UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Software

EVALUACIÓN DE RIESGOS DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA BIBLIOTECA DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON EL SOFTWARE PILAR, UTILIZANDO LA NORMA ISO/IEC 31000.

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

Autor:

Victor Hugo Terán Ballesteros

Director:

Msc. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2024

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:	100478639-6		
APELLIDOS Y NOMBRES:	VICTOR HUGO TERAN BALLESTEROS		
DIRECCIÓN:	OTAVALO, EL JORDAN		
EMAIL:	vhteranb@utn.edu.ec		
TELÉFONO FIJO:	2635-352	**TELEFONO MOVIL:**	0985032045

DATOS DE LA OBRA	
TÍTULO:	EVALUACIÓN DE RIESGOS DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA BIBLIOTECA DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON EL SOFTWARE PILAR, UTILIZANDO LA NORMA ISO/IEC 31000.
AUTOR(ES):	VICTOR HUGO TERAN BALLESTEROS
FECHA:	05/02/2024
PROGRAMA:	PREGADO
TÍTULO POR EL QUE OPTA:	INGENIERO DE SOFTWARE
DIRECTOR:	Msc. DAISY IMBAQUINGO
ASESOR 1:	PhD. 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 14 días del mes de febrero de 2024

EL AUTOR:

Estudiante
Victor Hugo Terán Ballesteros
C.I. 100478639-6

CERTIFICACIÓN DIRECTOR

Ibarra 05 de febrero del 2024

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN

Por medio del presente yo MSc. Daisy Elizabeth Imbaquingo Esparza, certifico que el Sr. Victor Hugo Terán Ballesteros portador de la cedula de ciudadanía número 1004786396, ha trabajado en el desarrollo del proyecto de grado "Evaluación de riesgos de la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte con el software PILAR, utilizando la norma ISO/IEC 31000.", 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

1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA

Firmado digitalmente por 1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA
Fecha: 2024.02.05 15:45:07 -05'00'

Msc. Daisy Imbaquingo

DIRECTOR DE TRABAJO DE GRADO

Dedicatoria

El presente trabajo de grado se lo dedico a mis padres Lupe Ballesteros y Hugo Terán y a mi hermana Fernanda Terán, quienes han estado conmigo en las etapas más difíciles de mi vida, por enseñarme a ser una persona de valores y por siempre brindarme su cariño, amor, confianza y apoyo incondicional para poder afrontar los problemas que se me presentaran, elementos esenciales para cumplir mi sueño.

A mis amigos, familiares y docentes, que me apoyaron en el transcurso de esta etapa, impartiéndome sus conocimientos y ayudándome a crecer como persona y profesional

Con gratitud infinita, dedico este trabajo de integración curricular a quienes han iluminado mi camino con su presencia y afecto.

Victor Hugo Terán Ballesteros

Agradecimientos

Agradezco infinitamente a Dios y a mis padres por ser mi guía, por darme la sabiduría y el conocimiento necesario durante todo este proceso, en especial a mi hermana Fernanda quien me ha inspirado a cumplir todos mis propósitos y sueños, por motivarme a nunca rendirme ante ninguna adversidad y seguir adelante.

Agradezco a mis amigos y compañeros que me ayudaron a convertir estos años de universidad en una aventura llena de conocimientos y alegrías.

También deseo manifestar mi agradecimiento a la Universidad Técnica del Norte, especialmente a la Facultad de Ciencias Aplicadas (FICA) y a la carrera de Ingeniería en Software, por permitirme alcanzar este logro. Expreso mi reconocimiento a mis docentes por compartir sus conocimientos y dedicar su tiempo a mi desarrollo personal y profesional. Agradezco a todas las personas que, de manera directa e indirecta, me han brindado su apoyo a lo largo de mi trayectoria académica.

Quiero expresar mi sincero agradecimiento a la MSc. Daisy Imbaquingo por su colaboración invaluable como directora de tesis. Su respaldo, orientación y sugerencias fueron fundamentales para el logro exitoso de este proyecto académico.

Un agradecimiento al MSc. Marco Pusdá, quien fue mi opositor, por dedicar su tiempo y brindar su colaboración durante la elaboración de este trabajo de integración curricular.

Victor Hugo Terán Ballesteros

Tabla de contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Resumen

El presente estudio de caso tiene como objetivo analizar la gestión de riesgos a la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte mediante la aplicación de la Norma ISO/IEC 31000:2018 y la herramienta EAR/PILAR, el documento se encuentra conformado por tres capítulos en los cuales se detallara todo el proceso para realizar el Trabajo de Grado: "EVALUACIÓN DE RIESGOS DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA BIBLIOTECA DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON EL SOFTWARE PILAR, UTILIZANDO LA NORMA ISO/IEC 31000."

Dentro de las Universidades Ecuatorianas, la Infraestructura Tecnológica de una Biblioteca es un proceso importante que ayuda a mejorar las metodologías de enseñanza y evitar fallos en la educación, lo que permite obtener la acreditación universitaria requerida por organismos de control como el Consejo de Educación Superior del Ecuador (CES).

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

Con el desarrollo constante de las tecnologías de la información y la implementación de sistemas en una variedad de empresas, procesos, productos y servicios, el manejo de los grandes volúmenes de información se vuelve incontrolable. La Universidad Técnica del Norte cuenta con un Departamento de Biblioteca académico que ofrece una variedad de servicios a los docentes, estudiantes y funcionarios administrativos. Y la Infraestructura Tecnológica de la Biblioteca, lo utiliza toda la comunidad de la Universidad.

La Infraestructura Tecnológica de la Biblioteca de la UTN se encuentra ubicada en el campus de el Olivo y necesita cumplir con ciertos requerimientos para preservar el activo más importante que son los datos y la información de la Biblioteca de la UTN por lo que se realizó un estudio de vulnerabilidades para conocer la situación actual establecer si cumple con las normas de seguridad de la información mediante la norma ISO 31000:2018.

Finalmente, se realizará una lista de comprobación para evaluar el cumplimiento de la norma de seguridad de la información de la Norma ISO/IEC 31000:2018 con la finalidad de conocer el estado actual y proponer recomendaciones adecuadas para mejorar el funcionamiento y la seguridad de la Infraestructura Tecnológica de la Biblioteca de la UTN.

Palabras claves: riesgo, gestión, vulnerabilidades, ISO, EAR/PILAR fuente de riesgo, evento, consecuencia, probabilidad.

Abstract

The objective of this case study is to analyze the risk management of the Technological Infrastructure of the Library of the Universidad Técnica del Norte through the application of the ISO/IEC 31000: 2018 and the EAR/PILAR tool, the document is made up of three chapters which will detail the entire process to perform the Degree Work: "RISK ASSESSMENT OF THE TECHNOLOGICAL INFRASTRUCTURE OF THE LIBRARY OF THE UNIVERSIDAD TÉCNICA DEL NORTE WITH THE PILAR SOFTWARE, USING THE ISO/IEC 31000 STANDARD. "

Within Ecuadorian Universities, the Technological Infrastructure of a Library is an important process that helps to improve teaching methodologies and avoid failures in education, which allows obtaining the university accreditation required by control agencies such as the Higher Education Council of Ecuador (CES).

The Introduction of this document defines the background, prospective, problem statement, current situation, general and specific objective, scope and justification.

With the constant development of information technologies and the implementation of systems in a variety of companies, processes, products and services, the management of large volumes of information is becoming uncontrollable. The Universidad Técnica del Norte has an academic Library Department that offers a variety of services to teachers, students and administrative staff. And the Technological Infrastructure of the Library is used by the entire University community.

The Technological Infrastructure of the UTN Library is located on the campus of El Olivo and needs to meet certain requirements to preserve the most important asset which is the data and information of the UTN Library so a study of vulnerabilities was conducted to know the current situation to establish if it complies with the information security standards through the ISO 31000:2018 standard.

Finally, a checklist will be made to assess compliance with the information security standard ISO/IEC 31000:2018 in order to know the current status and propose appropriate recommendations to improve the operation and security of the Technological Infrastructure of the Library of the UTN.

Keywords: risk, management, vulnerabilities, ISO, EAR/PILAR risk source, event, consequence, probability.

Introducción

Tema

Evaluación de riesgos de la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte con el software PILAR, utilizando la norma ISO/IEC 31000.

Problema

Antecedentes

Siempre existen riesgos inherentes en cualquier ámbito de la vida, tanto personal como empresarial, que pueden afectar negativamente nuestros objetivos y resultados. La gestión de riesgos es un campo importante que busca identificar, evaluar y reducir los riesgos potenciales para reducir su impacto y maximizar las oportunidades de éxito. En este contexto, comprender los diversos tipos de riesgos a los que nos enfrentamos es esencial, así como estar preparados para enfrentarlos de manera efectiva. Este párrafo introductorio destaca la importancia de la gestión de riesgos y sienta las bases para un análisis más exhaustivo de los riesgos específicos y las técnicas para abordarlos.

La gestión de riesgos es un proceso que implica identificar, analizar y evaluar los riesgos potenciales que pueden afectar a una organización, proyecto o incluso a nuestra propia vida diaria. Al identificar los riesgos, podemos tomar medidas proactivas para minimizar su impacto y maximizar nuestras oportunidades de éxito.

Dentro de una organización a diario se genera grandes cantidades de información de diversas fuentes como base de datos, correos electrónicos documentales en papel, etc. Por esta razón las empresas tienen una gran responsabilidad en proteger dicha información para que las personas no puedan hacer mal uso de esto.

Pero la gestión de riesgos no solo se aplica en el mundo empresarial. También es importante aplicarla en nuestra vida diaria. Por ejemplo, al conducir un automóvil, debemos identificar los posibles riesgos en la carretera y tomar precauciones para evitar accidentes. Del mismo modo, al invertir nuestro dinero o tomar decisiones importantes en nuestra vida personal, es fundamental evaluar los riesgos y tomar medidas para minimizarlos.

Situación Actual

Actualmente, la Biblioteca de la UTN cuenta con un determinado personal dedicado, entre los cuales está: el encargado de Informática y Digitalización del área de Informática. La distribución tecnológica de los laboratorios de informática y digitalización de la Biblioteca de la UTN es la siguiente:

8 áreas con prestaciones de equipos Lenovo con sistema Operativo Windows

La distribución de espacios de trabajo de la Biblioteca de la UTN está diseñada para ser utilizados por toda la Universidad y tienen una capacidad promedio de 15 equipos por área.

Actualmente, la información digital gestionada por la Biblioteca de la UTN posee un valor incalculable y ha adquirido una importancia fundamental en la institución. Esto se debe a que contiene datos del personal administrativo, lo que conlleva la posibilidad de que en algún momento dicha información sea vulnerada, alterada o eliminada debido a riesgos como robos de identidad y prácticas inadecuadas en la gestión de la información.

Según (Cano, 2004) en su artículo "Inseguridad Informática: un concepto dual en seguridad informática" manifiesta realizar un análisis actual dentro de cada organización, lo cual contribuya a fortalecer sus esquemas de seguridad.

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 la Biblioteca de la UTN.

Aunque se han elaborado diversos documentos que describen el uso sugerido de los equipos durante el horario académico, no hay políticas respaldadas por las autoridades ni un plan establecido para analizar y gestionar los riesgos con el fin de reducir las vulnerabilidades presentes en la Biblioteca de la 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 a la Norma ISO/IEC 31000:2018, para ser aplicado al departamento de estudio, que en este caso es el área de informática y digitalización de la Biblioteca de la Universidad Técnica del Norte.

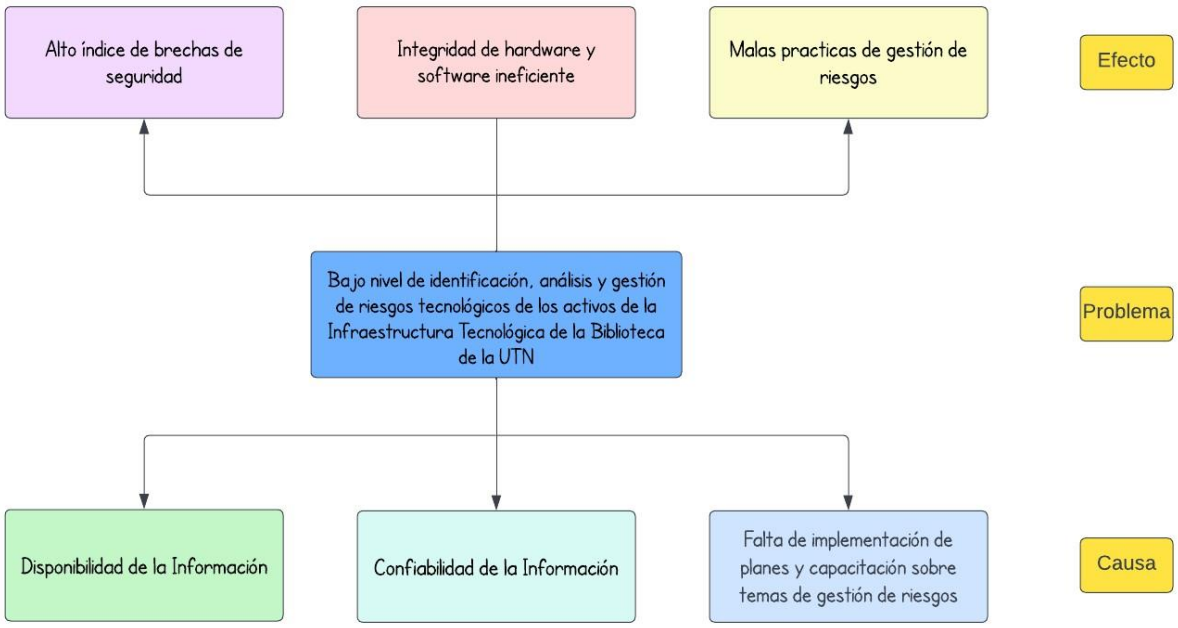
Planteamiento del problema

En la Biblioteca de la UTN no se ha realizado una evaluación pertinente aplicando herramientas adecuadas para analizar una gestión de riesgos que permita contrarrestar posibles problemas o vulnerabilidades que pueda tener la biblioteca y el área de Informática y Digitalización de la Universidad Técnica del Norte por cual se requiere utilizar herramientas que ayuden a analizar y gestionar riesgos tecnológicos para

después evaluar los resultados que se obtengan después de la investigación, como se muestra en la Figura 1.

Figura 1:

Árbol de problemas



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

Objetivos

Objetivo General

Evaluar los riesgos de la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte con el software PILAR, utilizando la norma ISO/IEC 31000.

Objetivos Específicos

- Documentar un marco teórico sobre el análisis y gestión de riesgos tecnológicos.
- Evaluar la gestión de riesgos tecnológicos de la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte con el Software PILAR, utilizando la norma ISO/IEC 31000.

- Validar la evaluación de gestión de riesgos de la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte, mediante el método Delphi.

Alcance

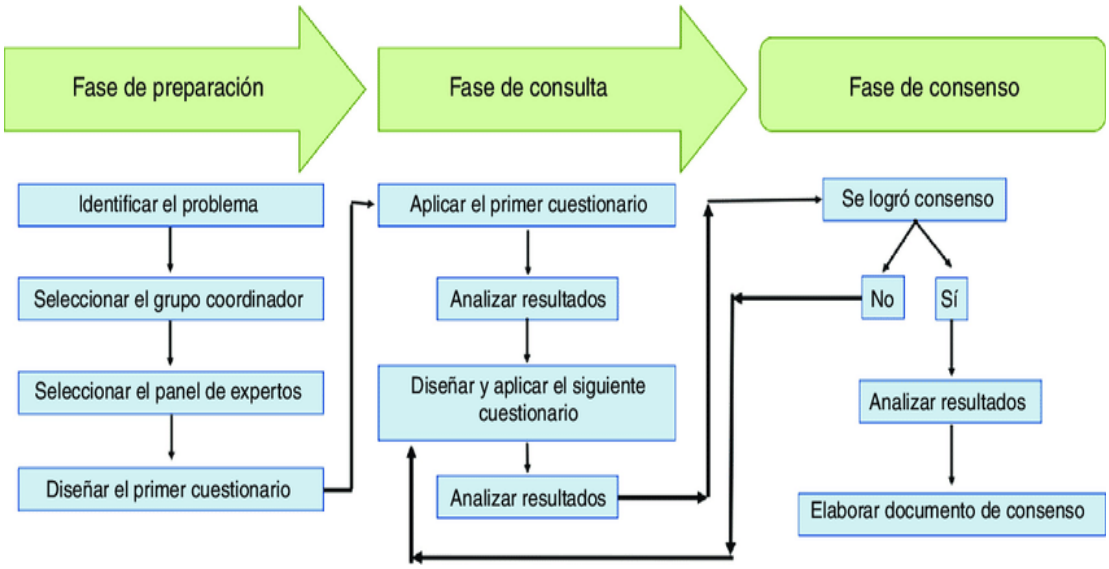
El presente proyecto se centrará en evaluar los riesgos de la Infraestructura Tecnológica en el Departamento de Biblioteca de la Universidad Técnica del Norte.

Toda esta gestión de riesgos que se realizará a la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte se llevará a cabo aplicando la ISO 31000 y con la herramienta PILAR en la evaluación de riesgos, una vez que se identifiquen los riesgos se procederá al análisis de estos y a la generación del plan de salvaguardas.

En la Figura 2 se puede apreciar proceso que sigue metodología Delphi.

Figura 2:

Proceso Metodología DELPHI



Nota: La figura presenta los distintos pasos a seguir para la validación de gestión de riesgos de los activos que se identificarán. Tomado de (Fernández-Ávila et al., 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 relevante destacar que, además, se utilizó la versión de prueba del software PILAR, una herramienta desarrollada por el Centro Nacional de Inteligencia de España, para llevar a cabo el análisis y la gestión de los riesgos en concordancia con los Criterios.

Metodología

En un principio se llevará a cabo una investigación acerca de la Metodología a utilizarse al igual que el kit de herramientas que nos ayudaran a solucionar los problemas que se encuentren.

Una vez que se realice el debido análisis y se encuentren los posibles problemas se llevara a cabo el método Delphi [Figura 2]. para determinar cómo debemos resolverlos y cuál será el kit de herramientas y metodologías que se van a usar en estos casos como se trata de una evaluación de riesgos y vamos a encontrar los posibles riesgos, fallos y vulnerabilidades que tendrá la Infraestructura Tecnológica de la Biblioteca de la UTN los procederemos a resolver con la ayuda de la herramienta PILAR aplicando la norma ISO/IEC 31000 como se puede observar en la [Figura 3] aplicando todas estas herramientas se podrá resolver estos problemas que se encuentren durante la Evaluación.

Para el cumplimiento del objetivo 1, el marco teórico tendrá un enfoque investigativo/analítico en el cual se realizará una búsqueda de numerosas referencias sobre temas de Gestión de Riesgos especialmente en el ámbito tecnológico, esta investigación tratará sobre buscar un kit de herramientas adecuadas para realizar la gestión de riesgos. Todas estas referencias serán investigadas de artículos científicos o de libros confiables, con información de calidad que sean veraces y tengan sustento científico. El proceso de investigación se ejecutará con una revisión minuciosa de artículos que dispongan de cuartil 1 a cuartil 4 para que la información disponga la mayor credibilidad posible.

Con el propósito de alcanzar el segundo objetivo, tras llevar a cabo una exhaustiva investigación de las herramientas que se emplearán, se abordará inicialmente el estado actual del caso de estudio mediante la ejecución de tres tareas.

- Recopilación de información: se realizará mediante entrevistas al equipo encargado del Departamento de Biblioteca del área de Informática y Digitalización de la UTN.
- Evaluación del problema: se realizará mediante la tabulación de encuestas realizadas a usuarios y encargados del área de Informática y Digitalización de la Biblioteca de la UTN.
- Estado de gestión de riesgos: se realizará mediante resultados de fichas de evaluación de riesgos al equipo encargado del área de Informática y Digitalización de la Biblioteca de la UTN.

Para determinar las fases comprendidas en el Plan de Gestión de Riesgos se tomará en cuenta la herramienta PILAR aplicando la ISO 31000 con 6 lineamientos presentes los cuales serían:

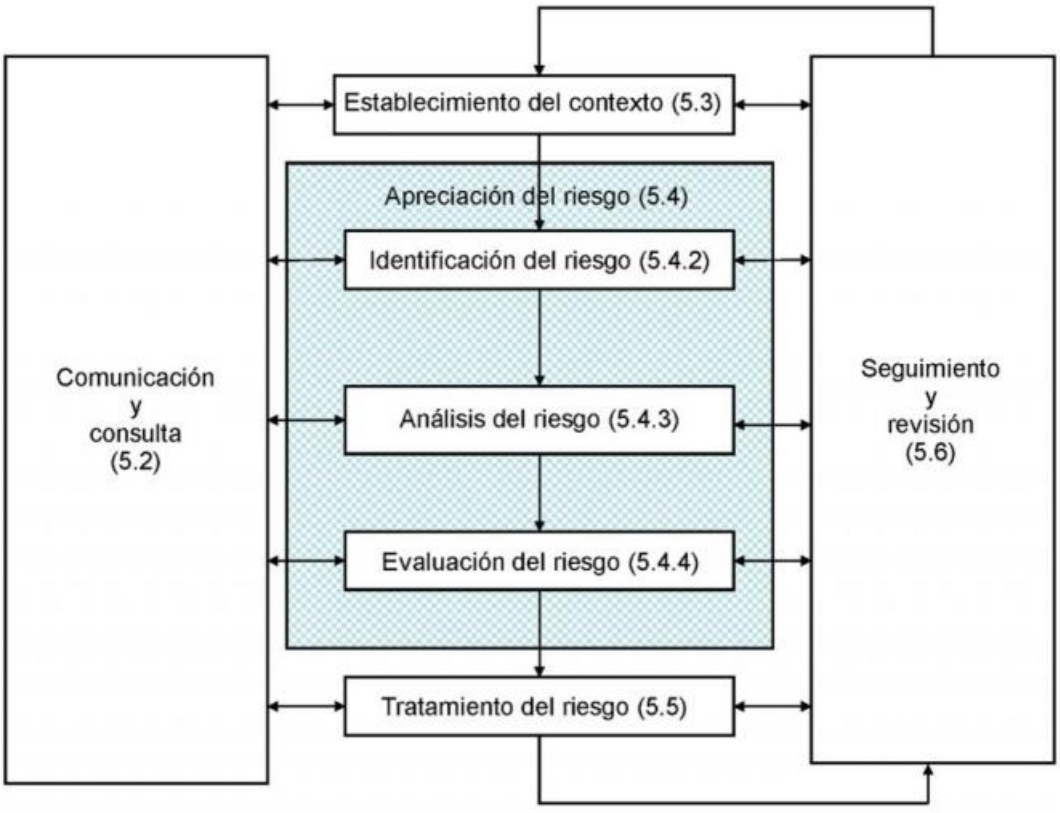
1. Principios
2. Liderazgo y compromiso

3. Diseño del marco de trabajo
4. Implementación de la gestión de riesgo
5. Seguimiento y Evaluación
6. Mejora continua

Con el propósito de alcanzar la meta 3, tras examinar detenidamente los riesgos mediante el uso de la herramienta PILAR, se contrastarán estos riesgos para posteriormente someterlos a una evaluación. Este proceso se realizará siguiendo las directrices de implementación establecidas por la norma ISO/IEC 31000. Para concluir, se llevará a cabo una evaluación del Plan de Gestión de Riesgos previamente elaborado mediante el método Delphi, mediante la consulta a expertos en la materia.

Figura 3:

Estructura de la norma ISO/IEC 31000



Nota: La figura presenta los pasos de la Norma ISO/IEC 31000:2018 correspondiente para cumplir con el segundo objetivo del trabajo de investigación. Tomado de (ISO 31000, 2018)

Justificación

El motivo para realizar esta Evaluación de Riesgos en la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte es porque no se ha

realizado una gestión de riesgos anteriormente ya sea por varios factores como pueden ser la Falta de política de la Institución, Falta de especialista para realizar este tipo de gestiones, Falta de buenas prácticas o por Falta de presupuesto ya que la institución depende del gobierno al ser una institución pública y no siempre el Estado aporta para este tipo de operaciones.

Los Objetivos de Desarrollo Sostenible constituyen la hoja de ruta fundamental para alcanzar un futuro sostenible para la humanidad. Están interconectados y abordan los desafíos globales que enfrentamos cotidianamente, tales como la pobreza, la desigualdad, el cambio climático, la degradación del medio ambiente, la prosperidad, la paz y la justicia. Para garantizar que nadie quede rezagado, es esencial alcanzar la realización de cada uno de estos objetivos antes del año 2030. (Objetivos y Metas de Desarrollo Sostenible, 2015).

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” (Objetivos y Metas de Desarrollo Sostenible, 2015).

El impulso de los entornos de datos a nivel regional y nacional se llevará a cabo mediante el fortalecimiento de las redes de innovación y tecnología. Se busca la colaboración potencial del sector privado y la sociedad civil con el objetivo de fomentar la apertura de datos. Este enfoque incluirá la integración de datos no convencionales, como registros administrativos, conjuntos de datos extensos y datos provenientes de la sociedad civil. Además, se buscará mejorar la información geográfica y aprovechar herramientas de visualización y georreferenciación. (Naciones Unidas, 2018).

Justificación Tecnológica

La importancia de realizar un análisis de riesgos al sistema con la pila de herramientas adecuadas nos dará un mejor resultado y nos ayudará para al final evaluar los resultados obtenidos durante el análisis.

Justificación Metodológica

Contar con un modelo que permita Gestionar los Riesgos puede vislumbrar un panorama importante para la administración de proyectos por lo que considero pertinente la utilización de la norma ISO/IEC 31000 para realizar este plan de gestión de riesgos, al estar preparados proactivamente para enfrentar las amenazas que afecten el resultado final de los proyectos teniendo en cuenta que el propósito principal es realizar el análisis para después evaluar los resultados finales

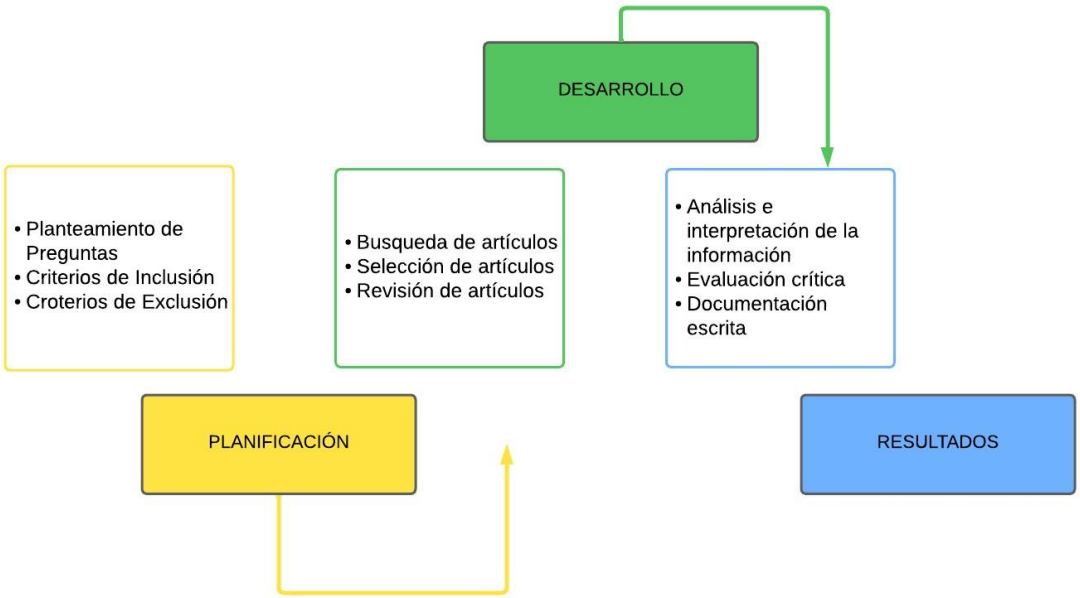
CAPÍTULO 1

Marco Teórico

Se empleó el método de revisión bibliográfica para desarrollar el Marco Teórico sobre el análisis y la gestión de riesgos en las áreas de Tecnologías de la Información (TI) de las Instituciones de Educación Superior. Este enfoque abarca las fases detalladas en la Figura 4.

Figura 4:

Proceso Revisión Bibliográfica



Nota: En la figura se ilustran las tres etapas junto con sus respectivas actividades relacionadas con la revisión de la literatura en la construcción del Marco Teórico. Elaboración propia.

Se propusieron diversos enfoques con preguntas clave durante la fase de planificación, centradas en el tema de la Gestión de Riesgos.

- Estas son algunas de las interrogantes planteadas para la caracterización del concepto de Gestión de Riesgos de Tecnologías de la Información en Instituciones de Educación Superior:

I. ¿Cuál es la definición precisa de Gestión de Riesgos?

II. ¿Cuáles son los conceptos relacionados que se vinculan con la gestión de riesgos?
III. ¿Cuáles son los beneficios inherentes al proceso de Gestión de Riesgos en el contexto organizacional?

- Descripción de Enfoques para la Administración de Riesgos en Tecnologías de la Información

I. ¿Cuáles son las distintas metodologías disponibles para la administración de riesgos en TI?
II. ¿Cuáles son los procedimientos o etapas que comprenden estas metodologías?
III. ¿Cuáles son las implicaciones positivas o negativas asociadas con estas metodologías?

- Análisis de Pautas para la Administración de Riesgos en Tecnologías de la Información

I. ¿Qué pautas a nivel nacional o internacional rigen la administración de riesgos en TI?
II. ¿Cuáles son las recomendaciones o requisitos de cumplimiento establecidos por estas pautas?
III. ¿Cuáles son los beneficios y limitaciones inherentes a estas normativas?

Los criterios de inclusión abarcan diversas condiciones que sirven como filtros para la selección del material, que puede ser de diversos tipos como artículos científicos, entrevistas, informes oficiales, libros, sitios web o tesis. En el caso de los artículos científicos, es necesario que provengan de revistas científicas clasificadas en los cuartiles Q1 a Q4, y que estén redactados en español o inglés.

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

1.1. Análisis y Gestión de Riesgos.

1.1.1 ¿Qué es la Gestión de Riesgos?

La gestión de los riesgos es el proceso de su identificación y evaluación, y la creación del plan para reducir o controlar esos riesgos inmediato con el efecto que podrían tener en la empresa. Un riesgo implica una posible pérdida o daño. Puede originarse por distintas causas, como la responsabilidad legal, los desastres naturales, los accidentes, los errores de gestión o las amenazas de ciberseguridad (Red Hat, 2019).

Las estrategias de gestión de riesgos son las tácticas que se utilizan para contender con ellos y para percibir sus posibles consecuencias. Deben incluirse en un plan de gestión de riesgos, un proceso documentado referente a la forma en la que la empresa o el equipo identificará y abordará los riesgos que surjan.

Tabla 1

Definición de Gestión de Riesgos por varios autores

Autor	Definición	País	Año
Bharathy, Gnana K. McShane, Michael K.	La gestión de riesgos empresariales (ERM) se ha convertido en el nuevo paradigma en la gestión de riesgos con el objetivo de gestionar de manera integral todos los riesgos que enfrenta una empresa. Sin embargo, las organizaciones aún gestionan los riesgos de manera fragmentada y luchan por implementar ERM de manera efectiva y administrar riesgos estratégicos complejos.	España	2015
Arias, Paola Ferro, Roberto Abuchar, Alexandra	La gestión de riesgos de proyecto por medio del proceso de identificación, análisis y respuesta a un riesgo, maximización de las consecuencias de los eventos positivos y la minimización de la ocurrencia de un evento negativo, permite anticipar problemas y oportunidades, asegurando el logro de metas de fechas, costos y alcance	Colombia	2019
Laurdet, Osmel Gordillo, Heriberto	La gestión del riesgo consiste en una serie de pasos que ayudan al equipo a comprender y a gestionar la incertidumbre, además de contribuir a la toma de decisiones. Un riesgo es un problema potencial (puede ocurrir o no), pero sin tener en cuenta el resultado, es necesario identificarlo, evaluar su probabilidad desaparición, estimar su impacto y establecer un plan	Cuba	2013

	de contingencia por si ocurre el problema. La gestión de riesgos se puede definir entonces como el proceso de identificación, análisis y prevención de los riesgos que amenazan activos, ganancias o personal de una organización, además de afectar los servicios que ésta provee		
Reañez, Maryoribel Vallejo, Byron Delgado, Mercedes	La gestión de riesgos se define como el conjunto de actividades que se realizan para reducir las incertidumbres asociadas con ciertas tareas, o eventos. En el contexto de los proyectos, esa misma gestión del riesgo reduce los impactos en ellos de los eventos no deseados, por lo cual requiere la realización de actividades del proceso de toma de decisiones.	Ecuador	2018

Nota: Elaboración Propia a partir de Artículos. Tomado de (Rossetti & Quiroga, 2023).

1.1.2 Seguridad Informática

Tabla 2

Definición de Seguridad Informática por varios autores

Autor	Definición	País	Año
Fernández A., Nilo Maquera Q, Henry Mercado R., Richard	La seguridad informática busca dar apoyo a los objetivos y misión de las organizaciones, a través de la protección de sus principales recursos y activos que son: la información, la tecnología que la soporta (software y hardware) y las personas que la utilizan o conocen a través de la selección y aplicación de protecciones adecuadas, manteniendo así el debido cuidado de sus recursos físicos, financieros, reputación y otros activos tangibles e intangibles.	Perú	2022
Cano, Jeimy J.	La seguridad informática como necesidad organizacional, no es más que el resultado de una propiedad emergente de un sistema que conoce	Colombia	2004

	sus condiciones extremas, su operación límite, así como sus recursos y posibilidades para darle sentido a la razón de su misión. Es decir, reconocer que los ataques y fallas de seguridad informática son una constante y por tanto, se requiere conocer y validar los niveles de siniestralidad o falla que la organización puede manejaren la operación de su negocio.		
Guaña-Moya, Javier	La seguridad informática desempeña un papel fundamental en la educación digital, destacado por diversos estudios; las soluciones propuestas incluyen la aplicación de normas internacionales, la implementación de buenas prácticas, el análisis de riesgos y vulnerabilidades, y la capacitación en competencias digitales, por lo que, es esencial promover una cultura de seguridad informática en el ámbito educativo para proteger la información y garantizar un entorno digital seguro para estudiantes, docentes y padres de familia.	Ecuador	2023
Patiño, Susana Mosquera, Carmen Suárez Franyelit Nevares, Ronnie	El sistema de gestión de la seguridad de la información se basa en salvaguardar la integridad, disponibilidad y confiabilidad de la información en una organización. Proteger la confiabilidad, integridad y disponibilidad de la información, es el eje principal de la norma. Su aplicación: es un proceso que debe identificar los problemas potenciales que afectarían a la información y luego, definir un plan donde se evite o mitigue los riesgos posibles.	Ecuador	2017

***Nota*:** Elaboración Propia a partir de Artículos. Tomado de (Norberto & Meza, 2023)

La seguridad informática de la misma manera denominada ciberseguridad se refiere a la protección de la información y, fundamentalmente, al procesamiento que se hace de la misma, con el objetivo de impedir el manejo de datos y procesos por personas no autorizadas. Su primordial objetivo es que las personas como equipos tecnológicos y datos estén protegidos en contra de daños y amenazas hechas por terceros.

La seguridad informática, la ciberseguridad o la seguridad de la tecnología de la información es la protección de los sistemas informáticos y las redes frente a ataques de actores malintencionados que pueden provocar la divulgación no autorizada de información, el robo o el daño del hardware, el software o los datos, así como la interrupción o desvío de los servicios que prestan.

Según el autor (Gómez, 2015) define la Seguridad Informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información de los equipos.

En caso de existir una amenaza o vulneración a la seguridad informática, se debe de buscar la forma de recuperar toda la información que haya sido robada y vulnerada.

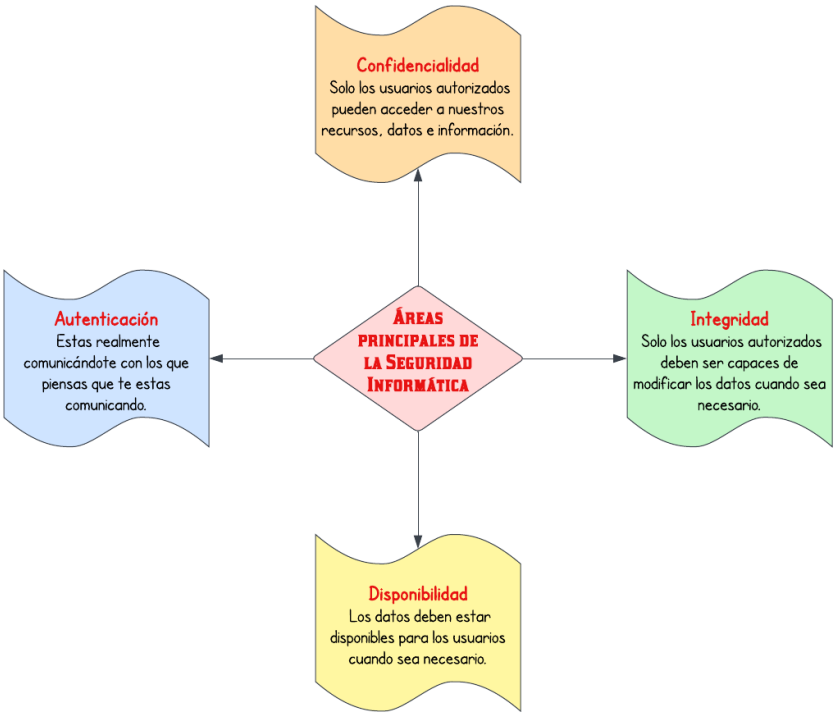


Figura 5: Áreas principales de la Seguridad Informática

Fuente: Propia

1.1.3 Seguridad de la Información

La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización. Es una pieza clave para que las empresas puedan llevar a cabo sus operaciones, ya que

los datos que maneja son esenciales para la actividad que desarrollan (ISO 27001:2013, 2021).

La seguridad de la información se refiere a la práctica de salvaguardar los datos y minimizar sus riesgos. Es un componente de la gestión de riesgos para la información. En general, esto es prevenir o reducir la probabilidad de acceso no autorizado o inapropiado a los datos, o de uso no autorizado, divulgación, interrupción, eliminación, corrupción, modificación, inspección, registro o devaluación de la información. Además, se refiere a acciones destinadas a aminorar los efectos negativos de tales ocurrencias. La información protegida puede adoptar cualquier forma, ya sea física o digital, tangible o inmaterial.

Teniendo en cuenta lo antes mencionado se obtiene un punto de vista más amplio en donde se define a la Seguridad de la Información como la preservación de su confidencialidad, su integridad y su disponibilidad además de sus áreas principales como se puede observar en la [Figura 5].

Además, como se puede observar en la Tabla 3 se tiene una comparación entre la definición de Seguridad Informática y Seguridad de la Información

Tabla 3

Comparación entre Seguridad Informática y Seguridad de la Información

Aspecto	Seguridad Informática	Seguridad de la Información
Definición	Se centra en la protección de los sistemas informáticos y la infraestructura tecnológica.	Se enfoca en la protección de la información en todas sus formas, incluyendo su confidencialidad, integridad y disponibilidad.
Alcance	Se ocupa principalmente de la seguridad de los sistemas informáticos y las redes.	Considera la seguridad de la información en un sentido más amplio, incluyendo aspectos físicos, humanos y tecnológicos.
Objetivo principal	Proteger los sistemas y redes contra amenazas informáticas como virus, malware, ataques cibernéticos, etc.	Garantizar la confidencialidad, integridad y disponibilidad de la información, así como protegerla contra amenazas internas y externas.
Enfoque	Se centra en aspectos técnicos y tecnológicos, como firewalls, antivirus, sistemas de detección de intrusos, etc.	Considera aspectos técnicos, pero también se ocupa de políticas, procedimientos, gestión de riesgos, concientización del personal, entre otros.

Alcance temporal	Enfocado en tiempo real, se centra en la protección y respuesta inmediata a las amenazas.	Considera aspectos a largo plazo, como la gestión de riesgos, continuidad del negocio y recuperación ante desastres.
Impacto	Un incidente de seguridad informática puede afectar la operación de los sistemas y redes, así como la privacidad y confidencialidad de la información.	Un incidente de seguridad de la información puede tener consecuencias más amplias, incluyendo daños reputacionales, pérdida de clientes, incumplimiento legal, entre otros.
Áreas relacionadas	Criptografía, protección de redes, pruebas de penetración, gestión de incidentes de seguridad, etc.	Gestión de riesgos, políticas de seguridad, concientización y capacitación del personal, continuidad del negocio, cumplimiento normativo, etc.
Enfoque regulatorio	Cumplimiento de normativas y estándares específicos en el ámbito de la seguridad informática.	Cumplimiento de regulaciones y estándares relacionados con la protección de la información, como la GDPR, ISO 27001, HIPAA, entre otros.

***Nota*:** Elaboración Propia.

1.1.4 Objetivos de la Seguridad de la Información

Si tomamos en cuenta que la seguridad de la información puede cambiar en función de las características de cada organización y del sector al que dedique su actividad económica, podemos obtener una serie de objetivos comunes que comparten todas las organizaciones del ámbito de la seguridad de la información y la protección de datos.

Estos objetivos de seguridad de la información se encuentran en la norma ISO 27001. La norma establece un marco para implementar sistemas de gestión de seguridad de la información. El objetivo principal que persigue la norma ISO 27001 es la protección de los recursos de información, es decir, dispositivos, usuarios e información (ISO 27001:2013, 2021).

La seguridad de la información asegura la confidencialidad e integridad de la información, evitando actividades no autorizadas relacionadas con la información, especialmente el uso, divulgación, distorsión, modificación, inspección y destrucción de la información. Las normas de seguridad de la información son las mismas para todas las formas de almacenamiento de información como puede ser física, digital o lo que sea. Con la llegada de los sistemas de información computarizados, la seguridad de los datos se ha vuelto prominente.

1.1.5 Requisitos de la Seguridad de la Información

Los recursos utilizados para implementar medidas de control deben sopesarse frente a la magnitud del daño que podría resultar de problemas de seguridad en ausencia de dichos controles. Los resultados de la evaluación de riesgos ayudarán a guiar y determinar las acciones de gestión y priorización más apropiadas para gestionar los riesgos de seguridad de la información e implementar controles seleccionados para protegerse contra estas amenazas (INEN, 2017).

En la [Figura 6] se detallan los requisitos de la seguridad de la Información.

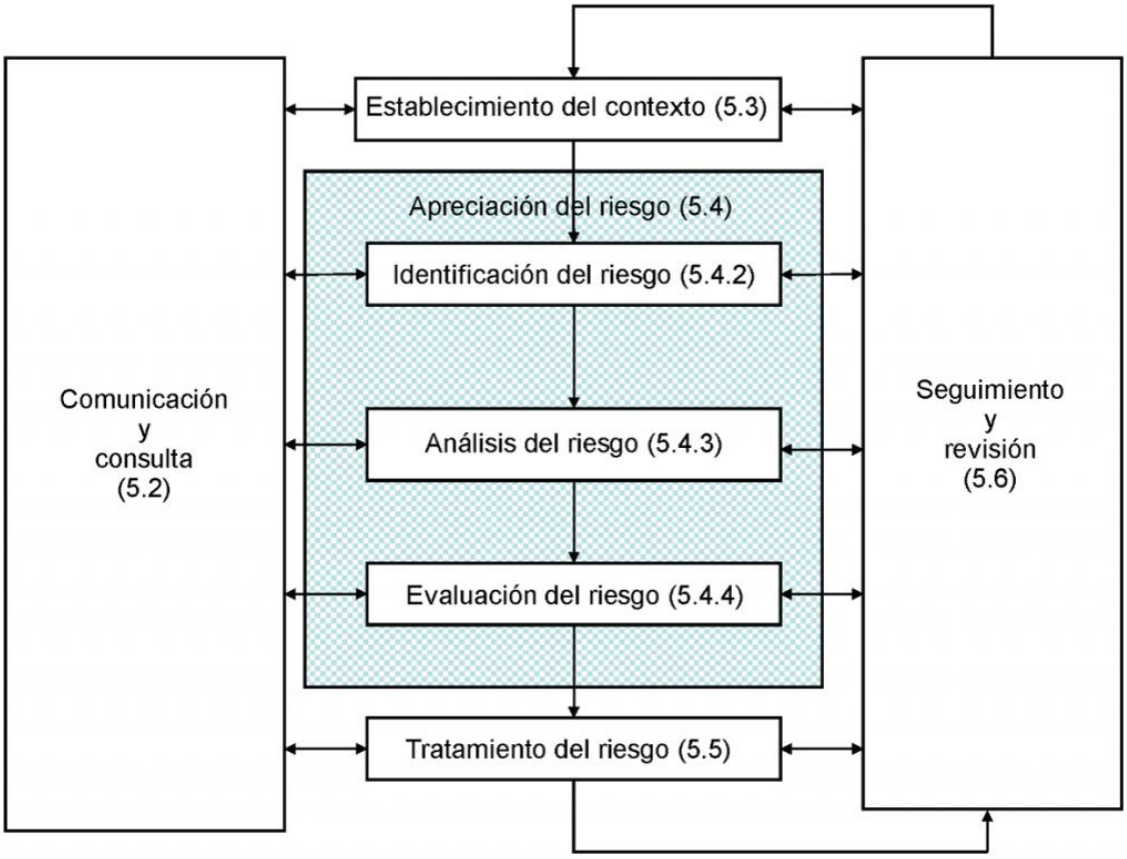


Figura 6: *Requisitos de la Seguridad de la Información*

Fuente: (ISO/IEC 31000, 2018)

1.1.6 Seguridad de la Información en la gestión de proyectos

La seguridad de la información asegura la confidencialidad e integridad de la información, evitando actividades no autorizadas relacionadas con la información, especialmente el uso, divulgación, distorsión, modificación,

inspección y destrucción de la información. Las normas de seguridad de la información son las mismas para todas las formas de almacenamiento de información como puede ser física, digital o lo que sea. Con la llegada de los sistemas de información computarizados, la seguridad de los datos se ha vuelto prominente (Campos, 2018).

