preventivo y correctivo de hardware y software	Minimizar
	Telefonía	
	Servidores internos	
[A.15] Modificación de la información	Nube Microsoft OneDrive	Minimizar
	Mantenimiento preventivo y correctivo de hardware y software	
	Telefonía	
	Servidores internos	
[A.18] Destrucción de la información	Nube Microsoft OneDrive	Evitar
[A.19] Revelación de información	Jefe de Laboratorios	Evitar
	Asistente de Enseñanza de los laboratorios 7	
	Asistente de Enseñanza de los laboratorios 8	
	Usuarios Laboratorios	
[A.22] Manipulación de programas	Sistema reserva instalaciones FICA	Minimizar
	Aplicación para el manejo de biométricos	
	Portal Web para Capacitaciones	
	Aplicaciones de ofimática / académicas	
[A.24] Denegación de servicio	Mantenimiento preventivo y correctivo de hardware y software	Minimizar
	Servidores internos	
	Equipos PC / didácticos	
	Equipos de seguridad	
	Equipos para redes de telecomunicaciones	
[A.25] Robo de equipos	Espacios físicos Lab 1 a 20	Minimizar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
	Equipos PC / didácticos	
	Equipamiento eléctrico	
	Equipos de seguridad	
[A.26] Ataque destructivo	Equipos PC / didácticos	Minimizar
	Equipos de seguridad	
	Equipos para redes de telecomunicaciones	

	Equipamiento eléctrico	
[A.27] Ocupación enemiga	Espacios físicos Lab 1 a 22	Aceptar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
[A.29] Extorsión	Jefe de Laboratorios	Evitar
[A.5] Suplantación de identidad	Documentos de administración interna	Minimizar
	Datos de configuración	
	Mantenimiento preventivo y correctivo de hardware y software	
	Telefonía	
	Servidores internos	
[A.8] Difusión de software dañino	Sistema reserva instalaciones FICA	Minimizar
	Aplicación para el manejo de biométricos	
	Portal Web para Capacitaciones	
	Portal Web para Capacitaciones	
	Aplicaciones de ofimática / académicas	
[E.18] Destrucción de la información	Nube Microsoft OneDrive	Evitar
[E.24] Caída del sistema por agotamiento de recursos	Mantenimiento preventivo y correctivo de hardware y software	Minimizar
	Telefonía	
	Telefonía	
	Servidores internos	
	Equipos PC / didácticos	
	Equipos de seguridad	
	Equipos para redes de telecomunicaciones	
[E.25] Pérdida de equipos	Equipos PC / didácticos	Minimizar
	Equipos de seguridad	
[I.] Desastres industriales	Espacios físicos Lab 1 a 14	Minimizar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
	Equipos PC / didácticos	
	Equipos de seguridad	
	Equipos para redes de telecomunicaciones	
	Equipamiento eléctrico	
	Mobiliario para los equipos	
	Nube Microsoft OneDrive	
[I.1] Fuego	Espacios físicos Lab 1 a 12	Minimizar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
	Equipos PC / didácticos	
	Equipos de seguridad	

	Equipos para redes de telecomunicaciones	
	Equipamiento eléctrico	
	Mobiliario para los equipos	
	Nube Microsoft OneDrive	
[I.10] Degradación de los soportes de almacenamiento de la información	Nube Microsoft OneDrive	Evitar
[I.2] Daños por agua	Espacios físicos Lab 1 a 13	Evitar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
[I.6] Corte de suministro eléctrico	Equipos PC / didácticos	Aceptar
	Equipos de seguridad	
	Equipos para redes de telecomunicaciones	
	Nube Microsoft OneDrive	
[I.7] Condiciones inadecuadas de temperatura o humedad	Equipos PC / didácticos	Minimizar
	Equipos de seguridad	
	Equipos para redes de telecomunicaciones	
	Nube Microsoft OneDrive	
[N.] Desastres naturales	Espacios físicos Lab 1 a 11	Minimizar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
[N.1] Fuego	Espacios físicos Lab 1 a 9	Minimizar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	
[N.2] Daño por agua	Espacios físicos Lab 1 a 10	Evitar
	Área de servidores y comunicaciones	
	Área de soporte y mantenimiento	

Nota: Elaboración propia.