Todos los proyectos esencialmente requieren recursos y actividades para desarrollar y establecer objetivos intermedios. La seguridad de la información se puede integrar en las actividades de gestión de proyectos de varias maneras como las siguientes: (Campos, 2018).

- Incluir objetivos de seguridad de la información en los objetivos de su proyecto.
- Llevar a cabo un análisis de riesgos en una etapa temprana del proyecto.
- Hacer frente a las amenazas identificadas e implementar medidas de seguridad.
- Hacer de la Política de Seguridad de la Información un elemento importante en todas las etapas del proyecto.
- Es especialmente importante (independientemente del tamaño de la organización) tener en cuenta la seguridad de la información en las actividades del proyecto, por ejemplo, en términos de integridad, confidencialidad e integridad de la información.

1.1.7 Sistema de Gestión de Seguridad de la Información (SGGI)

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de reglas para gestionar la información. Para entender mejor lo que incluye el SGSI, debemos comenzar con la definición dada en el estándar internacional ISO/IEC 27000 (Alvarado, 2021).

El SGSI consiste en un conjunto de reglas, procedimientos y pautas, junto con recursos y actividades relacionados, que son administrados conjuntamente por una organización que busca proteger sus activos de información críticos.

Además, debemos considerar la visión de ISO/IEC 27001:

Es un enfoque sistemático para establecer, implementar, operar, monitorear, analizar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (Alvarado, 2021).

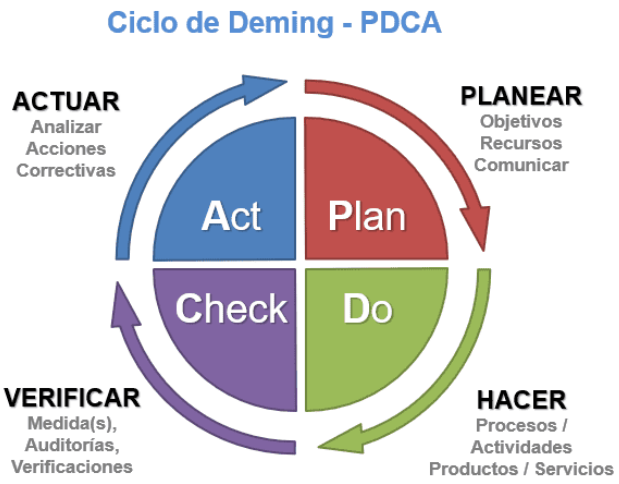


Figura 7: *Ciclo de Deming*

Fuente: (Shewhart, 2020)

El Ciclo de Deming se compone de 4 fases como se muestra en la [Figura 7] y se basa en el supuesto de que una empresa debe seguir mejorando para poder competir en el mercado.

El Ciclo de Deming es conocido también como:

- Ciclo de Shewhart
- Ciclo de la calidad
- Ciclo PDCA (Plan Do Check Act)
- Ciclo PHVA (Planear, Hacer, Verificar, Actuar)
- Espiral de Mejora Continua

1.2. Metodologías para el análisis de riesgo y trabajos relacionados

1.2.1. Metodologías para la gestión de riesgos de la seguridad de la Información

La introducción de sistemas de gestión de riesgos ha cobrado importancia década de los 90, época en la que era necesario remodelar y repensar la forma de hacer las cosas negocio por fraude, en el que se pierden entidades importantes confianza pública; Su impacto global ha motivado una serie de acciones esto conduce a las mejores prácticas para prevenir fraudes de cualquier tipo; se han desarrollado documentos técnicos y en algunos países han considerado la promulgación de reglamentos.

Los enfoques de gestión de riesgos utilizados en todo el mundo coinciden en que su uso planificado como parte de un proceso formal fortalece las actividades y procesos de las organizaciones, independientemente del tamaño o área de su negocio (Cañas, 2012).

El método de análisis y gestión de riesgos sigue un proceso de revisión sistemática el nivel de riesgo que enfrenta la organización, la elección implementar medidas de seguridad para comprender, prevenir, impedir, reducir o controlar los riesgos identificar.

1.2.2. Metodologías para el Análisis de Riesgos

Desde que comenzó la crisis financiera en 2008, el análisis de riesgos ha cobrado especial importancia en la gestión interna de las organizaciones. Anteriormente, el trabajo en esta dirección se hacía de forma caótica y aislada en todas las materias. Sin embargo, a partir de ese día, las empresas comenzaron a fortalecer sus controles internos aplicando la gestión de riesgos en todos los sectores y sectores (Alonso, 2021).

Actualmente, se utilizan varios métodos de análisis de riesgos para garantizar una gestión sistemática como se observa en la Tabla 4. Como parte del análisis de riesgos empresariales de una empresa, es muy importante tener en cuenta los riesgos que podrían amenazar la seguridad de la información. Existen diferentes métodos de evaluación de riesgos para abordar este análisis, en este artículo veremos 3 de los más famosos: Mehari, Ebios y Octave (Alonso, 2021).

Tabla 4

Comparación Metodologías MEHARI, EBIOS, MAGERIT, OCTAVE, CORAS, NIST

Metodología	Descripción	Enfoque	Desarrollada por	Referencia
MEHARI	Es una metodología desarrollada en Francia que se enfoca en el análisis de riesgos en sistemas de información. Proporciona una estructura para evaluar los riesgos y desarrollar estrategias de mitigación.	Basado en la identificación de activos, amenazas y vulnerabilidades, y la asignación de valores numéricos para evaluar el riesgo.	CLUSIF (Club de la Sécurité de l'Information Français)	CLUSIF. (2001). MEHARI: Méthode Harmonisée d'Analyse de Risques.
EBIOS	Es una metodología desarrollada en Francia para el análisis de riesgos en sistemas de	Utiliza una serie de fases y técnicas, como la identificación de activos, el análisis	ANSSI (Agence nationale de la sécurité des systèmes	ANSSI. (2010). EBIOS: Expression des Besoins

	información. Se enfoca en la identificación de activos, amenazas, vulnerabilidades y contramedidas, y proporciona un marco estructurado para el análisis y tratamiento de riesgos.	de impacto, el análisis de amenazas y vulnerabilidades, y la evaluación del riesgo.	d'information)	et Identificatio n des Objectifs de Sécurité.
MAGERIT	Es una metodología desarrollada en España para la gestión de riesgos en sistemas de información. Proporciona un enfoque estructurado para el análisis de riesgos y la selección de medidas de seguridad.	Se basa en la identificación de activos, amenazas, vulnerabilidades, impactos y medidas de seguridad, y utiliza una matriz de riesgos para evaluar el nivel de riesgo.	CCN (Centro Criptológico Nacional)	CCN. (2013). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT).
OCTAVE	Es una metodología desarrollada por el CERT (Computer Emergency Response Team) en Estados Unidos para la gestión de riesgos en sistemas de información. Se centra en la identificación de activos, amenazas y vulnerabilidades, y en el desarrollo de estrategias de mitigación.	Utiliza un enfoque basado en fases, que incluye la identificación de activos, el análisis de impacto, el análisis de riesgo y la selección de contramedidas.	CERT (Computer Emergency Response Team)	CERT. (2003). OCTAVE: Operationall y Critical Threat, Asset, and Vulnerability Evaluation.
CORAS	Es una metodología desarrollada en Noruega para el análisis de riesgos en sistemas de información. Se enfoca en la identificación de	Utiliza un enfoque basado en fases, que incluye la identificación de activos, el análisis de riesgo, el análisis de escenarios y la	SINTEF ICT (The Foundation for Scientific and Industrial Research)	Stølen, K., Lund, M. S., & Solhaug, B. (2004). CORAS: A Comprehens ive Method for the

	activos, amenazas, vulnerabilidades y contramedidas, y proporciona una estructura para el análisis y tratamiento de riesgos.	selección de contramedidas.		Analysis of Risk and Security.
NIST SP 800-30	Es una metodología desarrollada por el NIST (National Institute of Standards and Technology) en Estados Unidos para la gestión de riesgos en sistemas de información. Proporciona un marco general para la identificación, evaluación y respuesta a los riesgos de seguridad.	Se basa en una serie de fases, incluyendo la evaluación de riesgos, la selección de controles de seguridad y la implementación de medidas de mitigación.	NIST (National Institute of Standards and Technology)	NIST. (2018). NIST Special Publication 800-30: Guide for Conducting Risk Assessments.

***Nota*:** Elaboración Propia.

a) **Metodología MEHARI:** MEHARI es una metodología que fue desarrollado por CUSIF (Club de la Securité De L'information Français) en 1998 y publicado en 2007 y deriva de las metodologías previas Melissa y Marion.

   El objetivo de este enfoque es proporcionar un análisis directo e individual de los escenarios de riesgo descritos en diferentes escenarios y proporcionar un conjunto completo de herramientas diseñadas específicamente para la gestión de la seguridad a corto, mediano y largo plazo, adecuadas para diferentes niveles de madurez (Alonso, 2021).

   Este enfoque ha evolucionado para brindar orientación sobre cómo implementar la seguridad dentro de una instalación a lo largo de su ciclo de vida. Asimismo, evalúa el riesgo en base a criterios de disponibilidad, integridad y seguridad (Huerta, 2012).

b) **Metodología EBIOS:** EBIOS Es un método recomendado por la DCSSI (Direction centrale de la sécurité des systèmes d'information) para su uso en las administraciones públicas francesas. El propósito de este enfoque es proporcionar una visión global y consistente de la seguridad de

los sistemas de información, que permita definir los objetivos y requisitos de seguridad de la empresa (Alonso, 2021).

c) **Magerit:** Es una metodología destinada a resaltar la división de los activos de una organización en diferentes grupos para identificar más riesgos y permitir que se tomen contramedidas para evitar cualquier inconveniente.

   La razón de ser de MAGERIT está directamente relacionada con el uso generalizado de las tecnologías de la información, con claros beneficios para las personas; pero también tiene algunos riesgos potenciales que deben mitigarse con medidas de seguridad para garantizar la confianza (Sánchez, 2012).

d) **OCTAVE:** Es un método de análisis de riesgo desarrollado por la Universidad Carnegie Mellon en 2001 y su acrónimo significa Hazard, Asset and Vulnerability Assessment, examina el riesgo basado en tres principios: confidencialidad, integridad y disponibilidad. Este método es utilizado por varias agencias gubernamentales (Huerta, 2012).

   El marco conceptual que forma la base de la metodología OCTAVE fue publicado originalmente por el SEI (Instituto de Ingeniería de Software) en la Universidad Carnegie Mellon en 1999. El objetivo de este enfoque es abordar los desafíos de seguridad que enfrenta el Departamento de Defensa de los Estados Unidos (Alonso, 2021).

   Existen 3 versiones de la metodología OCTAVE:

   - La versión original de OCTAVE
   - La versión para pequeñas empresas OCTAVE-S
   - La versión simplificada de la herramienta OCTAVE-ALLEGRO

e) **Metodología CORAS (Construct a platform for Risk Analysis of Security critical system):** Desarrollado a partir del año 2001 por SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Fue desarrollado como parte del proyecto CORAS financiado por la Unión Europea (IST-2000-25031) [STOL01] [STOL02A] [STOL02B] [STOL06] [STOL07A] [STOL07B] [HOGG07A] (Sánchez, 2012).

   El método CORAS proporciona:

   - El método de análisis de riesgos basado en modelos de siete pasos se basa principalmente en entrevistas con expertos.

- Un lenguaje gráfico que se basa en UML (Unified Modeling Language) para ciertos modelos como lo pueden ser (activos, amenazas, riesgos y controles de seguridad) y guiar su uso a lo largo del proceso. El lenguaje se ha definido como una configuración UML.

- Un editor gráfico compatible con el modelado basado en Microsoft Visio.

- Biblioteca de tapas reutilizables.

- Herramientas de gestión de casos para gestionar y reutilizar casos.

- Representación de texto basada en XML (Extensible Markup Language).

- Un formato de reporte estándar que facilita la interacción de las diferentes partes en el proceso de análisis de riesgos.

f) Metodología NIST SP 800-30 (National Institute of Standards and Technology): NIST (Instituto Nacional de Estándares y Tecnología) ha dedicado una serie especial de publicaciones SP 800 a la seguridad de la información. Esta serie de documentos cubre una metodología de gestión y análisis de riesgos de seguridad de la información que es consistente y complementaria a los demás en esta serie (Sánchez, 2012).

1.2.3. METODOLOGIA MAGERIT

MAGERIT versión 3 es un método de análisis y gestión de riesgos desarrollado en su momento por el ex Consejo Supremo de Gobernanza Electrónica y ahora es mantenido por la Secretaría General de Gobernanza Digital (Ministerio de Seguridad Pública, Economía y Transformación Digital) en alianza con el Centro Criptográfico Nacional (CCN) (Amutio Gómez et al., 2012e).

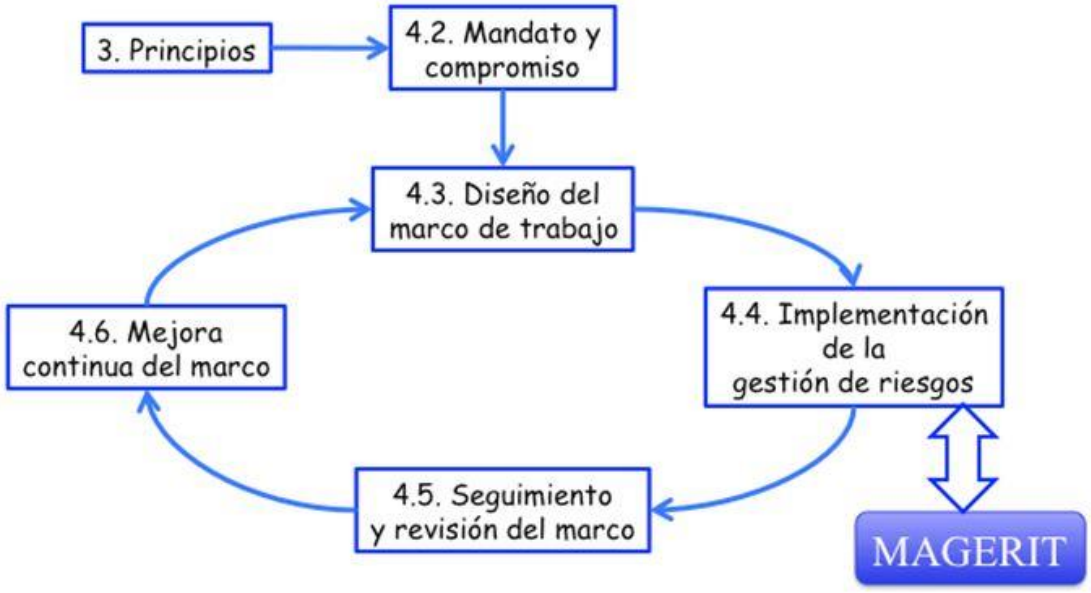


Figura 8: *Marco de trabajo para la gestión de riesgos*

Fuente: (ISO/IEC 31000, 2018)

Las agencias administrativas españolas pueden requerir una licencia sin un puesto en el Centro Nacional del Código; Para hacer esto, envíe su solicitud al Centro Nacional de Criptografía (Amutio Gómez et al., 2012e).

Objetivos

MAGERIT persigue los siguientes objetivos:

1. Aumentar la conciencia de aquellos responsables de las organizaciones que informan la existencia de riesgos y la necesidad de administrarlos
2. Proposición de un método de análisis de riesgos sistemático obtenido por tecnología de la información y comunicación (TIC)
3. Detección de apoyo y plan de tratamiento oportuno para mantener los riesgos bajo control indirecto
4. Prepare una organización para evaluar, auditar, certificar o reconocer, dependiendo de las necesidades en cada caso.

1.3. Norma Internacional para la gestión de riesgos ISO/IEC 31000

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de redacción de Normas Internacionales generalmente lo llevan a cabo los comités técnicos de ISO. Cualquier organización miembro interesada en un tema sobre el

cual se ha establecido un comité técnico tiene derecho a estar representada en ese comité. Las organizaciones internacionales, públicas y privadas, también están involucradas en el trabajo, en consulta con ISO. ISO trabaja en estrecha colaboración con la Comisión Electrotécnica Internacional (IEC) en todos los asuntos de estandarización de ingeniería eléctrica.

1.3.1. Norma ISO/IEC 31000

ISO 31000 es un estándar internacional que proporciona reglas líderes y principios de gestión de riesgos organizacionales. Este estándar fue publicado en 2018 por una organización estándar internacional (ISO) que cooperaba con IEC Development, trasplantando y mejorando la estructura de trabajo, con el objetivo de integrar procesos de gestión de riesgos con cada actividad (ISOTools, 2013).

Tabla 5

Comparación ISO/IEC 31000:2009 Y ISO/IEC 31000:2018

Aspecto	ISO 31000:2009	ISO 31000:2018
Estructura	Está compuesta por principios, marco y proceso.	Está estructurada en principios, marco y proceso, de manera similar a la versión anterior.
Alcance	Se centra en la gestión de riesgos en general.	También se centra en la gestión de riesgos en general, sin un enfoque específico en un sector o industria en particular.
Enfoque	Enfatiza la identificación, análisis y evaluación de riesgos.	Incluye un enfoque más amplio que abarca la integración de la gestión de riesgos en los procesos de toma de decisiones y la mejora continua.
Terminología	Utiliza términos como "amenaza", "vulnerabilidad" y "consecuencia".	Utiliza una terminología actualizada y más amplia, que incluye conceptos como "evento incierto", "efecto" y "contexto".
Proceso de gestión	Se compone de cinco pasos: establecimiento del contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos y tratamiento de riesgos.	Mantiene los mismos pasos del proceso de gestión de riesgos, pero agrega una mayor atención a la comunicación y consulta, así

		como a la monitorización y revisión.
Orientación	Proporciona orientación sobre cómo implementar un sistema de gestión de riesgos efectivo.	Además de brindar orientación para la implementación, enfatiza la importancia del liderazgo y el compromiso de la alta dirección en la gestión de riesgos.
Enfoque basado en COSO	No menciona explícitamente el enfoque basado en COSO (Committee of Sponsoring Organizations of the Treadway Commission).	Incluye referencias explícitas al enfoque de COSO, un marco ampliamente utilizado en la gestión de riesgos corporativos.

***Nota*:** Elaboración propia a partir de la Norma ISO 31000. Tomado de (D. Rodríguez, 2018).

Para complementar esta norma, se ha desarrollado otra norma: ISO 31010 "Gestión de riesgos. método de evaluación de riesgos". Esta Norma Internacional proporciona varios métodos de identificación y evaluación de riesgos, tanto positivos como negativos.

1.3.2. Estructura de la norma ISO 31000

ISO 31000 es un estándar internacional que proporciona reglas líderes y principios de gestión de riesgos organizacionales. Este estándar fue publicado en 2018 por una organización estándar internacional (ISO) que cooperaba con IEC Development, trasplantando y mejorando la estructura de trabajo, con el objetivo de integrar procesos de gestión de riesgos con cada actividad (ISOTools, 2013).

Tabla 6

Estructura de la Norma ISO/IEC 31000:2018

Componente	Descripción
Principios	Establece los principios fundamentales de la gestión de riesgos. Estos principios son: 1. Orientación basada en el contexto. 2. Integración en el proceso de gestión. 3. Enfoque basado en el ciclo de vida. 4. Inclusión de la estructura de la organización. 5. Toma de decisiones basada en la evidencia.

	6. Consideración de factores humanos y culturales. 7. Transparencia e inclusión de múltiples perspectivas. 8. Enfoque dinámico y adaptativo.
Marco	Proporciona una estructura general para la implementación de la gestión de riesgos en una organización. Incluye los siguientes elementos: 1. Comprensión del contexto. 2. Definición del alcance. 3. Establecimiento de los criterios de evaluación del riesgo. 4. Proceso de evaluación del riesgo. 5. Proceso de tratamiento del riesgo. 6. Comunicación y consulta. 7. Monitoreo y revisión.
Proceso de gestión	Describe los pasos necesarios para implementar y mantener un sistema de gestión de riesgos efectivo. Incluye los siguientes pasos: 1. Establecimiento del contexto. 2. Identificación de riesgos. 3. Análisis de riesgos. 4. Evaluación de riesgos. 5. Tratamiento de riesgos. 6. Monitoreo y revisión continuos. 7. Comunicación y consulta.

***Nota*:** Elaboración propia a partir de la Norma ISO 31000

- Para complementar esta norma, se ha desarrollado otra norma: ISO 31010 “Gestión de riesgos. método de evaluación de riesgos”.
- Esta Norma Internacional proporciona varios métodos de identificación y evaluación de riesgos, tanto positivos como negativos.

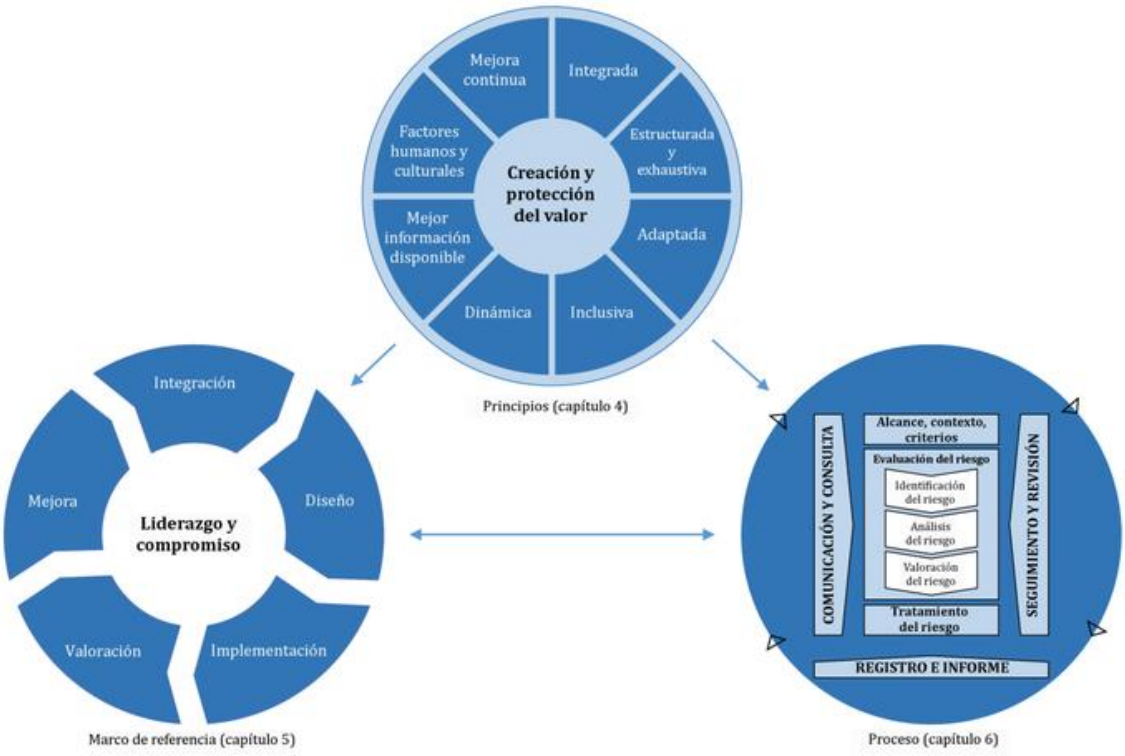


Figura 9: *Principios, marco de referencia y proceso ISO 31000*

Fuente: (ISO 31000, 2018)

1.3.3. Los principios para la gestión de riesgos

Según la norma **ISO31000**, los principios para la gestión de riesgos son los siguientes:

- Crear y proteger el valor. Contribuye a la consecución de objetivos, así como la mejora de ciertos aspectos tales como la seguridad y salud laboral, cumplimiento de los requisitos legales, protección ambiental, etc.
- Estar integrada en los procesos de una organización. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.
- Formar parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
- Tratar explícitamente la incertidumbre. La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.
- Ser sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.

- Facilitar la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

Tabla 7

Definición de Principios de la Norma ISO/IEC 31000:2018

Principio	Descripción
Integrada	La gestión del riesgo es parte integral de todas las actividades de la organización.
Estructurada y exhaustiva	Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
Adaptada	El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
Inclusiva	La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
Dinámica	Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
Mejor información disponible	Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
Factores humanos y culturales	El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
Mejora continua	La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

***Nota*:** Elaboración propia a partir de la Norma ISO 31000.

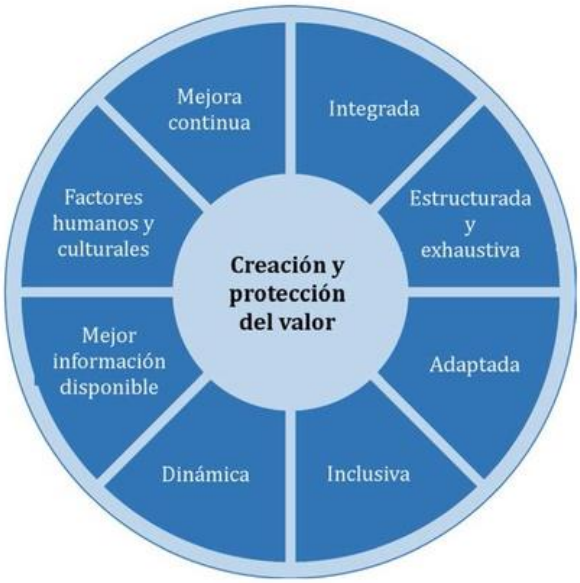


Figura 10: *Principios de la Norma ISO 31000*

Fuente: (ISO 31000, 2018)

1.3.4. Marco de Referencia para la gestión de riesgos

El propósito del marco de gestión del marco es apoyar a la organización que incorpora la gestión de riesgos en todos los aspectos importantes de su operación. La gestión de riesgos funciona bien si está integrada en la gestión de una organización, incluida la toma de decisiones. Esto requiere apoyo para todas las partes interesadas, especialmente en la alta dirección (Ramírez, 2020).

Tabla 8

Definición del Marco de Referencia de la Norma ISO/IEC 31000:2018

Principio	Descripción
Integrar	Integrar la gestión del riesgo en todos los niveles y funciones de la organización, asegurando la participación y el compromiso de todas las partes interesadas clave.
Diseñar	Diseñar un enfoque estructurado y sistemático para la gestión del riesgo, estableciendo políticas, roles y responsabilidades claras, y definiendo los procesos y procedimientos necesarios.

Implementar	Implementar el marco de gestión del riesgo, asegurando que los recursos adecuados estén disponibles, que se sigan los procedimientos establecidos y que se promueva una cultura de gestión del riesgo en toda la organización.
Valorar	Valorar regularmente el desempeño del marco de gestión del riesgo, utilizando indicadores clave de rendimiento y evaluando la eficacia de los controles implementados.
Mejorar	Identificar áreas de mejora y tomar medidas para mejorar continuamente el marco de gestión del riesgo, ajustando los enfoques, implementando lecciones aprendidas y adoptando mejores prácticas.

***Nota*:** Elaboración propia a partir de la Norma ISO 31000, Tomado de (Ramírez, 2020)

El desarrollo del marco de referencia de una gestión de riesgos implica integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización. En la [Figura 11] se puede observar los componentes del marco de referencia.

Figura 11: *Principios de la Norma ISO 31000*

Fuente: (ISO 31000, 2018)

1.3.5. ¿Dónde interviene la gestión de seguridad de la información en una entidad?

La seguridad de la información es parte de la gestión del riesgo en una entidad, los recursos utilizados para implementar medidas de control deben sopesarse frente a la magnitud del daño que podría resultar de problemas de seguridad en ausencia de dichos controles. Los resultados de la evaluación de riesgos ayudarán a guiar y determinar las acciones de gestión y priorización más apropiadas para gestionar los riesgos de seguridad de la información e implementar controles seleccionados para protegerse contra estas amenazas.

En la [Figura 12] se puede apreciar como la gestión de riesgos se enfoca en varios aspectos teniendo en cuenta el riesgo que puede afectar el rendimiento en una empresa

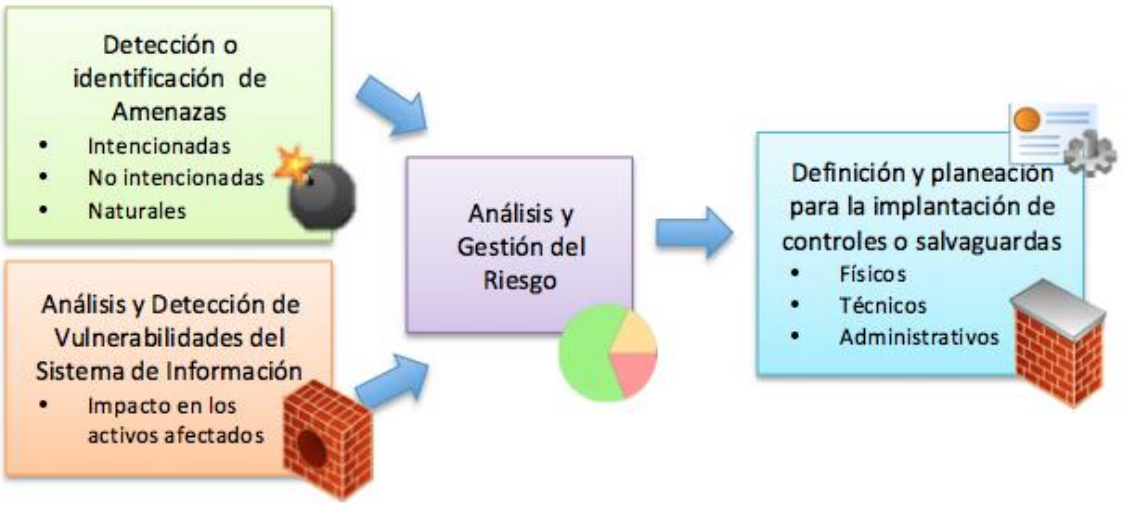


Figura 12: *Análisis y gestión de riesgos en una organización*

Fuente: (Prudente et al., 2015)

1.4. Software para Gestión de Riesgos

La gestión de riesgos tiene una serie de herramientas de software para la gestión de proyectos. Estos parámetros ayudan a simplificar e identificar los riesgos que amenazan la finalización exitosa del proyecto. El riesgo es una parte integral de la gestión de proyectos.

Este campo tiene en cuenta que los proyectos son eventos únicos que se ejecutan una sola vez, con objetivos específicos y representan un grado de incertidumbre en la gestión de riesgos. Esta incertidumbre es una fuente de riesgo.

1.4.1. ¿Qué es un Software de gestión de Riesgos?

El software de gestión de riesgos es una herramienta que ayuda a identificar, gestionar y reducir los riesgos en una organización, de acuerdo con la metodología,

los procesos organizativos y las reglas que las empresas deben seguir en este sistema.

Su principal ventaja frente a los métodos que utilizan hojas de cálculo de Excel para esta tarea es reducir el error humano y evitar la tediosa tarea de generar decenas de fórmulas para calcular el impacto. Estas características aseguran la optimización de todos los pasos del proceso (Pensemos SA, 2021)

1.4.2. ¿Cuáles son las características del Software de Gestión de Riesgos?

El software de gestión de riesgos, pensemos tiene muchas características que serán la base de su sistema de gestión de riesgos: cubre todos los aspectos del proceso de gestión de riesgos, desde la identificación inicial del riesgo hasta la gestión y seguimiento, análisis y evaluación. Además, es una herramienta útil para la gestión de incidencias o realizaciones, ya que asegura la ejecución de acciones y analiza los motivos de un mayor control.

Algunas de las características que debería de tener un Software para realizar una Gestión de Riesgos deberían ser las siguientes:

Identificación y evaluación de riesgos: Permite la identificación y evaluación de riesgos potenciales mediante análisis cualitativos y cuantitativos.

Registro y seguimiento de riesgos: Permite el registro y el seguimiento de los riesgos identificados, incluyendo información detallada sobre la descripción del riesgo, sus causas, sus consecuencias y las medidas para reducirlos.

Análisis de escenarios y simulaciones: Permite realizar análisis de escenarios y simulaciones para evaluar el impacto de los riesgos en diferentes situaciones y ayudar a tomar decisiones informadas.

Priorización y asignación de recursos: Ayuda a priorizar los riesgos en función de su impacto y probabilidad, lo que permite asignar recursos de manera más efectiva para abordar los riesgos más importantes.

Planificación y seguimiento de acciones de mitigación: permite la planificación y el seguimiento de acciones de mitigación para reducir los riesgos, asignar responsabilidades y establecer fechas límite.

Generación de informes y paneles de control: permite la creación de informes y paneles de control personalizados que ofrecen una visión general de los riesgos, el progreso de las acciones de mitigación y el estado general de la gestión de riesgos.

Integración con otros sistemas: Permite la integración con otros sistemas de la organización, como sistemas de gestión de calidad, sistemas de gestión ambiental o

sistemas de gestión de proyectos, para obtener una visión integral de los riesgos y sus relaciones.

Cumplimiento normativo y regulaciones: proporciona funcionalidades específicas para el cumplimiento y produce informes requeridos por los organismos reguladores para garantizar que se cumplan los requisitos normativos y regulaciones aplicables.

Integración con otros sistemas: Permite la integración con otros sistemas de la organización, como sistemas de gestión de calidad, sistemas de gestión ambiental o sistemas de gestión de proyectos, para obtener una visión integral de los riesgos y sus relaciones.

Colaboración y comunicación: facilita la colaboración y la comunicación entre los miembros del equipo de gestión de riesgos, permitiendo el intercambio de información, comentarios y actualizaciones en tiempo real.

Seguridad y privacidad de la información: Aplica medidas de protección de datos y controla el acceso a la información confidencial.

1.4.3. Herramientas de Software más utilizadas para la Gestión de Riesgos

- **@Risk**, de Palisade. Este software realiza análisis de riesgo a través de la simulación para mostrar muchos resultados posibles en el modelo de hoja de cálculo. Esto muestra la posibilidad de estos riesgos. @Risk presenta simulación de Monte Carlo, integración 100 % de Excel y cálculos para simulación, parámetros de distribución porcentual, correlación de entrada y series de tiempo (Riveros, 2018).

- **SE Risk**, SoftExpert. Esta herramienta le permite administrar el riesgo y apoyar la mejora continua. Brinda asistencia en la identificación de riesgos, la reducción de desperdicios y la maximización de las oportunidades de la organización. Los riesgos se pueden clasificar y evaluar con herramientas intuitivas fáciles de usar para mejorar la eficacia y la eficiencia de la prevención y el control de riesgos (Riveros, 2018).

  Con SE Risk, puede obtener una visión general entre las áreas de gestión de riesgos y control interno, identificar los riesgos potenciales que podrían afectar el logro de las metas de su organización y evaluar cualitativa, cuantitativa y mediante una matriz.

- **RiskProject Professional**, del Instituto Intaver. Este software se basa en análisis de riesgo de costo y tiempo. Le permite determinar el impacto del riesgo y la

incertidumbre. Con este programa puedes planificar y analizar riesgos cuantitativos (Riveros, 2018).

- **SOFRISK** es un software integral de cumplimiento y gestión de riesgos. Esta herramienta tecnológica implementa cuatro etapas del proceso de gestión: definir, medir, controlar y monitorear. Además, mantiene la trazabilidad de cada uno de ellos.

- **ISOTools** El software ISOTools es la mejor herramienta del mercado para la automatización de alto perfil. ISOTools es una herramienta sencilla para adaptarse a cualquier modelo de gestión por procesos. El uso de este software facilita la automatización y operación del modelo de control basado en procesos (ISOTools, 2013).

- **EAR/PILAR** Las herramientas PILAR soportan el análisis y la gestión de riesgos de los sistemas TI según el método Magerit.

  Los activos enfrentan amenazas que, cuando se materializan, degradan el activo al ejercer influencia. Al evaluar con qué frecuencia se materializan las amenazas, podemos determinar los riesgos que enfrenta el sistema. La degradación y la frecuencia determinan la vulnerabilidad del sistema.

  Los administradores de sistemas de TI cuentan con salvaguardas para reducir la frecuencia de ocurrencia o reducir o limitar el impacto. Dependiendo de qué tan bien se implementen estas protecciones, el sistema cambia a una nueva evaluación de riesgos, conocida como riesgo residual.

Tabla 9

Herramientas para realizar una Gestión de Riesgos

Herramienta	Descripción
Risk	Risk es una herramienta de gestión de riesgos ampliamente utilizada que permite identificar, evaluar y gestionar los riesgos en una organización. Proporciona funcionalidades para el análisis de riesgos, evaluación de impacto y seguimiento de acciones de mitigación.
SE Risk	SE Risk es una herramienta de gestión de riesgos específica para la industria de la ingeniería de sistemas. Ayuda a identificar y evaluar riesgos técnicos y de proyectos, y proporciona funcionalidades para el análisis de impacto y la planificación de mitigaciones.

RiskProject Professional	RiskProject Professional es una herramienta de gestión de riesgos orientada a proyectos. Permite identificar, evaluar y gestionar los riesgos específicos de un proyecto, y ofrece funcionalidades para la asignación de recursos y seguimiento de acciones de mitigación.
SOFRISK	SOFRISK es una herramienta de gestión de riesgos financieros utilizada en el sector bancario y financiero. Ayuda a identificar, medir y gestionar los riesgos financieros, incluyendo el riesgo de mercado, riesgo de crédito y riesgo operativo.
ISOTools	ISOTools es una plataforma de gestión basada en la nube que incluye módulos específicos para la gestión de riesgos. Proporciona funcionalidades para la identificación de riesgos, evaluación de impacto, seguimiento de acciones y generación de informes.
EAR/PILAR	EAR/PILAR (Enterprise-wide Assessment of Risk / Pilot Internal Loss Data Analysis) es una herramienta de gestión de riesgos utilizada en el sector de seguros. Ayuda a evaluar y gestionar los riesgos de pérdida interna en una organización aseguradora, utilizando datos históricos y análisis estadístico.

***Nota*:** Elaboración propia a partir del sitio web oficial de cada herramienta.

Todas estas herramientas son muy útiles al momento de realizar una gestión de riesgos y la mayoría de estas herramientas se basan en la estructura de la Norma ISO/IEC 31000 como se puede apreciar en la [Figura 13].

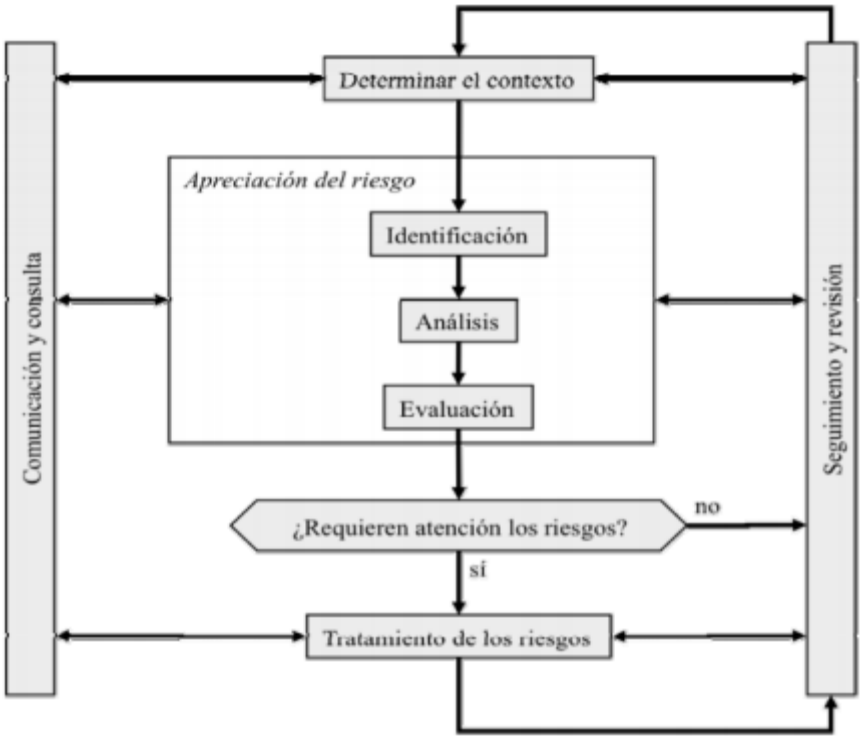


Figura 13: *Estructura de forma metódica con la Norma ISO/IEC 31000*

Fuente: (Artos, 2020)

1.4.4. Clasificación de las amenazas informáticas

De forma general se puede clasificar las amenazas informáticas en dos grupos principales:

- Amenazas Físicas
- Amenazas Lógicas

Estas amenazas que pueden ser, tanto físicas como lógicas son realizadas básicamente por:

- Personas
- Programas o aplicaciones maliciosas
- Catástrofes Naturales

1.4.5. Tipos de Amenazas Informáticas

El hecho de que las empresas dependan de la tecnología de la información para ejecutar sus negocios principales ha generado serias preocupaciones sobre la

ciberseguridad, como lo describe. (AMBIT TEAM, 2020)(AMBIT TEAM, 2020)(AMBIT TEAM, 2020)

- Algunas de estas amenazas son:
- Virus Informáticos
- Uso no autorizado de los sistemas informáticos
- Robo de Información
- Suplantación de Identidad
- Divulgación de la Información
- Desastres Naturales

Tabla 10

Definición de los Tipos de Amenazas Informáticas

Tipo de Amenaza	Descripción
Malware	Software malicioso diseñado para dañar, acceder o controlar sistemas informáticos sin autorización, como virus, gusanos, troyanos y ransomware.
Phishing	Intento de obtener información confidencial, como contraseñas o datos financieros, haciéndose pasar por una entidad confiable a través de comunicaciones electrónicas.
Ingeniería Social	Manipulación psicológica y engaño para obtener información confidencial o acceso no autorizado a sistemas y redes.
Ataques de Denegación de Servicio (DDoS)	Sobrecarga intencional de un sistema o red para interrumpir o bloquear su funcionamiento normal, negando el servicio a usuarios legítimos.
Ransomware	Tipo de malware que cifra los archivos de una víctima y exige un rescate (generalmente en criptomonedas) para desbloquearlos.
Ingeniería Inversa	Proceso de desmontar y analizar un producto o software para descubrir cómo fue diseñado, identificar vulnerabilidades o copiarlo sin autorización.
Ataque de Fuerza Bruta	Intento de descifrar contraseñas o claves mediante la prueba sistemática de todas las combinaciones posibles hasta encontrar la correcta.
Spyware	Software que recopila información sobre una persona o sistema sin su conocimiento o consentimiento, generalmente con fines de espionaje o publicitarios.

Man-in-the-Middle (MitM)	Ataque en el que un atacante se sitúa entre dos partes que se comunican y puede interceptar, modificar o suplantar los datos transmitidos.
Botnets	Red de dispositivos infectados controlados remotamente por un atacante para llevar a cabo actividades maliciosas, como enviar spam o lanzar ataques.

***Nota*:** Elaboración propia a partir de Artículos. Tomado de (Consuegra de Sucre, 2023)

Como se puede observar en la Tabla 10 se presentaron los diferentes tipos de amenazas informáticas y a continuación, veremos las principales amenazas y vulnerabilidades a las que se exponen las empresas hoy en día:

Amenazas de Malware:

El malware es una de las mayores ciber amenazas a las que se enfrentan las empresas. En el malware existen diferentes tipos de amenazas, siendo las más importantes (AMBIT TEAM, 2020).

- **Spyware:** Código malicioso cuyo objetivo principal es recopilar información sobre la actividad informática de un usuario (tendencias de navegación), mostrar ventanas emergentes de marketing no autorizadas o robar información personal (como el número de tarjeta de crédito).
- **Virus:** Los virus informáticos son programas que se instalan en el dispositivo para causar problemas en el funcionamiento del mismo. Se requiere la intervención del usuario (intencional o no) para que el virus infecte el sistema.
- **Gusanos:** Es uno de los malware más comunes que infecta computadoras y sistemas corporativos porque el usuario no necesita intervenir ni modificar archivos para infectar la computadora. El propósito del gusano es clonar e infectar tantos dispositivos como sea posible a través de la red. Representan una amenaza para las redes comerciales porque una computadora infectada puede afectar a toda la red en poco tiempo.
- **Troyanos:** Los troyanos son programas que se instalan en un ordenador y pasan desapercibidos para el usuario. Su finalidad es ir abriendo poco a poco la puerta a la instalación de otro tipo de malware.
- **Ransomware:** El ransomware se ha convertido en el malware más peligroso para las empresas en la actualidad. Implica cifrar toda la información de la empresa, impedir el acceso a datos y sistemas, y exigir un rescate si la información puede ser revelada (normalmente en criptomonedas como bitcoin).
- **Keyloggers:** Se instalan a través de troyanos y se encargan de sustraer datos de acceso a plataformas online, webs bancarias, etc.

- **Spam:** Recibir mensajes no solicitados, principalmente a través de correo electrónico, si el propósito es transmitir un gran mensaje comercial o promocional. Ha habido casos de transmisiones a sistemas de telefonía móvil, sistemas de SMS o fax.
- **Botnets** (Redes de robots): Son máquinas infectadas y controladas remotamente que se comportan como "zombis" y están incrustadas en redes informáticas distribuidas, llamadas botnets, que envían correos electrónicos masivos de "spam" o código malicioso con el objetivo de atacar los sistemas de otra persona; se ha descubierto una red de más de 200.000 nodos conectados y más de 10.000 modelos de "robot" diferentes.
- **Trashing:** Un método cuyo nombre hace referencia a la gestión de basura. Este no es un método que esté directamente relacionado con el sistema de TI, porque los atacantes usan una forma diferente de ingeniería social y también usan un mecanismo para encontrar basura u otros lugares para tirar papeles, documentos, extractos bancarios, facturas. facturas, borradores de documentos, etc., para luego utilizarlos adecuadamente, creando perfiles de víctimas para robar sus identidades o acceder directamente a información que debe mantenerse en secreto.
- **Adware:** El principal propósito es mostrar anuncios de manera invasiva. Aunque su intención es dañar computadores, algunas personas sin embargo clasifican como un spyware, ya que tiene la habilidad de recoger y transmitir datos en orden y de analizar a los usuarios su comportamiento y la dirección de anuncios.
- **Denegación de servicio distribuido (DDoS):** Los ataques DDoS ocurren cuando se envían demasiadas solicitudes al servidor, lo que provoca que el servidor se bloquee. Existen diferentes métodos, entre los cuales el más común es el uso de botnets, equipos infectados con troyanos y gusanos, donde el usuario desconoce que está participando en un ataque.