Anexo K: Identificación de Tareas por Salvaguardas para los laboratorios de informática FICA-UTN

RIESGO	ACTIVO AFECTADO	TRATAMIENTO	SALVAGUARDA	TIPO DE PROTECCIÓN	TAREA PROPUESTA
[A.11] Acceso no autorizado	Documentos de administración interna	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
	Datos de configuración		[IA] Identificación y autenticación	EL	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario
[A.13] Repudio (negación de actuaciones)	Mantenimiento preventivo y correctivo de hardware y software	Minimizar	[G] Organización	AD	Establecimiento de una normativa para el uso de firmas electrónicas en documentos
	Telefonía		[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras
	Servidores internos		[K] Protección de claves criptográficas	EL	Implementación del cifrado hash para el almacenamiento de contraseñas
[A.15] Modificación de la información	Nube Microsoft OneDrive	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN
	Mantenimiento preventivo y correctivo de hardware y software		[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN
	Telefonía		[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN
	Servidores internos		[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN

[A.18] Destrucción de la información	Nube Microsoft OneDrive	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos
[A.19] Revelación de información	Jefe de Laboratorios	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN
	Asistente de Enseñanza de los laboratorios 7		[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN
	Asistente de Enseñanza de los laboratorios 8		[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN
	Usuarios Laboratorios		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
[A.22] Manipulación de programas	Sistema reserva instalaciones FICA	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte
	Aplicación para el manejo de biométricos		[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte
	Portal Web para Capacitaciones		[IP] Sistema de protección de frontera lógica	PR	Implementación de firewall para la red interna de los laboratorios de informática FICA-UTN
	Aplicaciones de ofimática / académicas		[SW] Protección de las aplicaciones informáticas	CR	Desarrollo de la documentación de programas y archivos

[A.24] Denegación de servicio	Mantenimiento preventivo y correctivo de hardware y software	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
	Servidores internos		[BC] Continuidad del negocio	RC	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques
	Equipos PC / didácticos		[S] Protección de los servicios	PR	Establecimiento de un Plan de renovación de equipos de hardware por vida útil
	Equipos de seguridad		[SW] Protección de las aplicaciones informáticas	PR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
	Equipos para redes de telecomunicaciones		[SW] Protección de las aplicaciones informáticas	PR	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)
[A.25] Robo de equipos	Espacios físicos Lab 1 a 20	Minimizar	[A] Registro y auditoría	MN	Implementación de registro de acceso a los laboratorios
	Área de servidores y comunicaciones		[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
	Área de soporte y mantenimiento		[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
	Equipos PC / didácticos		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
	Equipamiento eléctrico		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
	Equipos de seguridad		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos

[A.26] Ataque destructivo	Equipos PC / didácticos	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
	Equipos de seguridad		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
	Equipos para redes de telecomunicaciones		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
	Equipamiento eléctrico		[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
[A.27] Ocupación enemiga	Espacios físicos Lab 1 a 22	Aceptar	[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
	Área de servidores y comunicaciones		[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
	Área de soporte y mantenimiento		[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
[A.29] Extorsión	Jefe de Laboratorios	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN
[A.5] Suplantación de identidad	Documentos de administración interna	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
	Datos de configuración		[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
	Mantenimiento preventivo y correctivo de		[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso

	hardware y software				
	Telefonía		[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
	Servidores internos		[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
[A.8] Difusión de software dañino	Sistema reserva instalaciones FICA	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte
	Aplicación para el manejo de biométricos		[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte
	Portal Web para Capacitaciones		[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte
	Aplicaciones de ofimática / académicas		[BC] Continuidad del negocio	RC	Implantación de un software de antivirus y antimalware efectivo
[E.18] Destrucción de la información	Nube Microsoft OneDrive	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de almacenamiento
[E.24] Caída del sistema por agotamiento de recursos	Mantenimiento preventivo y correctivo de hardware y software	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
	Telefonía		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software

	Servidores internos		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
	Equipos PC / didácticos		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
	Equipos de seguridad		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
	Equipos para redes de telecomunicaciones		[V] Gestión de vulnerabilidades	PR	Desarrollar un manual de emergencia para las redes de comunicaciones
[E.25] Pérdida de equipos	Equipos PC / didácticos	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
	Equipos de seguridad		[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
[I.] Desastres industriales	Espacios físicos Lab 1 a 14	Minimizar	[V] Gestión de vulnerabilidades	MI	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)
	Área de servidores y comunicaciones		[V] Gestión de vulnerabilidades	MI	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)
	Área de soporte y mantenimiento		[V] Gestión de vulnerabilidades	MI	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)
	Equipos PC / didácticos		[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware
	Equipos de seguridad		[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware
	Equipos para redes de telecomunicaciones		[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware

	Equipamiento eléctrico		[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware
	Mobiliario para los equipos		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Nube Microsoft OneDrive		[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)
[I.1] Fuego	Espacios físicos Lab 1 a 12	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Área de servidores y comunicaciones		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Área de soporte y mantenimiento		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Equipos PC / didácticos		[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Equipos de seguridad		[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Equipos para redes de telecomunicaciones		[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales

					(Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Equipamiento eléctrico		[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Mobiliario para los equipos		[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
	Nube Microsoft OneDrive		[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
[I.10] Degradación de los soportes de almacenamiento de la información	Nube Microsoft OneDrive	Evitar	[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet , mantenimiento)
[I.2] Daños por agua	Espacios físicos Lab 1 a 13	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de políticas de uso para los usuarios de los laboratorios de informática FICA-UTN
	Área de servidores y comunicaciones		[V] Gestión de vulnerabilidades	CR	Establecimiento de políticas de uso para los usuarios de los laboratorios de informática FICA-UTN
	Área de soporte y mantenimiento		[V] Gestión de vulnerabilidades	CR	Establecimiento de políticas de uso para los usuarios de los laboratorios de informática FICA-UTN
[I.6] Corte de suministro eléctrico	Equipos PC / didácticos	Aceptar	[AUX] Elementos auxiliares	PR	Implementación de UPS para mantener operativos los servicios
	Equipos de seguridad		[AUX] Elementos auxiliares	IM	Desarrollo de un Plan de Emergencia en caso de fallas eléctricas

	Equipos para redes de telecomunicaciones		[AUX] Elementos auxiliares	PR	Corrección de la carga de dispositvos electrónicos en la distribución de red eléctrica
	Nube Microsoft OneDrive		[AUX] Elementos auxiliares	PR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
[I.7] Condiciones inadecuadas de temperatura o humedad	Equipos PC / didácticos	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de equipo de aire acondicionado para evitar recalentamiento de equipos
	Equipos de seguridad		[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
	Equipos para redes de telecomunicaciones		[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
[N.] Desastres naturales	Espacios físicos Lab 1 a 11	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
	Área de servidores y comunicaciones		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres naturales (Incendio, sismo, tormenta eléctrica)
	Área de soporte y mantenimiento		[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
[N.1] Fuego	Espacios físicos Lab 1 a 9	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
	Área de servidores y comunicaciones		[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
	Área de soporte y mantenimiento		[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
[N.2] Daño por agua	Espacios físicos Lab 1 a 10	Evitar	[V] Gestión de vulnerabilidades	PR	Corregir las falencias en las paredes y techos para evitar humedad

	Área de servidores y comunicaciones		[V] Gestión de vulnerabilidades	CR	Establecimiento de políticas de uso para los usuarios de los laboratorios de informática FICA-UTN
	Área de soporte y mantenimiento		[V] Gestión de vulnerabilidades	CR	Establecimiento de políticas de uso para los usuarios de los laboratorios de informática FICA-UTN

Nota: Elaboración propia.

Anexo L: Descripción Tareas Propuestas para el cumplimiento de Salvaguardas en los Laboratorios de Informática FICA-TUN

N	Nombre	Descripción	Actividades	Presupuesto	Personal	Tiempo (meses)	Factibilidad
1	Corrección de la carga de dispositivos electrónicos en la distribución de red eléctrica	Revisión y pruebas de carga eléctrica a la red para evitar variaciones de voltaje y apagones.		$1,350.00	Un profesional en el área eléctrica	3	Media
2	Desarrollo de la documentación de programas y archivos	Desarrollo de informes con la información relevante a la descripción y configuración de programas instalados en los Equipos PC.		$900.00	Equipo encargado de la administración de los laboratorios	2	Media Alta
3	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)	Desarrollo de afiches con los números de contactos de emergencia tales como: policía, bomberos, ambulancia, servicios de emergencia (911), hospital, ambulancia y rescate general.		$450.00	Equipo encargado de la administración de los laboratorios	1	Muy Alta
4	Desarrollo de un Plan de Emergencia en caso de fallas eléctricas	Desarrollo de un conjunto de actividades a realizar en caso de fallas de		$1,350.00	Un profesional en el área eléctrica	3	Media