  De todos los tipos de ataques informáticos, este es uno de los más famosos y peligrosos porque es muy barato de realizar y muy difícil encontrar al atacante.

  Por lo tanto, la efectividad de los ataques DDoS se debe a que no tienen que eludir la capa de seguridad que protege el servidor, ya que no intentan penetrar sino bloquearlo, causando un daño económico severo al negocio objetivo.

1.4.6. Ataques Informáticos

La principal desventaja que permite a los usuarios ser hackeados y ser víctimas de una gran cantidad de amenazas que se nos plantean es que en muchos casos la tecnología no se maneja con la adecuada protección de la información y sin la conciencia de los riesgos asociados al uso de las tecnologías y herramientas como Internet, donde los esfuerzos se desperdician o se desvían. La inversión en tecnologías de seguridad como solución a los problemas planteados debe hacerse en un marco integrado con una serie de otras actividades creando el denominado "Sistema de Gestión de Seguridad de la Información" (Tarazona, 2007).

En la siguiente figura se puede apreciar que según, (Petrosyan, 2022). En 2022, alrededor del 70 por ciento de las empresas fueron víctimas de ransomware. Este fue un aumento con respecto a los cinco años anteriores y la cifra más alta reportada hasta ahora. En general, más de la mitad del total de los encuestados cada año afirmaron que su empleador había sido víctima de ransomware como se muestra en la [Figura 14].

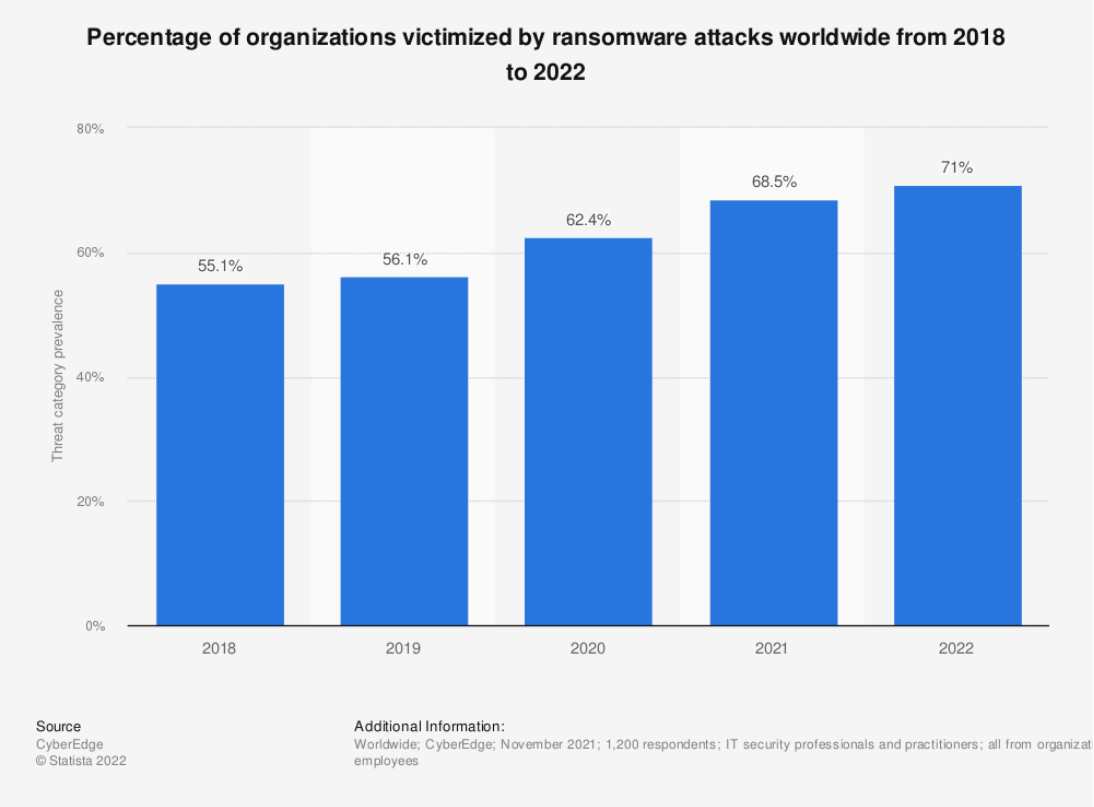


Figura 14: *Tasa de victimización entre empresas de todo el mundo 2018 – 2022*

Fuente: (Petrosyan, 2022)

1.4.7. ¿Qué es un ataque informático o ciberataque?

Los ataques informáticos son un intento organizado y deliberado de explotar una vulnerabilidad o debilidad en un sistema o red informática, tanto en

software como en hardware, con fines económicos o simplemente anarquistas (Andruz, 2021).

Un ataque informático, también conocido como ciberataque, se refiere a cualquier intento malicioso de violar la seguridad de sistemas informáticos, redes, dispositivos o datos con el objetivo de acceder, alterar, robar, destruir o interrumpir el funcionamiento normal de los mismos. Los ciberataques son llevados a cabo por personas o grupos con intenciones maliciosas, como hackers, ciberdelincuentes, grupos organizados o incluso entidades estatales.

Existe un acuerdo generalizado de que los ataques cibernéticos son una amenaza de alto nivel que puede provocar cualquier cosa, desde pequeñas pérdidas hasta una catástrofe global.

1.4.8. ¿Cuáles son las consecuencias de sufrir un ciberataque?

Según (Andruz, 2021), Un ataque informático puede desencadenar diversas consecuencias que perjudican directamente a la organización como:

1. **Pérdida de Reputación:** Sin duda, esto es el más grave resultado para cualquier organización porque un ciberataque puede conllevar a la pérdida de datos o información de los clientes y la confianza se vea afectada. Nadie confía en una empresa con vulnerabilidades, ya que no se quiere que nuestros datos e información puedan caer en manos equivocadas o mal intencionadas.

2. **Pérdida de la continuidad del negocio:** La interrupción o el retraso en los procesos y las operaciones causados por cualquier ataque informático es una pérdida financiera y de reputación para cualquier empresa. Por esta razón, es fundamental contar con planes de recuperación ante desastres para garantizar la continuidad del negocio.

3. **Pérdidas económicas:** Retrasar un ataque siempre tendrá una connotación negativa, sobre todo cuando se trata de dinero, ya que tras un incidente supone una gran inversión de recursos para repeler el ataque y reforzar las medidas de seguridad para evitar que se repita. Sin embargo, durante un incidente, la información puede ser interceptada (ransomware) cuando se necesita un rescate, aumentando los costos de la organización.

4. **Disminución de clientes y proveedores:** Los clientes y proveedores cuando se pierde la reputación y dinero por sufrir un ataque informático. Varios de estos ataques han sucedido a lo largo de los años, pero poco a poco se han ido

actualizando y desarrollando nuevos ataques a lo largo del tiempo con las nuevas tecnologías y también han evolucionado en hardware y aplicaciones.

1.4.9. Tipos de Vulnerabilidades Informáticas

Los sistemas y aplicaciones informáticas siempre tienen fallas en su diseño, estructura o código que crean vulnerabilidades. Por pequeño que sea el error, siempre puede poner en riesgo los sistemas y la información al ser la puerta de entrada para recibir ataques desde el exterior o desde el interior. Las principales vulnerabilidades suelen encontrarse en: (AMBIT TEAM, 2020).

- Configuración.
- Gestión de recursos.
- Sistemas de validación.
- Permiten el acceso a directorios.
- Gestión y asignación de permisos.

Vulnerabilidades producidas por contraseñas

Gracias al trabajo remoto y la computación en la nube, la gestión de contraseñas se ha convertido en uno de los aspectos más importantes de la ciberseguridad. Es necesario utilizar un usuario y contraseña para acceder a la plataforma de trabajo de la empresa. El uso de contraseñas débiles crea vulnerabilidades en el sistema porque si son fáciles de descifrar, pueden provocar la intrusión de terceros no autorizados que pueden robar, cambiar o eliminar información, reemplazar, cambiar configuraciones si tienen permiso e incluso desactivar la computadora.

Vulnerabilidades producidas por usuarios

Una de las principales causas de los ataques informáticos es el mal uso o descuido del usuario. La concesión incorrecta de permisos o permisos puede dar al usuario acceso a opciones de configuración o administrativas para las que no se preparó, lo que puede generar errores que amenazan a la empresa.

El error humano es otra causa de las amenazas a la ciberseguridad. Los usuarios siempre corren el riesgo de cometer errores que pueden crear agujeros de seguridad que amenazan las computadoras. Como resultado, la ciberseguridad tiende a automatizar procesos críticos para reducir o eliminar el factor de riesgo del error humano (AMBIT TEAM, 2020)(AMBIT TEAM, 2020)(AMBIT TEAM, 2020).

Vulnerabilidades producidas por usuarios

Una de las principales causas de los ataques informáticos es el mal uso o descuido del usuario. La concesión incorrecta de privilegios o permisos puede otorgar a los

usuarios acceso a opciones administrativas o de configuración para las que no estaban preparados, lo que podría generar errores que amenazan a la empresa.

Tabla 11

Definición de los Tipos de Vulnerabilidades Informáticas

Tipo de Vulnerabilidad	Descripción
Vulnerabilidades de software	Son debilidades o fallos en el código de un software o aplicación que podrían ser explotados por un atacante para comprometer la seguridad del sistema.
Vulnerabilidades de red	Estas vulnerabilidades se refieren a debilidades en la configuración o implementación de redes, como puertos abiertos no necesarios o filtrado inadecuado de tráfico.
Vulnerabilidades del sistema operativo	Son debilidades en el sistema operativo subyacente que podrían permitir a un atacante obtener acceso no autorizado o controlar el sistema.
Vulnerabilidades de configuración	Estas vulnerabilidades ocurren cuando se configuran incorrectamente sistemas o aplicaciones, lo que puede facilitar el acceso no autorizado o la exposición de datos sensibles.
Vulnerabilidades de contraseña	Se refieren a debilidades en las prácticas de gestión de contraseñas, como contraseñas débiles, reutilización de contraseñas o almacenamiento inseguro de contraseñas.
Vulnerabilidades de inyección	Estas vulnerabilidades ocurren cuando datos no confiables se insertan en una aplicación o sistema sin la debida validación o filtrado, lo que permite la ejecución de comandos maliciosos.
Vulnerabilidades de desbordamiento de búfer	Se producen cuando se inserta más información en un búfer de memoria de lo que puede manejar, lo que puede permitir a un atacante sobrescribir datos o ejecutar código malicioso.
Vulnerabilidades de Cross-Site Scripting (XSS)	Son debilidades que permiten a un atacante inyectar código malicioso en sitios web visitados por otros usuarios, lo que puede conducir al robo de información o la ejecución de acciones no deseadas.

Vulnerabilidades de Cross-Site Request Forgery (CSRF)	Estas vulnerabilidades permiten a un atacante realizar acciones no autorizadas en nombre de un usuario legítimo, aprovechando la confianza del sitio web en la identidad del usuario.
Vulnerabilidades de seguridad física	Se refieren a debilidades en los controles físicos de seguridad, como acceso no autorizado a instalaciones o equipos, lo que podría permitir a un atacante comprometer la infraestructura física.

***Nota*:** Elaboración propia a partir de Artículos. Tomado de (González Brito et al., 2017)

Como se pudo observar en la Tabla 11. Existen diferentes tipos de vulnerabilidades informáticas por esta razón podemos deducir que, las vulnerabilidades informáticas son fallas o debilidades en un sistema que los atacantes pueden explotar para comprometer la seguridad del sistema, acceder a información confidencial o realizar acciones maliciosas. Las diferentes partes de un sistema informático, como el software, el hardware, las redes, los sistemas operativos y las configuraciones, pueden contener estas vulnerabilidades.

CAPITULO II

Diseño del Plan de Gestión de Riesgos

2.1. Metodología de la 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 la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte.

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 la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte, 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 la Biblioteca de la UTN. Los documentos revisados serán el fichaje de inventario de los distintos bienes fijos, manual de procedimientos, 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 al Encargado del departamento de Informática de la Biblioteca de las Universidad Técnica del Norte, con finalidad recabar información sobre la conciencia que tienen los mismos en relación con los riesgos presentados durante el uso de la Biblioteca. Las preguntas de la encuesta se encuentran en el Anexo A.

  - La otra encuesta será de tipo "Encuesta 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 la encuesta se encuentran en el Anexo O respectivamente.

- **Entrevista:** Se desarrolló dos entrevistas a las personas relacionadas con la administración del área de tecnología de la Biblioteca de la Universidad Técnica del Norte, la primera entrevista realizada al Encargado del Área de Informática y Digitalización de la Biblioteca de la UTN, que se desarrolló con un enfoque dirigido al proceso administrativo, operacional, y de gestión dentro de la Biblioteca, la segunda entrevista fue realizada al encargado del área de informática y Digitalización de la Biblioteca de la 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 la Biblioteca de la 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 la Biblioteca.

2.3. Nivel de Madurez de Gestión de Riesgos

Para definir el nivel de Madurez en la Gestión de Riesgos de la Infraestructura Tecnológica de la Biblioteca de la 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 12 muestra como la Comunidad de Gestión de Riesgos (2020) define los cinco niveles.

Tabla 12

Definición de los niveles de madurez de Gestión de Riesgos

Nivel de madurez de Gestión de Riesgos	Definición
Muy Básico	Conciencia mínima o nula / No existen procesos implementados / Insatisfactorio.
Básico	Aplicado de manera inconstante / Algunos procesos formales establecidos / Satisfactorio.

Emergente	Implementado consistentemente en toda la organización / No todos los procesos implementados completamente / Bueno.
Maduro	Implementado de manera consistente y completa. / Se revisan los procesos para mejorarlos / Muy Bueno.
Avanzado	La gestión de riesgos se considera un generador de valor / Se utilizan procesos avanzados / Excelente

Nota: Elaboración propia.

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

- Efectividad: Capacidad de un proceso de gestión de riesgos para lograr los objetivos establecidos de manera eficaz.
- Proactividad: Capacidad de una organización para anticipar, identificar y abordar proactivamente los riesgos antes de que se conviertan en problemas significativos.
- Cobertura: Extensión o alcance de las medidas de mitigación implementadas para abordar los riesgos identificados

Estas dimensiones que se presentan 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. Estos 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, el encargado del área de

Informática y Digitalización de la Biblioteca de la UTN, y la Directora de la Dirección de Biblioteca de la Universidad Técnica del Norte 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 al encargado del área de Informática y Digitalización de la Biblioteca de la UTN se encuentran en el Anexo B, mientras que las preguntas referentes a la encuesta realizada a la directora de Biblioteca se encuentran en el Anexo C.

Los resultados obtenidos se encuentran a continuación en la Tabla 13.

Tabla 13

Resultados Risk Maturity Model aplicado a la Infraestructura Tecnológica de la Biblioteca de la 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	1	0	1
	Visión previsora de gestión de riesgos	0	1	1
	Soporte ejecutivo de ERM	3	1	1
Descubrir el riesgo	Propiedad del riesgo por área de negocio	3	2	1
	Indicadores y Medidas de Riesgo Formalizados	0	0	0
	Informes de seguimiento	1	1	1
	Eventos adversos como oportunidades	0	1	0
	Supervisión del programa ERM	2	1	2

Gestión de procesos ERM	Pasos del proceso ERM	0	1	1
	Cultura de Riesgo, Rendición de Cuentas y Comunicación	0	0	0
	Informes de gestión de riesgos	1	1	2
	Repetibilidad y Escalabilidad	1	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	2	2
	Recopilación de información sobre riesgos y oportunidades	2	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	1	0	1
Gestión del rendimiento	Comunicación de metas	6	5	3
	Información y planificación de ERM	0	0	0
	Objetivos y actividades del proceso de ERM	1	0	1
	TOTAL	32	31	29

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 14 de niveles de gestión de riesgos, determinar en cuál se encuentran la Infraestructura Tecnológica de la UTN.

Tabla 14

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 la Infraestructura de la Biblioteca de la UTN es de 92 puntos, por lo que según la Tabla 14, 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 Tecnológicos

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": Implica el desarrollo de diversas actividades relacionadas con los aspectos de "Comunicación y Consulta" y "Establecimiento de Contexto" según la Norma ISO 31000:2018, con el objetivo de lograr una gestión efectiva del riesgo.

Estas actividades incluyen la determinación de principios que guíen el comportamiento del Plan de Gestión de Riesgos, la identificación de las actividades facilitadas por el equipo encargado del Área de Informática y Digitalización de la Biblioteca para una gestión eficaz del riesgo, y la presentación de la situación actual de la Biblioteca.

Esta última abarca elementos como la estructura organizativa, el personal a cargo, la infraestructura física y tecnológica, los servicios, la seguridad y el control de acceso, incidentes pasados, así como el contexto interno y externo.

La ejecución de esta fase se llevó a cabo mediante la aplicación de la técnica de observación de campo, visitas técnicas a la Biblioteca de la UTN, y entrevistas con el Encargado del área de Informática y Digitalización y la Directora de la Biblioteca.

Fase 2 "Evaluación y Tratamiento del Riesgo": En esta etapa se llevan a cabo todas las actividades correspondientes con la guía de la metodología MAGERIT. Estas actividades comprenden:

I. **Identificación de activos:** Se realiza la recopilación, análisis y síntesis de los bienes y servicios que generan valor en la Biblioteca.
II. **Identificación de dependencia entre activos:** Se determinan las relaciones existentes entre los activos y la posible propagación de daño.
III. **Valoración de activos:** Se asigna un valor cuantitativo a cada activo en distintas dimensiones de valoración (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) relacionadas con la seguridad.
IV. **Identificación de amenazas:** Se recopila y analiza información sobre las amenazas que pueden afectar a cada uno de los activos identificados en la Biblioteca.
V. **Valoración de amenazas:** Se asignan valores cuantitativos a cada una de las posibles amenazas que podrían afectar a los activos en cada dimensión de valoración.
VI. **Determinación del impacto potencial:** Se calcula el daño que podría ocurrir en caso de materialización de una amenaza sobre un activo.
VII. **Determinación del riesgo potencial:** Se calcula la relación entre la probabilidad de ocurrencia de una amenaza y el impacto negativo que esta tendría sobre un activo.
VIII. **Identificación de salvaguardas:** Se determina el tipo de medidas para reducir los riesgos calculados y se proponen tareas que pueden ser implementadas.
IX. **Valoración de salvaguardas:** Se asigna un valor cuantitativo a cada una de las tareas propuestas y tipos de salvaguardas que pueden aplicarse para minimizar el riesgo.

X. **Estimación del impacto residual:** Se simula el cálculo del impacto residual asumiendo que las tareas de salvaguardas fueron aplicadas.

XI. **Estimación del riesgo residual:** Se simula el cálculo de la 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, "Supervisión y Evaluación del riesgo": Sugiere actividades que incluyen:

I. **Supervisión:** Se propone un conjunto de actividades para seguir de cerca los incidentes que hayan ocurrido desde la implementación del Plan de Gestión de Riesgos.

II. **Validación de la Gestión del Riesgo:** Se propone un método para validar los resultados obtenidos.

III. **Mejora Continua:** Se aborda la comprensión de la mejora continua según se define en los Planes de Gestión de Riesgos.

Estas actividades desempeñarán un papel importante en trabajos futuros con el objetivo de asegurar una gestión efectiva del riesgo.

Se planificaron las etapas y actividades utilizando la herramienta "Diagrama de Gantt", la cual resulta muy beneficiosa para la programación de actividades con duraciones específicas.

Además, demostró ser altamente efectiva para supervisar el progreso de las fases. La planificación detallada se puede encontrar en la Tabla 15.

Tabla 15

Diagrama de Gantt para la Planificación del Plan de Gestión de Riesgos en la Biblioteca de la UTN

Gestión de Riesgos Tecnológicos
Biblioteca UTN

TAREA	RESPONSABLE	PROGRESO	INICIO	FIN	DIAS
	INICIO DEL PROYECTO		lun, 09/10/2023		
FASE 1: Comunicación y consulta, Establecimeinto del contexto.		100%			15
Definicion de Principios	Victor Terán	100%	09/10/2023	11/10/2023	3
Compromiso del Departamento	Victor Terán	100%	12/10/2023	14/10/2023	3
Establecimiento del Contexto Actual	Victor Terán	100%	14/10/2023	18/10/2023	5
Recopilacion de informacion	Victor Terán	100%	18/10/2023	21/10/2023	4
FASE 2: Evaluación y tratamiento del riesgo.		100%			41
Identificacion de Activos	Victor Terán	100%	22/10/2023	27/10/2023	5
Identificación de dependencia entre activos	Victor Terán	100%	27/10/2023	28/10/2023	2
Valoración de Activos	Victor Terán	100%	28/10/2023	31/10/2023	3
Identificación de Amenazas	Victor Terán	100%	31/10/2023	02/11/2023	3
Valoración de Amenazas	Victor Terán	100%	02/11/2023	04/11/2023	3
Determinación del Impacto Potencial	Victor Terán	100%	04/11/2023	07/11/2023	4
Determinación del Riesgo Potencial	Victor Terán	100%	07/11/2023	10/11/2023	4
Identificación de Salvaguardas	Victor Terán	100%	10/11/2023	16/11/2023	7
Valoración de Salvaguardas	Victor Terán	100%	13/11/2023	16/11/2023	4
Estimación del Impacto Residual	Victor Terán	100%	15/11/2023	17/11/2023	3
Estimación del Riesgo Residual	Victor Terán	100%	17/11/2023	19/11/2023	3
FASE 3: Seguimiento y Revisión del Riesgo		100%			14
Monitoreo	Victor Terán	100%	19/11/2023	21/11/2023	3
Validación	Victor Terán	100%	21/11/2023	23/11/2023	3
Mejora Continua	Victor Terán	100%	23/11/2023	25/11/2023	3
Socialización	Victor Terán	100%	18/12/2023	19/12/2023	2
Análisis de Riesgo Cuantitativo	Victor Terán	100%	15/12/2023	17/12/2023	3
	Porcentaje de Avance	100%			

Nota: Elaboración propia.

IMPLEMENTACIÓN

2.5. Aspectos Generales

A continuación, se describe los aspectos generales de la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte, esta información es relevante y concisa sobre varios aspectos clave.

Misión

La Biblioteca de la Universidad Técnica del Norte tiene como misión satisfacer las necesidades de información de los usuarios a fin de contribuir a los procesos de enseñanza aprendizaje, así como el desarrollo de la ciencia y la tecnología.

Visión

La Biblioteca de la Universidad Técnica del Norte será un referente a nivel nacional e internacional, con prestación de servicios de excelencia, incluyentes e innovadores, que cuente con recursos bibliográficos pertinentes, suficientes y actualizados con espacios físicos adecuados y un recurso humano capacitado que satisfaga las expectativas de los usuarios.

Propósito

El propósito de este informe consiste en detallar el proceso establecido para la Gestión de Riesgos en la Biblioteca de la Universidad Técnica del Norte (UTN), con el objetivo de incrementar la probabilidad de éxito en el cumplimiento de los siguientes propósitos:

- Reforzar la capacidad de gestión de riesgos en la Biblioteca de la UTN.
- Contextualizar la situación
- actual de la Biblioteca de la UTN.
- Identificar los activos, amenazas, riesgos y salvaguardas en la Biblioteca de la UTN.
- Sugerir tareas como salvaguardas que, en caso de implementarse, reduzcan al mínimo las pérdidas o impactos negativos derivados de la materialización de riesgos.
- Elaborar una propuesta para la supervisión del Plan de Gestión de Riesgos.

Alcance

Este procedimiento se aplica para realizar El Plan de Gestión de Riesgos con 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 de 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 la Biblioteca. 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 la Biblioteca para decidir implementarlas o modificarlas según sea necesario.

Usuarios

Los usuarios de este procedimiento son todo el personal que realiza labores para la Biblioteca de UTN dentro del alcance definido.

Valores

Calidad

Nuestros proyectos serán elaborados con calidad y actitud de servicio con la Universidad Técnica del Norte.

Responsabilidad

Cumplimos nuestros proyectos con responsabilidad, creando confianza en nuestros colaboradores

Creatividad

Aporte de ideas innovadoras para la optimización de los procesos institucionales.

Liderazgo

Nuestro compromiso es realizar las actividades con eficiencia, comprometimiento para brindar un aporte generador de valor en las gestiones institucionales.

Trabajo en equipo

Sumamos esfuerzos y talentos para lograr nuestros objetivos y ayudarnos unos a otros.

Honestidad

Nos basamos en los reglamentos que gobiernan a la Universidad y el estatuto propio de nuestra Institución para trabajar con armonía, verdad, respeto y lealtad.

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

Comunicación y consulta

La gestión de riesgos implica una comunicación y consulta esenciales, ya que facilitan el intercambio de información entre las partes involucradas. Este proceso es fundamental para determinar las acciones a tomar frente a los riesgos, al tiempo que contribuye a mejorar la toma de decisiones y la comprensión de los riesgos.

En relación con los riesgos tecnológicos en la Biblioteca de la UTN, se han identificado a los siguientes individuos como partes interesadas.

- Directora de la Dirección de Biblioteca UTN.
- Encargado del Área de Informática y Digitalización de la Biblioteca de la 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 Área de Informática y Digitalización de la Biblioteca de la UTN no dejará aislada al proceso de gestión de riesgos de las demás actividades integrales del departamento.

Estructurada y exhaustiva

El Área de Informática Y Digitalización de la UTN efectuará la gestión de riesgos de manera sistemática y ordenada, de forma que se puede llevar un correcto proceso iterativo.

Adaptada

El Área de Informática Y Digitalización de la 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 Área de Informática Y Digitalización de la UTN tendrá una participación apropiada y oportuna en las actividades relacionadas con la gestión del riesgo.

Dinámica

El Área de Informática Y Digitalización de la UTN responderá de manera oportuna a los cambios que puedan existir al contexto de la gestión de riesgos.

Mejor información posible

El Área de Informática Y Digitalización de la 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 Área de Informática Y Digitalización de la UTN mejorará el nivel de interés y minimizará la resistencia al cambio que presenta la implementación de la gestión de riesgos.

Mejora Continua

El Área de Informática Y Digitalización de la 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:

- Suministrar la información y documentación requerida durante la etapa de implementación.
- Proporcionar los recursos necesarios.
- Autorizar la ejecución del plan de gestión de riesgos en la Biblioteca.
- Conferir un cierto grado de autoridad al encargado durante la ejecución de las actividades asociadas al plan de gestión de riesgos.

- Facilitar la asistencia necesaria cuando sea solicitada.

2.6.1. Establecimiento del Contexto

Situación Actual

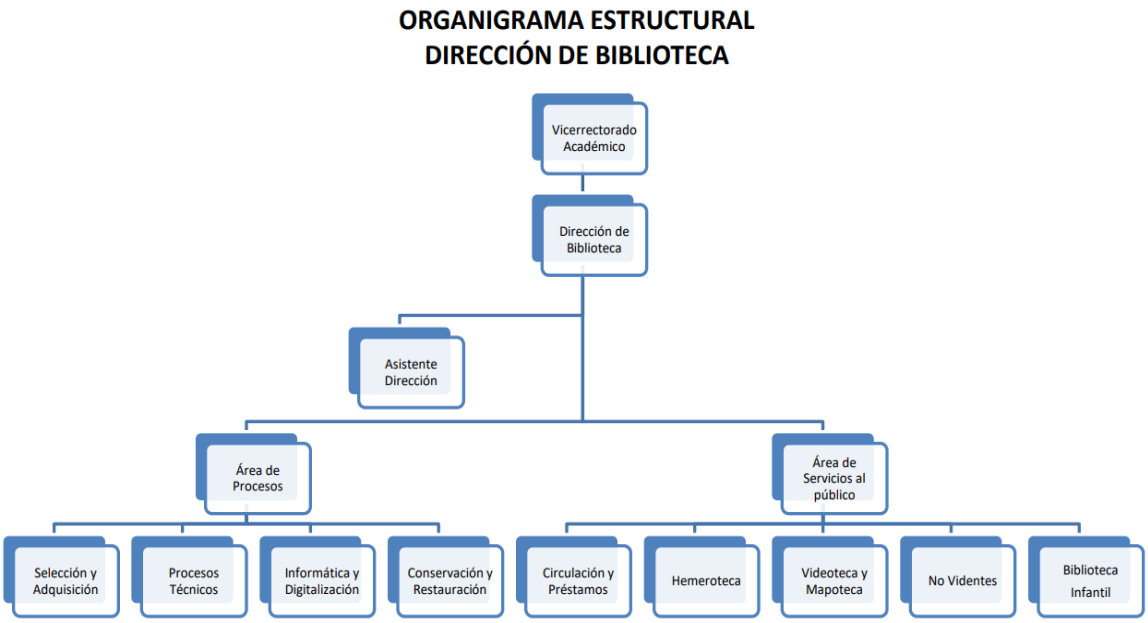
La Universidad Técnica del Norte (UTN) se destaca actualmente como un punto de referencia en la región norte del país en el ámbito de la Educación Superior. Es especialmente reconocida por la calidad de los profesionales que gradúa en cada ciclo académico y ha ganado una destacada reputación en el ámbito tecnológico debido a su bien equipada infraestructura tecnológica.

Para abordar todos los aspectos relacionados con el aprendizaje en la Universidad, se estableció de manera consolidada la Dirección de Biblioteca UTN, el cual tiene su ubicación en el campus principal denominado "El Olivo".

En la Figura 15 del Organigrama Estructural de la UTN en 2023, se puede observar cómo el área de Informática y Digitalización de la Biblioteca de la UTN constituye uno de los departamentos fundamentales en el nivel de apoyo.

Figura 15

Organigrama de la Estructural Dirección de Biblioteca



Nota: Entregado de Dirección de Biblioteca, por (UTN, 2023).

La Dirección de Biblioteca comprometida con el apoyo al cumplimiento de los objetivos de la UTN, implementa dos servicios, el primer espacio conocido como “Área para No Videntes”, mismo que conforma y cuenta con todos los equipos tecnológicos dentro de

la UTN, y el segundo referente al área de Informática y Digitalización en el cual se está digitalizando todos los documentos como las tesis para que los estudiantes las puedan revisar en el repositorio de la Universidad a disposición de todos los usuarios. Parte de la digitalización de los documentos se realizan en el área de Informática y Digitalización de la Biblioteca de la Universidad.

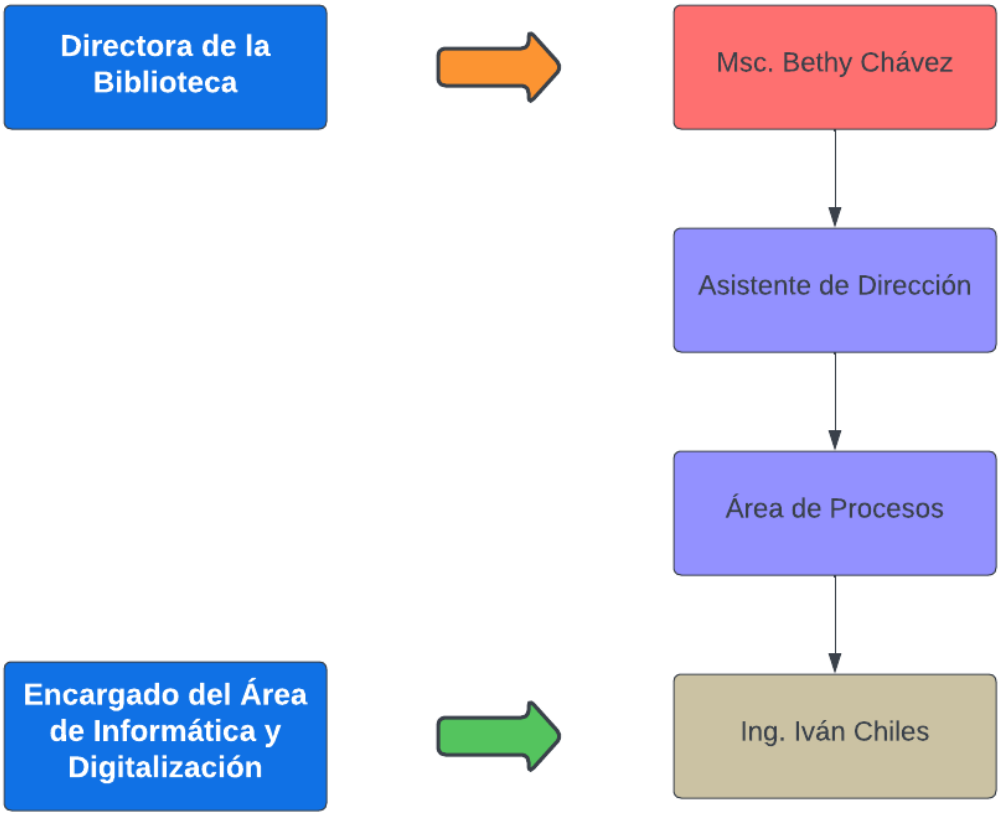
Estructura Organizacional de la Dirección de Biblioteca de la UTN

La Dirección de Biblioteca es responsabilidad de Vicerrectorado Académico, en este caso, la Biblioteca contempla al área de Informática y Digitalización como un departamento interno de la Biblioteca, necesario para su correcto funcionamiento.

El alto nivel de importancia de esta área ha ocasionado la necesidad de designar a un personal con capacidades específicas para cubrir los requerimientos de la Dirección de Biblioteca. En la Figura 16 se aprecia la organización interna del área de Informática y Digitalización de la Biblioteca de la UTN.

Figura 16

Organigrama del Área de Informática y Digitalización de la UTN



Nota: Elaboración propia.

Según la página web oficial de la UTN, los directivos actuales de la Dirección de Biblioteca se conforman como se indica en la Tabla 16:

Tabla 16

Directivos de la Dirección de Biblioteca de la UTN

DIRECTIVOS UTN
Rector
Vicerrectora Académica
Vicerrectora de Investigación
Vicerrector Administrativo
DIRECTIVOS DIRECCION DE BIBLIOTECA UTN
Directora de Dirección de Biblioteca
Asistente de Dirección
Área de Procesos
Área de Servicios al Publico

Nota: Elaboración propia

Infraestructura física

La Dirección de Biblioteca de la Universidad Técnica del Norte cuenta con su infraestructura física en el Campus Universitario principal ubicado en "EL Olivo", dentro de este edificio que compone la Biblioteca se encuentran de forma distribuida las diferentes áreas y el área de Informática y Digitalización.

En la Tabla 17 se presenta la distribución de ambientes físicos pertenecientes a la Biblioteca de la UTN.

Tabla 17

Distribuciones ambientes físicos de la Biblioteca de la UTN

Ambiente Físico	Descripción
Entrada a la Biblioteca	En la entrada de la Biblioteca se encuentran cuatro computadores para que los estudiantes registren su ingreso.

Área de servidores	Conjunto de computadores con servidores como: Servidor proxy y DHCP Servidor de antivirus Instaladores Servidor de base de datos de los sistemas informáticos
Oficinas	Oficinas con computador, impresora, teléfono IP para las personas encargadas de las diferentes áreas.
Cuarto de Comunicaciones	Área con rack de conexiones de fibra y cobre, switches de acceso a la red.
Área de Informática	Conjunto de 4 ambientes físicos con equipos de altas prestaciones.
Área de Servicios al Publico	Conjunto de 5 ambientes físicos con equipos de altas prestaciones.

Nota: Elaboración propia

Cada una de las Áreas de la Biblioteca está dotada de distintos tipos de equipos para procurar cubrir las distintas necesidades académicas de los estudiantes. En la Tabla 18 se presenta los tipos de equipos con los que está provisto cada Área.

Tabla 18

Distribución de equipos en las Áreas de la Biblioteca de la UTN

Planta	Área	Tipo de Equipos	N. Equipos
1	Biblioteca Infantil	Sistema Operativo Windows	7
	Discapacitados	Sistema Operativo Windows	4
	Registro de Entrada	Sistema Operativo Windows	4
2	Referencia 1	Sistema Operativo Windows	2
	Recepción Tesis	Sistema Operativo Windows	1
	Referencia 2	Sistema Operativo Windows	3
	Dirección	Sistema Operativo Windows	2
3	Préstamo Estudiantes	Sistema Operativo Windows	12
	Hemeroteca	Sistema Operativo Windows	13
	Laboratorio Videoteca	Sistema Operativo Windows	8

	Informática	Sistema Operativo Windows	6
4	Catálogo 1	Sistema Operativo Windows	5
	Catálogo 2	Sistema Operativo Windows	3
	Procesos Técnicos	Sistema Operativo Windows	3

Nota: Elaboración propia.

Infraestructura Tecnológica

La Biblioteca es parte integral de la Universidad Técnica del Norte, estos pertenecen al área de "Préstamo Estudiantiles", del cual está encargada cada el área de servicios al público. La Tabla 19 presenta la distribución de software utilizada en el área de Prestamos Estudiantiles de la Biblioteca de la UTN.

Tabla 19

Distribución de Software en la Biblioteca de la UTN

Software	Descripción
Software	La Biblioteca utilizan el software original, así como también el software con las versiones de demostración (demos)
Sistemas Informáticos Internos	• Sistema Integrado • Sistema Biblioteca Virtual • Registro de Usuarios • Repositorio Digital • Libros Digitales • Sitio Web: Biblioteca y Tifloteca

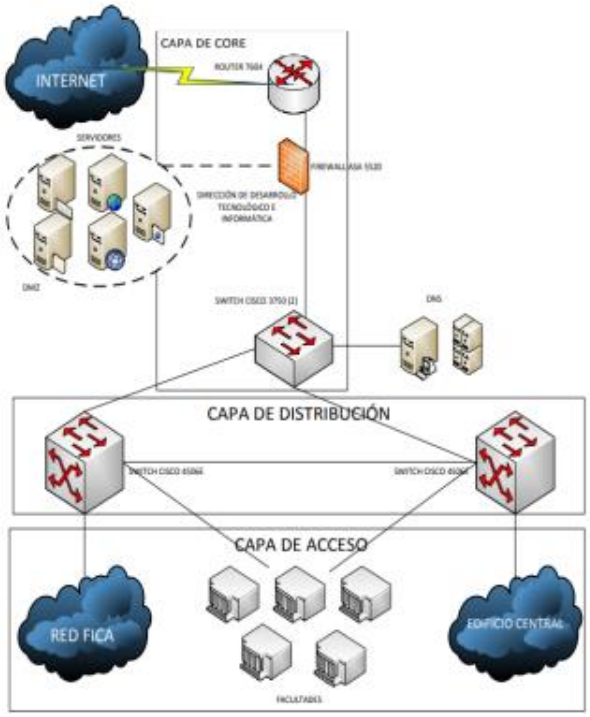
Nota: En la siguiente tabla se puede observar la distribución de software de la Biblioteca de la UTN en la cual se encuentra el sitio web y la Tifloteca, la cual es un espacio que tiene la Biblioteca con procedimientos y técnicas para la utilización de personas no videntes. Elaboración Propia.

En el caso de la Biblioteca, la persona encargada de la administración y gestión de los equipos computacionales es un Ingeniero. Sin embargo, los servicios presentes en la Biblioteca 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 la Biblioteca se encuentra debidamente registrada por el Departamento de Almacén y Bodega de la UTN, misma información almacenada en la base de datos utilizada por la Universidad. Dentro de los activos físicos también se comprende a los bienes tecnológicos pertenecientes a la Biblioteca de la UTN, 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 17.

Figura 17

Topología Básica de Red UTN



Nota: Tomada de "Plan Estratégico UTN", por Dirección de Desarrollo Tecnológico e Informático, (UTN, 2021).

En el caso de la Biblioteca, la Tabla 20 presenta como están distribuidas las conexiones de red.

Tabla 20

Distribución de equipos de comunicaciones y conexiones de red en la Biblioteca de la UTN

Ubicación	Rack	Switch CISCO	Puntos de Red
Biblioteca Infantil	1	1	20
No Videntes	0	1	4

Videoteca y Mapoteca	0	1	10
Hemeroteca	0	1	13 PCs conectadas directamente a un Switch
Circulación y Prestamos	0	5	12 PCs conectadas directamente a un Switch
Dirección de Biblioteca	0	1	10
Conservación y Restauración	0	1	20
Informática y Digitalización	0	2	6 PCs conectadas directamente a un Switch
Selección y Adquisición	0	1	10
Procesos Técnicos	1	1	10

Nota: Elaboración propia.

Servicios

La Biblioteca de la UTN son parte integral de las actividades dentro de la Universidad, debido a que brindan una serie de servicios necesarios tanto para la parte académica, como para la parte administrativa. Estos servicios son:

- Acceder en condiciones adecuadas a los diferentes servicios tradicionales y virtuales que presta la Biblioteca Universitaria.
- Recibir información, asesoramiento y colaboración en la localización y acceso a fuentes bibliográficas y documentales.
- Recibir la formación necesaria para la utilización eficaz de la Biblioteca Universitaria, de sus recursos y servicios.
- Recibir una atención cordial, eficiente y oportuna por parte del personal de la Biblioteca.
- Disponer de espacios y medios adecuados para consulta e investigación.
- Encontrar el soporte bibliográfico adecuado y acorde a los requerimientos académicos de las diferentes asignaturas.

Seguridad y control de acceso

La distribución de la Biblioteca se encuentra ubicada de esta manera debido a las disposiciones impuestas por el equipo de infraestructura y electricidad de la Universidad. Además de las áreas, 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 la Biblioteca, 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

La Biblioteca cada cierto tiempo optan por solicitar la actualización de los sistemas de vigilancia, más recurrentemente del sistema de seguridad biométrica, por lo que no todas las áreas cuentan con todos los sistemas de seguridad. Como se puede observar en la Tabla 21.

Tabla 21

Sistema de Seguridad en la Biblioteca de la UTN

Área	Seguridad Biométrica Dactilar	Seguridad Biométrica Facial	Seguridad Física	Cámaras de Vigilancia
Biblioteca Infantil	NO	NO	SI	SI
No Videntes	NO	NO	SI	SI
Videoteca y Mapoteca	SI	SI	SI	SI
Hemeroteca	SI	NO	SI	SI
Circulación y Prestamos	NO	NO	SI	SI
Dirección de Biblioteca	SI	SI	SI	SI
Conservación y Restauración	SI	NO	SI	SI
Informática y Digitalización	SI	SI	SI	SI

Selección y Adquisición	SI	SI	SI	SI
Procesos Técnicos	SI	NO	SI	SI

Nota: Elaboración propia.

Incidentes pasados

Desde la consolidación de la Biblioteca de la 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 la Biblioteca 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.

Han existido diversos casos de hurto de componentes pertenecientes a los equipos de la Biblioteca, 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 de la Biblioteca se ve afectado por los cambios externos que sufren las áreas de la Biblioteca. 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 de la Biblioteca.

2.7. 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 la Biblioteca de la UTN, se optó por la versión PILAR RM (versión 16.6.2023) con su licenciamiento de evaluación debido a su amplia gama de características en comparación con sus otras versiones.

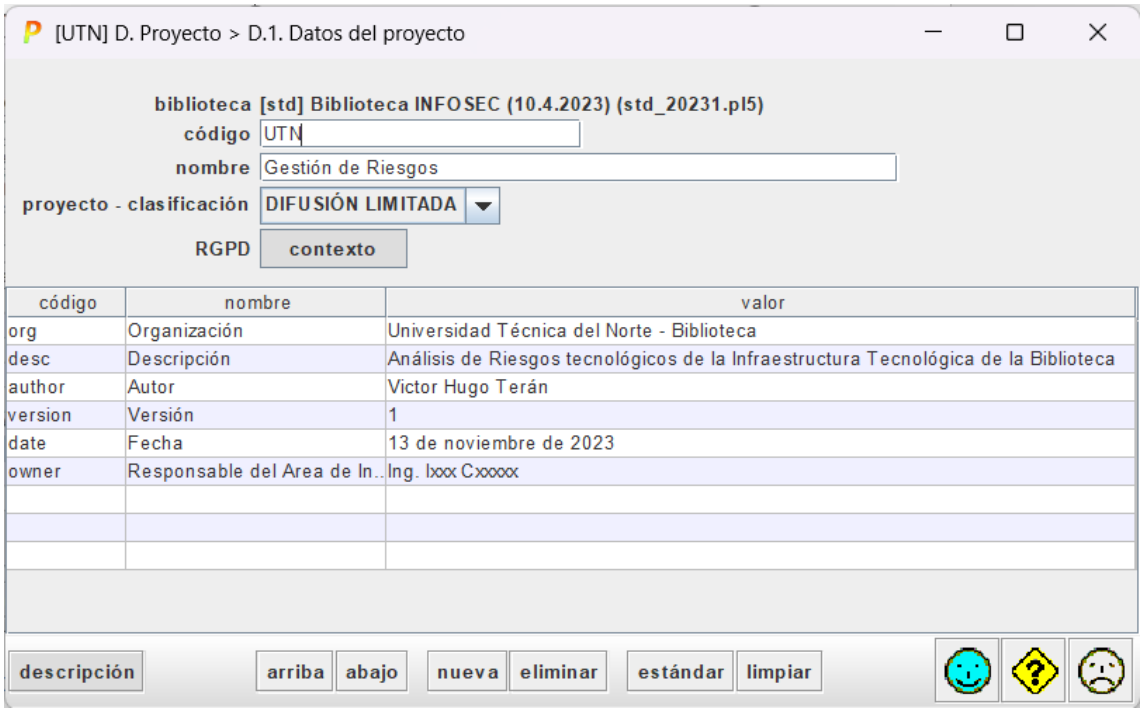
Para facilitar el desarrollo de las actividades de análisis de riesgos, mediante un listado de tipos de activos, dimensiones y criterios de valoración y tipos de amenazas para cada activo.

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 del Área de Informática y Digitalización de la Biblioteca de la 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 13.

Figura 18:

Creación del proyecto en el Software PILAR



Nota Elaboración propia.

2.7.1. 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 22 presenta la clasificación de activos según el segundo escrito de la metodología MAGERIT “Catálogo de Elementos”.