		energía o fallo de los equipos UPS.				
5	Diseño de un Sistema de Gestión de Seguridad de la Información para los laboratorios de informática FICA-UTN	Desarrollo de un conjunto de políticas de administración de la información, es comúnmente desarrollado con ayuda de la Norma ISO/IEC 27001. Trabaja bajo el Modelo PDCA (Plan, Do, Check, Act). Su actividad principal es la de gestionar los activos de información en cuanto a confidencialidad, integridad y disponibilidad.	$4,000.00	Un profesional en seguridad informática / equipo de trabajo afín a informática	8	Media Baja
6	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos	Desarrollar backups de los programas y sistemas importantes para las actividades académicas desarrolladas en los Equipos PC de los laboratorios de informática FICA	$900.00	Equipo encargado de la administración de los laboratorios	2	Muy Alta

7	Establecer un proceso de hardering para los Equipos PC de los laboratorios de informática FICA-UTN y el área de oficinas y soporte	Aseguramiento de sistemas mediante la reducción de vulnerabilidades mediante la eliminación de software, servicios, usuarios, etc. que son innecesarios para el sistema	Establecimiento de contraseñas para el arranque de equipos y configuración de BIOS Particiones seguras del sistema operativo Activación y restricción de actualizaciones de software Implantación de programas de seguridad (antivirus) Establecimiento de protocolos de red Aseguramiento del control por acceso remoto	$2,250.00	Equipo técnico especializado en informática	5	Alta
8	Establecimiento de un Plan de simulacros ante desastres industriales (fuego, sismo, tormenta eléctrica)	Desarrollo de un conjunto de acciones como guía para el comportamiento de las personas involucradas en el espacio de ocurrencia del desastre industrial (provenientes de los equipos tecnológicos). Las acciones deben ser identificadas, analizadas, evaluadas e implementadas para		$1,000.00	Equipo técnico especializado equipos tecnológicos	6	Alta

		los desastres potenciales.					
9	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)	Desarrollo de un conjunto de acciones como guía para el comportamiento de las personas involucradas en el espacio de ocurrencia del desastre natural. Las acciones deben ser identificadas, analizadas, evaluadas e implementadas para los desastres potenciales (sismos, terremotos, incendios y tormentas eléctricas)		$1,000.00	Equipo técnico especializado en desastres y catastros	6	Alta
10	Establecimiento de buenas prácticas para la adquisición de Hardware	Desarrollo de un conjunto de actividades para el proceso de adquisición de equipos de hardware	Recepción de solicitudes de necesidades de los usuarios de los laboratorios Análisis de solicitudes y desarrollo de términos de referencia para el proceso de adquisición Recepción y prueba	$450.00	Equipo técnico para dispositivos de hardware	1	Media Alta

			de los equipos de hardware				
11	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)	Desarrollo de actividades de procedimiento o diagramas de respuesta ante desastres industriales (ocasionados por los mismos equipos) como fuego, daños por agua, explosiones, sobrecarga eléctrica		$1,000.00	Equipo técnico especializado en desastres y catastros	6	Alta
12	Establecimiento de un Plan de renovación de equipos de hardware por vida útil	Análisis y establecimiento de fechas para el cambio de equipos a consecuencia de la degradación de estos por su tiempo de vida útil.		$450.00	Equipo encargado de la administración de los laboratorios	1	Media Alta
13	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques	Desarrollo de actividades que contengan el problema de ciberataque para evitar pérdidas	Definir una política sobre ciberseguridad Definir una estrategia de continuidad y recuperación de perdidas Contención del incidente Respaldo de información y cambio de contraseñas	$4,000.00	Equipo altamente capacitado en ciberseguridad	8	Media Baja

		Concientización sobre el ataque generado				
14	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware	Definición de actividades que garanticen llevar un seguimiento de la condición física actual de los equipos de hardware (PC, Monitores, UPS, Racks, etc)	$1,000.00	Equipo encargado de la administración de los laboratorios	2	Muy Alta
15	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware	Estudio, análisis y reubicación de equipos dependiendo las necesidades de estos dentro de los laboratorios. Por ejemplo, ubicación de los CPU, monitores, ups, para garantizar la minimización de perdidas por fallos de entorno.	$1,500.00	Equipo técnico especializado en hardware	3	Media
16	Establecimiento de una normativa para el uso de firmas electrónicas en documentos	Integración del uso de firmas electrónicas para cualquier proceso que requiera validez del personal de los laboratorios, con el fin de no suplantar la identidad y mantener	$200.00	Equipo encargado de la administración de los laboratorios	1	Muy Alta