Tabla 22

Tipos de Activos según la Metodología MAGERIT

TIPO DE ACTIVO	DESCRIPCION
Datos / Información	Los datos constituyen el núcleo esencial que habilita a una entidad para ofrecer sus servicios. La información se presenta como un activo intangible que se almacenará en dispositivos o medios de información (comúnmente organizados como archivos o bases de datos) o se trasladará de un lugar a otro mediante los medios de transmisión de datos.
Servicios	La función atiende a una demanda de los usuarios del servicio. En esta sección, se consideran los servicios proporcionados por el sistema.
Software	Bajo diversas denominaciones como programas, aplicativos o desarrollos, este apartado hace referencia a operaciones que han sido automatizadas y son ejecutadas por un equipo informático. Estas aplicaciones se encargan de gestionar, analizar y transformar datos, posibilitando así la explotación de la información para la provisión de servicios como pueden ser desarrollo propio, desarrollo a medida, ofimática, etc.
Hardware	Se refiere a los recursos tangibles o físicos destinados a respaldar de manera directa o indirecta los servicios ofrecidos por la organización. Estos recursos actúan como depositarios temporales o permanentes de la información, sirven como base para la ejecución de las aplicaciones informáticas y son responsables de procesar o transmitir datos como lo pueden ser medios de impresión, módems, computadores, etc.
Redes de comunicaciones	Englobando tanto las instalaciones específicas como los servicios de comunicación externalizados; como pueden ser redes telefónicas, comunicaciones radio, telefonía móvil, red de datos, etc.

Soporte de información	En esta sección, se incluyen dispositivos tangibles que posibilitan el almacenamiento de información de manera duradera, o al menos, a lo largo de extensos intervalos temporales como lo pueden ser discos, memorias USB, DVD, etc.
Equipamiento auxiliar	En esta sección, se incluyen otros dispositivos que proporcionan respaldo a los sistemas de información, aunque no estén directamente vinculados a datos como pueden ser el cableado, fibra óptica, generadores eléctricos, etc.
Instalaciones	Este apartado aborda los sitios que albergan los sistemas de información y comunicación como pueden ser contenedores, canalización, instalaciones de respaldo, etc.
Personal	En este apartado se presentan los individuos vinculados a los sistemas de información como pueden ser usuarios internos, usuarios externos, administradores de sistema, etc.

Nota: Elaboración propia a partir de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (Amutio Gómez et al., 2012e)

La identificación de activos se desarrolló con ayuda de la persona encargada del área de Informática y Digitalización de la Biblioteca de la UTN, y con base en la clasificación establecida por la metodología MAGERIT, en la Tabla 23 se describen los 42 activos identificados.

Tabla 23

Identificación de Activos de la Biblioteca de la UTN

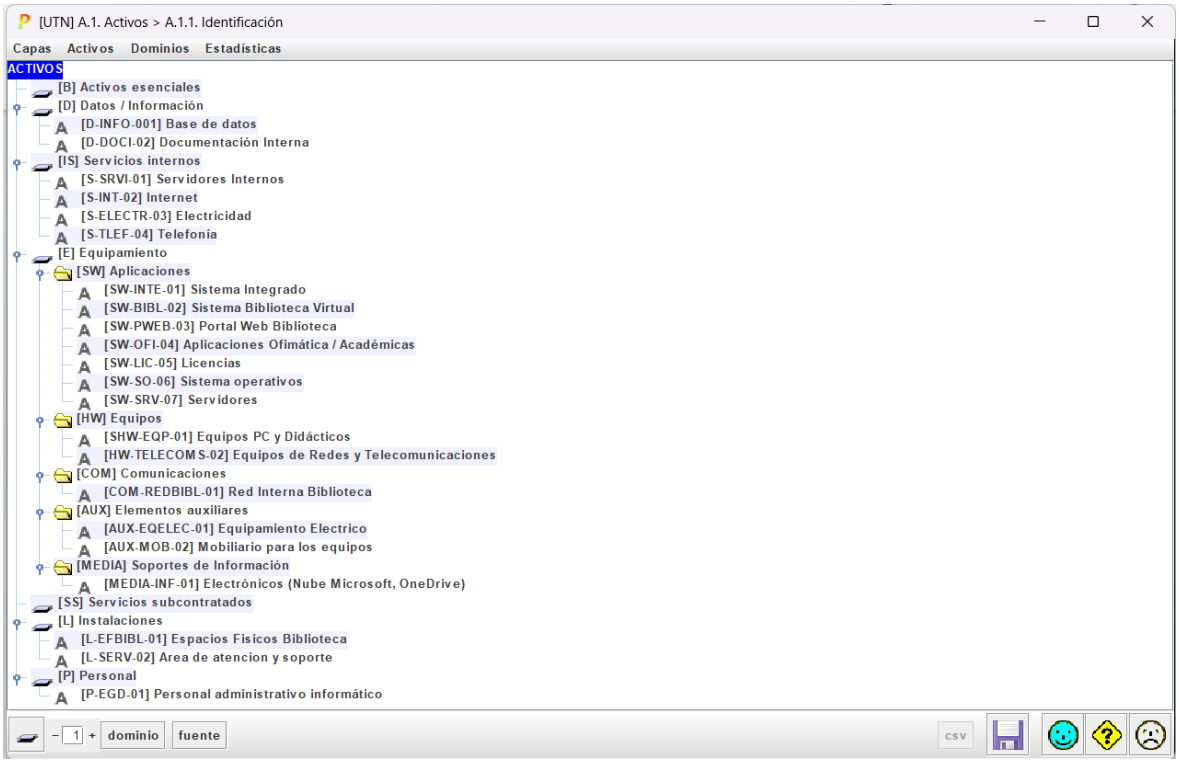
Tipo de activos	Activo	Activo Agrupado	Código
Datos/Información	Base de datos		D-INFO-001
	Documentación Interna		D-DOCI-02
Servicios	Servidor proxy	Servidores Internos	S-SRVI-01
	Correo		
	Internet		S-INT-02
	Electricidad		S-ELECTR-03
	Telefonía		S-TLEF-04
Software	Sistema Integrado	Aplicaciones Informáticas	SW-INTE-01
	Sistema Biblioteca Virtual		SW-BIBL-02
	Portal Web Biblioteca		SW-PWEB-03
	Antivirus	Aplicaciones Ofimática / Académicas	SW-OFI-04
	Firewall		
	Navegación		

	Aplicaciones de Ofimática		
	Licencias		SW-LIC-05
	Sistemas operativos		SW-SO-06
	Servidores		SW-SRV-07
Hardware	Monitores / Computadores	Equipos PC y Didácticos	HW-EQP-01
	Asistente Digital Portátil		
	Impresora		
	Laptop		
	Proyector		
	Router	Equipos de Redes y Telecomunicaciones	HW-TELECOMS-02
	Switch		
	Racks		
	Access Point		
	Cableado estructural		
Redes de comunicación	Internet	Red Interna Biblioteca	COM-REDBIBL-01
	Red inalámbrica		
	Red telefónica		
Soportes de información	Electrónicos (Nube Microsoft, OneDrive)		MEDIA-INF-01
Equipamiento auxiliar	Reguladores de Voltaje	Equipamiento Eléctrico	AUX-EQELEC-01
	Fuentes de Poder		
	Cableado eléctrico		
	Fibra óptica		
	Cable de energía		
	UPS		
	NVR		
	Mobiliario para los equipos		AUX-MOB-02
Instalaciones	Espacios Físicos Biblioteca		L-EFBIBL-01
	Área de atención y soporte		L-SERV-02
Personal	Personal administrativo	Encargado de la Dirección de Informática y Digitalización	P-EGD-01

Nota: Elaboración propia.

Figura 19:

Identificación de Activos de la Biblioteca de la UTN en el software PILAR



Nota: Elaboración propia.

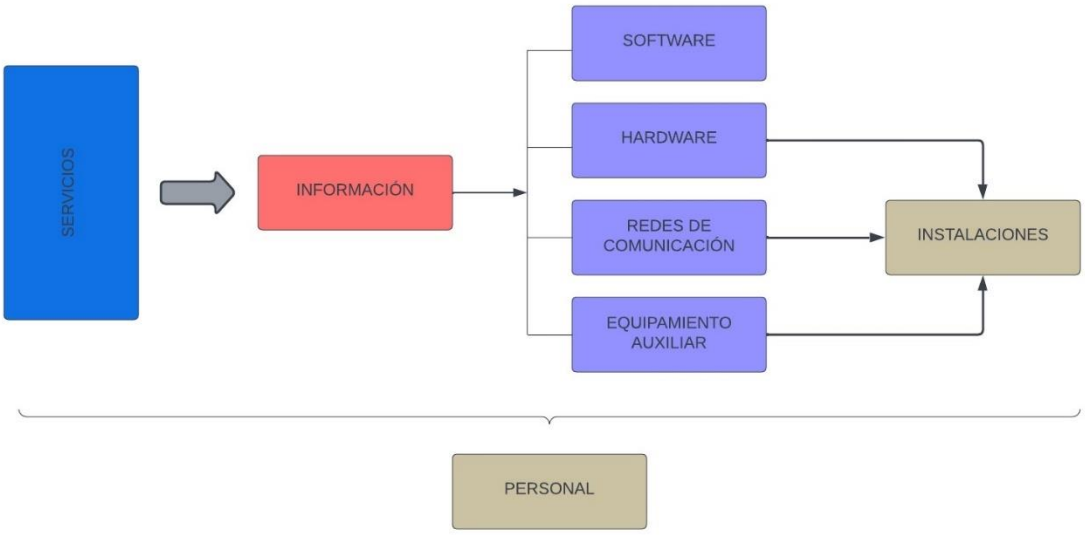
2.7.2. Identificación de la dependencia de los activos

Luego de identificar los activos, es crucial examinar las interconexiones que existen entre ellos. Aunque este análisis de riesgos no ha abordado explícitamente dichas interconexiones para evitar complicaciones adicionales en la evaluación, es esencial reconocer que un riesgo elevado en los activos de nivel inferior puede generar un impacto en cadena en los activos superiores, subrayando la importancia del personal como un elemento crítico en todos los activos.

A continuación, se ofrece un resumen general de las interdependencias entre las distintas categorías de activos: En la Figura 20 se aprecia el árbol de dependencia de activos.

Figura 20:

Dependencia de los Activos



Nota: Elaboración propia.

2.7.3. Valoración de los Activos

Una vez que los activos de la Biblioteca han sido identificados, es esencial llevar a cabo una evaluación para asignarles un valor según sus características relevantes y su impacto potencial en la institución. En este estudio de caso, se empleará una valoración cualitativa a través de encuestas, así como una valoración cuantitativa mediante una matriz dirigida a los responsables de los procesos asociados con cada activo. Estas herramientas han sido diseñadas para cumplir con los estándares fundamentales de confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad establecidos por Magerit V3 (Metodología de análisis y gestión de riesgos de los Sistemas de Información, Libro I: Método, 2012).

La valoración cualitativa proporcionará una comprensión más profunda de la importancia de cada activo en el modelo de negocio y cómo su eventual pérdida afectaría la continuidad de la Biblioteca. Con el fin de asegurar una evaluación precisa, se formularán preguntas específicas para cada parámetro. MAGERIT evalúa la importancia de los activos en distintas dimensiones, estas se presentan en la Tabla 24:

Tabla 24

Definiciones de las dimensiones de valoración de activos

Dimensión	Definición

Disponibilidad	La propiedad o atributo de los activos se refiere a la capacidad de permitir el acceso a entidades o procesos autorizados en el momento que lo necesiten.
Integridad	Integridad se refiere a la propiedad o característica que indica que el activo de información no ha sufrido modificaciones no permitidas.
Confidencialidad	Atributo o cualidad que implica que la información no es compartida ni revelada a personas, entidades o procesos no autorizados.
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: Adaptado a partir de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de Elementos, por Dirección General de Modernización Administrativa, (Amutio Gómez et al., 2012c)

- Disponibilidad

¿Cómo afectaría a la Biblioteca no poder utilizar un activo?

- Integridad

¿Qué perjuicio causaría para la Biblioteca que estuviera dañado o corrupto?

- Confidencialidad

¿Cómo afectaría a la Biblioteca que la información sea conocida por personas ajenas no autorizadas?

- Autenticidad

¿Qué importancia tendría que quien accede a los servicios de la Biblioteca no sea realmente quien se cree?

- Trazabilidad

¿Qué importancia tendría para la Biblioteca que no quedara constancia del acceso a los datos?

Estas dimensiones operan como una faceta o perspectiva de los activos, a través de las cuales es posible evaluar las implicaciones que surgen a consecuencia de la realización

de diversas amenazas. En la evaluación de los activos, se consideró la escala de criterios que se presenta en la Tabla 25.

Tabla 25

Escala de Valoración de activos

Nivel de Valor	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 menos
0	Despreciable	Irrelevante a efectos prácticos

Nota: Elaboración propia a partir de Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de elementos, por Dirección General de Modernización Administrativa, (Amutio Gómez et al., 2012d).

Los valores obtenidos de esta tabla indican la magnitud del daño potencial para la organización en el caso de que el activo se vea afectado en esa dimensión específica.

En la Tabla 26 se encuentra la asignación de valoración de cada uno de los activos.

Tabla 26

Valoración de activos de la Biblioteca de la UTN

Tipo de activos	Activo	D	I	C	A	T	Ponderación	Valor
Datos/Información	Base de datos	10	10	10	10	10	10	Extremo
	Documentación interna	10	10	10	10	10	10	Extremo
Servicios	Servidores Internos	10	10	10	10	10	10	Muy Alto
	Internet	10	10	10	10	9	10	Extremo
	Electricidad	10	7	8	8	7	8	Alto
	Telefonía	9	9	9	10	8	9	Muy Alto
Software	Sistema Integrado	10	10	10	10	10	10	Extremo

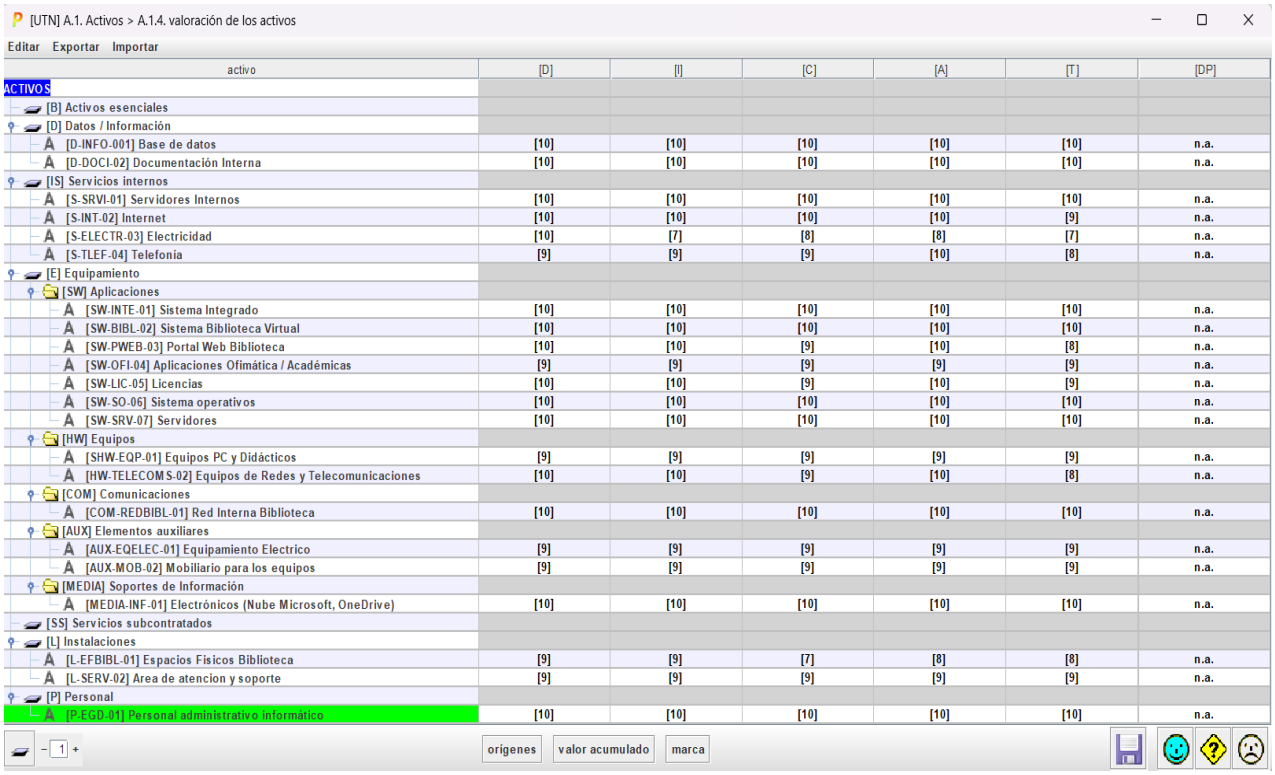
	Sistema Biblioteca Virtual	10	10	10	10	10	10	Extremo
	Portal Web Biblioteca	10	10	9	10	8	9	Muy Alto
	Aplicaciones Ofimática / Académicas	9	9	9	9	9	9	Muy Alto
	Licencias	10	10	9	10	9	10	Extremo
	Sistemas operativos	10	9	9	7	7	8	Alto
	Servidores	10	10	10	10	10	10	Extremo
Hardware	Equipos PC y Didácticos	9	9	9	9	9	9	Muy Alto
	Equipos de Redes y Telecomunicaciones	10	10	9	10	8	9	Muy Alto
Redes de comunicación	Red Interna Biblioteca	10	10	10	10	10	10	Extremo
Soportes de información	Electrónicos (Nube Microsoft, OneDrive)	10	10	10	10	10	10	Extremo
Equipamiento auxiliar	Equipamiento Eléctrico	9	9	9	9	9	9	Muy Alto
	Mobiliario para los equipos	9	9	9	9	9	9	Muy Alto
Instalaciones	Espacios Físicos Biblioteca	9	9	7	8	8	8	Alto

	Área de atención y soporte	9	9	9	9	9	9	Muy Alto
Personal	Encargado de la Dirección de Informática y Digitalización	10	10	10	10	10	10	Extremo

Nota: Elaboración propia. 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 la Biblioteca de la UTN.

Figura 21:

Valoración de Activos Software Pilar

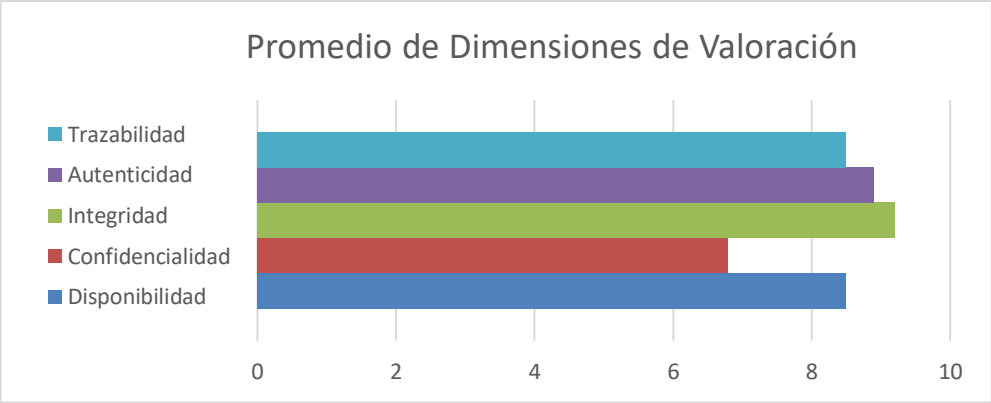


Nota: Elaboración propia.

La Figura 21 presenta un promedio de las valoraciones cuantitativas por dimensión de valoración de todos los activos identificados en la Biblioteca de la UTN.

Figura 22:

Promedio dimensiones de valoración activos de la Biblioteca de la UTN

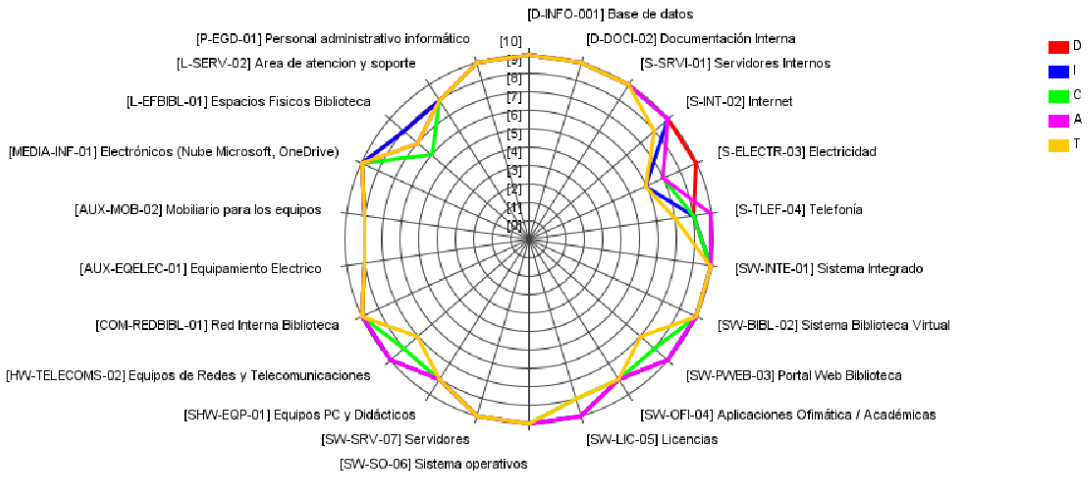


Nota: Elaboración propia.

La Figura 22 presenta en un gráfico de tipo área, el valor de activo en su respectiva dimensión dentro de la Biblioteca de la UTN.

Figura 23:

Valor de los activos de la Biblioteca de la UTN



Nota: Elaboración propia.

2.7.4. Identificación de Amenazas

La siguiente etapa después de caracterizar los activos consiste en la identificación de las posibles amenazas que podrían afectar a cada uno de ellos. En el segundo documento de la metodología MAGERIT, titulado "Catálogo de Elementos", se enumeran cuatro tipos distintos de amenazas:

[N] Desastres Naturales

[I] Origen Industrial

[E] Errores y fallos no intencionados

[A] Ataques intencionados

En el caso de los 22 activos agrupados pertenecientes a la Biblioteca de la UTN, se identificaron un total de 250 amenazas. Estas amenazas se detallan en el Anexo E, y una muestra de la lista se presenta en la Tabla 27.

Tabla 27

Identificación de amenazas por activos de la Biblioteca de la UTN

ACTIVO	AMENAZAS
DATOS/INFORMACION	
Base de datos	[E.15] Alteración de la información
Base de datos	[E.18] Destrucción de la información
Base de datos	[E.19] Fugas de información
Base de datos	[A.5] Suplantación de la identidad
Base de datos	[A.6] Abuso de privilegios de acceso
Base de datos	[A.11] Acceso no autorizado
Documentación interna	[E.15] Alteración de la información
Documentación interna	[E.18] Destrucción de la información
Documentación interna	[E.19] Fugas de información
Documentación interna	[A.5] Suplantación de la identidad
Documentación interna	[A.6] Abuso de privilegios de acceso
Documentación interna	[A.11] Acceso no autorizado
SERVICIOS	
Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales
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 la 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

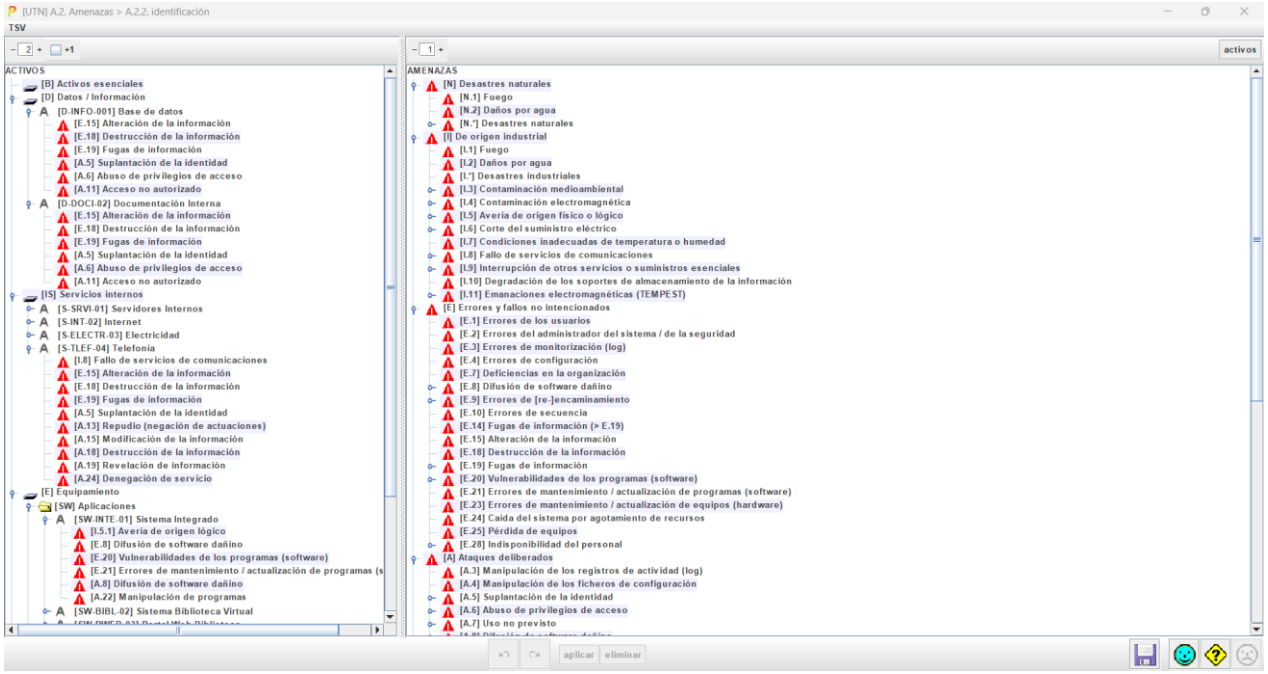
Servidores internos	[A.19] Revelación de información
Servidores internos	[A.24] Denegación de servicio
Internet	[I.8] Fallo de servicios de comunicaciones
Internet	[E.15] Alteración de la información
Internet	[E.18] Destrucción de la información
Internet	[E.19] Fugas de información
Internet	[A.5] Suplantación de la identidad

Nota: Elaboración propia.

De igual manera, PILAR nos ayuda a identificar de manera automática las amenazas en relación de los activos identificados, como se presenta en la Figura 24.

Figura 24:

Identificación de amenazas por activos de la Biblioteca de la UTN en el software PILAR



Nota: Elaboración propia.

2.7.5. Valoración de Amenazas

Después de reconocer las posibles amenazas asociadas con cada tipo de activo, se realiza una evaluación recíproca utilizando una escala predefinida.

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 28. Pero para el uso del software PILAR, se necesitan valores numéricos, por lo que se utiliza un porcentaje de 0 a 100.

Tabla 28

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 I: Método, por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (Amutio Gómez et al., 2012a).

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 29.

Tabla 29

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 I: Método, por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (Amutio Gómez et al., 2012a).

En colaboración con el área de informática y digitalización a cargo de la Biblioteca de la UTN, se asignaron valores cuantitativos para evaluar el Impacto (Tabla 28) y la Probabilidad de ocurrencia (Tabla 29) de cada amenaza identificada. Dado que no se disponía de un registro de incidentes ocurridos en la Biblioteca, esta evaluación se realizó mediante suposiciones, influenciada por los valores predeterminados proporcionados por PILAR.

La valoración de todas las amenazas, considerando su probabilidad de ocurrencia (frecuencia) y la degradación de valor (impacto), se detalla en el Anexo F. Además, la Tabla 30 proporciona una muestra representativa de dicha lista.

Tabla 30

Valoración de amenazas por activos de la Biblioteca de la UTN

ACTIVOS	AMENAZAS	F	D	I	C	A	T
DATOS / INFORMACIÓN							
Base de datos	[E.15] Alteración de la información	1		1%			
Base de datos	[E.18] Destrucción de la información	1	1%				
Base de datos	[E.19] Fugas de información	1			10%		
Base de datos	[A.5] Suplantación de la identidad	10		10%	50%	100 %	
Base de datos	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Base de datos	[A.11] Acceso no autorizado	100		10%	50%		
Documentación interna	[E.15] Alteración de la información	1		1%			
Documentación interna	[E.18] Destrucción de la información	1	1%				
Documentación interna	[E.19] Fugas de información	1			10%		
Documentación interna	[A.5] Suplantación de la identidad	10		10%	50%	100 %	
Documentación interna	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Documentación interna	[A.11] Acceso no autorizado	100		10%	50%		
SERVICIOS							
Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales	1	50 %				
Servidores internos	[E.1] Errores de los usuarios	1	10 %	10%	10%		

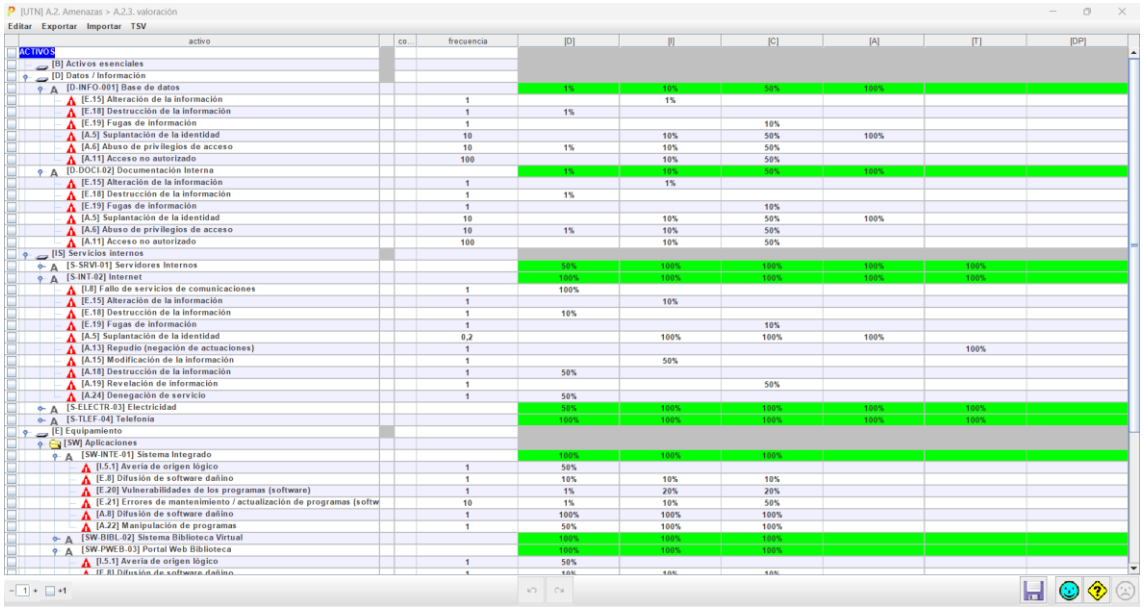
Servidores internos	[E.2] Errores del administrador del sistema / de la seguridad	1	20 %	20%	20%	
Servidores internos	[E.15] Alteración de la información	1		10%		
Servidores internos	[E.18] Destrucción de la información	1	10 %			
Servidores internos	[E.19] Fugas de información	1			10%	
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	10	50 %			
Servidores internos	[A.5] Suplantación de la identidad	1		100 %	100 %	100 %
Servidores internos	[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	100 %

Nota: La tabla presenta una muestra del listado de la valoración de amenazas que podrían afectar a los activos identificados en la Biblioteca de la 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 20 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 25:

Valoración de amenazas por activos de la Biblioteca de la UTN en el software PILAR



Nota: Elaboración propia.

2.7.6. Determinación del impacto potencial

El potencial impacto se refiere al perjuicio causado por la materialización de una amenaza en relación con un activo. Este impacto potencial guarda proporción con el valor del activo y su degradación, siendo esencial determinarlo para establecer las salvaguardas más apropiadas. La evaluación del valor del impacto se llevó a cabo para cada activo, considerando cada amenaza y en cada dimensión de valoración según su grado de degradación.

La evaluación de este impacto puede realizarse desde dos perspectivas diferentes:

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:

$$\textbf{\textit{Impacto potencial acumulado}} = \%\ Degradación\ de\ amenaza \times Valor\ acumulado\ del\ activo$$

El cálculo del impacto potencial acumulado se encuentra en el Anexo G, mientras que la Tabla 31 presenta una muestra de dicha lista.

Tabla 31

Impacto potencial acumulado de afectación de activos en la Biblioteca de la UTN

	Impacto Potencial Acumulado					Peso Ponderado
ACTIVOS - AMENAZAS	**D**	**I**	**C**	**A**	**T**	
DATOS/INFORMACIÓN	**4**	**7**	**9**	**10**		
Base de datos	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			7.0
[A.5] Suplantación de la 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
Documentación 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			7.0
[A.5] Suplantación de la 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	**10**	**10**	**10**	**10**	**10**	
Servidores internos	9	10	10	10	10	
[I.9] Interrupción de otros servicios o suministros esenciales	9					9.0
[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		7				7.0
[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 la identidad		10	10	10		10.0
[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.19] Revelación de información			9			9.0
[A.24] Denegación de servicio	9					9.0
Internet	10	10	10	10	9	
[I.8] Fallo de servicios de comunicaciones	10					10.0
[E.15] Alteración de la información		7				7.0
[E.18] Destrucción de la información	7					7.0

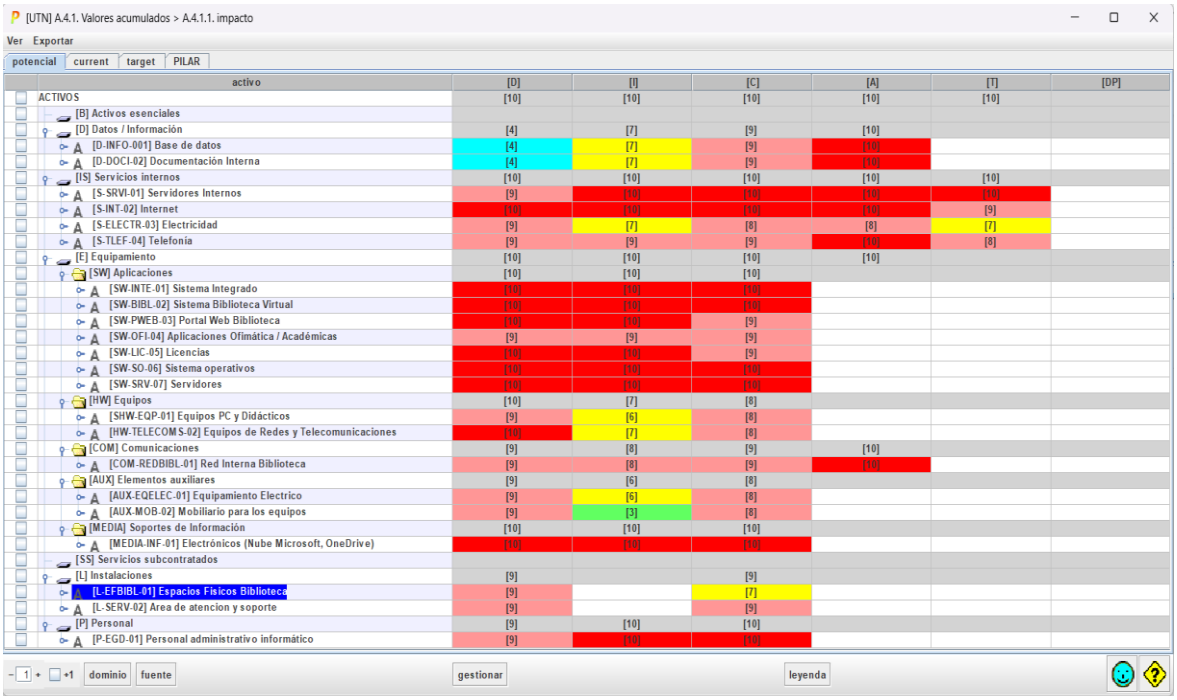
[E.19] Fugas de información			7			7.0
[A.5] Suplantación de la identidad		10	10	10		10.0
[A.13] Repudio (negación de actuaciones)					9	9.0
[A.15] Modificación de la información		9				9.0
[A.18] Destrucción de la información	9					9.0
[A.19] Revelación de información			9			9.0
[A.24] Denegación de servicio	9					9.0
Electricidad	9	7	8	8	7	
[I.9] Interrupción de otros servicios o suministros esenciales	9					9.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	7					7.0
[E.19] Fugas de información			5			5.0
[A.5] Suplantación de la identidad		7	8	8		7.7

Nota: La siguiente tabla presenta la acumulación del impacto, donde D: representa la degradación en la disponibilidad, I: la degradación en la integridad, C: la degradación en la confidencialidad, A: la degradación en la autenticidad y T: la degradación en la trazabilidad. Elaboración propia.

En la Figura 26 se presenta el impacto potencial acumulado en el software PILAR.

Figura 26:

Impacto potencia acumulado de afectación de activos en de la Biblioteca de la UTN



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.

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

El cálculo del impacto potencial repercutido se encuentra en la Tabla 32.

Tabla 32

Impacto potencial repercutido de afectación de activos de la Biblioteca de la UTN

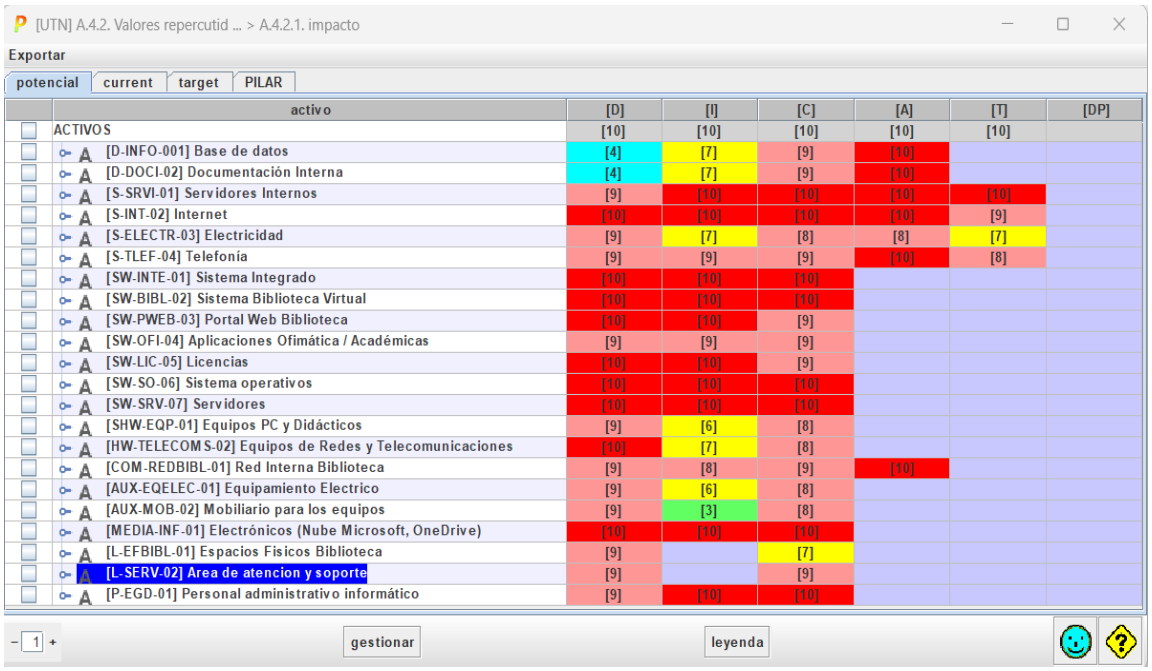
	Impacto Potencial Repercutido					Peso Ponderado
ACTIVOS - AMENAZAS	**D**	**I**	**C**	**A**	**T**	
Base de datos	4	7	9	10		7.5
Documentación Interna	4	7	9	10		7.5
Servidores Internos	9	10	10	10	10	9.8
Internet	10	10	10	10	9	9.8
Electricidad	9	7	8	8	7	7.8
Telefonía	9	9	9	10	8	9.0
Sistema Integrado	10	10	10			10.0
Sistema Biblioteca Virtual	10	10	10			10.0
Portal Web Biblioteca	10	10	9			9.7
Aplicaciones Ofimática / Académicas	9	9	9			9.0
Licencias	10	10	9			9.7
Sistemas operativos	10	10	10			10.0
Servidores	10	10	10			10.0
Equipos PC y Didácticos	9	6	8			7.7
Equipos de Redes y Telecomunicaciones	10	7	8			8.3
Red Interna Biblioteca	9	8	9	10		9.0
Electrónicos (Nube Microsoft, OneDrive)	10	10	10			10.0
Equipamiento Eléctrico	9	6	8			7.7
Mobiliario para los equipos	9	3	8			6.7
Espacios Físicos Biblioteca	9		7			8.0
Área de atención y soporte	9		9			9.0
Encargado de la Dirección de Informática y Digitalización	9	10	10			9.7

Nota: La tabla presenta una muestra del listado del impacto potencial repercutido de los activos identificados en la Biblioteca de la 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 23 se presenta el impacto potencial repercutido para cada activo de la Biblioteca de la UTN.

Figura 27:

Impacto potencial repercutido de afectación de activos de la Biblioteca de la UTN en el software PILAR

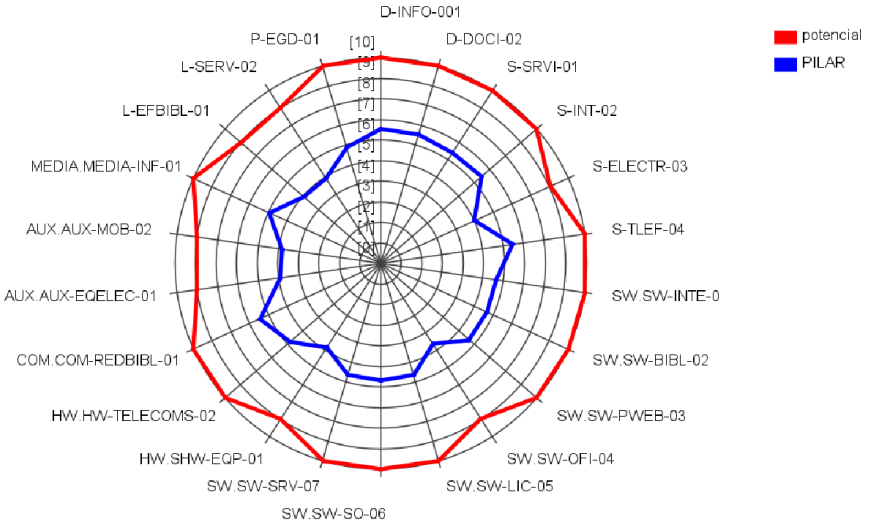


Nota: Elaboración propia.

En la Figura 28 a continuación 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 el Software PILAR.

Figura 28:

Gráfico de valores de impacto potencial acumulado de afectación de activos de la Biblioteca de la UTN



Nota: Elaboración propia.

El cálculo del impacto potencial acumulado, basado en el valor total de los activos del sistema, es esencial para identificar las salvaguardas en el proceso de gestión de riesgos. Por otro lado, al calcular el impacto potencial sobre el valor específico de los activos, se logra determinar exclusivamente las consecuencias de las amenazas en incidentes particulares.

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 33.

Tabla 33

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	MA
		PROBABILIDAD				

Nota: Adaptado a partir de "Risk management methodology in the supply chain: a case study applied" (p.1058), por (Hermoso-Orzáez & Garzón-Moreno, 2022), Annals of Operations Research, 2 (313).

La evaluación del riesgo se realiza de manera personalizada para cada activo, tomando en cuenta cada amenaza y en todas las dimensiones de evaluación pertinentes. Hay dos enfoques desde los cuales se puede abordar el riesgo mencionado, estos son:

Riesgo acumulado potencial: Consideramos la suma total del impacto en el activo debido a una amenaza, junto con la probabilidad de esa amenaza. La fórmula para su cálculo es la siguiente:

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

La metodología para calcular el riesgo acumulado potencial se detalla en el Anexo H, y la Tabla 34 proporciona un ejemplo ilustrativo de dicha lista.

Tabla 34

Riesgo potencial acumulado de afectación de activos en la Biblioteca de la UTN

	Impacto Potencial Acumulado					Peso Ponderado
ACTIVOS - RIESGOS	**D**	**I**	**C**	**A**	**T**	
DATOS/INFORMACIÓN	**4.2**	**6.8**	**8.1**	**7.7**		
Base de datos	**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 la identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			4.4
[A.11] Acceso no autorizado		6.8	8.1			7.5
Documentación 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 la identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			4.4
[A.11] Acceso no autorizado		6.8	8.1			7.5
SERVICIOS	**7.2**	**7.2**	**6.8**	**6.8**	**7.4**	
Servidores internos	**7.2**	**7.2**	**6.8**	**6.8**	**7.4**	
[I.9] Interrupción de otros servicios o suministros esenciales	6.3					6.3
[E.1] Errores de los usuarios	5.1	5.1	5.1			3.4

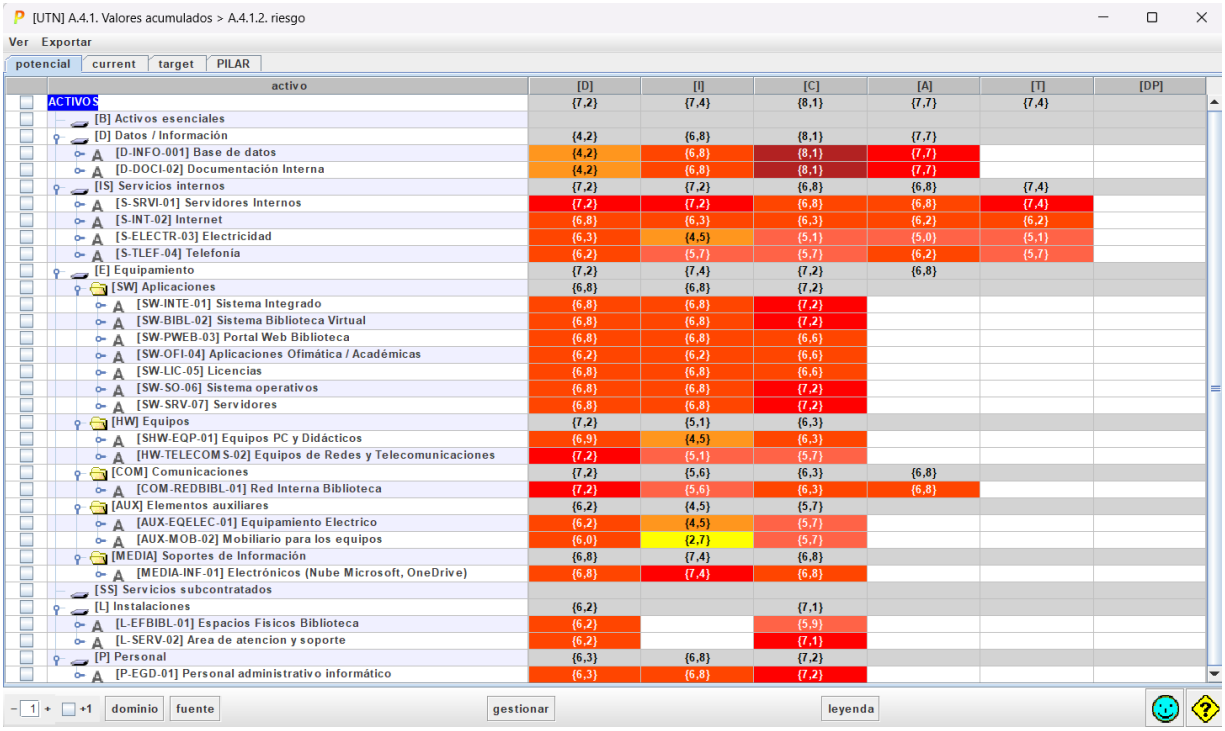
[E.2] Errores del administrador del sistema / de la seguridad	5.6	5.6	5.6			3.7
[E.15] Alteración de la información		5.1				5.1
[E.18] Destrucción de la información	5.1					5.1
[E.19] Fugas de información			5.1			5.1
[E.24] Caída del sistema por agotamiento de recursos	7.2					7.2
[A.5] Suplantación de la identidad		6.8	6.8	6.8		6.8
[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.19] Revelación de información			6.3			6.3
[A.24] Denegación de servicio	7.2					7.2
Internet	**6.8**	**6.3**	**6.3**	**6.2**	**6.2**	
[I.8] Fallo de servicios de comunicaciones	6.8					6.8
[E.15] Alteración de la información		5.1				5.1
[E.18] Destrucción de la información	5.1					5.1
[E.19] Fugas de información			5.1			5.1
[A.5] Suplantación de la identidad		6.2	6.2	6.2		6.2
[A.13] Repudio (negación de actuaciones)					6.2	6.2
[A.15] Modificación de la información		6.3				6.3
[A.18] Destrucción de la información	6.3					6.3
[A.19] Revelación de información			6.3			6.3
[A.24] Denegación de servicio	6.3					6.3
Electricidad	**6.3**	**4.5**	**5.1**	**5**	**5.1**	
[I.9] Interrupción de otros servicios o suministros esenciales	6.3					6.3
[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			3.9			3.9
[A.5] Suplantación de la identidad		4.5	5	5		4.8

Nota: La tabla presenta la evaluación del riesgo acumulado potencial, donde D: representa la disminución en la dimensión de disponibilidad, I: la disminución en integridad, C: la disminución en confidencialidad, A: la disminución en autenticidad, y T: la disminución en trazabilidad. Este análisis es resultado de Elaboración propia.

En la Figura 25 se presenta los valores de riesgo potencial acumulado en el software PILAR para cada activo identificado.

Figura 29:

Riesgo potencial acumulado de afectación de activos en la Biblioteca de la UTN en el software PILAR



Nota: Elaboración propia.

Riesgo potencial repercutido: Se considera el impacto repercutido en el activo debido a una amenaza y la probabilidad de la amenaza. La fórmula para calcular el riesgo potencial repercutido es la siguiente:

$$\textbf{\textit{Riesgo potencial repercutido}} = \textit{Probabilidad de amenaza} \times \textit{Valor repercutido del impacto}$$

La Tabla 35 contiene el cálculo del riesgo potencial repercutido.

Tabla 35

Riesgo potencial repercutido de afectación de activos en la Biblioteca de la UTN

	Impacto Potencial Repercutido					Peso Ponderado
ACTIVOS - RIESGOS	**D**	**I**	**C**	**A**	**T**	
Base de datos	4.2	6.8	8.1	7.7		6.7
Documentación Interna	4.2	6.8	8.1	7.7		6.7
Servidores Internos	7.2	7.2	6.8	6.8	7.4	7.0
Internet	6.8	6.3	6.3	6.2	6.2	6.4
Electricidad	6.3	4.5	5.1	5.0	5.1	5.2
Telefonía	6.2	5.7	5.7	6.2	5.7	6.0
Sistema Integrado	6.8	6.8	7.2			5.2
Sistema Biblioteca Virtual	6.8	6.8	7.2			5.2
Portal Web Biblioteca	6.8	6.8	6.6			5.1

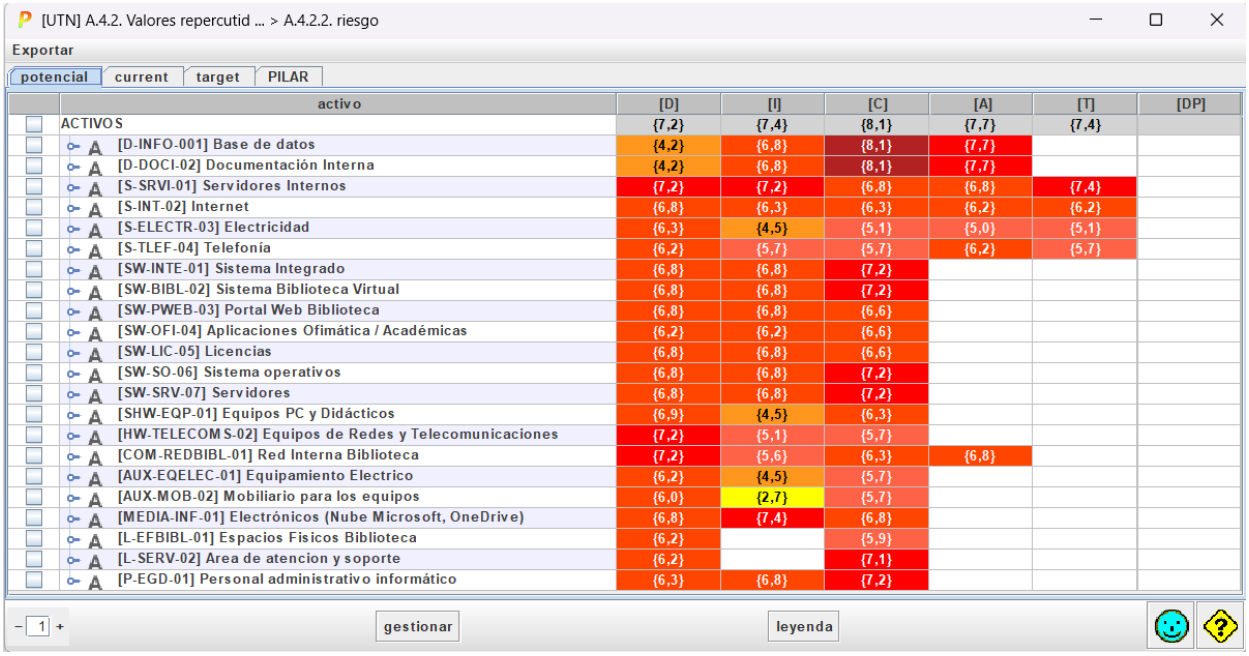
Aplicaciones Ofimática / Académicas	6.2	6.2	6.6		4.8
Licencias	6.8	6.8	6.6		5.1
Sistemas operativos	6.8	6.8	7.2		5.2
Servidores	6.8	6.8	7.2		5.2
Equipos PC y Didácticos	6.9	4.5	6.3		4.4
Equipos de Redes y Telecomunicaciones	7.2	5.1	5.7		4.5
Red Interna Biblioteca	7.2	5.6	6.3	6.8	6.5
Electrónicos (Nube Microsoft, OneDrive)	6.2	4.5	5.7		4.1
Equipamiento Eléctrico	6.0	2.7	5.7		3.6
Mobiliario para los equipos	6.8	7.4	6.8		5.3
Espacios Físicos Biblioteca	6.2		5.9		3.0
Área de atención y soporte	6.2		7.1		3.3
Encargado de la Dirección de Informática y Digitalización	6.3	6.8	7.2		5.1

Nota: La tabla presenta muestra el cálculo del riesgo potencial repercutido de los activos identificados en la Biblioteca de la 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 30 se presenta los valores de riesgo potencial repercutido en el software PILAR para cada activo.

Figura 30:

Riesgo potencial repercutido de afectación de activos en la Biblioteca de la UTN



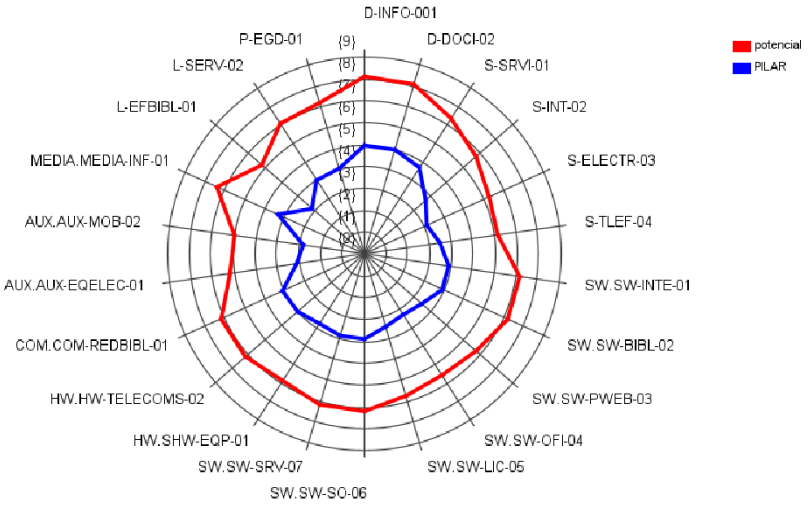
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{7,2}	{7,4}	{8,1}	{7,7}	{7,4}	
[D-INFO-001] Base de datos	{4,2}	{6,8}	{8,1}	{7,7}		
[D-DOCI-02] Documentación Interna	{4,2}	{6,8}	{8,1}	{7,7}		
[S-SRVI-01] Servidores Internos	{7,2}	{7,2}	{6,8}	{6,8}	{7,4}	
[S-INT-02] Internet	{6,8}	{6,3}	{6,3}	{6,2}	{6,2}	
[S-ELECTR-03] Electricidad	{6,3}	{4,5}	{5,1}	{5,0}	{5,1}	
[S-TLEF-04] Telefonía	{6,2}	{5,7}	{5,7}	{6,2}	{5,7}	
[SW-INTE-01] Sistema Integrado	{6,8}	{6,8}	{7,2}			
[SW-BIBL-02] Sistema Biblioteca Virtual	{6,8}	{6,8}	{7,2}			
[SW-PWEB-03] Portal Web Biblioteca	{6,8}	{6,8}	{6,6}			
[SW-OFI-04] Aplicaciones Ofimática / Académicas	{6,2}	{6,2}	{6,6}			
[SW-LIC-05] Licencias	{6,8}	{6,8}	{6,6}			
[SW-SO-06] Sistema operativos	{6,8}	{6,8}	{7,2}			
[SW-SRV-07] Servidores	{6,8}	{6,8}	{7,2}			
[SHW-EQP-01] Equipos PC y Didácticos	{6,9}	{4,5}	{6,3}			
[HW-TELECOMS-02] Equipos de Redes y Telecomunicaciones	{7,2}	{5,1}	{5,7}			
[COM-REDBIBL-01] Red Interna Biblioteca	{7,2}	{5,6}	{6,3}	{6,8}		
[AUX-EQELEC-01] Equipamiento Electrico	{6,2}	{4,5}	{5,7}			
[AUX-MOB-02] Mobiliario para los equipos	{6,0}	{2,7}	{5,7}			
[MEDIA-INF-01] Electrónicos (Nube Microsoft, OneDrive)	{6,8}	{7,4}	{6,8}			
[L-EFBIBL-01] Espacios Fisicos Biblioteca	{6,2}		{5,9}			
[L-SERV-02] Area de atencion y soporte	{6,2}		{7,1}			
[P-EGD-01] Personal administrativo informático	{6,3}	{6,8}	{7,2}			

Nota: Elaboración propia.

En la Figura 31 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 31:

Gráfico valores de riesgo acumulado de afectación de activos de la Biblioteca de la UTN



Nota: Elaboración propia.

El riesgo acumulado potencial, al evaluarse utilizando el valor acumulado de los activos del sistema, facilita la identificación de las medidas de protección durante el proceso de gestión de riesgos. En cambio, el riesgo potencial repercutido, al evaluarse sobre el valor

intrínseco de los activos, proporciona información únicamente sobre las consecuencias de posibles incidentes causados por amenazas.

Implementación del Plan de Gestión de Riesgos

2.7.7. Identificación de Salvaguardas

Antes de identificar las salvaguardas, es necesario estandarizar las amenazas según los riesgos potenciales acumulados (Anexo H) que han sido identificados con mayor peso. En este proceso, se consideró el promedio de pesos asociados con riesgos tecnológicos como el software malicioso, acceso no autorizado y alteración de la información, entre otros. El valor establecido fue de 5,6, lo que resultó en la identificación de 52 riesgos, detallados en el Anexo I. La Tabla 36 ya proporciona un listado de amenazas junto con los activos afectados.

Tabla 36

Riesgos de peso mayor identificados en la Biblioteca de la UTN

ACTIVO	AMENAZAS	PESO PONDERADO
Base de datos	[A.11] Acceso no autorizado	7.5
Documentación interna	[A.11] Acceso no autorizado	7.5
Servidores internos	[A.13] Repudio (negación de actuaciones)	7.4
Electrónicos (Nube Microsoft, OneDrive)	[A.15] Modificación de la información	7.4
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	7.2
Servidores internos	[A.15] Modificación de la información	7.2
Servidores internos	[A.24] Denegación de servicio	7.2
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	7.2
Red Interna Biblioteca	[A.24] Denegación de servicio	7.2
Personal administrativo informático	[A.19] Revelación de información	7.2
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio	7.1
Área de atención y soporte	[A.25] Robo de equipos	7.1
Base de datos	[A.5] Suplantación de la identidad	6.9
Documentación interna	[A.5] Suplantación de la identidad	6.9
Servidores internos	[A.5] Suplantación de la identidad	6.8
Internet	[I.8] Fallo de servicios de comunicaciones	6.8
Sistema Integrado	[A.8] Difusión de software dañino	6.8
Sistema Biblioteca Virtual	[A.8] Difusión de software dañino	6.8
Servidores	[A.8] Difusión de software dañino	6.8

Equipos de Redes y Telecomunicaciones	[I.6] Corte del suministro eléctrico	6.8
Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Equipos de Redes y Telecomunicaciones	[A.26] Ataque destructivo	6.8
Electrónicos (Nube Microsoft, OneDrive)	[I.6] Corte del suministro eléctrico	6.8
Electrónicos (Nube Microsoft, OneDrive)	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Electrónicos (Nube Microsoft, OneDrive)	[I.10] Degradación de los soportes de almacenamiento de la información	6.8
Electrónicos (Nube Microsoft, OneDrive)	[E.18] Destrucción de la información	6.8
Electrónicos (Nube Microsoft, OneDrive)	[A.18] Destrucción de la información	6.8
Sistema Integrado	[A.22] Manipulación de programas	6.6
Sistema Biblioteca Virtual	[A.22] Manipulación de programas	6.6
Sistemas operativos	[A.22] Manipulación de programas	6.6
Servidores	[A.22] Manipulación de programas	6.6
Personal administrativo informático	[A.29] Extorsión	6.6
Portal Web Biblioteca	[A.8] Difusión de software dañino	6.6
Licencias	[A.8] Difusión de software dañino	6.6
Equipos PC y Didácticos	[E.24] Caída del sistema por agotamiento de recursos	6.6
Equipos PC y Didácticos	[E.25] Pérdida de equipos	6.6
Equipos PC y Didácticos	[A.25] Robo de equipos	6.6
Equipos de Redes y Telecomunicaciones	[I.1] Fuego	6.6
Equipos de Redes y Telecomunicaciones	[I.*] Desastres industriales	6.6
Electrónicos (Nube Microsoft, OneDrive)	[I.1] Fuego	6.6
Electrónicos (Nube Microsoft, OneDrive)	[I.*] Desastres industriales	6.6
Equipos PC y Didácticos	[A.24] Denegación de servicio	6.5
Sistemas operativos	[A.8] Difusión de software dañino	6.5
Portal Web Biblioteca	[A.22] Manipulación de programas	6.4
Licencias	[A.22] Manipulación de programas	6.4
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	6.4
Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales	6.3
Servidores internos	[A.18] Destrucción de la información	6.3
Servidores internos	[A.19] Revelación de información	6.3

Internet	[A.15] Modificación de la información	6.3
Internet	[A.18] Destrucción de la información	6.3
Internet	[A.19] Revelación de información	6.3
Internet	[A.24] Denegación de servicio	6.3

Nota: Elaboración propia.

2.7.8. Criterio para el tratamiento de riesgos

Una vez que se han especificado los niveles de riesgo asociados con las amenazas que pueden impactar a cada activo de información, se definen los criterios para aceptar dichos riesgos. Estos criterios facilitan la identificación del tipo de riesgo y la determinación de la pertinencia de aplicar controles específicos. Para obtener información detallada sobre las acciones recomendadas, se puede hacer referencia a la Tabla 37.

Tabla 37

Criterios para tratamiento de riesgos

Zona	Acción a tomar
Aceptable	Aceptar
Tolerable	Transferir
Moderada	Reducir
Inaceptable	Evitar

Nota: Elaboración propia basada en ISO/IEC 27001, 2018

La Norma ISO 31000 en su apartado de Tratamiento de Riesgos, considera tres opciones de tratamiento, estos se encuentran en la Tabla 38.

Tabla 38

Opciones de Tratamiento del Riesgo según la Norma ISO 31000:2018

Tratamiento	Definición
Evitar	Eliminar la fuente del riesgo o cambiar el proyecto o actividad para reducir la probabilidad de ocurrencia.
Minimizar	Implementar medidas para minimizar la probabilidad de ocurrencia o reducir el impacto del riesgo.
Aceptar o Retener	Aceptar conscientemente el riesgo sin implementar medidas específicas de tratamiento. Esto se hace cuando el costo de mitigación es mayor que el beneficio esperado.

Nota: Adaptación propia a partir de Guía para la aplicación de UNE-ISO 31000:2018, por (Bonet et al, 2019). Asociación Española de Normalización y Certificación.

Es fundamental que la organización realice una vigilancia periódica de los riesgos identificados. Esto permitirá identificar los factores que los generan y, en consecuencia, asignar los recursos necesarios para abordarlos de manera efectiva.

A todos tipos de 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 39 presenta una muestra de dicho anexo.

Tabla 39

Asignación de opción de tratamiento a los riesgos identificados en la Biblioteca de la UTN

ACTIVO	RIESGO	PESO PONDERADO	ACCIÓN
Base de datos	[A.11] Acceso no autorizado	7.5	Minimizar
Documentación interna	[A.11] Acceso no autorizado	7.5	Minimizar
Servidores internos	[A.13] Repudio (negación de actuaciones)	7.4	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[A.15] Modificación de la información	7.4	Minimizar
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	7.2	Minimizar
Servidores internos	[A.15] Modificación de la información	7.2	Minimizar
Servidores internos	[A.24] Denegación de servicio	7.2	Minimizar
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	7.2	Minimizar
Red Interna Biblioteca	[A.24] Denegación de servicio	7.2	Minimizar
Personal administrativo informático	[A.19] Revelación de información	7.2	Evitar
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio	7.1	Minimizar
Área de atención y soporte	[A.25] Robo de equipos	7.1	Minimizar
Base de datos	[A.5] Suplantación de la identidad	6.9	Minimizar
Documentación interna	[A.5] Suplantación de la identidad	6.9	Minimizar
Servidores internos	[A.5] Suplantación de la identidad	6.8	Minimizar
Internet	[I.8] Fallo de servicios de comunicaciones	6.8	Minimizar
Sistema Integrado	[A.8] Difusión de software dañino	6.8	Minimizar
Sistema Biblioteca Virtual	[A.8] Difusión de software dañino	6.8	Minimizar
Servidores	[A.8] Difusión de software dañino	6.8	Minimizar

Equipos de Redes y Telecomunicaciones	[I.6] Corte del suministro eléctrico	6.8	Aceptar
Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8	Minimizar
Equipos de Redes y Telecomunicaciones	[A.26] Ataque destructivo	6.8	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.6] Corte del suministro eléctrico	6.8	Aceptar
Electrónicos (Nube Microsoft, OneDrive)	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.10] Degradación de los soportes de almacenamiento de la información	6.8	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[E.18] Destrucción de la información	6.8	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[A.18] Destrucción de la información	6.8	Evitar
Sistema Integrado	[A.22] Manipulación de programas	6.6	Minimizar
Sistema Biblioteca Virtual	[A.22] Manipulación de programas	6.6	Minimizar
Sistemas operativos	[A.22] Manipulación de programas	6.6	Minimizar
Servidores	[A.22] Manipulación de programas	6.6	Minimizar
Personal administrativo informático	[A.29] Extorsión	6.6	Evitar
Portal Web Biblioteca	[A.8] Difusión de software dañino	6.6	Minimizar
Licencias	[A.8] Difusión de software dañino	6.6	Minimizar
Equipos PC y Didácticos	[E.24] Caída del sistema por agotamiento de recursos	6.6	Minimizar
Equipos PC y Didácticos	[E.25] Pérdida de equipos	6.6	Minimizar
Equipos PC y Didácticos	[A.25] Robo de equipos	6.6	Minimizar
Equipos de Redes y Telecomunicaciones	[I.1] Fuego	6.6	Minimizar
Equipos de Redes y Telecomunicaciones	[I.*] Desastres industriales	6.6	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.1] Fuego	6.6	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.*] Desastres industriales	6.6	Minimizar
Equipos PC y Didácticos	[A.24] Denegación de servicio	6.5	Minimizar
Sistemas operativos	[A.8] Difusión de software dañino	6.5	Minimizar
Portal Web Biblioteca	[A.22] Manipulación de programas	6.4	Minimizar
Licencias	[A.22] Manipulación de programas	6.4	Minimizar
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	6.4	Evitar

Nota: Elaboración propia.

Después de asignar las estrategias de tratamiento para los riesgos, es importante tener en cuenta cuáles son las salvaguardas prioritarias en la gestión de riesgos. Estas salvaguardas son acciones que buscan minimizar el riesgo. En el documento llamado "Catálogo de Elementos", se detallan varios tipos de salvaguardas específicas para cada categoría de activo.

Para determinar las medidas de protección necesarias, es esencial considerar diversos aspectos, entre ellos:

- El tipo de activo que requiere resguardo.
- Las amenazas que se deben contrarrestar.
- Alternativas disponibles para salvaguardar.

Además, se aplicó el principio de proporcionalidad al evaluar los valores de los activos y la probabilidad de que las amenazas se materialicen.

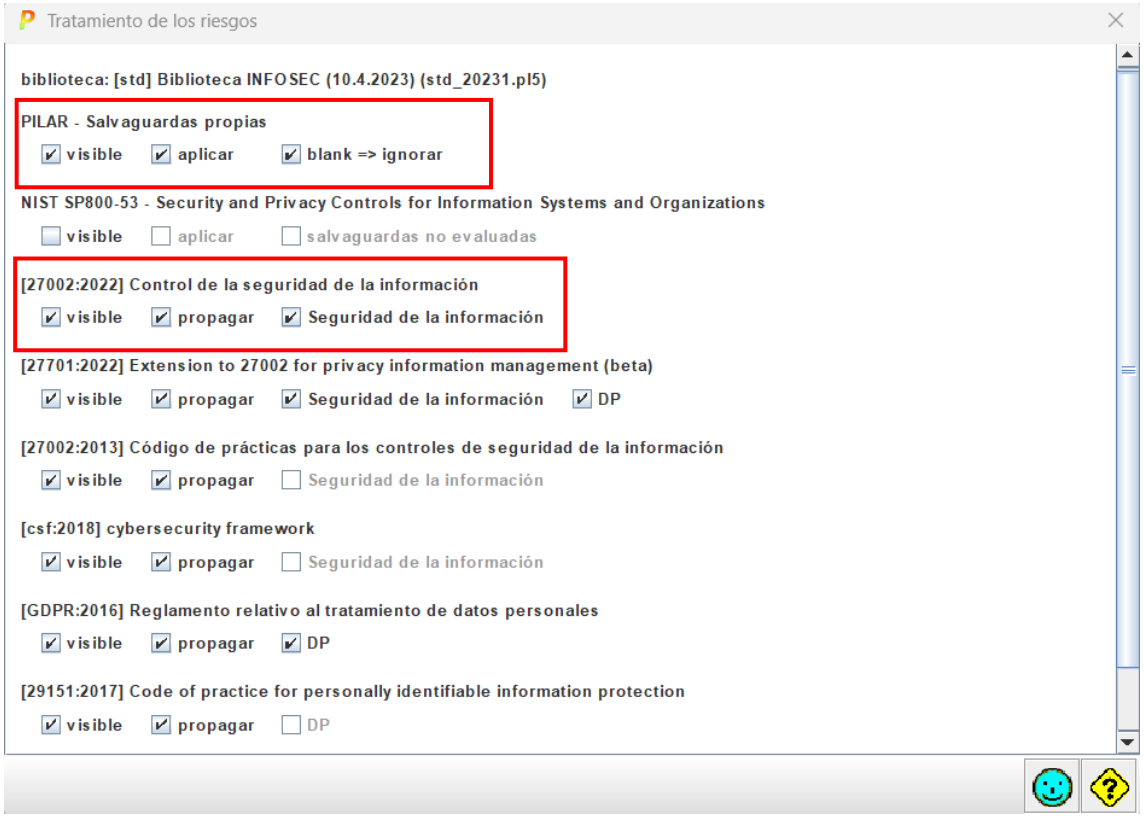
Las salvaguardas ofrecen distintos tipos de protección, que incluyen:

- [PR] Prevención: Reduce las posibilidades de que ocurra un incidente.
- [DS] Disuasión: Desalienta al atacante, disuadiéndolo de llevar a cabo el ataque.
- [EL] Eliminación: Impide que el incidente tenga lugar eliminando la posibilidad de su ocurrencia.
- [IM] Minimización del impacto: Limita las consecuencias de un incidente.
- [CR] Corrección: Repara el daño ya ocasionado.
- [RC] Recuperación: Facilita la restauración al estado previo al incidente.
- [MN] Monitorización: Supervisa eventos pasados y presentes para anticiparse a futuros incidentes.
- [DC] Detección: Identifica un ataque y notifica su ocurrencia.
- [AW] Concienciación: Ofrece formación a personas vinculadas al sistema.
- [AD] Administración: Constituyen los elementos de seguridad del sistema.

La herramienta PILAR ofrece la flexibilidad de realizar diversas modificaciones en su configuración para adaptarse a los requisitos específicos de gestión de riesgos de una organización. En este escenario particular, se ajustó la configuración de "Tratamiento del Riesgo" (salvaguardas) con el propósito de cumplir con los estándares de seguridad requeridos. Se utilizaron tanto las salvaguardas incorporadas en PILAR como las establecidas por la Norma ISO/IEC 27002:2022, que aborda la seguridad de la información, ciberseguridad y protección de la privacidad. Estas salvaguardas están diseñadas para asegurar la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información. La configuración específica se detalla en la Figura 32.

Figura 32:

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

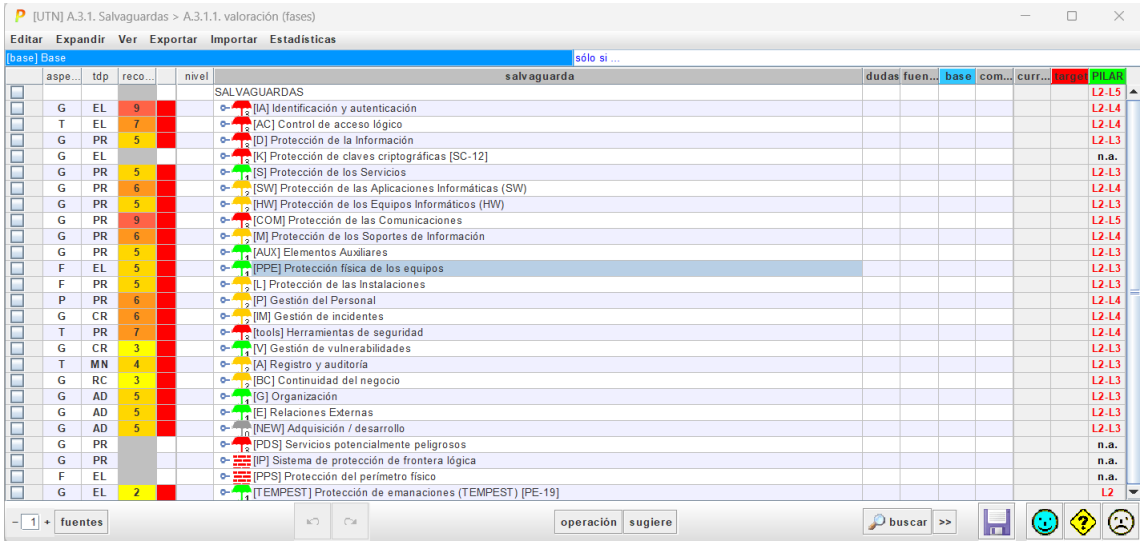


Nota: Elaboración propia.

Según la elección de los estándares de seguridad para abordar los riesgos, la metodología MAGERIT sugiere diferentes medidas de seguridad. En esta situación particular, se han identificado un total de 25 salvaguardas, las cuales están detalladas en la Figura 33.

Figura 33:

Identificación de salvaguardas para la Biblioteca de la UTN en el Software PILAR



Nota: Elaboración propia.

Diversos tipos de medidas de protección pueden ser empleados para gestionar una amenaza de manera efectiva. Para garantizar la implementación adecuada de estas medidas de protección, se requiere proponer distintas tareas que contribuyan a reducir la amenaza. En el Anexo K, se detalla una lista de activos, amenazas, categorías de salvaguardas y las tareas sugeridas para su implementación. Por otro lado, la Tabla 40 proporciona un ejemplo representativo de este listado.

Tabla 40

Identificación de Tareas por Salvaguardas para la Biblioteca de la UTN

ACTIVO AFECTADO	RIESGO	TRATAMIENTO	SALVAGUARDA	TIPO DE PROTECCIÓN	TAREA PROPUESTA
Base de datos	[A.11] Acceso no autorizado	Minimizar	[IA] Identificación y autenticación	EL	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario
Documentación interna	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
Servidores internos	[A.13] Repudio (negación de actuaciones)	Minimizar	[K] Protección de claves criptográficas	EL	Implementación del cifrado hash para el almacenamiento de contraseñas
Electrónicos (Nube Microsoft, OneDrive)	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Servidores internos	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN

Servidores internos	[A.24] Denegación de servicio	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	Minimizar	[V] Gestión de vulnerabilidades	PR	Desarrollar un manual de emergencia para las redes de comunicaciones
Red Interna Biblioteca	[A.24] Denegación de servicio	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)
Personal administrativo informático	[A.19] Revelación de información	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)

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 70 tareas, distribuidas entre 14 de los 25 tipos de salvaguardas aplicables a este caso de estudio. Estas tareas fueron revisadas por el encargado del Área de Informática y Digitalización y la Directora de la Biblioteca de la UTN para determinar si alguna de estas tareas ya está implantada. Esta información se la encuentra en la Tabla 41.

Tabla 41

Sintetización de Tareas propuestas para el cumplimiento de salvaguardas en la Biblioteca de la UTN

SALVAGUARDA	TIPO DE PROTECCIÓN	TAREA PROPUESTA	¿EXISTE?
[IA] Identificación y autenticación	EL	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario	SI
[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores	SI
[K] Protección de claves criptográficas	EL	Implementación del cifrado hash para el almacenamiento de contraseñas	NO
[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN	NO
[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software	NO
[BC] Continuidad del negocio	RC	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques	NO
[V] Gestión de vulnerabilidades	PR	Desarrollar un manual de emergencia para las redes de comunicaciones	NO
[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN	SI
[SW] Protección de las aplicaciones informáticas	PR	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)	NO

[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones	SI
[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso	SI
[BC] Continuidad del negocio	RC	Implementación de un Plan en caso de fallo de Internet	SI
[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte	NO
[AUX] Elementos auxiliares	PR	Corrección de la carga de dispositivos electrónicos en la distribución de red eléctrica	NO
[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware	SI
[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos	SI
[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)	/
[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de almacenamiento	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	Implementación de firewall para la red interna de la Biblioteca de la UTN	SI

Nota: Los valores en “¿Existente?” son; Si: Quiere decir que ya existe un proceso relacionado a esa tarea de salvaguarda, No: Quiere decir que No existe un proceso relacionado a esa tarea de salvaguarda, /: Existe un proceso que no es óptimo o no se lo ha implementado completamente para cumplir con esa tarea de salvaguarda. Elaboración propia.

Para concluir la identificación de medidas de protección, se seleccionarán aquellas que no estén presentes o cuyo proceso actual no sea eficiente. Se han identificado 48 tareas que se describirán de manera concisa en el Anexo L, presentadas en forma de tabla junto con estimaciones de presupuestos, personal y tiempos basados en consultas realizadas en Internet.

La ejecución de todas estas tareas implicaría un costo aproximado de $50,350.00, y el tiempo necesario sería variable dependiendo de la decisión de llevar a cabo una implementación simultánea de varias tareas.

2.7.9. Valoración de Salvaguarda

Después de introducir las actividades sugeridas para implementar medidas de seguridad, es crucial evaluar su eficacia.

La efectividad de estas medidas dependerá de su idoneidad y de la calidad de su implementación. En la Tabla 42, se muestra el nivel de eficacia de estas salvaguardas.

Tabla 42

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, por Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (Amutio Gómez et al., 2012b).

La evaluación de la efectividad se llevó a cabo considerando dos perspectivas: la actual y la proyectada. La dimensión actual se refiere al valor presente de la salvaguarda en caso de su implementación, mientras que la dimensión proyectada es el valor esperado una vez que haya sido implementada. Estas evaluaciones fueron realizadas en colaboración con el encargado del Área de Informática y Digitalización y de la Directora de la Biblioteca de la UTN y se detallan en la Tabla 43.

Tabla 43

Valoración eficacia de tareas para las salvaguardas en la Biblioteca de la UTN

N°	TAREA PROPUESTA	ACTUAL	OBJETIVO
1	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario	4	5
2	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores	1	4
3	Implementación del cifrado hash para el almacenamiento de contraseñas	0	3
4	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN	0	4
5	Establecimiento de un Plan de Mantenimiento de Hardware y Software	0	4
6	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques	0	4
7	Desarrollar un manual de emergencia para las redes de comunicaciones	0	4
8	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN	2	5
9	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)	0	4
10	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones	1	3
11	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso	2	4
12	Implementación de un Plan en caso de fallo de Internet	2	4
13	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte	0	3
14	Corrección de la carga de dispositivos electrónicos en la distribución de red eléctrica	0	4
15	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware	4	5

Nota: Elaboración propia.

Después de evaluar las actividades propuestas, es posible calcular un promedio de las actividades asociadas a cada medida de seguridad para obtener una evaluación global de las mismas. Este resultado se registra en la Tabla 44.

Tabla 44

Valoración de la eficacia de las salvaguardas en la Biblioteca de la UTN

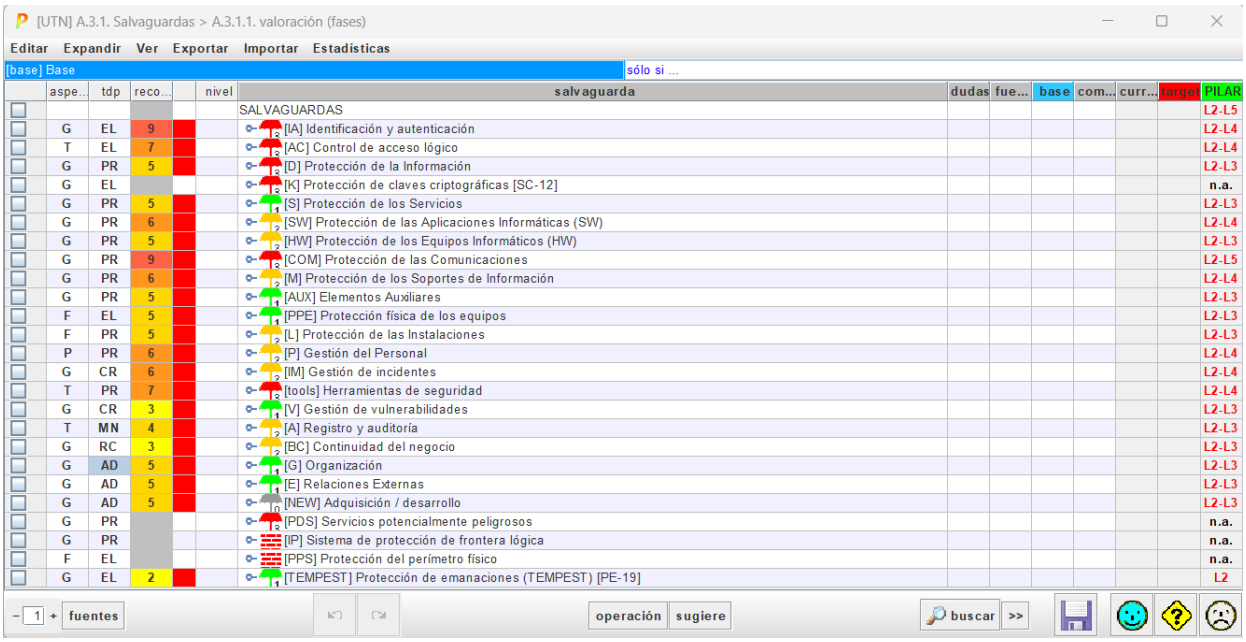
N°	SALVAGUARDA	ACTUAL	OBJETIVO
1	[IA] Identificación y autenticación	2	5
2	[AC] Control de acceso lógico	4	5
3	[K] Protección de claves criptográficas	2	4
4	[D] Protección de la información	4	5
5	[V] Gestión de vulnerabilidades	5	5
6	[BC] Continuidad del negocio	4	5
7	[P] Gestión del Personal	1	3
8	[SW] Protección de las aplicaciones informáticas	3	5
9	[PPS] Protección del perímetro físico	4	4
10	[AUX] Elementos auxiliares	1	3
11	[PPE] Protección física de los equipos	4	5
12	[S] Protección de los servicios	2	3
13	[HW] Protección de los equipos informáticos	3	5
14	[A] Registro y auditoría	2	4

Nota: Elaboración propia.

De igual manera, en la Figura 34 se nota que el programa PILAR posibilita la introducción de estos datos, incluyendo una sugerencia recomendada, con el fin de generar un resultado visual en forma de gráfico para evaluar el impacto y riesgo residual.

Figura 34:

Valoración de eficacia de salvaguardas de la Biblioteca de la UTN en el software PILAR



Nota: Elaboración propia.

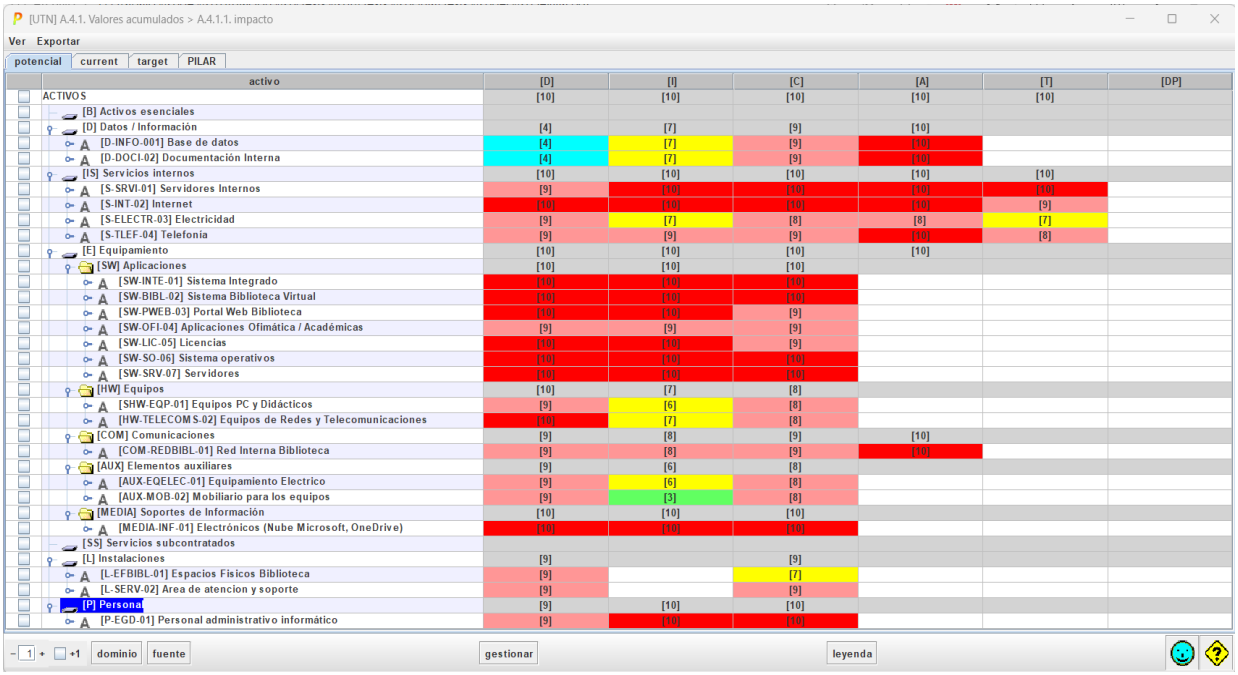
2.7.10. Estimación del Impacto Residual

Si las tareas propuestas para implementar las salvaguardas se ejecutan, el sistema altera su impacto potencial original a un impacto residual. Esto ocurre porque el software PILAR simula la implementación de las salvaguardas, proporcionando así una evaluación del impacto residual acumulado y el impacto residual repercutido.

La Figura 35 muestra el impacto residual acumulado, mientras que la Figura 36 representa el impacto residual repercutido.

Figura 35:

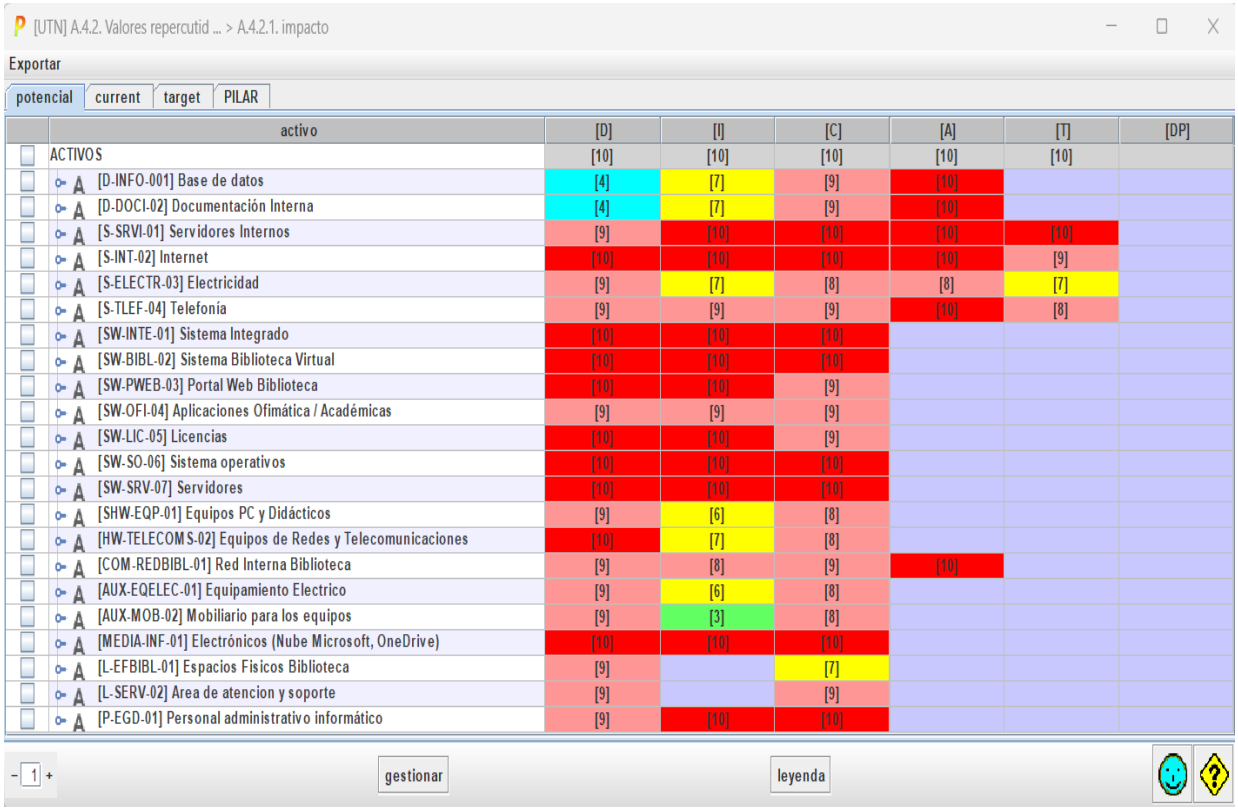
Impacto residual acumulado de afectación de activos de la Biblioteca de la UTN en el software PILAR



Nota: Elaboración propia.