		la integridad de la información.					
17	Establecimiento de una normativa para imponer sanciones ante daños a los activos	Definición de acciones a seguir frente a daños resultantes de acciones negativas por parte del usuario hacia los activos de los laboratorios. Por ejemplo, definición de multas, citaciones, aprensiones, etc.		$0.00	Equipo encargado de la administración de los laboratorios	1	Muy Alta
18	Implantación de un software de antivirus y antimalware efectivo	Adquisición de aplicaciones de antivirus y antimalware para evitar el ingreso de software maliciosos a los equipos PC de los laboratorios		$3,000.00	Equipo encargado de la administración de los laboratorios	3	Alta
19	Implementación de Acuerdos de confidencialidad a los miembros encargados de los laboratorios de informática FICA-UTN	Desarrollo de acuerdos de confidencialidad sobre la información de carácter delicado referente a los laboratorios a todo el personal encargado.		$600.00	Personal especializado en carácter jurídico	1	Alta
20	Implementación de registro de actividades mediante bitácoras	Desarrollo y almacenamiento de un registro digital de todos los proceso y actividades realizadas los	Registro de mantenimiento a equipos y aplicaciones Registro de llamadas Registro de incidentes	$1,000.00	Equipo encargado de la administración de los laboratorios	1	Alta

		laboratorios de informática FICA-UTN.	de activos Registro de acceso a espacios físicos				
21	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)	IDS es un componente de software dentro del modelo de seguridad para detectar actividades inapropiadas que provienen de un dispositivo o desde la red. IPS es un componente de software dentro del modelo de seguridad para prevenir actividades inapropiadas provenientes de la red.		$4,000.00	Equipo experto en seguridad informática	4	Media
22	Implementación de UPS para mantener operativos los servicios	Adquisición de equipos UPS para mantener operativos los servicios provistos por los laboratorios de informática FICA-UTN (Sistema de Reservaciones, FlexSIM, biométricos)		$200.00	Equipo especializado en instalaciones eléctricas	1	Alta
23	Implementación del cifrado hash para el	Contratación de un sistema en la nube para el		$500.00	Equipo encargado de la	1	Media

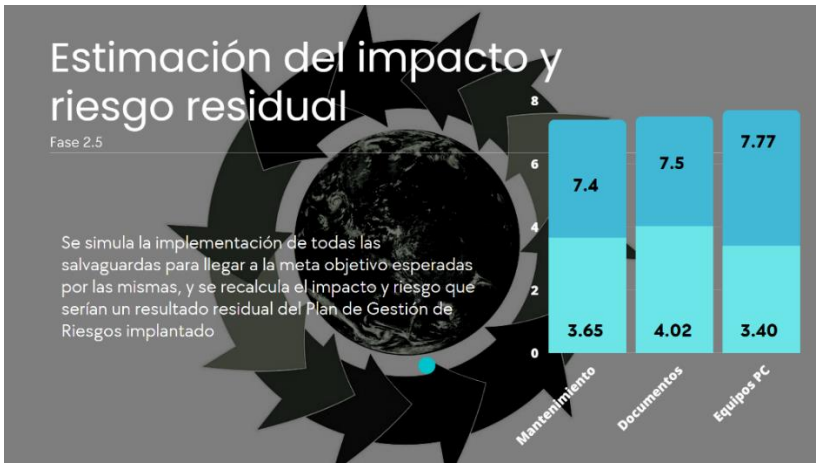
	almacenamiento de contraseñas	almacenamiento de contraseñas con encriptación segura mediante cifrado hash		administración de los laboratorios		
24	Instalación de detectores de humo, alarmas contra incendios, extintores	Adquisición e instalación de detectores de humo de preferencia con baterías para garantizar protección si hubiese problemas eléctricos, adquisición de extintores contra incendios para cada espacio físico	$3,000.00	Equipo de instalación para los equipos	6	Media Alta
25	Instalación de equipo de aire acondicionado para evitar recalentamiento de equipos	Instalación de dispositivos de ventilación de tipo aire acondicionado en ubicaciones específicas para mejorar el control de temperatura en los equipos eléctricos.	$5,000.00	Equipo de instalación para los equipos de ventilación	6	Media
		TOTAL:	$39,100.00			