Figura 36:

Impacto residual repercutido de afectación de activos de la Biblioteca de la UTN en el software PILAR



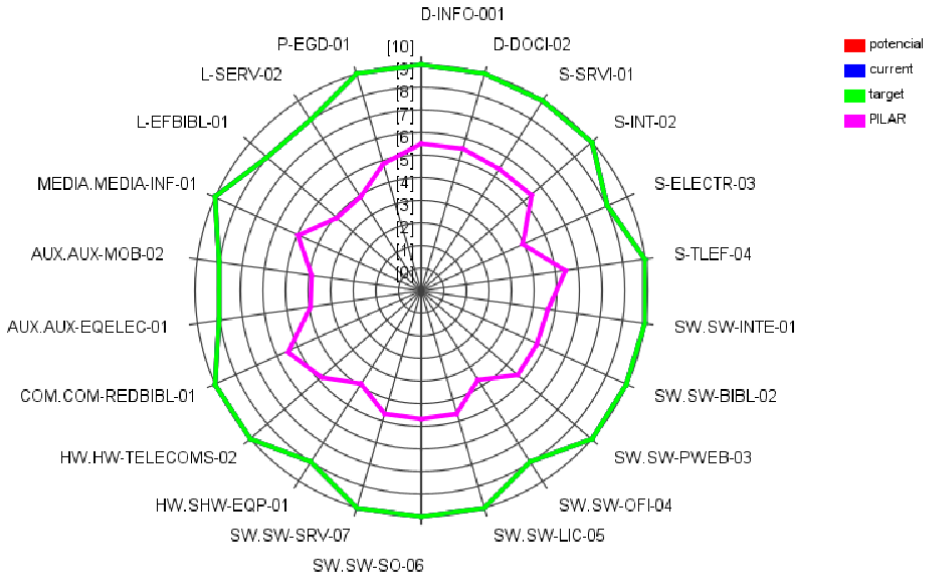
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	[10]	[10]	[10]	[10]	[10]	
[D-INFO-001] Base de datos	[4]	[7]	[9]	[10]		
[D-DOCI-02] Documentación Interna	[4]	[7]	[9]	[10]		
[S-SRVI-01] Servidores Internos	[9]	[10]	[10]	[10]	[10]	
[S-INT-02] Internet	[10]	[10]	[10]	[10]	[9]	
[S-ELECTR-03] Electricidad	[9]	[7]	[8]	[8]	[7]	
[S-TLEF-04] Telefonía	[9]	[9]	[9]	[10]	[8]	
[SW-INTE-01] Sistema Integrado	[10]	[10]	[10]			
[SW-BIBL-02] Sistema Biblioteca Virtual	[10]	[10]	[10]			
[SW-PWEB-03] Portal Web Biblioteca	[10]	[10]	[9]			
[SW-OFI-04] Aplicaciones Ofimática / Académicas	[9]	[9]	[9]			
[SW-LIC-05] Licencias	[10]	[10]	[9]			
[SW-SO-06] Sistema operativos	[10]	[10]	[10]			
[SW-SRV-07] Servidores	[10]	[10]	[10]			
[SHW-EQP-01] Equipos PC y Didácticos	[9]	[6]	[8]			
[HW-TELECOMS-02] Equipos de Redes y Telecomunicaciones	[10]	[7]	[8]			
[COM-REDBIBL-01] Red Interna Biblioteca	[9]	[8]	[9]	[10]		
[AUX-EQELEC-01] Equipamiento Electrico	[9]	[6]	[8]			
[AUX-MOB-02] Mobiliario para los equipos	[9]	[3]	[8]			
[MEDIA-INF-01] Electrónicos (Nube Microsoft, OneDrive)	[10]	[10]	[10]			
[L-EFBIBL-01] Espacios Fisicos Biblioteca	[9]		[7]			
[L-SERV-02] Area de atencion y soporte	[9]		[9]			
[P-EGD-01] Personal administrativo informático	[9]	[10]	[10]			

Nota: Elaboración propia.

Como se puede observar en la Figura 37 se presenta el gráfico resumen de los impactos potencial, actual, objetivo y recomendado que nos muestra el software PILAR

Figura 37:

Gráfico valores de impactos de afectación de activos de la Biblioteca de la UTN



Nota: Elaboración propia.

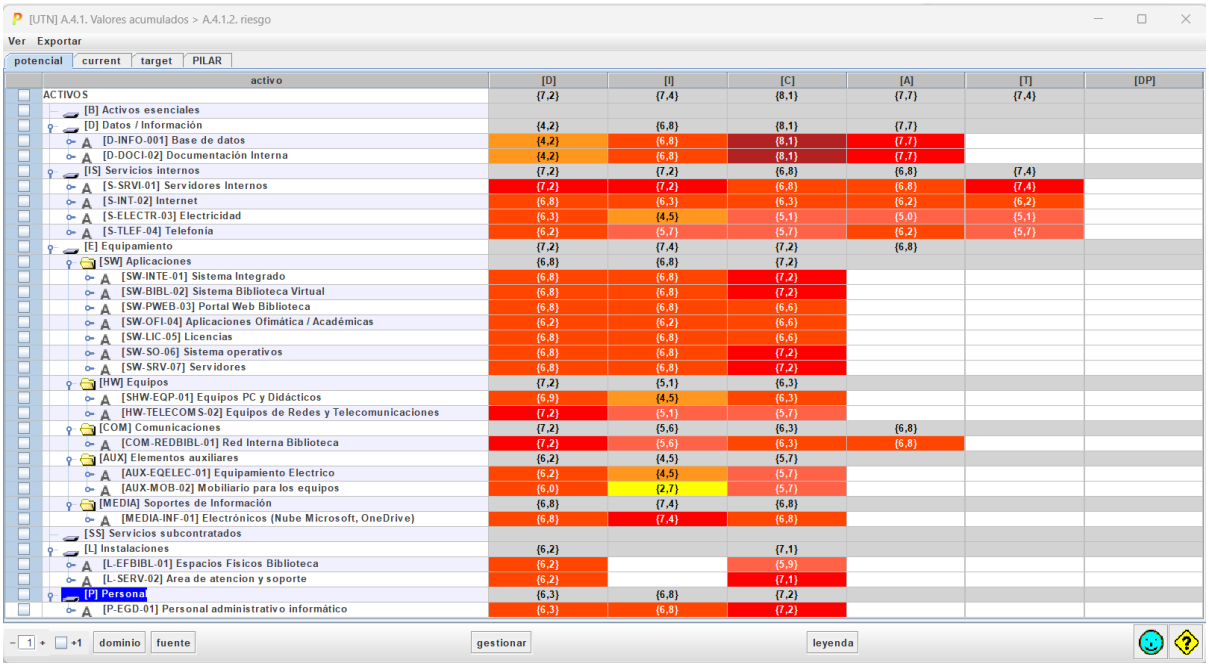
2.7.11. Estimación del Riesgo Residual

De manera similar al efecto persistente, el programa PILAR simula la implementación de salvaguardas, proporcionando así una evaluación del riesgo residual acumulado y el riesgo residual repercutido.

La representación del riesgo residual total se muestra en la Figura 38, mientras que la representación del riesgo residual repercutido se encuentra en la Figura 39.

Figura 38:

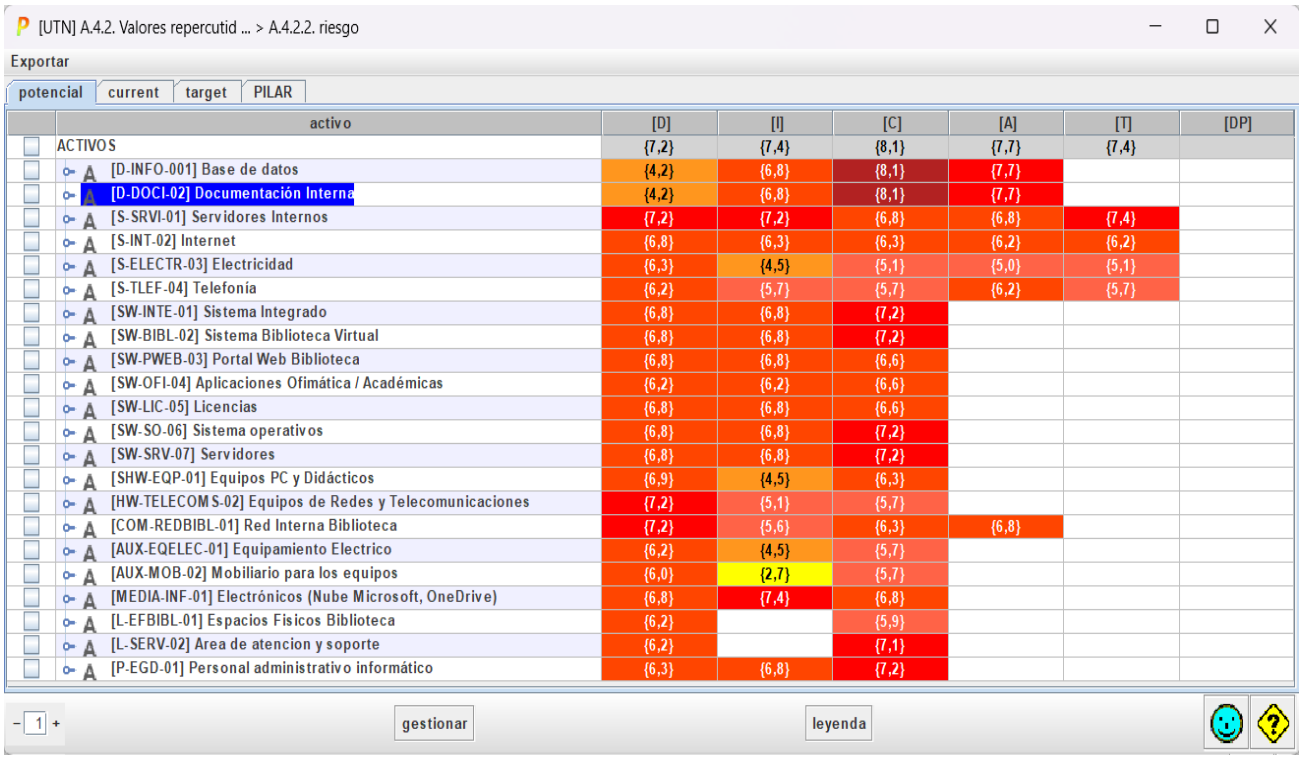
Riesgo residual acumulado de afectación de activos de la Biblioteca de la UTN en el software PILAR



Nota: Elaboración propia.

Figura 39:

Riesgo residual repercutido de afectación de activos de la Biblioteca de UTN en el software PILAR



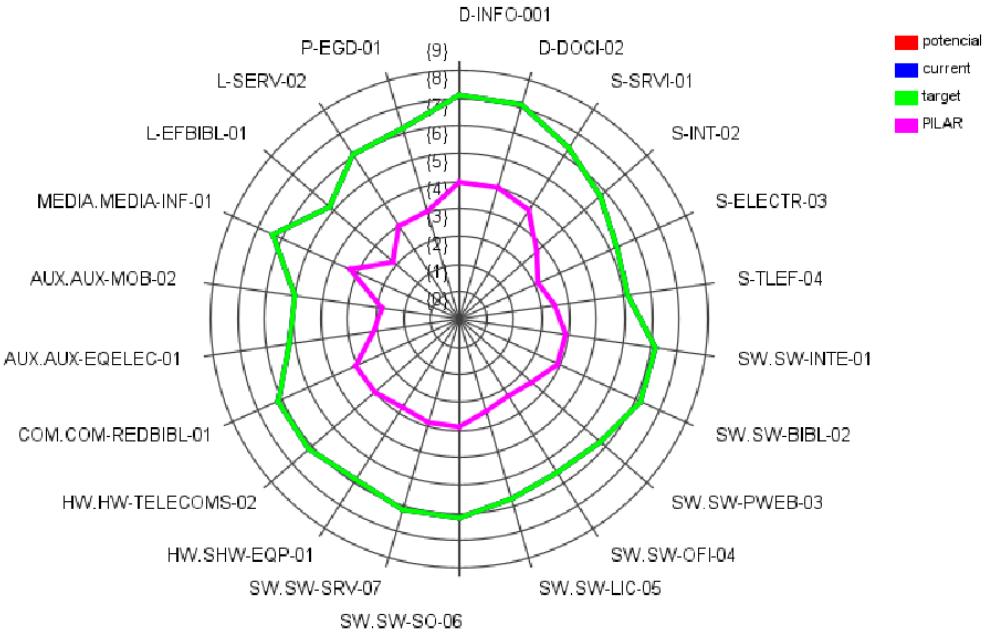
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{7,2}	{7,4}	{8,1}	{7,7}	{7,4}	
[D-INFO-001] Base de datos	{4,2}	{6,8}	{8,1}	{7,7}		
[D-DOCI-02] Documentación Interna	{4,2}	{6,8}	{8,1}	{7,7}		
[S-SRVI-01] Servidores Internos	{7,2}	{7,2}	{6,8}	{6,8}	{7,4}	
[S-INT-02] Internet	{6,8}	{6,3}	{6,3}	{6,2}	{6,2}	
[S-ELECTR-03] Electricidad	{6,3}	{4,5}	{5,1}	{5,0}	{5,1}	
[S-TLEF-04] Telefonía	{6,2}	{5,7}	{5,7}	{6,2}	{5,7}	
[SW-INTE-01] Sistema Integrado	{6,8}	{6,8}	{7,2}			
[SW-BIBL-02] Sistema Biblioteca Virtual	{6,8}	{6,8}	{7,2}			
[SW-PWEB-03] Portal Web Biblioteca	{6,8}	{6,8}	{6,6}			
[SW-OFI-04] Aplicaciones Ofimática / Académicas	{6,2}	{6,2}	{6,6}			
[SW-LIC-05] Licencias	{6,8}	{6,8}	{6,6}			
[SW-SO-06] Sistema operativos	{6,8}	{6,8}	{7,2}			
[SW-SRV-07] Servidores	{6,8}	{6,8}	{7,2}			
[SHW-EQP-01] Equipos PC y Didácticos	{6,9}	{4,5}	{6,3}			
[HW-TELECOMS-02] Equipos de Redes y Telecomunicaciones	{7,2}	{5,1}	{5,7}			
[COM-REDBIBL-01] Red Interna Biblioteca	{7,2}	{5,6}	{6,3}	{6,8}		
[AUX-EQELEC-01] Equipamiento Electrico	{6,2}	{4,5}	{5,7}			
[AUX-MOB-02] Mobiliario para los equipos	{6,0}	{2,7}	{5,7}			
[MEDIA-INF-01] Electrónicos (Nube Microsoft, OneDrive)	{6,8}	{7,4}	{6,8}			
[L-EFBIBL-01] Espacios Fisicos Biblioteca	{6,2}		{5,9}			
[L-SERV-02] Area de atencion y soporte	{6,2}		{7,1}			
[P-EGD-01] Personal administrativo informático	{6,3}	{6,8}	{7,2}			

Nota: Elaboración propia.

En la Figura 40 se presenta el gráfico resumen de los riesgo potencial, actual, objetivo y recomendado por el software PILAR.

Figura 40:

Gráfico valores de riesgo de afectación de activos de la Biblioteca de la UTN



Nota: Elaboración propia.

2.8. Fase 3 Seguimiento y Revisión

La etapa de Seguimiento y Revisión se lleva a cabo a través de las fases de Monitoreo, Confirmación y Mejora Continua, y tiene como objetivo verificar el adecuado cumplimiento de las funciones previstas en el Plan de Gestión de Riesgos, especialmente en lo que respecta a la mitigación y reducción de riesgos. Este proceso de revisión y seguimiento se representa gráficamente en la Figura 41 y sigue un ciclo continuo.

Figura 41:

Proceso Cíclico de Seguimiento y Revisión Plan de Gestión de Riesgos Biblioteca de la UTN.

Nota: Elaboración Propia

Debido al extenso período de tiempo que implicaría llevar a cabo el análisis de viabilidad y la implementación de las medidas de seguridad, se sugiere considerar esto como una tarea que se abordará en trabajos futuros. Mientras tanto, se contempla la propuesta de diseño del monitoreo.

2.8.1. Monitoreo

El Plan de Gestión de Riesgos, diseñado para una organización de pequeña escala con aproximadamente 1500 usuarios rotativos en un periodo de seis meses, sugiere realizar evaluaciones de monitoreo dos veces al año.

Durante este proceso, se recomienda llevar un registro detallado de los incidentes ocurridos en ese lapso. Este registro será elaborado por cualquier miembro encargado del Área de Informática y Digitalización de la Biblioteca de la UTN, utilizando una plantilla

de ficha diseñada en Microsoft Excel. Este documento será almacenado en una carpeta compartida en el servicio de Microsoft One Drive, identificada como "INCIDENCIA_RIESGOS_2024".

La plantilla se encuentra en la Tabla 45.

Tabla 45

Plantilla registro de incidentes de la Biblioteca de la UTN

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE SOFTWARE

Trabajo de Integracion Curricular

Registro de Incidencias y Riesgos 2023-2024

Nota: La siguiente matriz se realizó con el fin de recaudar información acerca de incidentes que puedan ocurrir posteriormente a la implementación de la gestión de riesgos en el Área de Informática y Digitalización de la Biblioteca de la UTN.

Instrucciones: Por favor ingrese los datos según corresponda, escoger de la lista desplegable en los casos que sea posible, caso contrario llenar como se crea conveniente.

	Nro.	FECHA Y HORA	RESPONSABLE	ACTIVO AFECTADO	AMENAZA IDENTIFICADA	IMPACTO	PROBABILIDAD	SALVAGUARDA	ACCIONES	EFECTIVIDAD (0-10)	COMENTARIO
Ejemplo	X	01/01/2023 08:00	Ixxx Cxxxx	Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	100%	1	[PPE] Protección física de los equipos	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware	9	Con el cambio de lugar los equipos de redes y telecomunicaciones tendran una mejor proteccion y podran funcionar mas tiempo
	1										
	2										
	3										
	4										
	5										
	6										
	7										
	8										
	9										
	10										

Nota: Elaboración propia

2.8.2. Valoración

Para evaluar adecuadamente el Plan de Gestión de Riesgos, se sugiere emplear un método comparativo, siguiendo el siguiente procedimiento:

I. Identificación de los riesgos más significativos en la etapa inicial (este trabajo de tesis) del proceso de Gestión de Riesgos.
II. Implementación de las actividades propuestas para llevar a cabo las salvaguardas, según la viabilidad evaluada por los encargados del Área de Informática y Digitalización de la Biblioteca de la UTN en un período de seis meses.
III. Recálculo del peso actualizado de los riesgos identificados en el paso I.
IV. Análisis y comparación de los pesos atribuidos a estos riesgos.

Es importante destacar que cualquier disminución mínima en el peso del riesgo se considera un logro en la reducción de las pérdidas asociadas con dichos riesgos.

2.8.3. Mejora Continua

La constante mejora continua del Plan de Gestión de Riesgos implica examinar los resultados obtenidos a través de la Evaluación, con el propósito de ajustar el Plan Existente en lo que respecta a las contramedidas destinadas a mitigar los riesgos residuales (salvaguardas). Este ajuste se logra mediante la propuesta de nuevas tareas, con el objetivo de reducir aún más los riesgos que puedan persistir.

2.9. Socialización

La sección de socialización desempeña un papel fundamental en la conclusión de la Implementación del Plan de Gestión de Riesgos.

Sus objetivos abarcan la compartición de conocimientos adquiridos a lo largo del proceso, la comunicación de las actividades realizadas, la explicación detallada de las tareas propuestas para la aplicación de salvaguardas, la presentación de la guía propuesta para el apartado de Seguimiento y Revisión del Plan, y la resolución de posibles dudas.

El proceso de socialización se llevó a cabo de manera presencial mediante una exposición respaldada por material didáctico elaborado con herramientas visuales "Power Point, Canva y Prezi", cuyos detalles se encuentran en el Anexo M.

El público objetivo consistió en el personal encargado del Área de Informática y Digitalización y la Directora de la Biblioteca de la UTN, Se estima que la duración de la socialización fue de aproximadamente una hora, seguida del tiempo destinado a preguntas y aclaraciones.

Paralelamente, se creó un documento entregable denominado "Plan de Gestión de Riesgos para la Biblioteca de la UTN 2023-2024", detallando todas las actividades en formato de informe. Este documento, junto con archivos adicionales como hojas de cálculo y el archivo .mgr referente al software PILAR, se entregan oficialmente a la persona a cargo del Área de Informática y Digitalización y a la Directora de la Biblioteca de la UTN.

Adicionalmente, con el objetivo de mejorar la conciencia sobre los riesgos presentes en la Biblioteca de la UTN, se diseñó material POP (afiches y trípticos) destinado a los usuarios de la Biblioteca, incluyendo tanto funcionarios como estudiantes. Este material se encuentra detallado en el Anexo N.

2.10. Análisis de Riesgos Cuantitativo

¿Qué es el análisis de riesgos cualitativo?

La evaluación cualitativa de riesgos implica calificar o puntuar los riesgos según la percepción individual sobre la gravedad y probabilidad de sus posibles consecuencias. El propósito de este análisis es generar una lista concisa de riesgos que requieran prioridad sobre otros.

La gestión de riesgos de manera cualitativa puede ser entendida como la principal salvaguardia en la gestión de proyectos. Funciona como una barrera inicial ante posibles amenazas al éxito del proyecto, abordando incluso aquellos riesgos que pueden no representar un daño significativo. Al priorizar la atención en los riesgos más críticos, los responsables del proyecto pueden optimizar la asignación de tiempo y recursos de manera más eficiente (SafetyCulture, 2023).

¿Qué es el análisis cuantitativo de riesgos?

La cuantificación del riesgo implica el cálculo del riesgo basado en la información recopilada. El propósito del análisis cuantitativo de riesgos es detallar con mayor precisión el impacto financiero que el riesgo puede tener en la empresa. Este proceso se logra al utilizar el conocimiento existente para prever o estimar posibles resultados.

Para que los datos sean aptos para el análisis cuantitativo de riesgos, es necesario haberlos examinado a lo largo de un extenso periodo o haberlos observado en diversas situaciones. Por ejemplo, si en los últimos cinco proyectos el equipo de tipo A falló después de 7 horas de uso, con esta información se puede inferir que, si un proyecto requiere que los trabajadores utilicen el equipo de tipo A durante 8 horas, existe un riesgo del 100% de que se rompa (SafetyCulture, 2023).

Diferencia entre el análisis cualitativo y cuantitativo

La principal distinción entre el análisis cualitativo y cuantitativo de riesgos radica en la base utilizada para evaluar dichos riesgos. Mientras que el análisis cualitativo se fundamenta en la percepción o juicio subjetivo de una persona, el análisis cuantitativo se apoya en datos verificables y específicos.

Otra disparidad se refiere a los valores asociados a los riesgos. En el análisis cualitativo, dicho valor se expresa mediante una calificación o puntuación asignada al riesgo, clasificándolo, por ejemplo, como "Bajo" o asignándole un valor de 1 para indicar que no requiere atención inmediata. Por otro lado, en el análisis cuantitativo de riesgos, el valor asociado suele expresarse en términos porcentuales, indicando la probabilidad de que el riesgo se materialice o cause un impacto negativo específico en los objetivos del proyecto.

Cuando realizar un análisis de riesgos cualitativo y cuantitativo

El examen cualitativo de riesgos se debe llevar a cabo al cambiar la percepción de un riesgo o al identificar uno nuevo. En términos generales, los gestores de proyectos deberían realizar un análisis cualitativo de riesgos al inicio de cada proyecto, ya que este proceso es fácil, rápido y de bajo costo. Además, puede llevarse a cabo en cualquier etapa del proyecto o cuando el director lo considere necesario.

En contraste, el análisis cuantitativo de riesgos se realiza cuando se cuenta con abundante información sobre el riesgo y su impacto, y se busca validar el análisis cualitativo. Debido a su complejidad y al tiempo requerido, la mayoría de los directores de proyectos no lo recomiendan, a menos que la seguridad del proyecto dependa de una estimación precisa del riesgo. En ciertos contextos, la realización de un análisis cuantitativo de riesgos puede ser obligatoria por ley o solicitada por las partes interesadas en el proyecto.

Cómo realizar un análisis de riesgos cuantitativo

Tras elegir el análisis de riesgos que mejor se adapta a su situación, los directores de proyecto pueden realizar el análisis de riesgos. Para aquellos que buscan una guía sobre cómo realizar análisis de riesgos cuantitativos, sigan los siguientes pasos:

Paso 1: Identificar el objetivo, el alcance y el método

Paso 2: Preparar los datos, las herramientas y las personas necesarias

Paso 3: Aplicar el método elegido a los datos recogidos

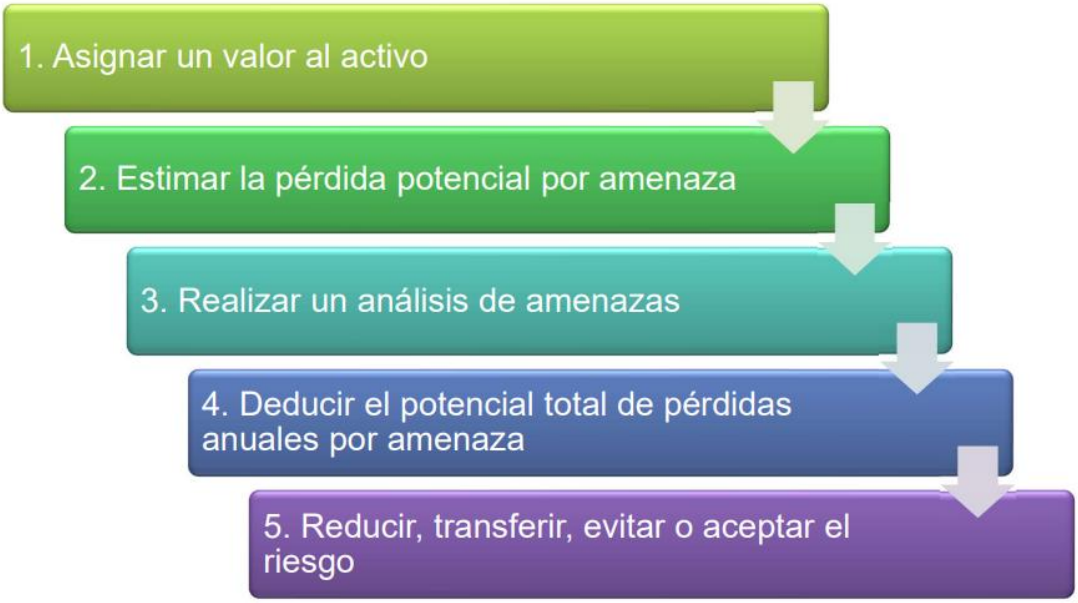


Figura 42: *Pasos para realizar un Análisis de Riesgos Cuantitativo*

Estimar la pérdida potencial por amenaza

SLE: (Expectativa de una Sola Pérdida)

SLE es el valor monetario que se pierde si la amenaza de un activo ocurre.

SLE = Valor del Activo x Factor de exposición.

Como se puede observar en la Figura 43 la fórmula para calcular el SLE

Figura 43:

Fórmula para calcular el SLE

SLE = Valor del Activo x Factor de exposición

Factor de exposición (EF: Exposure Factor) = porcentaje de pérdida que causaría la amenaza

Nota: Elaboración propia

Para poder calcular el SLE primero necesitamos saber el valor del activo y el Factor de exposición y se podrá realizar con la fórmula que se presentó anteriormente esto se presenta en la Tabla 46.

Tabla 46

Cálculo del SLE de los Activos de la Biblioteca de la UTN

Tipo de activos	Activo	Activo Agrupado	Valor del Activo	Perdida Potencial del Activo	AMENAZA	EF	SLE
Software	Sistema Integrado	Aplicaciones Informáticas	$1,800.00	$576.00	[A.15] Modificación de la información	68%	$1,224.00
	Sistema Biblioteca Virtual		$1,500.00	$480.00	[A.15] Modificación de la información	68%	$1,020.00
	Portal Web Biblioteca		$800.00	$272.00	[A.19] Revelación de información	66%	$528.00
Hardware	Monitores / Computadores	Equipos PC y Didácticos	$1,100.00	$374.00	[A.19] Revelación de información	66%	$726.00
	Asistente Digital Portátil		$5,600.00	$1,904.00			$3,696.00
	Impresora		$170.00	$57.80			$112.20
	Laptop		$1,500.00	$510.00			$990.00
	Proyector		$750.00	$255.00			$495.00
	Router	Equipos de Redes y Telecomunicaciones	$614.47	$172.05	[A.11] Acceso no autorizado	72%	$442.42
	Switch		$7,279.24	$2,038.19			$5,241.05
	Racks		$1,500.00	$420.00			$1,080.00
	Access Point		$1,503.67	$421.03			$1,082.64
	Cableado estructural		$200.00	$56.00			$144.00
Equipamiento auxiliar	Reguladores de Voltaje	Equipamiento Eléctrico	$35.00	$13.30	[A.30] Ingeniería social (picaresca)	62%	$21.70
	Fuentes de Poder		$50.00	$19.00			$31.00
	Cableado eléctrico		$250.00	$95.00			$155.00
	Fibra óptica		$150.00	$57.00			$93.00
	Cable de energía		$200.00	$76.00			$124.00
	UPS		$69.64	$26.46			$43.18
	NVR		$534.00	$202.92			$331.08
	Mobiliario para los equipos		$350.00	$133.00	[I.2] Daños por agua	48%	$217.00

Nota: Elaboración propia.

Realizar un análisis de las amenazas

Calcular la probabilidad de que cada amenaza se materialice.

Se debe calcular el ARO

- ARO: (Tasa anual de ocurrencia)
- Cuántas veces la amenaza se puede materializar en un periodo de 12 meses.

0.0 = Nunca

1.0 = Al menos 1 vez al año

Si ocurre cada 25 años:

ARO = 1/25 = 0.04

En la Tabla 47 se muestra la información sobre el ARO de los activos de la Biblioteca de la UTN.

Tabla 47

Probabilidad del ARO de los Activos de la Biblioteca de la UTN

Activo	Activo Agrupado	Valor del Activo	Perdida Potencial del Activo	AMENAZA	EF	SLE	ARO
Sistema Integrado	Aplicaciones Informáticas	$1,800.00	$576.00	[A.15] Modificación de la información	68%	$1,224.00	0.0
Sistema Biblioteca Virtual		$1,500.00	$480.00	[A.15] Modificación de la información	68%	$1,020.00	0.0
Portal Web Biblioteca		$800.00	$272.00	[A.19] Revelación de información	66%	$528.00	1.0
Monitores / Computadores	Equipos PC y Didácticos	$1,100.00	$374.00	[A.19] Revelación de información	66%	$726.00	0.2
Asistente Digital Portátil		$5,600.00	$1,904.00			$3,696.00	0.2
Impresora		$170.00	$57.80			$112.20	0.2
Laptop		$1,500.00	$510.00			$990.00	0.2
Proyector		$750.00	$255.00			$495.00	0.2
Router	Equipos de Redes y Telecomunicaciones	$614.47	$172.05	[A.11] Acceso no autorizado	72%	$442.42	1.0
Switch		$7,279.24	$2,038.19			$5,241.05	1.0
Racks		$1,500.00	$420.00			$1,080.00	1.0
Access Point		$1,503.67	$421.03			$1,082.64	1.0
Cableado estructural		$200.00	$56.00			$144.00	1.0
Reguladores de Voltaje	Equipamiento Eléctrico	$35.00	$13.30	[A.30] Ingeniería social (picaresca)	62%	$21.70	0.1
Fuentes de Poder		$50.00	$19.00			$31.00	0.1
Cableado eléctrico		$250.00	$95.00			$155.00	0.1
Fibra óptica		$150.00	$57.00			$93.00	0.1
Cable de energía		$200.00	$76.00			$124.00	0.1
UPS		$69.64	$26.46			$43.18	0.1
NVR		$534.00	$202.92			$331.08	0.1
Mobiliario para los equipos		$350.00	$133.00	[I.2] Daños por agua	48%	$217.00	0.07

Nota: Elaboración propia

Deducir el potencial total de pérdidas anuales por amenaza

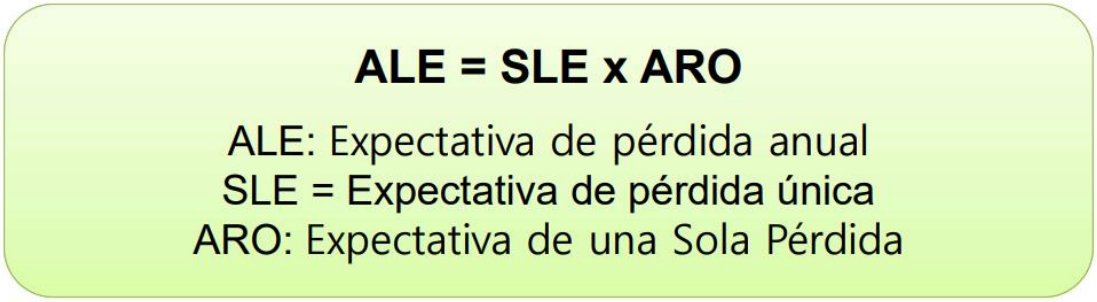
Calcular el ALE

ALE: (Expectativa de pérdida anual)

En la Figura 44 se muestra la fórmula para calcular el ALE

Figura 44:

Fórmula para calcular el ARO



Nota: Elaboración propia

Para poder calcular el ALE primero necesitamos saber el valor del SLE (Expectativa de pérdida única) y el valor del ARO (Expectativa de una Sola Pérdida) y se podrá realizar con la fórmula que se presentó anteriormente esto se presenta en la Tabla 48.

Tabla 48

Cálculo del ALE de los Activos de la Biblioteca de la UTN

Activo	Activo Agrupado	Valor del Activo	Perdida Potencial del Activo	AMENAZA	EF	SLE	ARO	ALE
Sistema Integrado	Aplicaciones Informáticas	$1,800.00	$576.00	[A.15] Modificación de la información	68%	$1,224.00	0.0	$0.0
Sistema Biblioteca Virtual		$1,500.00	$480.00	[A.15] Modificación de la información	68%	$1,020.00	0.0	$0.0
Portal Web Biblioteca		$800.00	$272.00	[A.19] Revelación de información	66%	$528.00	1.0	$528.0
Monitores / Computadores	Equipos PC y Didácticos	$1,100.00	$374.00	[A.19] Revelación de información	66%	$726.00	0.2	$145.20
Asistente Digital Portátil		$5,600.00	$1,904.00			$3,696.00	0.2	$739.20
Impresora		$170.00	$57.80			$112.20	0.2	$22.44
Laptop		$1,500.00	$510.00			$990.00	0.2	$198.00
Proyector		$750.00	$255.00			$495.00	0.2	$99.00
Router	Equipos de Redes y Telecomunicaciones	$614.47	$172.05	[A.11] Acceso no autorizado	72%	$442.42	1.0	$442.42
Switch		$7,279.24	$2,038.19			$5,241.05	1.0	$5241.05
Racks		$1,500.00	$420.00			$1,080.00	1.0	$1080.00
Access Point		$1,503.67	$421.03			$1,082.64	1.0	$1082.64
Cableado estructural		$200.00	$56.00			$144.00	1.0	$144.00
Reguladores de Voltaje	Equipamiento Eléctrico	$35.00	$13.30	[A.30] Ingeniería social (picaresca)	62%	$21.70	0.1	$2.17
Fuentes de Poder		$50.00	$19.00			$31.00	0.1	$3.10
Cableado eléctrico		$250.00	$95.00			$155.00	0.1	$15.50
Fibra óptica		$150.00	$57.00			$93.00	0.1	9.30
Cable de energía		$200.00	$76.00			$124.00	0.1	12.40
UPS		$69.64	$26.46			$43.18	0.1	4.32
NVR		$534.00	$202.92			$331.08	0.1	33.11
Mobiliario para los equipos		$350.00	$133.00	[I.2] Daños por agua	48%	$217.00	0.07	14.47

Nota: Elaboración propia

CAPÍTULO 3

Resultados

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

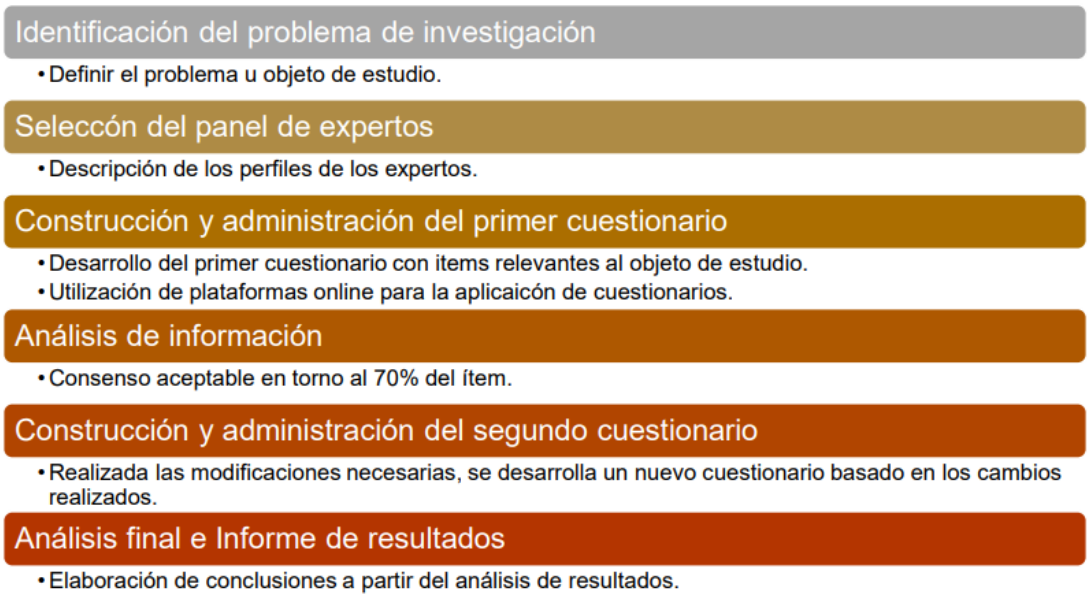
Después de completar el diseño e implementación del Plan de Gestión de Riesgos, es crucial confirmar el éxito de su elaboración. Para verificar la eficacia de este documento, específicamente el Plan de Gestión de Riesgos Tecnológicos, se ha elegido realizar una evaluación utilizando el método Delphi.

El enfoque Delphi es una técnica interactiva e iterativa para recopilar información, donde se aprovecha la experiencia de expertos en el campo con el fin de alcanzar los objetivos de una investigación. En distintas rondas, cada experto responde a un cuestionario diseñado en relación con el tema de estudio, y se realiza un proceso de retroalimentación correspondiente.

Se considera a seis como los elementos pertenecientes al método Delphi de consulta a expertos

Figura 45:

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.

3.1.1. 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 la Biblioteca de la 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.

3.1.2. Selección del panel de expertos

(García et al., 2013) asegura que el conjunto se conoce comúnmente como panel, y su composición precisa es fundamental, ya que puede influir en los resultados alcanzados. Es esencial tomar decisiones fundamentadas sobre el número de participantes necesarios para la consulta, así como establecer los criterios para su inclusión o exclusión en el panel.

Los especialistas asumen la responsabilidad de expresar juicios y opiniones, que constituyen el núcleo del método. Los criterios para seleccionarlos varían según la naturaleza del tema y el propósito del estudio. En algunos casos, se eligen expertos con un enfoque tradicional, como médicos especialistas o subespecialistas, considerando su nivel de conocimiento, experiencia, publicaciones y prestigio en su campo.

En situaciones diferentes, los expertos pueden ser personas afectadas por una situación, como pacientes de una clínica, quienes no necesariamente tienen conocimientos especializados, pero forman parte del grupo sobre el cual se aplicará la decisión del estudio. Además, el grupo de expertos puede estar compuesto por individuos con la capacidad de clarificar, sintetizar o estimular, que no pertenecen a ninguna de las dos categorías anteriores, como profesores y/o estudiantes de medicina con creatividad y motivación frente al problema del estudio. Según Powell, aspectos clave de la técnica incluyen el número y la calidad de los expertos participantes (Varela-Ruiz et al., 2012).

En el estudio realizado por (García et al., 2013) Los criterios comúnmente considerados incluyen:

a) La profesión
b) El cargo
c) La experiencia laboral,
d) La categoría docente, el grado científico,

e) La afiliación a un grupo o centro específico,

f) La vinculación actual con la actividad y el tipo de capacitación especializada.

La inclusión en un panel puede requerir estándares más rigurosos dependiendo de la sensibilidad del tema a investigar, como el número de investigaciones relacionadas, la relevancia y el impacto de las publicaciones, así como las citas recibidas por sus trabajos. Además, se ha utilizado con menor aceptación un Coeficiente de Competencia, el cual se calcula a partir de una escala de autoevaluaciones solicitadas a los posibles candidatos (García et al., 2013).

En cuanto al número ideal, según investigaciones previas de la Rand Corporation, se ha observado que, a partir de un mínimo de siete expertos, la tasa de error disminuye significativamente con la incorporación de cada experto adicional. Sin embargo, (García et al., 2013) advierte que no se recomienda contar con más de 30 expertos, ya que el beneficio en términos de mejora en la precisión es mínimo, y el aumento en los costos de investigación no justifica dicha mejora. En la práctica, se observa una amplia variabilidad y una inclinación hacia paneles compuestos por un número mayor de expertos.

Tabla 49

Expertos seleccionados para la validación con el Método Delphi

N°	Institución	Categoría de la Institución	Grado Académico
E1	Universidad de las Fuerzas Armadas ESPE	Institución Pública de Educación Superior	Magíster en Evaluación y Auditoría de Sistemas Tecnológicos
E2	Universidad Técnica del Norte	Institución Pública de Educación Superior	Ingeniera en Sistemas Computacionales
E3	Universidad Técnica del Norte	Institución Pública de Educación Superior	Ingeniero de Software

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

El número de rondas llevadas a cabo en el método Delphi puede variar según las exigencias y la complejidad del objeto de estudio. En este contexto, se sugiere limitar las rondas a un máximo de dos para evitar una prolongada validación.

3.1.3. Construcción y administración del cuestionario inicial

Una vez que se estableció el propósito de la investigación, se diseñó un cuestionario compuesto por 10 preguntas, las cuales se centrarán en el objetivo de la investigación y abordarán los aspectos más relevantes del Plan de Gestión de Riesgos. Este cuestionario

inicial se detalla en el Anexo O. La recopilación de datos se llevó a cabo de manera electrónica, con la invitación a participar enviada a través de correo electrónico. Se acordó que el período previsto entre el envío de la información y la recepción de respuestas sería de una semana laborable. La información enviada incluía el informe del Plan de Gestión de Riesgos y un enlace para acceder 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 que se presenta en la Tabla 50.

Tabla 50

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.

3.1.4. 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 determinar el índice de validez de contenido reflejada por cada ítem, se aplica la siguiente fórmula:

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

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

Según la literatura especializada, un instrumento de evaluación se considera válido cuando su Índice de Validez de Contenido (CVI) total es igual o superior al 90%. Asimismo, cada ítem debe poseer un CVI mayor o igual al 78% para ser considerado válido. La consecución de estos valores se interpreta como la obtención de un consenso. En caso de no alcanzarse estos criterios, es posible solicitar comentarios o sugerencias para mejorar y/o eliminar ítems.

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

Estadística Descriptiva: La estadística descriptiva constituye una parte esencial de la estadística, enfocándose en la recolección, organización, representación y resumen de datos numéricos con el propósito de comprender y comunicar de manera clara y eficiente las características fundamentales de la información. Esta área de estudio proporciona las herramientas y técnicas necesarias para analizar de manera significativa grandes conjuntos de datos, siendo crucial en diversos ámbitos que van desde la investigación científica hasta los estudios de mercado y en la toma de decisiones empresariales (J. Rodríguez, 2023).

Alfa de Cronbach: El índice alfa de Cronbach es una métrica empleada para analizar la confiabilidad o coherencia interna de un conjunto de escalas o elementos de evaluación en un cuestionario.

La interpretación del coeficiente implica tener en cuenta el valor esperado máximo de 0.90. Si el coeficiente supera este valor, se sugiere que la información puede contener duplicaciones o redundancias, lo que indica la necesidad de eliminar algunos ítems. Por otro lado, se considera un valor aceptable mínimo de 0.70; cualquier cifra por debajo de este umbral indica una consistencia interna baja. En consecuencia, se prefiere que los valores estén en el rango de 0.80 a 0.90.

A continuación, en la Tabla 51 se indican los resultados obtenidos por parte de los expertos.

Tabla 51

Resultados primer cuestionario a expertos

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
E1	1	2	1	1	1	1	2	1	1	Ninguno
E2	1	1	2	1	1	1	2	1	2	No, no lo cambiaria
E3	1	1	1	1	2	1	1	1	1	No

Nota: La tabla indica los datos obtenidos en el cuestionario, donde P son las preguntas y E son los expertos. Elaboración propia

Para calcular los índices de validez del contenido, se requiere una tabla de respuestas por pregunta y valor en la escala Likert. Esta matriz se puede encontrar en la Tabla 52 y gráficamente en la Figura 46.

Tabla 52

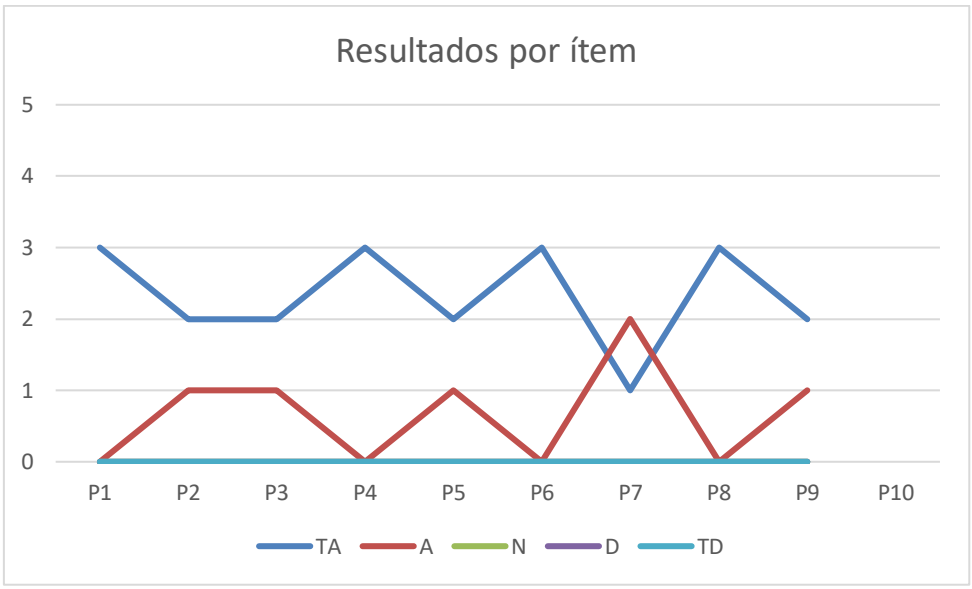
Tabulación respuestas del primer cuestionario a expertos por pregunta y valor en la escala de Likert

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

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

Figura 46:

Respuestas por ítem del primer cuestionario a expertos



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

Después de que las respuestas fueron tabuladas, se pueden hacer los cálculos de Índice de Validez de Contenido con las fórmulas anteriormente mencionadas. Estos se presentan en la Tabla 53.

Tabla 53

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 y Áreas Tecnológicas como la "Biblioteca de la UTN"?	-	-	-	-	100%	100%
2. ¿En su opinión, el Plan de Gestión de Riesgos Tecnológicos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización" es un informe fácil de comprender?	-	-	-	33.3%	66.7%	100%
3. ¿A su criterio, el informe del Plan de Gestión de Riesgos Tecnológicos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización" cuenta con la información necesaria?	-	-	-	33.3%	66.7%	100%
4. ¿En su opinión, la selección de la norma ISO/IEC 31000 para el desarrollo del Plan de Gestión de Riesgos Tecnológicos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización" fue acertada?	-	-	-	-	100%	100%
5. ¿Considera usted, que los pasos desarrollados en el Plan de Gestión de Riesgos Tecnológicos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización" fueron los necesarios?	-	-	-	33.3%	66.7%	100%
6. ¿A su criterio, 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 Biblioteca de la UTN "Área de Informática y Digitalización"?	-	-	-	-	100%	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 Biblioteca de la UTN "Área de Informática y Digitalización" fueron las idóneas?	-	-	-	66.7%	33.3%	100%
8. ¿Considera usted, ¿Qué el Plan de Gestión de Riesgos cumplió con su objetivo	-	-	-	-	100%	100%

de identificación, análisis y mitigación de riesgos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización"?						
9. ¿A su criterio, el Plan de Gestión de Riesgos Tecnológicos desarrollado para el departamento de Biblioteca de la UTN "Área de Informática y Digitalización", ¿puede ser aplicado en otras Instituciones de Educación Superior?	-	-	-	33.3%	66.7%	100%
10. ¿Cambiaría usted algún elemento presentado en el Plan de Gestión de Riesgos Tecnológicos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización", ¿Cuál sería?	-	-	-	-	-	-
IVC TOTAL				100%		

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

En la primera fase de encuestas, se logró un Índice de Validez de Contenido (IVC) Total del 100%, un puntaje considerado adecuado según la literatura para validar el cuestionario. Todas las preguntas presentan un IVC de ítem igual o superior al 90%, indicando un consenso en los resultados y sugiriendo que no es necesario modificar ni eliminar ítems.

Además de evaluar el IVC, se aplicó la técnica estadística Alfa de Cronbach al cuestionario completo para confirmar su validez. La fórmula para calcular 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 54, mientras que los cálculos del alfa de Cronbach en la Tabla 55.

Tabla 54

Varianza de ítems del primer cuestionario a expertos

	P1	P2	P3	P4	P5	P6	P7	P8	P9	Sumatoria
E1	2	2	2	1	2	1	2	2	1	15
E2	2	2	2	2	3	1	3	2	1	18
E3	1	1	2	1	2	1	2	1	1	12
Varianza	0.22	0.22	0.00	0.22	0.22	0.00	0.22	0.22	0.00	6.00

Nota: P: Preguntas del cuestionario, E: Número de expertos. Elaboración propia

Tabla 55

Alfa de Cronbach del primer cuestionario a expertos

K	9
Suma de Varianzas (Vi)	1.33
Varianza Total (Vt)	6.0
Cronbach	**0.88**

Nota: Elaboración propia

La puntuación del Alfa de Cronbach es de 0,88, lo que está en un rango aceptable para la validez interna del cuestionario puesto que la literatura nos dice que en una categoría de 0.72 a 0.99 su confiabilidad es excelente.

A pesar de ello, el ítem 10 se considera una pregunta argumentativa referente a si se optaría por algún cambio o mejora en el Plan de Gestión de Riesgos realizado. Pero como no hay sugerencias ni observaciones no sería necesario una segunda ronda del método Delphi.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La exploración y revisión de la literatura resultó ser un paso fundamental para obtener una comprensión clara de los conceptos asociados con la gestión de riesgos tecnológicos en el ámbito de Tecnologías de la Información (TI). Este proceso fue esencial para llevar a cabo la comparación y selección de la normativa y la metodología necesarias para desarrollar y definir el presente trabajo de titulación.

2. El análisis de la gestión de riesgos en la Dirección de Biblioteca de la UTN se llevó a cabo a través de la aplicación de la norma ISO 31000 versión 2018 y el Software PILAR. La Biblioteca de la UTN considera la gestión de riesgos como una estrategia que ha generado valor y ha cultivado una cultura preventiva. Como resultado de este estudio, se puede concluir que la norma ISO 31000 promueve una gestión de riesgos proactiva, centrada en la prevención en lugar de la reacción, lo que contribuye a mejorar la calidad de la información y la gestión empresarial.

3. El Plan de Gestión de Riesgos ayudo a la identificación de riesgos tecnológicos asociados a la seguridad de la información, tales como la alteración, destrucción y acceso no autorizado. No obstante, también se detectaron riesgos tecnológicos con enfoques diversos, como el robo de equipos, eventos naturales e industriales adversos, la denegación de servicios y la propagación de software perjudicial. A partir de esta fundamentación y la comparación realizada en el primer capítulo, se llega a la conclusión de que la elección de la Norma ISO/IEC 31000:2018 conjunto con el Software PILAR fueron las herramientas más apropiadas para el proceso de Gestión de Riesgos, ya que no se limita a un único tipo de riesgo.

4. La utilización del método Delphi para validar el Plan de Gestión de Riesgos posibilitó obtener la perspectiva de diversos especialistas respecto al informe elaborado. Estos expertos lo describieron como esencial, respaldado, claro, susceptible de reproducción, y acertado en la elección de normativas, metodologías y herramientas de software.

5. La ejecución del Plan de Gestión de Riesgos generó efectos positivos entre los miembros del equipo de los Laboratorios, ya que, gracias al informe elaborado, tienen la capacidad de llevar a cabo diversas acciones, tales como la

identificación de los activos más críticos, el reconocimiento de amenazas y riesgos existentes, y la disponibilidad de opciones para mitigar el impacto de estos mediante la implementación de medidas de seguridad propuestas.

6. La aplicación de la norma ISO/IEC 31000:2018 fue altamente positiva, demostrando un rendimiento destacado al ser adaptable a diversas organizaciones y fácilmente integrable con distintas metodologías de gestión de riesgos. Asimismo, la experiencia con la Metodología MAGERIT resultó satisfactoria, permitiendo la optimización eficiente de tiempos y esfuerzos gracias a sus ventajas, como la disponibilidad en español e inglés, tres documentos digitales gratuitos y la herramienta de software "PILAR".

Recomendaciones

1. Se sugiere incorporar de manera continua la revisión de literatura por parte de los encargados de la Dirección de Biblioteca en futuros proyectos relacionados con la gestión de riesgos en entornos tecnológicos, aprovechando sus beneficios para la toma de decisiones informadas. Se recomienda mantener actualizada la revisión bibliográfica para estar al tanto de las mejores prácticas, normativas y metodologías actualizadas, asegurando así la optimización continua de la gestión de riesgos en proyectos académicos o profesionales. Este enfoque constante garantizará la pertinencia y eficacia de las decisiones basadas en la información más reciente.

2. Utilizar estrategias anticipadas es otra de las recomendaciones que podría aplicar la Biblioteca de la UTN, además de implementar otras herramientas y normas internacionales como la Norma ISO 31000, ISO 9001, ISO 27002, y la Norma Australiana como base para asegurar la calidad, gestión y salud del trabajador. Esto ayudará a que sea una de las primeras instituciones quienes implementen directrices internacionales y sea escogido como institución prestigiosa a nivel local y nacional.

3. Se recomienda designar a un miembro del personal del área de Informática y Digitalizaciones de la UTN a ser el responsable del registro y revisión de incidentes relacionados al riesgo, Además se recomienda realizar un análisis y evaluación de factibilidad de las tareas propuestas a manera de salvaguardas para la minimización del impacto de riesgos presentes en la Dirección de Biblioteca.

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

5. Se sugiere llevar a cabo el mismo procedimiento de Gestión de Riesgos en los Departamentos de Informática de otras Facultades en la Universidad Técnica del Norte. Posteriormente, se puede presentar como una metodología estándar para toda la institución, sirviendo como un modelo ejemplar que otras Instituciones Públicas de Educación Superior podrían adoptar.

6. Considerando los resultados altamente positivos obtenidos al aplicar la norma ISO/IEC 31000:2018 y la satisfactoria experiencia con la Metodología MAGERIT, se sugiere encarecidamente que la organización continúe utilizando y promoviendo la implementación de estas herramientas en la gestión de riesgos. Se recomienda también compartir estas experiencias positivas con otras organizaciones similares, destacando las ventajas observadas, para fomentar la adopción de estas prácticas eficaces en el ámbito de la gestión de riesgos.

REFERENCIAS Y BIBLIOGRAFÍA

BIBLIOGRAFÍA

Alonso, C. (2021, May 24). *Métodos de evaluación de riesgos | GlobalSuite Solutions*. https://www.globalsuitesolutions.com/es/metodos-de-evaluacion-de-riesgos/

Alvarado, C. (2021, March 26). *Sistema de gestión de seguridad de la información: qué es y sus etapas*. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

AMBIT TEAM. (2020, November 10). *Tipos de Vulnerabilidades y Amenazas informáticas*. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012a). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. http://administracionelectronica.gob.es/

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012d). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos*. http://administracionelectronica.gob.es/

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012e, October). *PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Artos, A. (2020, October 7). *MAGERIT 3.0: VISIÓN DE CONJUNTO – Interpolados*. https://interpolados.wordpress.com/2020/10/07/magerit-3-0-vision-de-conjunto/

Campos, J. C. (2018, July 12). *¿Cómo gestionar la Seguridad de la Información en la Administración de Proyectos?* http://blogalphaconsultoria.blogspot.com/2018/07/como-gestionar-la-seguridad-de-la.html

Cañas, P. L. E. (2012). *Desarrollo e Implementación de Sistemas de Gestión de Riesgos - Gestión de riesgos de negocio. - Studocu*. https://www.studocu.com/latam/document/universidad-francisco-gavidia/practicas-de-auditoria/desarrollo-e-implementacion-de-sistemas-de-gestion-de-riesgos/17838951

Consuegra de Sucre, D. (2023). CONTROL PARENTAL. *Revista Saberes APUDEP*, *6*(2), 198–215. https://doi.org/10.48204/j.saberes.v6n2.a4090

Riveros, A. (2018, February 28). *3 herramientas de software para la Gestión de Riesgos*. https://www.ealde.es/software-gestion-de-riesgos/

Fernández-Ávila, D. G., Rojas, M. X., & Rosselli, D. (2020). Delphi method in rheumatology research: Are we doing well? *Revista Colombiana de Reumatologia*, *27*(3), 177–189. https://doi.org/10.1016/j.rcreu.2019.04.001

García, M. M., Suárez, M., & Ii, M. (2013). El método Delphi para la consulta a expertos en la investigación científica. *Revista Cubana de Salud Pública*, *39*(2), 253–267. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662013000200007&lng=es&nrm=iso&tlng=es

González Brito, H. R., Anglada Martínez, R. A., & Reyes, D. G. (2017). *CIBERSEGURIDAD*.

Huerta, A. (2012, April 2). *Introducción al análisis de riesgos – Metodologías (II) - Security Art Work*. https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

INEN. (2017). *NTE INEN-ISO/IEC PDF Free Download*. https://docplayer.es/48819724-Nte-inen-iso-iec-27002.html

ISO 27001:2013. (2021, March 11). *¿Qué es la seguridad de la información y cuantos tipos hay?* Seguridad de La Información . https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

ISO 31000. (2018). *ISO 31000:2018(es), Gestión del riesgo — Directrices*. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISO/IEC 31000. (2018). *ISO 31000: La norma para gestionar los riesgos en su organización*. https://www.isotools.org/2015/03/25/iso-31000-norma-gestionar-riesgos-organizacion/

ISOTools. (2013, November 7). *ISO 31000 Software ISO*. https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000/

Norberto, A., & Meza, G. (2023). *La relación entre compiladores y la seguridad informática: un análisis estático*. https://www.researchgate.net/publication/370654209

Andruz, L. (2021, December 27). *Ataques informáticos: Causas, Tipos, Consecuencias y Prevenciones*. https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/

Pensemos SA. (2021, January 20). *Software de Gestión de Riesgos - Pensemos S.A.* https://pensemos.com/software-de-gestion-de-riesgos/

Petrosyan, A. (2022, September 16). *Tasa global de victimización de ransomware 2022 | estatista*. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

Prudente, L., Sánchez, G., & Vázquez, J. de J. (2015, June 25). *Gestión de seguridad de la información basado en el MAAGTICSI para programas académicos en Instituciones de Educación Superior*. https://revista.seguridad.unam.mx/print/2218

Red Hat. (2019, May 19). *¿Qué es la gestión de riesgos?* ¿Qué Es La Gestión de Riesgos? https://www.redhat.com/es/topics/management/what-is-risk-management

Rodríguez, D. (2018, April 5). *ISO 31000 Norma Internacional del Riesgo*. https://www.ceslatam.com/post/2018/04/05/iso-31000-norma-internacional-del-riesgo

Rodríguez, J. (2023, August 22). *Estadística Descriptiva: definición, conceptos y ejemplos | Fundación iS+D*. https://isdfundacion.org/2023/08/22/estadistica-descriptiva-definicion-conceptos-y-ejemplos/

Rossetti, G. H., & Quiroga, O. D. (2023). Metodología de gestión de riesgos para el desarrollo de productos tecnológicos en una empresa multinacional. *Revista Tecnología En Marcha*. https://doi.org/10.18845/tm.v36i7.6856

SafetyCulture. (2023, June 19). *Análisis cuantitativo y cualitativo de riesgos | SafetyCulture*. https://safetyculture.com/es/temas/analisis-cualitativo/

Sánchez, A. (2012, August 18). *Metodologías para el análisis de riesgos en Seguridad Informática | Seguridad Informática*. https://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

Ramírez, C. (2020, November 27). *Norma ISO 31000:2018: principios y marco de referencia para la gestión de riesgos*. https://www.revistaseguridadminera.com/gestion-seguridad/norma-iso-310002018-principios-y-marco-de-referencia-para-la-gestion-de-riesgos/

Shewhart, W. A. (2020, September 27). *Ciclo de Deming: Metodología de mejora continua | PDCA - PHVA | Ingeniería de Calidad | Quality Engineering*. https://www.ingenieriadecalidad.com/2020/02/ciclo-de-deming.html

Tarazona, C. H. (2007). *AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN*.

Varela-Ruiz, M., Díaz-Bravo, L., & García-Durán, R. (2012). Descripción y usos del método Delphi en investigaciones del área de la salud. *Investigación En Educación Médica*, *1*(2), 90–95. https://www.elsevier.es/es-revista-investigacion-educacion-medica-343-articulo-descripcion-usos-del-metodo-delphi-X2007505712427047

Anexos

Anexo A: Encuesta sobre conciencia de gestión de riesgos

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE SOFTWARE

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.

1. **¿Utiliza o a utilizado usted los equipos (computadores) disponibles en la Biblioteca de la UTN?**

   Si

   No

2. **¿Con qué frecuencia usted utiliza la Biblioteca de la UTN?**

   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

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE SOFTWARE

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 la Infraestructura Tecnológica de la Biblioteca de la Universidad Técnica del Norte.

Para esta entrevista se tomó en consideración al encargado del área de Informática y Digitalización de la Biblioteca de la Universidad Técnica del Norte, Ingeniero Iván Chiles. La transcripción de la entrevista es la siguiente.

1. **Dentro de la organización de la Biblioteca de la UTN. ¿Existe algún tipo de Organigrama Estructural Interno? ¿Cuál es?**

2. **¿Cuál es el número total de áreas en la Biblioteca de la Universidad Técnica del Norte?**

3. **¿Cuál es el promedio ocupacional de equipos en la Biblioteca?**

4. **¿Cuál es el proceso para poder acceder a la Biblioteca?**

5. **¿Cuál es el proceso de mantenimiento que se les da a los equipos?**

6. **Dentro del personal vigente del área de Informática y Digitalización ¿Existen responsables sobre los activos como: computadores, proyectores, mouse?**

7. **¿Se cuenta con algún tipo de control o firewall para restringir el acceso hacia redes privadas por parte de los estudiantes?**

8. **¿Los equipos (computadoras) solicitan el inicio de sesión a todos los usuarios?**

9. **¿Se cuenta con algún tipo de servicio para mantener respaldos de la información en los equipos?**

10. **¿Se maneja de alguna forma el control de acceso a internet para los estudiantes?**

11. **¿Existen políticas de gestión de riesgos en la Biblioteca de la UTN, como, por ejemplo, que hacer ante incendios, fallos eléctricos, robo, programa maligno?**

12. **¿Qué sucede cuando algún activo se daña o está defectuoso?**

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

14. **¿Se ha desarrollado capacitaciones al personal de la Biblioteca de la UTN sobre la gestión de riesgos?**

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

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

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

18. **¿Cómo funciona la seguridad en la Biblioteca?**

19. **¿Es permitido almacenar la información personal en los equipos de la Biblioteca?**

20. **¿Se puede instalar software en los equipos de la Biblioteca?**

Anexo C: Entrevista encargado del área de informática y Digitalización de la Biblioteca de la UTN.

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE SOFTWARE

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 la Biblioteca de la UTN.

Para esta entrevista se tomó en consideración al responsable del Área de Informática y Digitalización de la Biblioteca de la UTN, Ingeniero Iván Chiles. Las interrogantes de la entrevista son la siguiente.

1. **¿El Área de Informática y Digitalización de Biblioteca de la UTN, es parte de la Universidad o es responsabilidad de cada facultad?**

2. **¿Qué bases de datos se utilizan?**

3. **¿Existe un apartado en la base de datos para los datos de la Biblioteca de la UTN?**

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 149

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 riesgorecompensa 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 operativa y otras actividades de sostenibilidad se abordan con una metodología basada en el riesgo	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?
			¿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	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?

	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		¿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 que se muestra indica los 7 factores, con sus requerimientos y tareas específicas para la 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,

Anexo E: Identificación de Amenazas en la Biblioteca de la UTN

ACTIVO	AMENAZAS
DATOS/INFORMACION	
Base de datos	[E.15] Alteración de la información
Base de datos	[E.18] Destrucción de la información
Base de datos	[E.19] Fugas de información
Base de datos	[A.5] Suplantación de la identidad
Base de datos	[A.6] Abuso de privilegios de acceso
Base de datos	[A.11] Acceso no autorizado
Documentación interna	[E.15] Alteración de la información
Documentación interna	[E.18] Destrucción de la información
Documentación interna	[E.19] Fugas de información
Documentación interna	[A.5] Suplantación de la identidad
Documentación interna	[A.6] Abuso de privilegios de acceso
Documentación interna	[A.11] Acceso no autorizado
SERVICIOS	
Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales
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 la 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.19] Revelación de información
Servidores internos	[A.24] Denegación de servicio
Internet	[I.8] Fallo de servicios de comunicaciones
Internet	[E.15] Alteración de la información
Internet	[E.18] Destrucción de la información
Internet	[E.19] Fugas de información
Internet	[A.5] Suplantación de la identidad
Internet	[A.13] Repudio (negación de actuaciones)
Internet	[A.15] Modificación de la información
Internet	[A.18] Destrucción de la información
Internet	[A.19] Revelación de información
Internet	[A.24] Denegación de servicio
Electricidad	[I.9] Interrupción de otros servicios o suministros esenciales
Electricidad	[E.15] Alteración de la información
Electricidad	[E.18] Destrucción de la información
Electricidad	[E.19] Fugas de información
Electricidad	[A.5] Suplantación de la identidad
Electricidad	[A.13] Repudio (negación de actuaciones)
Electricidad	[A.15] Modificación de la información
Electricidad	[A.18] Destrucción de la información
Electricidad	[A.19] Revelación de información
Electricidad	[A.24] Denegación de servicio

Telefonía	[I.8] Fallo de servicios de comunicaciones
Telefonía	[E.15] Alteración de la información
Telefonía	[E.18] Destrucción de la información
Telefonía	[E.19] Fugas de información
Telefonía	[A.5] Suplantación de la identidad
Telefonía	[A.13] Repudio (negación de actuaciones)
Telefonía	[A.15] Modificación de la información
Telefonía	[A.18] Destrucción de la información
Telefonía	[A.19] Revelación de información
Telefonía	[A.24] Denegación de servicio
	SOFTWARE
Sistema Integrado	[I.5.1] Avería de origen lógico
Sistema Integrado	[E.8] Difusión de software dañino
Sistema Integrado	[E.20] Vulnerabilidades de los programas (software)
Sistema Integrado	[E.21] Errores de mantenimiento / actualización de programas (software)
Sistema Integrado	[A.8] Difusión de software dañino
Sistema Integrado	[A.22] Manipulación de programas
Sistema Biblioteca Virtual	[I.5.1] Avería de origen lógico
Sistema Biblioteca Virtual	[E.8] Difusión de software dañino
Sistema Biblioteca Virtual	[E.20] Vulnerabilidades de los programas (software)
Sistema Biblioteca Virtual	[E.21] Errores de mantenimiento / actualización de programas (software)
Sistema Biblioteca Virtual	[A.8] Difusión de software dañino
Sistema Biblioteca Virtual	[A.22] Manipulación de programas
Portal Web Biblioteca	[I.5.1] Avería de origen lógico
Portal Web Biblioteca	[E.8] Difusión de software dañino
Portal Web Biblioteca	[E.20] Vulnerabilidades de los programas (software)
Portal Web Biblioteca	[E.21] Errores de mantenimiento / actualización de programas (software)

Portal Web Biblioteca	[A.8] Difusión de software dañino
Portal Web Biblioteca	[A.22] Manipulación de programas
Aplicaciones Ofimática / Académicas	[I.5.1] Avería de origen lógico
Aplicaciones Ofimática / Académicas	[E.8] Difusión de software dañino
Aplicaciones Ofimática / Académicas	[E.20] Vulnerabilidades de los programas (software)
Aplicaciones Ofimática / Académicas	[E.21] Errores de mantenimiento / actualización de programas (software)
Aplicaciones Ofimática / Académicas	[A.8] Difusión de software dañino
Aplicaciones Ofimática / Académicas	[A.22] Manipulación de programas
Licencias	[I.5.1] Avería de origen lógico
Licencias	[E.8] Difusión de software dañino
Licencias	[E.20] Vulnerabilidades de los programas (software)
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)
Licencias	[A.8] Difusión de software dañino
Licencias	[A.22] Manipulación de programas
Sistemas operativos	[I.5.1] Avería de origen lógico
Sistemas operativos	[E.8] Difusión de software dañino
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)
Sistemas operativos	[A.8] Difusión de software dañino
Sistemas operativos	[A.22] Manipulación de programas
Servidores	[I.5.1] Avería de origen lógico
Servidores	[E.8] Difusión de software dañino
Servidores	[E.20] Vulnerabilidades de los programas (software)
Servidores	[E.21] Errores de mantenimiento / actualización de programas (software)
Servidores	[A.8] Difusión de software dañino
Servidores	[A.22] Manipulación de programas
HARDWARE	

Equipos PC y Didácticos	[N.1] Fuego
Equipos PC y Didácticos	[N.2] Daños por agua
Equipos PC y Didácticos	[N.*] Desastres naturales
Equipos PC y Didácticos	[I.1] Fuego
Equipos PC y Didácticos	[I.2] Daños por agua
Equipos PC y Didácticos	[I.*] Desastres industriales
Equipos PC y Didácticos	[I.3] Contaminación medioambiental
Equipos PC y Didácticos	[I.4] Contaminación electromagnética
Equipos PC y Didácticos	[I.5.2] Avería de origen físico
Equipos PC y Didácticos	[I.6] Corte del suministro eléctrico
Equipos PC y Didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad
Equipos PC y Didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipos PC y Didácticos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Equipos PC y Didácticos	[E.24] Caída del sistema por agotamiento de recursos
Equipos PC y Didácticos	[E.25] Pérdida de equipos
Equipos PC y Didácticos	[A.7] Uso no previsto
Equipos PC y Didácticos	[A.11] Acceso no autorizado
Equipos PC y Didácticos	[A.23] Manipulación del hardware
Equipos PC y Didácticos	[A.24] Denegación de servicio
Equipos PC y Didácticos	[A.25] Robo de equipos
Equipos PC y Didácticos	[A.26] Ataque destructivo
Equipos de Redes y Telecomunicaciones	[N.1] Fuego
Equipos de Redes y Telecomunicaciones	[N.2] Daños por agua
Equipos de Redes y Telecomunicaciones	[N.*] Desastres naturales
Equipos de Redes y Telecomunicaciones	[I.1] Fuego
Equipos de Redes y Telecomunicaciones	[I.2] Daños por agua

Equipos de Redes y Telecomunicaciones	[I.*] Desastres industriales
Equipos de Redes y Telecomunicaciones	[I.3] Contaminación medioambiental
Equipos de Redes y Telecomunicaciones	[I.4] Contaminación electromagnética
Equipos de Redes y Telecomunicaciones	[I.5.2] Avería de origen físico
Equipos de Redes y Telecomunicaciones	[I.6] Corte del suministro eléctrico
Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad
Equipos de Redes y Telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)
Equipos de Redes y Telecomunicaciones	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos
Equipos de Redes y Telecomunicaciones	[E.25] Pérdida de equipos
Equipos de Redes y Telecomunicaciones	[A.7] Uso no previsto
Equipos de Redes y Telecomunicaciones	[A.11] Acceso no autorizado
Equipos de Redes y Telecomunicaciones	[A.23] Manipulación del hardware
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio
Equipos de Redes y Telecomunicaciones	[A.25] Robo de equipos
Equipos de Redes y Telecomunicaciones	[A.26] Ataque destructivo
REDES DE COMUNICACIÓN	
Red Interna Biblioteca	[I.8] Fallo de servicios de comunicaciones
Red Interna Biblioteca	[E.2] Errores del administrador del sistema / de la seguridad
Red Interna Biblioteca	[E.9] Errores de [re-]encaminamiento
Red Interna Biblioteca	[E.10] Errores de secuencia
Red Interna Biblioteca	[E.15] Alteración de la información
Red Interna Biblioteca	[E.19] Fugas de información
Red Interna Biblioteca	[E.24] Caída del sistema por agotamiento de recursos
Red Interna Biblioteca	[A.5] Suplantación de la identidad
Red Interna Biblioteca	[A.7] Uso no previsto
Red Interna Biblioteca	[A.9] [Re-]encaminamiento de mensajes

Red Interna Biblioteca	[A.10] Alteración de secuencia
Red Interna Biblioteca	[A.11] Acceso no autorizado
Red Interna Biblioteca	[A.12] Análisis de tráfico
Red Interna Biblioteca	[A.14] Interceptación de información (escucha)
Red Interna Biblioteca	[A.15] Modificación de la información
Red Interna Biblioteca	[A.18] Destrucción de la información
Red Interna Biblioteca	[A.24] Denegación de servicio
SOPORTES DE INFORMACIÓN	
Electrónicos (Nube Microsoft, OneDrive)	[N.1] Fuego
Electrónicos (Nube Microsoft, OneDrive)	[N.2] Daños por agua
Electrónicos (Nube Microsoft, OneDrive)	[N.*] Desastres naturales
Electrónicos (Nube Microsoft, OneDrive)	[I.1] Fuego
Electrónicos (Nube Microsoft, OneDrive)	[I.2] Daños por agua
Electrónicos (Nube Microsoft, OneDrive)	[I.*] Desastres industriales
Electrónicos (Nube Microsoft, OneDrive)	[I.3] Contaminación medioambiental
Electrónicos (Nube Microsoft, OneDrive)	[I.4] Contaminación electromagnética
Electrónicos (Nube Microsoft, OneDrive)	[I.5.2] Avería de origen físico
Electrónicos (Nube Microsoft, OneDrive)	[I.6] Corte del suministro eléctrico
Electrónicos (Nube Microsoft, OneDrive)	[I.7] Condiciones inadecuadas de temperatura o humedad
Electrónicos (Nube Microsoft, OneDrive)	[I.10] Degradación de los soportes de almacenamiento de la información
Electrónicos (Nube Microsoft, OneDrive)	[I.11] Emanaciones electromagnéticas (TEMPEST)
Electrónicos (Nube Microsoft, OneDrive)	[E.1] Errores de los usuarios
Electrónicos (Nube Microsoft, OneDrive)	[E.15] Alteración de la información
Electrónicos (Nube Microsoft, OneDrive)	[E.18] Destrucción de la información
Electrónicos (Nube Microsoft, OneDrive)	[E.19] Fugas de información
Electrónicos (Nube Microsoft, OneDrive)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Electrónicos (Nube Microsoft, OneDrive)	[E.25] Pérdida de equipos

Electrónicos (Nube Microsoft, OneDrive)	[A.7] Uso no previsto
Electrónicos (Nube Microsoft, OneDrive)	[A.11] Acceso no autorizado
Electrónicos (Nube Microsoft, OneDrive)	[A.15] Modificación de la información
Electrónicos (Nube Microsoft, OneDrive)	[A.18] Destrucción de la información
Electrónicos (Nube Microsoft, OneDrive)	[A.23] Manipulación del hardware
Electrónicos (Nube Microsoft, OneDrive)	[A.25] Robo de equipos
Electrónicos (Nube Microsoft, OneDrive)	[A.26] Ataque destructivo
ELEMENTOS AUXILIARES	
Equipamiento Eléctrico	[N.1] Fuego
Equipamiento Eléctrico	[N.2] Daños 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] Daños 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
INSTALACIONES	
Espacios Físicos Biblioteca	[N.1] Fuego
Espacios Físicos Biblioteca	[N.2] Daños por agua
Espacios Físicos Biblioteca	[N.*] Desastres naturales
Espacios Físicos Biblioteca	[I.1] Fuego
Espacios Físicos Biblioteca	[I.2] Daños por agua
Espacios Físicos Biblioteca	[I.*] Desastres industriales
Espacios Físicos Biblioteca	[I.3] Contaminación medioambiental
Espacios Físicos Biblioteca	[I.4] Contaminación electromagnética
Espacios Físicos Biblioteca	[E.25] Pérdida de equipos
Espacios Físicos Biblioteca	[A.6] Abuso de privilegios de acceso
Espacios Físicos Biblioteca	[A.7] Uso no previsto
Espacios Físicos Biblioteca	[A.25] Robo de equipos
Espacios Físicos Biblioteca	[A.26] Ataque destructivo
Espacios Físicos Biblioteca	[A.27] Ocupación enemiga
Área de atención y soporte	[N.1] Fuego
Área de atención y soporte	[N.2] Daños por agua
Área de atención y soporte	[N.*] Desastres naturales
Área de atención y soporte	[I.1] Fuego

Área de atención y soporte	[I.2] Daños por agua
Área de atención y soporte	[I.*] Desastres industriales
Área de atención y soporte	[I.3] Contaminación medioambiental
Área de atención y soporte	[I.4] Contaminación electromagnética
Área de atención y soporte	[E.25] Pérdida de equipos
Área de atención y soporte	[A.6] Abuso de privilegios de acceso
Área de atención y soporte	[A.7] Uso no previsto
Área de atención y soporte	[A.25] Robo de equipos
Área de atención y soporte	[A.26] Ataque destructivo
Área de atención y soporte	[A.27] Ocupación enemiga
PERSONAL	
Personal administrativo informático	[E.15] Alteración de la información
Personal administrativo informático	[E.18] Destrucción de la información
Personal administrativo informático	[E.19] Fugas de información
Personal administrativo informático	[E.28] Indisponibilidad del personal
Personal administrativo informático	[A.15] Modificación de la información
Personal administrativo informático	[A.18] Destrucción de la información
Personal administrativo informático	[A.19] Revelación de información
Personal administrativo informático	[A.28] Indisponibilidad del personal
Personal administrativo informático	[A.29] Extorsión
Personal administrativo informático	[A.30] Ingeniería social (picaresca)

Nota: Elaboración propia

Anexo F: Valoración de amenazas por activos de la Biblioteca de la UTN

ACTIVOS	AMENAZAS	F	D	I	C	A	T
DATOS / INFORMACIÓN							
Base de datos	[E.15] Alteración de la información	1		1%			
Base de datos	[E.18] Destrucción de la información	1	1%				
Base de datos	[E.19] Fugas de información	1			10%		
Base de datos	[A.5] Suplantación de la identidad	10		10%	50%	100%	
Base de datos	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Base de datos	[A.11] Acceso no autorizado	100		10%	50%		
Documentación interna	[E.15] Alteración de la información	1		1%			
Documentación interna	[E.18] Destrucción de la información	1	1%				
Documentación interna	[E.19] Fugas de información	1			10%		
Documentación interna	[A.5] Suplantación de la identidad	10		10%	50%	100%	
Documentación interna	[A.6] Abuso de privilegios de acceso	10	1%	10%	50%		
Documentación interna	[A.11] Acceso no autorizado	100		10%	50%		
SERVICIOS							
Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales	1	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		10%			
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 la identidad	1		100%	100%	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.19] Revelación de información	1			50%		
Servidores internos	[A.24] Denegación de servicio	10	50%				
Internet	[I.8] Fallo de servicios de comunicaciones	1	100%				
Internet	[E.15] Alteración de la información	1		10%			
Internet	[E.18] Destrucción de la información	1	10%				
Internet	[E.19] Fugas de información	1			10%		
Internet	[A.5] Suplantación de la identidad	0,2		100%	100%	100%	
Internet	[A.13] Repudio (negación de actuaciones)	1					100%
Internet	[A.15] Modificación de la información	1		50%			
Internet	[A.18] Destrucción de la información	1	50%				

Internet	[A.19] Revelación de información	1			50%		
Internet	[A.24] Denegación de servicio	1	50%				
Electricidad	[I.9] Interrupción de otros servicios o suministros esenciales	1	50%				
Electricidad	[E.15] Alteración de la información	1		10%			
Electricidad	[E.18] Destrucción de la información	1	10%				
Electricidad	[E.19] Fugas de información	1			10%		
Electricidad	[A.5] Suplantación de la identidad	0,2		100%	100%	100%	
Electricidad	[A.13] Repudio (negación de actuaciones)	1					100%
Electricidad	[A.15] Modificación de la información	1		50%			
Electricidad	[A.18] Destrucción de la información	1	50%				
Electricidad	[A.19] Revelación de información	1			50%		
Electricidad	[A.24] Denegación de servicio	1	50%				
Telefonía	[I.8] Fallo de servicios de comunicaciones	1	100%				
Telefonía	[E.15] Alteración de la información	1		10%			
Telefonía	[E.18] Destrucción de la información	1	10%				
Telefonía	[E.19] Fugas de información	1			10%		
Telefonía	[A.5] Suplantación de la identidad	0,2		100%	100%	100%	
Telefonía	[A.13] Repudio (negación de actuaciones)	1					100%
Telefonía	[A.15] Modificación de la información	1		50%			
Telefonía	[A.18] Destrucción de la información	1	50%				

Telefonía	[A.19] Revelación de información	1			50%
Telefonía	[A.24] Denegación de servicio	1	50%		
SOFTWARE					
Sistema Integrado	[I.5.1] Avería de origen lógico	1	50%		
Sistema Integrado	[E.8] Difusión de software dañino	1	10%	10%	10%
Sistema Integrado	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Sistema Integrado	[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%
Sistema Integrado	[A.8] Difusión de software dañino	1	100%	100%	100%
Sistema Integrado	[A.22] Manipulación de programas	1	50%	100%	100%
Sistema Biblioteca Virtual	[I.5.1] Avería de origen lógico	1	50%		
Sistema Biblioteca Virtual	[E.8] Difusión de software dañino	1	10%	10%	10%
Sistema Biblioteca Virtual	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Sistema Biblioteca Virtual	[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%
Sistema Biblioteca Virtual	[A.8] Difusión de software dañino	1	100%	100%	100%
Sistema Biblioteca Virtual	[A.22] Manipulación de programas	1	50%	100%	100%
Portal Web Biblioteca	[I.5.1] Avería de origen lógico	1	50%		
Portal Web Biblioteca	[E.8] Difusión de software dañino	1	10%	10%	10%
Portal Web Biblioteca	[E.20] Vulnerabilidades	1	1%	20%	20%

	de los programas (software)				
Portal Web Biblioteca	[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%
Portal Web Biblioteca	[A.8] Difusión de software dañino	1	100%	100%	100%
Portal Web Biblioteca	[A.22] Manipulación de programas	1	50%	100%	100%
Aplicaciones Ofimática / Académicas	[I.5.1] Avería de origen lógico	1	50%		
Aplicaciones Ofimática / Académicas	[E.8] Difusión de software dañino	1	10%	10%	10%
Aplicaciones Ofimática / Académicas	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Aplicaciones Ofimática / Académicas	[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%
Aplicaciones Ofimática / Académicas	[A.8] Difusión de software dañino	1	100%	100%	100%
Aplicaciones Ofimática / Académicas	[A.22] Manipulación de programas	1	50%	100%	100%
Licencias	[I.5.1] Avería de origen lógico	1	50%		
Licencias	[E.8] Difusión de software dañino	1	10%	10%	10%
Licencias	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%

Licencias	[A.8] Difusión de software dañino	1	100%	100%	100%
Licencias	[A.22] Manipulación de programas	1	50%	100%	100%
Sistemas operativos	[I.5.1] Avería de origen lógico	1	50%		
Sistemas operativos	[E.8] Difusión de software dañino	1	10%	10%	10%
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%
Sistemas operativos	[A.8] Difusión de software dañino	1	100%	100%	100%
Sistemas operativos	[A.22] Manipulación de programas	1	50%	100%	100%
Servidores	[I.5.1] Avería de origen lógico	1	50%		
Servidores	[E.8] Difusión de software dañino	1	10%	10%	10%
Servidores	[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%
Servidores	[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	10%	50%
Servidores	[A.8] Difusión de software dañino	1	100%	100%	100%
Servidores	[A.22] Manipulación de programas	1	50%	100%	100%
HARDWARE					
Equipos PC y Didácticos	[N.1] Fuego	0,1	100%		
Equipos PC y Didácticos	[N.2] Daños por agua	0,1	50%		

Equipos PC y Didácticos	[N.*] Desastres naturales	0,1	100%		
Equipos PC y Didácticos	[I.1] Fuego	0,5	100%		
Equipos PC y Didácticos	[I.2] Daños por agua	0,5	50%		
Equipos PC y Didácticos	[I.*] Desastres industriales	0,5	100%		
Equipos PC y Didácticos	[I.3] Contaminación medioambiental	0,1	50%		
Equipos PC y Didácticos	[I.4] Contaminación electromagnética	1	10%		
Equipos PC y Didácticos	[I.5.2] Avería de origen físico	1	50%		
Equipos PC y Didácticos	[I.6] Corte del suministro eléctrico	1	100%		
Equipos PC y Didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
Equipos PC y Didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipos PC y Didácticos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%		
Equipos PC y Didácticos	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Equipos PC y Didácticos	[E.25] Pérdida de equipos	5	100%		50%
Equipos PC y Didácticos	[A.7] Uso no previsto	1	10%	1%	10%
Equipos PC y Didácticos	[A.11] Acceso no autorizado	1	10%	10%	50%
Equipos PC y Didácticos	[A.23] Manipulación del hardware	0,5	100%		50%
Equipos PC y Didácticos	[A.24] Denegación de servicio	2	100%		
Equipos PC y Didácticos	[A.25] Robo de equipos	5	100%		50%

Equipos PC y Didácticos	[A.26] Ataque destructivo	1	100%		
Equipos de Redes y Telecomunicaciones	[N.1] Fuego	0,1	100%		
Equipos de Redes y Telecomunicaciones	[N.2] Daños por agua	0,1	50%		
Equipos de Redes y Telecomunicaciones	[N.*] Desastres naturales	0,1	100%		
Equipos de Redes y Telecomunicaciones	[I.1] Fuego	0,5	100%		
Equipos de Redes y Telecomunicaciones	[I.2] Daños por agua	0,5	50%		
Equipos de Redes y Telecomunicaciones	[I.*] Desastres industriales	0,5	100%		
Equipos de Redes y Telecomunicaciones	[I.3] Contaminación medioambiental	0,1	50%		
Equipos de Redes y Telecomunicaciones	[I.4] Contaminación electromagnética	1	10%		
Equipos de Redes y Telecomunicaciones	[I.5.2] Avería de origen físico	1	50%		
Equipos de Redes y Telecomunicaciones	[I.6] Corte del suministro eléctrico	1	100%		
Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
Equipos de Redes y Telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%
Equipos de Redes y Telecomunicaciones	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%		
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	10	50%		
Equipos de Redes y Telecomunicaciones	[E.25] Pérdida de equipos	1	100%		50%
Equipos de Redes y Telecomunicaciones	[A.7] Uso no previsto	1	10%		10%
Equipos de Redes y Telecomunicaciones	[A.11] Acceso no autorizado	1	10%	10%	50%

Equipos de Redes y Telecomunicaciones	[A.23] Manipulación del hardware	0,5	100%		50%	
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio	2	100%			
Equipos de Redes y Telecomunicaciones	[A.25] Robo de equipos	0,5	100%		50%	
Equipos de Redes y Telecomunicaciones	[A.26] Ataque destructivo	1	100%			
REDES DE COMUNICACIÓN						
Red Interna Biblioteca	[I.8] Fallo de servicios de comunicaciones	1	50%			
Red Interna Biblioteca	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	
Red Interna Biblioteca	[E.9] Errores de [re-]encaminamiento	1			10%	
Red Interna Biblioteca	[E.10] Errores de secuencia	1		10%		
Red Interna Biblioteca	[E.15] Alteración de la información	1		1%		
Red Interna Biblioteca	[E.19] Fugas de información	1			10%	
Red Interna Biblioteca	[E.24] Caída del sistema por agotamiento de recursos	1	50%			
Red Interna Biblioteca	[A.5] Suplantación de la identidad	1		10%	50%	100%
Red Interna Biblioteca	[A.7] Uso no previsto	1	10%	10%	10%	
Red Interna Biblioteca	[A.9] [Re-]encaminamiento de mensajes	1			10%	
Red Interna Biblioteca	[A.10] Alteración de secuencia	1		10%		
Red Interna Biblioteca	[A.11] Acceso no autorizado	1		10%	50%	100%
Red Interna Biblioteca	[A.12] Análisis de tráfico	1			2%	
Red Interna Biblioteca	[A.14] Interceptación de información (escucha)	1			10%	

Red Interna Biblioteca	[A.15] Modificación de la información	1		10%	
Red Interna Biblioteca	[A.18] Destrucción de la información	1	50%		
Red Interna Biblioteca	[A.24] Denegación de servicio	10	50%		
ELEMENTOS AUXILIARES					
Equipamiento Eléctrico	[N.1] Fuego	0,1	100%		
Equipamiento Eléctrico	[N.2] Daños 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] Daños 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%		
INSTALACIONES					
Espacios Físicos Biblioteca	[N.1] Fuego	1	100%		
Espacios Físicos Biblioteca	[N.2] Daños por agua	1	100%		
Espacios Físicos Biblioteca	[N.*] Desastres naturales	0,5	100%		
Espacios Físicos Biblioteca	[I.1] Fuego	1	100%		
Espacios Físicos Biblioteca	[I.2] Daños por agua	1	100%		
Espacios Físicos Biblioteca	[I.*] Desastres industriales	1	100%		
Espacios Físicos Biblioteca	[I.3] Contaminación medioambiental	1	10%		
Espacios Físicos Biblioteca	[I.4] Contaminación electromagnética	0,1	10%		
Espacios Físicos Biblioteca	[E.25] Pérdida de equipos	10			10%

Espacios Físicos Biblioteca	[A.6] Abuso de privilegios de acceso	1	10%	
Espacios Físicos Biblioteca	[A.7] Uso no previsto	1	10%	
Espacios Físicos Biblioteca	[A.25] Robo de equipos	10		100%
Espacios Físicos Biblioteca	[A.26] Ataque destructivo	0,1	100%	
Espacios Físicos Biblioteca	[A.27] Ocupación enemiga	1	100%	
Área de atención y soporte	[N.1] Fuego	1	100%	
Área de atención y soporte	[N.2] Daños por agua	1	100%	
Área de atención y soporte	[N.*] Desastres naturales	0,5	100%	
Área de atención y soporte	[I.1] Fuego	1	100%	
Área de atención y soporte	[I.2] Daños por agua	1	100%	
Área de atención y soporte	[I.*] Desastres industriales	1	100%	
Área de atención y soporte	[I.3] Contaminación medioambiental	1	10%	
Área de atención y soporte	[I.4] Contaminación electromagnética	0,1	10%	
Área de atención y soporte	[E.25] Pérdida de equipos	10		10%
Área de atención y soporte	[A.6] Abuso de privilegios de acceso	1	10%	
Área de atención y soporte	[A.7] Uso no previsto	1	10%	
Área de atención y soporte	[A.25] Robo de equipos	10		100%
Área de atención y soporte	[A.26] Ataque destructivo	0,1	100%	
Área de atención y soporte	[A.27] Ocupación enemiga	1	100%	
PERSONAL				
Personal administrativo informático	[E.15] Alteración de la información	1	10%	

Personal administrativo informático	[E.18] Destrucción de la información	1	1%		
Personal administrativo informático	[E.19] Fugas de información	1			10%
Personal administrativo informático	[E.28] Indisponibilidad del personal	1	10%		
Personal administrativo informático	[A.15] Modificación de la información	1		50%	
Personal administrativo informático	[A.18] Destrucción de la información	1	10%		
Personal administrativo informático	[A.19] Revelación de información	10			50%
Personal administrativo informático	[A.28] Indisponibilidad del personal	0,5	20%		
Personal administrativo informático	[A.29] Extorsión	0,9	50%	100%	100%
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	0,5	50%	100%	100%

Nota: La tabla presenta una muestra del listado de la valoración de amenazas que podrían afectar a los activos identificados en la Biblioteca de la 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 la Biblioteca de la UTN