Nota: Elaboración propia

Anexo M: Material didáctico utilizado para la socialización del Plan de Gestión de Riesgos

Nota: Elaboración propia

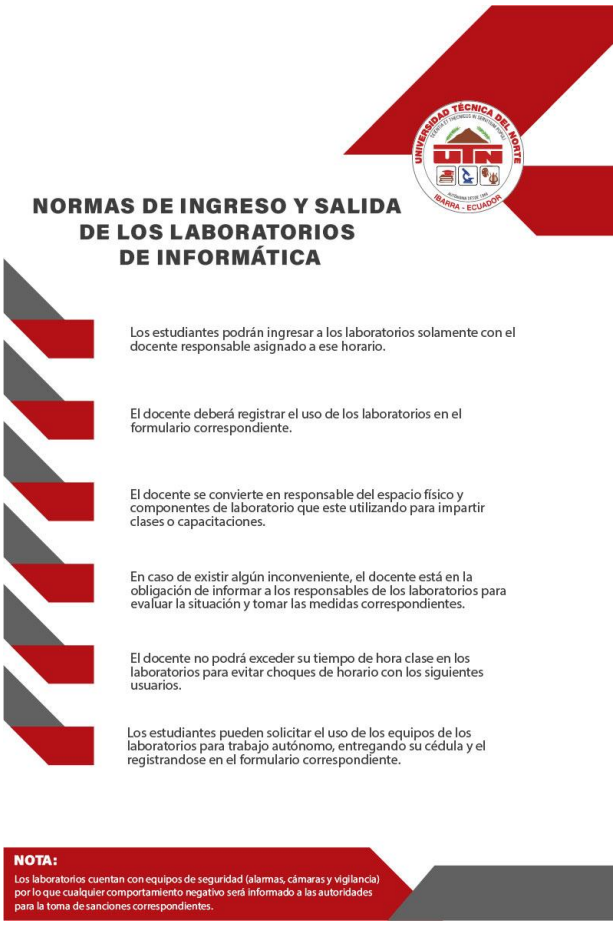
Nota: Elaboración propia



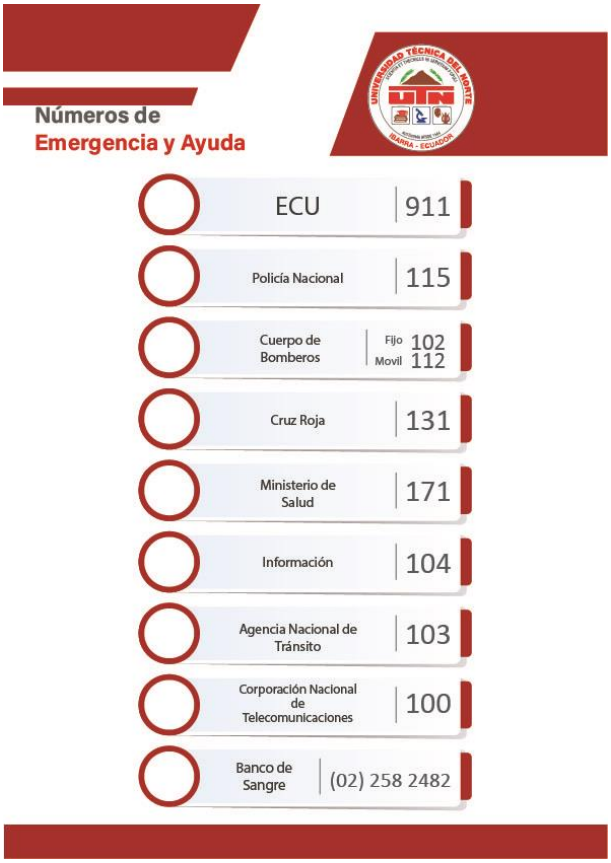
Nota: Elaboración propia

Anexo N: Material POP para los usuarios de los laboratorios de informática FICA-UTN

Nota: Elaboración propia



Nota: Elaboración propia



Nota: Elaboración propia

Nota: Elaboración propia

Nota: Elaboración propia

Anexo O: Primer Cuestionario Validación con el Método Delphi

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución No 001-073 CEAACES – 2013 – 13
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Cuestionario Inicial

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Plan de Gestión de Riesgos Tecnológicos para los Laboratorios de Informática de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte (UTN).

1. **¿Considera usted, qué es necesario el desarrollo de un Plan de Gestión de Riesgos Tecnológicos en departamentos de tecnologías como los "Laboratorios de Informática FICA-UTN"?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

2. **¿En su opinión, el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "Laboratorios de Informática FICA-UTN" es un informe fácil de comprender?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

3. **¿A su juicio, el informe de Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "Laboratorios de Informática FICA-UTN" cuenta con la información necesaria?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo

5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

4. **¿En su opinión, la selección de la metodología MAGERIT versión 3 y la norma ISO 31000 para el desarrollo del Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "Laboratorios de Informática FICA-UTN" fue acertada?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

5. **¿Considera usted, que los pasos desarrollados en el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "Laboratorios de Informática FICA-UTN" fueron los necesarios?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

6. **¿A su juicio, la utilización del software PILAR y las hojas de cálculo de Excel fueron acertadas para el manejo de la información relevante en el desarrollo del Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "Laboratorios de Informática FICA-UTN"?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

7. **¿En su opinión, las tareas propuestas a manera de salvaguardas para la mitigación de riesgos en el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "Laboratorios de Informática FICA-UTN" fueron las idóneas?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

8. **¿Considera usted, qué el Plan de Gestión de Riesgos cumplió con su objetivo de identificación, análisis y mitigación de riesgos en el departamento de tecnología "Laboratorios de Informática FICA-UTN"?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

9. **¿A su juicio, el Plan de Gestión de Riesgos Tecnológicos desarrollado para el departamento de tecnología "Laboratorios de Informática FICA-UTN", puede ser aplicado en otras Instituciones de Educación Superior?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario (opcional): _____
_____
_____

10. **¿Cambiaría usted algún elemento presentado en el Plan de Gestión de Riesgos Tecnológicos en el departamento de tecnología "Laboratorios de Informática FICA-UTN", cuál sería?**

Anexo P: Segundo Cuestionario Validación con el Método Delphi

UNIVERSIDAD TÉCNICA DEL NORTE

UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución No 001-073 CEAACES – 2013 – 13
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Segundo Cuestionario

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Plan de Gestión de Riesgos Tecnológicos para los Laboratorios de Informática de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte (UTN).

1. **¿A su juicio, el estándar de seguridad ISO/IEC 27002 en su versión actualizada de 2022 utilizado por MAGERIT mediante su herramienta PILAR RM (v.1.2.2022) para el tratamiento de los riesgos es el más acertado respecto a este proceso de Gestión de Riesgos Tecnológicos desarrollado para los Laboratorios de Informática FICA-UTN?**
   1) Totalmente de acuerdo
   2) De acuerdo
   3) Indiferente o neutro
   4) En desacuerdo
   5) Totalmente en desacuerdo

2. **¿Considera usted que, debido al beneficio de amplia gama de características y funcionalidades provistas en su licenciamiento de prueba, la herramienta PILAR en su versión RM (1.2.2022) fue la mejor opción para desarrollar el proceso de Gestión de Riesgos Tecnológicos en los Laboratorios de Informática FICA-UTN?**
   1) Totalmente de acuerdo
   2) De acuerdo
   3) Indiferente o neutro
   4) En desacuerdo
   5) Totalmente en desacuerdo

3. **¿Estaría usted de acuerdo con, que al no contar con registro de incidentes ocurridos en los laboratorios de informática FICA-UTN, fue acertado a valorar la frecuencia de amenazas en base a los valores asignados por el software PILAR?**
   1) Totalmente de acuerdo
   2) De acuerdo
   3) Indiferente o neutro
   4) En desacuerdo
   5) Totalmente en desacuerdo

4. **¿Considera usted que, en respuesta al enfoque de Mejora Continua, fue acertada el planteamiento de realizar una revisión de la Gestión de Riesgos Tecnológicos en los laboratorios de informática FICA-UTN una vez hayan trascurridos seis meses del desarrollo de esta?**
   1) Totalmente de acuerdo
   2) De acuerdo
   3) Indiferente o neutro
   4) En desacuerdo
   5) Totalmente en desacuerdo

5. **¿En su opinión, los cambios implementados en el Informe del Plan de Gestión de Riesgos Tecnológicos desarrollados para los Laboratorios de Informática FICA-UTN mejoraron la calidad de este a raíz de las consideraciones tomadas del análisis del primer cuestionario?**
   1) Totalmente de acuerdo
   2) De acuerdo
   3) Indiferente o neutro
   4) En desacuerdo
   5) Totalmente en desacuerdo