	Impacto Potencial Acumulado					Peso Ponderado
Activos-Amenazas	**D**	**I**	**C**	**A**	**T**	
DATOS/INFORMACIÓN	**4**	**7**	**9**	**10**		
Base de datos	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			7.0
[A.5] Suplantación de la 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
Documentación 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			7.0
[A.5] Suplantación de la 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	**10**	**10**	**10**	**10**	**10**	
Servidores internos	9	10	10	10	10	
[I.9] Interrupción de otros servicios o suministros esenciales	9					9.0
[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		7				7.0
[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 la identidad		10	10	10		10.0
[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.19] Revelación de información			9			9.0
[A.24] Denegación de servicio	9					9.0
Internet	10	10	10	10	9	
[I.8] Fallo de servicios de comunicaciones	10					10.0
[E.15] Alteración de la información		7				7.0
[E.18] Destrucción de la información	7					7.0
[E.19] Fugas de información			7			7.0
[A.5] Suplantación de la identidad		10	10	10		10.0
[A.13] Repudio (negación de actuaciones)					9	9.0
[A.15] Modificación de la información		9				9.0

[A.18] Destrucción de la información	9					9.0
[A.19] Revelación de información			9			9.0
[A.24] Denegación de servicio	9					9.0
Electricidad	9	7	8	8	7	
[I.9] Interrupción de otros servicios o suministros esenciales	9					9.0
[E.15] Alteración de la información		4				4.0
[E.18] Destrucción de la información	7					7.0
[E.19] Fugas de información			5			5.0
[A.5] Suplantación de la identidad		7	8	8		7.7
[A.13] Repudio (negación de actuaciones)					7	7.0
[A.15] Modificación de la información		6				6.0
[A.18] Destrucción de la información	9					9.0
[A.19] Revelación de información			7			7.0
[A.24] Denegación de servicio	9					9.0
Telefonía	9	9	9	10	8	
[I.8] Fallo de servicios de comunicaciones	9					9.0
[E.15] Alteración de la información		6				6.0
[E.18] Destrucción de la información	6					6.0
[E.19] Fugas de información			6			6.0
[A.5] Suplantación de la identidad		9	9	10		9.3
[A.13] Repudio (negación de actuaciones)					8	8.0
[A.15] Modificación de la información		8				8.0
[A.18] Destrucción de la información	8					8.0

[A.19] Revelación de información			8		8.0
[A.24] Denegación de servicio	8				8.0
SOFTWARE	**10**	**10**	**10**		
Sistema Integrado	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 (software)	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
Sistema Biblioteca Virtual	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 (software)	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 Biblioteca	10	10	9		
[I.5.1] Avería de origen lógico	9				9.0
[E.8] Difusión de software dañino	7	7	6		6.7
[E.20] Vulnerabilidades de los programas (software)	4	8	7		6.3
[E.21] Errores de mantenimiento / actualización de programas (software)	4	7	8		6.3
[A.8] Difusión de software dañino	10	10	9		9.7
[A.22] Manipulación de programas	9	10	9		9.3

Aplicaciones Ofimática / Académicas	9	9	9		
[I.5.1] Avería de origen lógico	8				8.0
[E.8] Difusión de software dañino	6	6	6		6.0
[E.20] Vulnerabilidades de los programas (software)	3	7	7		5.7
[E.21] Errores de mantenimiento / actualización de programas (software)	3	6	8		5.7
[A.8] Difusión de software dañino	9	9	9		9.0
[A.22] Manipulación de programas	8	9	9		8.7
Licencias	10	10	9		
[I.5.1] Avería de origen lógico	9				9.0
[E.8] Difusión de software dañino	7	7	6		6.7
[E.20] Vulnerabilidades de los programas (software)	4	8	7		6.3
[E.21] Errores de mantenimiento / actualización de programas (software)	4	7	8		6.3
[A.8] Difusión de software dañino	10	10	9		9.7
[A.22] Manipulación de programas	9	10	9		9.3
Sistemas operativos	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 (software)	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
Servidores	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 (software)	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**	**8**		
Equipos PC y Didácticos	9	6	8		
[N.1] Fuego	9				9.0
[N.2] Daños por agua	8				8.0
[N.*] Desastres naturales	9				9.0
[I.1] Fuego	9				9.0
[I.2] Daños por agua	8				8.0
[I.*] Desastres industriales	9				9.0
[I.3] Contaminación medioambiental	8				8.0
[I.4] Contaminación electromagnética	6				6.0
[I.5.2] Avería de origen físico	8				8.0
[I.6] Corte del suministro eléctrico	9				9.0
[I.7] Condiciones inadecuadas de temperatura o humedad	9				9.0
[I.11] Emanaciones electromagnéticas (TEMPEST)			3		3.0
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	6				6.0
[E.24] Caída del sistema por agotamiento de recursos	8				8.0
[E.25] Pérdida de equipos	9		8		8.5
[A.7] Uso no previsto	6	3	6		5.0

[A.11] Acceso no autorizado	6	6	8		6.7
[A.23] Manipulación del hardware	9		8		8.5
[A.24] Denegación de servicio	9				9.0
[A.25] Robo de equipos	9		8		8.5
[A.26] Ataque destructivo	9				9.0
Equipos de Redes y Telecomunicaciones	10	7	8		
[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 del suministro eléctrico	10				10.0
[I.7] Condiciones inadecuadas de temperatura o humedad	10				10.0
[I.11] Emanaciones electromagnéticas (TEMPEST)			3		3.0
[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		8		9.0
[A.7] Uso no previsto	7		6		6.5
[A.11] Acceso no autorizado	7	7	8		7.3
[A.23] Manipulación del hardware	10		8		9.0

[A.24] Denegación de servicio	10					10.0
[A.25] Robo de equipos	10		8			9.0
[A.26] Ataque destructivo	10					10.0
REDES DE COMUNICACIÓN	**9**	**8**	**9**	**10**		
Red Interna Biblioteca	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-]encaminamiento			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 la identidad		7	9	10		5.3
[A.7] Uso no previsto	7	7	7			7.0
[A.9] [Re-]encaminamiento de mensajes			7			7.0
[A.10] Alteración de secuencia		7				7.0
[A.11] Acceso no autorizado		7	9	10		5.3
[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
SOPORTES DE INFORMACIÓN	**10**	**10**	**10**			
Electrónicos (Nube Microsoft, OneDrive)	10	10	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 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		4.0
[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
ELEMENTOS AUXILIARES	**9**	**6**	**8**			
Equipamiento Eléctrico	9	6	8			
[N.1] Fuego	9					9.0
[N.2] Daños por agua	8					8.0
[N.*] Desastres naturales	9					9.0
[I.1] Fuego	9					9.0
[I.2] Daños por agua	8					8.0
[I.*] Desastres industriales	9					9.0
[I.3] Contaminación medioambiental	8					8.0
[I.4] Contaminación electromagnética	6					6.0
[I.11] Emanaciones electromagnéticas (TEMPEST)			3			3.0
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	6					6.0
[A.7] Uso no previsto	8	3	3			4.7
[A.11] Acceso no autorizado		6	8			4.0
[A.23] Manipulación del hardware	8		8			8.0
[A.25] Robo de equipos	9					9.0
[A.26] Ataque destructivo	9					9.0
Mobiliario para los equipos	9	3	8			
[N.1] Fuego	9					9.0
[N.2] Daños por agua	8					8.0
[N.*] Desastres naturales	9					9.0
[I.1] Fuego	9					9.0
[I.2] Daños por agua	8					8.0

[I.*] Desastres industriales	9				9.0
[I.3] Contaminación medioambiental	8				8.0
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	6				6.0
[A.7] Uso no previsto	8	3	3		4.7
[A.23] Manipulación del hardware	8		8		8.0
[A.25] Robo de equipos	6		8		7.0
[A.26] Ataque destructivo	6				6.0
INSTALACIONES	9		9		
Espacios Físicos Biblioteca	9		7		
[N.1] Fuego	9				9.0
[N.2] Daños por agua	9				9.0
[N.*] Desastres naturales	9				9.0
[I.1] Fuego	9				9.0
[I.2] Daños por agua	9				9.0
[I.*] Desastres industriales	9				9.0
[I.3] Contaminación medioambiental	6				6.0
[I.4] Contaminación electromagnética	6				6.0
[E.25] Pérdida de equipos			4		4.0
[A.6] Abuso de privilegios de acceso	6				6.0
[A.7] Uso no previsto	6				6.0
[A.25] Robo de equipos			7		7.0
[A.26] Ataque destructivo	9				9.0
[A.27] Ocupación enemiga	9				9.0
Área de atención y soporte	9		9		
[N.1] Fuego	9				9.0

[N.2] Daños por agua	9			9.0
[N.*] Desastres naturales	9			9.0
[I.1] Fuego	9			9.0
[I.2] Daños por agua	9			9.0
[I.*] Desastres industriales	9			9.0
[I.3] Contaminación medioambiental	6			6.0
[I.4] Contaminación electromagnética	6			6.0
[E.25] Pérdida de equipos			6	6.0
[A.6] Abuso de privilegios de acceso	6			6.0
[A.7] Uso no previsto	6			6.0
[A.25] Robo de equipos			9	9.0
[A.26] Ataque destructivo	9			9.0
[A.27] Ocupación enemiga	9			9.0
PERSONAL	**9**	**10**	**10**	
Personal administrativo informático	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

Nota: La siguiente tabla presenta la acumulación del impacto, donde D: representa la degradación en la disponibilidad, I: la degradación en la integridad, C: la degradación en la confidencialidad, A: la degradación en la autenticidad y T: la degradación en la trazabilidad. Elaboración propia.

Anexo H: Riesgo potencial acumulado de Amenazas en la Biblioteca de la UTN

	Impacto Potencial Acumulado					**Peso Ponderado**
Activos-Riesgos	**D**	**I**	**C**	**A**	**T**	
DATOS/INFORMACIÓN	**4.2**	**6.8**	**8.1**	**7.7**		
Base de datos	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 la identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			4.4
[A.11] Acceso no autorizado		6.8	8.1			7.5
Documentación 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 la identidad		5.9	7.2	7.7		6.9
[A.6] Abuso de privilegios de acceso	4.2	5.9	7.2			4.4
[A.11] Acceso no autorizado		6.8	8.1			7.5
SERVICIOS	**7.2**	**7.2**	**6.8**	**6.8**	**7.4**	
Servidores internos	7.2	7.2	6.8	6.8	7.4	

[I.9] Interrupción de otros servicios o suministros esenciales	6.3					6.3
[E.1] Errores de los usuarios	5.1	5.1	5.1			3.4
[E.2] Errores del administrador del sistema / de la seguridad	5.6	5.6	5.6			3.7
[E.15] Alteración de la información		5.1				5.1
[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 la identidad		6.8	6.8	6.8		6.8
[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.19] Revelación de información			6.3			6.3
[A.24] Denegación de servicio	7.2					7.2
Internet	6.8	6.3	6.3	6.2	6.2	
[I.8] Fallo de servicios de comunicaciones	6.8					6.8
[E.15] Alteración de la información		5.1				5.1
[E.18] Destrucción de la información	5.1					5.1
[E.19] Fugas de información			5.1			5.1

[A.5] Suplantación de la identidad		6.2	6.2	6.2		6.2
[A.13] Repudio (negación de actuaciones)					6.2	6.2
[A.15] Modificación de la información		6.3				6.3
[A.18] Destrucción de la información	6.3					6.3
[A.19] Revelación de información			6.3			6.3
[A.24] Denegación de servicio	6.3					6.3
Electricidad	6.3	4.5	5.1	5	5.1	
[I.9] Interrupción de otros servicios o suministros esenciales	6.3					6.3
[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			3.9			3.9
[A.5] Suplantación de la identidad		4.5	5	5		4.8
[A.13] Repudio (negación de actuaciones)					5.1	5.1
[A.15] Modificación de la información		4.5				4.5
[A.18] Destrucción de la información	6.3					6.3
[A.19] Revelación de información			5.1			5.1
[A.24] Denegación de servicio	6.3					6.3
Telefonía	6.2	5.7	5.7	6.2	5.7	
[I.8] Fallo de servicios de comunicaciones	6.2					6.2
[E.15] Alteración de la información		4.5				4.5
[E.18] Destrucción de la información	4.5					4.5

[E.19] Fugas de información			4.5			4.5
[A.5] Suplantación de la identidad		5.6	5.6	6.2		5.8
[A.13] Repudio (negación de actuaciones)					5.7	5.7
[A.15] Modificación de la información		5.7				5.7
[A.18] Destrucción de la información	5.7					5.7
[A.19] Revelación de información			5.7			5.7
[A.24] Denegación de servicio	5.7					5.7
SOFTWARE	**6.8**	**6.8**	**7.2**			
Sistema Integrado	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 (software)	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
Sistema Biblioteca Virtual	6.8	6.8	7.2			6.9
[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 (software)	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 Biblioteca	6.8	6.8	6.6	
[I.5.1] Avería de origen lógico	6.3			6.3
[E.8] Difusión de software dañino	5.1	5.1	4.5	4.9
[E.20] Vulnerabilidades de los programas (software)	3.3	5.6	5	4.6
[E.21] Errores de mantenimiento / actualización de programas (software)	4.2	5.9	6.6	5.6
[A.8] Difusión de software dañino	6.8	6.8	6.2	6.6
[A.22] Manipulación de programas	6.3	6.8	6.2	6.4
Aplicaciones Ofimática / Académicas	6.2	6.2	6.6	
[I.5.1] Avería de origen lógico	5.7			5.7
[E.8] Difusión de software dañino	4.5	4.5	4.5	4.5
[E.20] Vulnerabilidades de los programas (software)	2.7	5.0	5.0	4.2
[E.21] Errores de mantenimiento / actualización de programas (software)	3.6	5.4	6.6	5.2
[A.8] Difusión de software dañino	6.2	6.2	6.2	6.2
[A.22] Manipulación de programas	5.7	6.2	6.2	6.0
Licencias	6.8	6.8	6.6	
[I.5.1] Avería de origen lógico	6.3			6.3
[E.8] Difusión de software dañino	5.1	5.1	4.5	4.9
[E.20] Vulnerabilidades de los programas (software)	3.3	5.6	5.0	4.6
[E.21] Errores de mantenimiento / actualización de programas (software)	4.2	5.9	6.6	5.6
[A.8] Difusión de software dañino	6.8	6.8	6.2	6.6

[A.22] Manipulación de programas	6.3	6.8	6.2	6.4
Sistemas operativos	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 (software)	4.2	5.9	7.2	5.8
[A.8] Difusión de software dañino	6.8	6.8	5.8	6.5
[A.22] Manipulación de programas	6.3	6.8	6.8	6.6
Servidores	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 (software)	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	**7.2**	**5.1**	**6.3**	
Equipos PC y Didácticos	6.9	4.5	6.3	
[N.1] Fuego	5.4			5.4
[N.2] Daños por agua	4.8			4.8
[N.*] Desastres naturales	5.4			5.4
[I.1] Fuego	6.0			6.0
[I.2] Daños por agua	5.4			5.4
[I.*] Desastres industriales	6.0			6.0

[I.3] Contaminación medioambiental	4.8			4.8
[I.4] Contaminación electromagnética	4.5			4.5
[I.5.2] Avería de origen físico	5.7			5.7
[I.6] Corte del suministro eléctrico	6.2			6.2
[I.7] Condiciones inadecuadas de temperatura o humedad	6.2			6.2
[I.11] Emanaciones electromagnéticas (TEMPEST)			2.7	2.7
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5			4.5
[E.24] Caída del sistema por agotamiento de recursos	6.6			6.6
[E.25] Pérdida de equipos	6.9		6.3	6.6
[A.7] Uso no previsto	4.5	2.7	4.5	3.9
[A.11] Acceso no autorizado	4.5	4.5	5.7	4.9
[A.23] Manipulación del hardware	6.0		5.4	5.7
[A.24] Denegación de servicio	6.5			6.5
[A.25] Robo de equipos	6.9		6.3	6.6
[A.26] Ataque destructivo	6.2			6.2
Equipos de Redes y Telecomunicaciones	7.2	5.1	5.7	
[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	6.0			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 del suministro eléctrico	6.8				6.8
[I.7] Condiciones inadecuadas de temperatura o humedad	6.8				6.8
[I.11] Emanaciones electromagnéticas (TEMPEST)			2.7		2.7
[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		5.7		6.25
[A.7] Uso no previsto	5.1		4.5		4.8
[A.11] Acceso no autorizado	5.1	5.1	5.7		5.3
[A.23] Manipulación del hardware	6.6		5.4		6.0
[A.24] Denegación de servicio	7.1				7.1
[A.25] Robo de equipos	6.6		5.4		6.0
[A.26] Ataque destructivo	6.8				6.8
REDES DE COMUNICACIÓN	**7.2**	**5.6**	**6.3**	**6.8**	
Red Interna Biblioteca	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-]encaminamiento			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 la 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 mensajes			5.1		5.1
[A.10] Alteración de secuencia		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
SOPORTES DE INFORMACIÓN	**6.8**	**7.4**	**6.8**		
Electrónicos (Nube Microsoft, OneDrive)	6.8	7.4	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	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
ELEMENTOS AUXILIARES	**6.2**	**4.5**	**5.7**	
Equipamiento Eléctrico	6.2	4.5	5.7	

[N.1] Fuego	5.4			5.4
[N.2] Daños por agua	4.8			4.8
[N.*] Desastres naturales	5.4			5.4
[I.1] Fuego	6.0			6.0
[I.2] Daños por agua	5.4			5.4
[I.*] Desastres industriales	6.0			6.0
[I.3] Contaminación medioambiental	4.8			4.8
[I.4] Contaminación electromagnética	4.2			4.2
[I.11] Emanaciones electromagnéticas (TEMPEST)			2.7	2.7
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5			4.5
[A.7] Uso no previsto	5.7	2.7	2.7	3.7
[A.11] Acceso no autorizado		4.5	5.7	5.1
[A.23] Manipulación del hardware	5.7		5.7	5.7
[A.25] Robo de equipos	6.2			6.2
[A.26] Ataque destructivo	6.2			6.2
Mobiliario para los equipos	6.0	2.7	5.7	
[N.1] Fuego	5.4			5.4
[N.2] Daños por agua	4.8			4.8
[N.*] Desastres naturales	5.4			5.4
[I.1] Fuego	6.0			6.0
[I.2] Daños por agua	5.4			5.4
[I.*] Desastres industriales	6.0			6.0
[I.3] Contaminación medioambiental	4.8			4.8

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5			4.5
[A.7] Uso no previsto	5.7	2.7	2.7	3.7
[A.23] Manipulación del hardware	5.7		5.7	5.7
[A.25] Robo de equipos	4.2		5.4	4.8
[A.26] Ataque destructivo	4.5			4.5
INSTALACIONES	**6.2**		**7.1**	
Espacios Fisicos Biblioteca	6.2		5.9	
[N.1] Fuego	6.2			6.2
[N.2] Daños por agua	6.2			6.2
[N.*] Desastres naturales	6.0			6.0
[I.1] Fuego	6.2			6.2
[I.2] Daños por agua	6.2			6.2
[I.*] Desastres industriales	6.2			6.2
[I.3] Contaminación medioambiental	4.5			4.5
[I.4] Contaminación electromagnética	3.6			3.6
[E.25] Pérdida de equipos			4.2	4.2
[A.6] Abuso de privilegios de acceso	4.5			4.5
[A.7] Uso no previsto	4.5			4.5
[A.25] Robo de equipos			5.9	5.9
[A.26] Ataque destructivo	5.4			5.4
[A.27] Ocupación enemiga	6.2			6.2
Área de atención y soporte	6.2		7.1	
[N.1] Fuego	6.2			6.2
[N.2] Daños por agua	6.2			6.2

[N.*] Desastres naturales	6.0			6.0
[I.1] Fuego	6.2			6.2
[I.2] Daños por agua	6.2			6.2
[I.*] Desastres industriales	6.2			6.2
[I.3] Contaminación medioambiental	4.5			4.5
[I.4] Contaminación electromagnética	3.6			3.6
[E.25] Pérdida de equipos			5.4	5.4
[A.6] Abuso de privilegios de acceso	4.5			4.5
[A.7] Uso no previsto	4.5			4.5
[A.25] Robo de equipos			7.1	7.1
[A.26] Ataque destructivo	5.4			5.4
[A.27] Ocupación enemiga	6.2			6.2
PERSONAL	**6.3**	**6.8**	**7.2**	
Personal administrativo informático	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)	6.0	6.6	6.6	6.4

Nota: La tabla presenta la evaluación del riesgo acumulado potencial, donde D: representa la disminución en la dimensión de disponibilidad, I: la disminución en integridad, C: la disminución en confidencialidad, A: la disminución en autenticidad, y T: la disminución en trazabilidad. Este análisis es resultado de Elaboración propia.

Anexo I: Recopilación Riesgos de mayor peso en laboratorios de informática FICA-UTN

ACTIVO	AMENAZAS	PESO PONDERADO
Base de datos	[A.11] Acceso no autorizado	7.5
Documentación interna	[A.11] Acceso no autorizado	7.5
Servidores internos	[A.13] Repudio (negación de actuaciones)	7.4
Electrónicos (Nube Microsoft, OneDrive)	[A.15] Modificación de la información	7.4
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	7.2
Servidores internos	[A.15] Modificación de la información	7.2
Servidores internos	[A.24] Denegación de servicio	7.2
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	7.2
Red Interna Biblioteca	[A.24] Denegación de servicio	7.2
Personal administrativo informático	[A.19] Revelación de información	7.2
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio	7.1
Área de atención y soporte	[A.25] Robo de equipos	7.1
Base de datos	[A.5] Suplantación de la identidad	6.9
Documentación interna	[A.5] Suplantación de la identidad	6.9
Servidores internos	[A.5] Suplantación de la identidad	6.8
Internet	[I.8] Fallo de servicios de comunicaciones	6.8
Sistema Integrado	[A.8] Difusión de software dañino	6.8
Sistema Biblioteca Virtual	[A.8] Difusión de software dañino	6.8
Servidores	[A.8] Difusión de software dañino	6.8

Equipos de Redes y Telecomunicaciones	[I.6] Corte del suministro eléctrico	6.8
Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Equipos de Redes y Telecomunicaciones	[A.26] Ataque destructivo	6.8
Electrónicos (Nube Microsoft, OneDrive)	[I.6] Corte del suministro eléctrico	6.8
Electrónicos (Nube Microsoft, OneDrive)	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8
Electrónicos (Nube Microsoft, OneDrive)	[I.10] Degradación de los soportes de almacenamiento de la información	6.8
Electrónicos (Nube Microsoft, OneDrive)	[E.18] Destrucción de la información	6.8
Electrónicos (Nube Microsoft, OneDrive)	[A.18] Destrucción de la información	6.8
Sistema Integrado	[A.22] Manipulación de programas	6.6
Sistema Biblioteca Virtual	[A.22] Manipulación de programas	6.6
Sistemas operativos	[A.22] Manipulación de programas	6.6
Servidores	[A.22] Manipulación de programas	6.6
Personal administrativo informático	[A.29] Extorsión	6.6
Portal Web Biblioteca	[A.8] Difusión de software dañino	6.6
Licencias	[A.8] Difusión de software dañino	6.6
Equipos PC y Didácticos	[E.24] Caída del sistema por agotamiento de recursos	6.6
Equipos PC y Didácticos	[E.25] Pérdida de equipos	6.6
Equipos PC y Didácticos	[A.25] Robo de equipos	6.6
Equipos de Redes y Telecomunicaciones	[I.1] Fuego	6.6
Equipos de Redes y Telecomunicaciones	[I.*] Desastres industriales	6.6
Electrónicos (Nube Microsoft, OneDrive)	[I.1] Fuego	6.6

Electrónicos (Nube Microsoft, OneDrive)	[I.*] Desastres industriales	6.6
Equipos PC y Didácticos	[A.24] Denegación de servicio	6.5
Sistemas operativos	[A.8] Difusión de software dañino	6.5
Portal Web Biblioteca	[A.22] Manipulación de programas	6.4
Licencias	[A.22] Manipulación de programas	6.4
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	6.4
Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales	6.3
Servidores internos	[A.18] Destrucción de la información	6.3
Servidores internos	[A.19] Revelación de información	6.3
Internet	[A.15] Modificación de la información	6.3
Internet	[A.18] Destrucción de la información	6.3
Internet	[A.19] Revelación de información	6.3
Internet	[A.24] Denegación de servicio	6.3
Electricidad	[I.9] Interrupción de otros servicios o suministros esenciales	6.3
Electricidad	[A.18] Destrucción de la información	6.3
Electricidad	[A.24] Denegación de servicio	6.3
Sistema Integrado	[I.5.1] Avería de origen lógico	6.3
Sistema Biblioteca Virtual	[I.5.1] Avería de origen lógico	6.3
Portal Web Biblioteca	[I.5.1] Avería de origen lógico	6.3
Licencias	[I.5.1] Avería de origen lógico	6.3
Sistemas operativos	[I.5.1] Avería de origen lógico	6.3
Servidores	[I.5.1] Avería de origen lógico	6.3
Equipos de Redes y Telecomunicaciones	[I.5.2] Avería de origen físico	6.3
Red Interna Biblioteca	[I.8] Fallo de servicios de comunicaciones	6.3
Red Interna Biblioteca	[E.24] Caída del sistema por agotamiento de recursos	6.3

Red Interna Biblioteca	[A.18] Destrucción de la información	6.3
Electrónicos (Nube Microsoft, OneDrive)	[I.3] Contaminación medioambiental	6.3
Electrónicos (Nube Microsoft, OneDrive)	[I.5.2] Avería de origen físico	6.3
Personal administrativo informático	[A.15] Modificación de la información	6.3
Equipos de Redes y Telecomunicaciones	[E.25] Pérdida de equipos	6.3
Internet	[A.5] Suplantación de la identidad	6.2
Internet	[A.13] Repudio (negación de actuaciones)	6.2
Telefonía	[I.8] Fallo de servicios de comunicaciones	6.2
Aplicaciones Ofimática / Académicas	[A.8] Difusión de software dañino	6.2
Equipos PC y Didácticos	[I.6] Corte del suministro eléctrico	6.2
Equipos PC y Didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad	6.2
Equipos PC y Didácticos	[A.26] Ataque destructivo	6.2
Equipamiento Eléctrico	[A.25] Robo de equipos	6.2
Equipamiento Eléctrico	[A.26] Ataque destructivo	6.2
Espacios Físicos Biblioteca	[N.1] Fuego	6.2
Espacios Físicos Biblioteca	[N.2] Daños por agua	6.2
Espacios Físicos Biblioteca	[I.1] Fuego	6.2
Espacios Físicos Biblioteca	[I.2] Daños por agua	6.2
Espacios Físicos Biblioteca	[I.*] Desastres industriales	6.2
Espacios Físicos Biblioteca	[A.27] Ocupación enemiga	6.2
Área de atención y soporte	[N.1] Fuego	6.2
Área de atención y soporte	[N.2] Daños por agua	6.2
Área de atención y soporte	[I.1] Fuego	6.2
Área de atención y soporte	[I.2] Daños por agua	6.2
Área de atención y soporte	[I.*] Desastres industriales	6.2

Área de atención y soporte	[A.27] Ocupación enemiga	6.2
Servidores internos	[A.11] Acceso no autorizado	6.1
Red Interna Biblioteca	[A.5] Suplantación de la identidad	6.1
Red Interna Biblioteca	[A.11] Acceso no autorizado	6.1
Electrónicos (Nube Microsoft, OneDrive)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	6.1
Aplicaciones Ofimática / Académicas	[A.22] Manipulación de programas	6.0
Equipos PC y Didácticos	[I.1] Fuego	6
Equipos PC y Didácticos	[I.*] Desastres industriales	6
Equipos de Redes y Telecomunicaciones	[I.2] Daños por agua	6.0
Equipos de Redes y Telecomunicaciones	[A.23] Manipulación del hardware	6.0
Equipos de Redes y Telecomunicaciones	[A.25] Robo de equipos	6.0
Electrónicos (Nube Microsoft, OneDrive)	[I.2] Daños por agua	6.0
Equipamiento Eléctrico	[I.1] Fuego	6.0
Equipamiento Eléctrico	[I.*] Desastres industriales	6.0
Mobiliario para los equipos	[I.1] Fuego	6.0
Mobiliario para los equipos	[I.*] Desastres industriales	6.0
Espacios Físicos Biblioteca	[N.*] Desastres naturales	6.0
Área de atención y soporte	[N.*] Desastres naturales	6.0
Electrónicos (Nube Microsoft, OneDrive)	[A.25] Robo de equipos	6.0
Equipos de Redes y Telecomunicaciones	[N.1] Fuego	5.9
Equipos de Redes y Telecomunicaciones	[N.*] Desastres naturales	5.9
Electrónicos (Nube Microsoft, OneDrive)	[N.1] Fuego	5.9
Electrónicos (Nube Microsoft, OneDrive)	[N.*] Desastres naturales	5.9

Espacios Físicos Biblioteca	[A.25] Robo de equipos	5.9
Telefonía	[A.5] Suplantación de la identidad	5.8
Sistema Integrado	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8
Sistema Biblioteca Virtual	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8
Servidores	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8
Telefonía	[A.13] Repudio (negación de actuaciones)	5.7
Telefonía	[A.15] Modificación de la información	5.7
Telefonía	[A.18] Destrucción de la información	5.7
Telefonía	[A.19] Revelación de información	5.7
Telefonía	[A.24] Denegación de servicio	5.7
Aplicaciones Ofimática / Académicas	[I.5.1] Avería de origen lógico	5.7
Equipos PC y Didácticos	[I.5.2] Avería de origen físico	5.7
Equipos PC y Didácticos	[A.23] Manipulación del hardware	5.7
Equipamiento Eléctrico	[A.23] Manipulación del hardware	5.7
Mobiliario para los equipos	[A.23] Manipulación del hardware	5.7
Electrónicos (Nube Microsoft, OneDrive)	[E.25] Pérdida de equipos	5.7
Red Interna Biblioteca	[E.2] Errores del administrador del sistema / de la seguridad	5.6
Portal Web Biblioteca	[E.21] Errores de mantenimiento / actualización de programas (software)	5.6
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)	5.6
Equipos PC y Didácticos	[N.1] Fuego	5.4
Equipos PC y Didácticos	[N.*] Desastres naturales	5.4
Equipos PC y Didácticos	[I.2] Daños por agua	5.4

Equipos de Redes y Telecomunicaciones	[N.2] Daños por agua	5.4
Equipos de Redes y Telecomunicaciones	[I.3] Contaminación medioambiental	5.4
Electrónicos (Nube Microsoft, OneDrive)	[N.2] Daños por agua	5.4
Electrónicos (Nube Microsoft, OneDrive)	[A.23] Manipulación del hardware	5.4
Equipamiento Eléctrico	[N.1] Fuego	5.4
Equipamiento Eléctrico	[N.*] Desastres naturales	5.4
Equipamiento Eléctrico	[I.2] Daños por agua	5.4
Mobiliario para los equipos	[N.1] Fuego	5.4
Mobiliario para los equipos	[N.*] Desastres naturales	5.4
Mobiliario para los equipos	[I.2] Daños por agua	5.4
Espacios Físicos Biblioteca	[A.26] Ataque destructivo	5.4
Área de atención y soporte	[E.25] Pérdida de equipos	5.4
Área de atención y soporte	[A.26] Ataque destructivo	5.4
Equipos de Redes y Telecomunicaciones	[A.11] Acceso no autorizado	5.3
Personal administrativo informático	[A.28] Indisponibilidad del personal	5.3
Aplicaciones Ofimática / Académicas	[E.21] Errores de mantenimiento / actualización de programas (software)	5.2
Base de datos	[E.19] Fugas de información	5.1
Documentación interna	[E.19] Fugas de información	5.1
Servidores internos	[E.15] Alteración de la información	5.1
Servidores internos	[E.18] Destrucción de la información	5.1
Servidores internos	[E.19] Fugas de información	5.1
Internet	[E.15] Alteración de la información	5.1
Internet	[E.18] Destrucción de la información	5.1
Internet	[E.19] Fugas de información	5.1
Electricidad	[E.18] Destrucción de la información	5.1

Electricidad	[A.13] Repudio (negación de actuaciones)	5.1
Electricidad	[A.19] Revelación de información	5.1
Sistema Integrado	[E.8] Difusión de software dañino	5.1
Sistema Biblioteca Virtual	[E.8] Difusión de software dañino	5.1
Sistemas operativos	[E.8] Difusión de software dañino	5.1
Servidores	[E.8] Difusión de software dañino	5.1
Equipos de Redes y Telecomunicaciones	[I.4] Contaminación electromagnética	5.1
Equipos de Redes y Telecomunicaciones	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5.1
Red Interna Biblioteca	[E.9] Errores de [re-]encaminamiento	5.1
Red Interna Biblioteca	[E.10] Errores de secuencia	5.1
Red Interna Biblioteca	[E.19] Fugas de información	5.1
Red Interna Biblioteca	[A.7] Uso no previsto	5.1
Red Interna Biblioteca	[A.9] [Re-]encaminamiento de mensajes	5.1
Red Interna Biblioteca	[A.10] Alteración de secuencia	5.1
Red Interna Biblioteca	[A.14] Interceptación de información (escucha)	5.1
Red Interna Biblioteca	[A.15] Modificación de la información	5.1
Electrónicos (Nube Microsoft, OneDrive)	[I.4] Contaminación electromagnética	5.1
Electrónicos (Nube Microsoft, OneDrive)	[E.19] Fugas de información	5.1
Electrónicos (Nube Microsoft, OneDrive)	[A.26] Ataque destructivo	5.1
Equipamiento Eléctrico	[A.11] Acceso no autorizado	5.1
Personal administrativo informático	[E.15] Alteración de la información	5.1
Personal administrativo informático	[E.19] Fugas de información	5.1
Personal administrativo informático	[E.28] Indisponibilidad del personal	5.1

Personal administrativo informático	[A.18] Destrucción de la información	5.1
Servidores internos	[A.6] Abuso de privilegios de acceso	5.1
Portal Web Biblioteca	[E.8] Difusión de software dañino	4.9
Licencias	[E.8] Difusión de software dañino	4.9
Equipos PC y Didácticos	[A.11] Acceso no autorizado	4.9
Electricidad	[A.5] Suplantación de la identidad	4.8
Sistema Integrado	[E.20] Vulnerabilidades de los programas (software)	4.8
Sistema Biblioteca Virtual	[E.20] Vulnerabilidades de los programas (software)	4.8
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	4.8
Servidores	[E.20] Vulnerabilidades de los programas (software)	4.8
Mobiliario para los equipos	[A.25] Robo de equipos	4.8
Equipos PC y Didácticos	[N.2] Daños por agua	4.8
Equipos PC y Didácticos	[I.3] Contaminación medioambiental	4.8
Equipos de Redes y Telecomunicaciones	[A.7] Uso no previsto	4.8
Electrónicos (Nube Microsoft, OneDrive)	[A.11] Acceso no autorizado	4.8
Equipamiento Eléctrico	[N.2] Daños por agua	4.8
Equipamiento Eléctrico	[I.3] Contaminación medioambiental	4.8
Mobiliario para los equipos	[N.2] Daños por agua	4.8
Mobiliario para los equipos	[I.3] Contaminación medioambiental	4.8
Portal Web Biblioteca	[E.20] Vulnerabilidades de los programas (software)	4.6
Licencias	[E.20] Vulnerabilidades de los programas (software)	4.6
Electricidad	[A.15] Modificación de la información	4.5
Telefonía	[E.15] Alteración de la información	4.5
Telefonía	[E.18] Destrucción de la información	4.5

Telefonía	[E.19] Fugas de información	4.5
Aplicaciones Ofimática / Académicas	[E.8] Difusión de software dañino	4.5
Equipos PC y Didácticos	[I.4] Contaminación electromagnética	4.5
Equipos PC y Didácticos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5
Equipamiento Eléctrico	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5
Mobiliario para los equipos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5
Mobiliario para los equipos	[A.26] Ataque destructivo	4.5
Espacios Físicos Biblioteca	[I.3] Contaminación medioambiental	4.5
Espacios Físicos Biblioteca	[A.6] Abuso de privilegios de acceso	4.5
Espacios Físicos Biblioteca	[A.7] Uso no previsto	4.5
Área de atención y soporte	[I.3] Contaminación medioambiental	4.5
Área de atención y soporte	[A.6] Abuso de privilegios de acceso	4.5
Área de atención y soporte	[A.7] Uso no previsto	4.5
Servidores internos	[A.7] Uso no previsto	4.5
Base de datos	[A.6] Abuso de privilegios de acceso	4.4
Documentación interna	[A.6] Abuso de privilegios de acceso	4.4
Electrónicos (Nube Microsoft, OneDrive)	[E.1] Errores de los usuarios	4.3
Aplicaciones Ofimática / Académicas	[E.20] Vulnerabilidades de los programas (software)	4.2
Equipamiento Eléctrico	[I.4] Contaminación electromagnética	4.2
Espacios Físicos Biblioteca	[E.25] Pérdida de equipos	4.2
Electricidad	[E.19] Fugas de información	3.9
Equipos PC y Didácticos	[A.7] Uso no previsto	3.9
Red Interna Biblioteca	[A.12] Análisis de tráfico	3.8
Servidores internos	[E.2] Errores del administrador del sistema / de la seguridad	3.7
Equipamiento Eléctrico	[A.7] Uso no previsto	3.7

Mobiliario para los equipos	[A.7] Uso no previsto	3.7
Espacios Físicos Biblioteca	[I.4] Contaminación electromagnética	3.6
Área de atención y soporte	[I.4] Contaminación electromagnética	3.6
Servidores internos	[E.1] Errores de los usuarios	3.4
Base de datos	[E.15] Alteración de la información	3.3
Base de datos	[E.18] Destrucción de la información	3.3
Documentación interna	[E.15] Alteración de la información	3.3
Documentación interna	[E.18] Destrucción de la información	3.3
Electricidad	[E.15] Alteración de la información	3.3
Red Interna Biblioteca	[E.15] Alteración de la información	3.3
Electrónicos (Nube Microsoft, OneDrive)	[I.11] Emanaciones electromagnéticas (TEMPEST)	3.3
Electrónicos (Nube Microsoft, OneDrive)	[E.15] Alteración de la información	3.3
Electrónicos (Nube Microsoft, OneDrive)	[A.7] Uso no previsto	3.3
Personal administrativo informático	[E.18] Destrucción de la información	3.3
Equipos PC y Didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2.7
Equipos de Redes y Telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)	2.7
Equipamiento Eléctrico	[I.11] Emanaciones electromagnéticas (TEMPEST)	2.7
Personal administrativo informático	[E.19] Fugas de información	1
Personal administrativo informático	[E.28] Indisponibilidad del personal	1
Personal administrativo informático	[A.15] Modificación de la información	1
Personal administrativo informático	[A.18] Destrucción de la información	1
Personal administrativo informático	[A.19] Revelación de información	10

Personal administrativo informático	[A.28] Indisponibilidad del personal	0,5
Personal administrativo informático	[A.29] Extorsión	0,9
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	0,5

Nota: Elaboración propia.

Anexo J: Asignación de opción de tratamiento a los riesgos identificados en la Biblioteca de la UTN

ACTIVO	RIESGO	PESO PONDERADO	ACCIÓN
Base de datos	[A.11] Acceso no autorizado	7.5	Minimizar
Documentación interna	[A.11] Acceso no autorizado	7.5	Minimizar
Servidores internos	[A.13] Repudio (negación de actuaciones)	7.4	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[A.15] Modificación de la información	7.4	Minimizar
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	7.2	Minimizar
Servidores internos	[A.15] Modificación de la información	7.2	Minimizar
Servidores internos	[A.24] Denegación de servicio	7.2	Minimizar
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	7.2	Minimizar
Red Interna Biblioteca	[A.24] Denegación de servicio	7.2	Minimizar
Personal administrativo informático	[A.19] Revelación de información	7.2	Evitar
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio	7.1	Minimizar
Área de atención y soporte	[A.25] Robo de equipos	7.1	Minimizar
Base de datos	[A.5] Suplantación de la identidad	6.9	Minimizar

Documentación interna	[A.5] Suplantación de la identidad	6.9	Minimizar
Servidores internos	[A.5] Suplantación de la identidad	6.8	Minimizar
Internet	[I.8] Fallo de servicios de comunicaciones	6.8	Minimizar
Sistema Integrado	[A.8] Difusión de software dañino	6.8	Minimizar
Sistema Biblioteca Virtual	[A.8] Difusión de software dañino	6.8	Minimizar
Servidores	[A.8] Difusión de software dañino	6.8	Minimizar
Equipos de Redes y Telecomunicaciones	[I.6] Corte del suministro eléctrico	6.8	Aceptar
Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8	Minimizar
Equipos de Redes y Telecomunicaciones	[A.26] Ataque destructivo	6.8	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.6] Corte del suministro eléctrico	6.8	Aceptar
Electrónicos (Nube Microsoft, OneDrive)	[I.7] Condiciones inadecuadas de temperatura o humedad	6.8	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.10] Degradación de los soportes de almacenamiento de la información	6.8	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[E.18] Destrucción de la información	6.8	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[A.18] Destrucción de la información	6.8	Evitar
Sistema Integrado	[A.22] Manipulación de programas	6.6	Minimizar
Sistema Biblioteca Virtual	[A.22] Manipulación de programas	6.6	Minimizar
Sistemas operativos	[A.22] Manipulación de programas	6.6	Minimizar
Servidores	[A.22] Manipulación de programas	6.6	Minimizar
Personal administrativo informático	[A.29] Extorsión	6.6	Evitar

Portal Web Biblioteca	[A.8] Difusión de software dañino	6.6	Minimizar
Licencias	[A.8] Difusión de software dañino	6.6	Minimizar
Equipos PC y Didácticos	[E.24] Caída del sistema por agotamiento de recursos	6.6	Minimizar
Equipos PC y Didácticos	[E.25] Pérdida de equipos	6.6	Minimizar
Equipos PC y Didácticos	[A.25] Robo de equipos	6.6	Minimizar
Equipos de Redes y Telecomunicaciones	[I.1] Fuego	6.6	Minimizar
Equipos de Redes y Telecomunicaciones	[I.*] Desastres industriales	6.6	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.1] Fuego	6.6	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.*] Desastres industriales	6.6	Minimizar
Equipos PC y Didácticos	[A.24] Denegación de servicio	6.5	Minimizar
Sistemas operativos	[A.8] Difusión de software dañino	6.5	Minimizar
Portal Web Biblioteca	[A.22] Manipulación de programas	6.4	Minimizar
Licencias	[A.22] Manipulación de programas	6.4	Minimizar
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	6.4	Evitar
Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales	6.3	Minimizar
Servidores internos	[A.18] Destrucción de la información	6.3	Evitar
Servidores internos	[A.19] Revelación de información	6.3	Evitar
Internet	[A.15] Modificación de la información	6.3	Minimizar
Internet	[A.18] Destrucción de la información	6.3	Evitar
Internet	[A.19] Revelación de información	6.3	Evitar
Internet	[A.24] Denegación de servicio	6.3	Minimizar
Electricidad	[I.9] Interrupción de otros servicios o suministros esenciales	6.3	Minimizar

Electricidad	[A.18] Destrucción de la información	6.3	Evitar
Electricidad	[A.24] Denegación de servicio	6.3	Minimizar
Sistema Integrado	[I.5.1] Avería de origen lógico	6.3	Minimizar
Sistema Biblioteca Virtual	[I.5.1] Avería de origen lógico	6.3	Minimizar
Portal Web Biblioteca	[I.5.1] Avería de origen lógico	6.3	Minimizar
Licencias	[I.5.1] Avería de origen lógico	6.3	Minimizar
Sistemas operativos	[I.5.1] Avería de origen lógico	6.3	Minimizar
Servidores	[I.5.1] Avería de origen lógico	6.3	Minimizar
Equipos de Redes y Telecomunicaciones	[I.5.2] Avería de origen físico	6.3	Minimizar
Red Interna Biblioteca	[I.8] Fallo de servicios de comunicaciones	6.3	Minimizar
Red Interna Biblioteca	[E.24] Caída del sistema por agotamiento de recursos	6.3	Minimizar
Red Interna Biblioteca	[A.18] Destrucción de la información	6.3	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[I.3] Contaminación medioambiental	6.3	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.5.2] Avería de origen físico	6.3	Minimizar
Personal administrativo informático	[A.15] Modificación de la información	6.3	Minimizar
Equipos de Redes y Telecomunicaciones	[E.25] Pérdida de equipos	6.3	Minimizar
Internet	[A.5] Suplantación de la identidad	6.2	Minimizar
Internet	[A.13] Repudio (negación de actuaciones)	6.2	Minimizar
Telefonía	[I.8] Fallo de servicios de comunicaciones	6.2	Minimizar
Aplicaciones Ofimática / Académicas	[A.8] Difusión de software dañino	6.2	Minimizar

Equipos PC y Didácticos	[I.6] Corte del suministro eléctrico	6.2	Aceptar
Equipos PC y Didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad	6.2	Minimizar
Equipos PC y Didácticos	[A.26] Ataque destructivo	6.2	Minimizar
Equipamiento Eléctrico	[A.25] Robo de equipos	6.2	Minimizar
Equipamiento Eléctrico	[A.26] Ataque destructivo	6.2	Minimizar
Espacios Físicos Biblioteca	[N.1] Fuego	6.2	Minimizar
Espacios Físicos Biblioteca	[N.2] Daños por agua	6.2	Evitar
Espacios Físicos Biblioteca	[I.1] Fuego	6.2	Minimizar
Espacios Físicos Biblioteca	[I.2] Daños por agua	6.2	Evitar
Espacios Físicos Biblioteca	[I.*] Desastres industriales	6.2	Minimizar
Espacios Físicos Biblioteca	[A.27] Ocupación enemiga	6.2	Aceptar
Área de atención y soporte	[N.1] Fuego	6.2	Minimizar
Área de atención y soporte	[N.2] Daños por agua	6.2	Evitar
Área de atención y soporte	[I.1] Fuego	6.2	Minimizar
Área de atención y soporte	[I.2] Daños por agua	6.2	Evitar
Área de atención y soporte	[I.*] Desastres industriales	6.2	Minimizar
Área de atención y soporte	[A.27] Ocupación enemiga	6.2	Aceptar
Servidores internos	[A.11] Acceso no autorizado	6.1	Minimizar
Red Interna Biblioteca	[A.5] Suplantación de la identidad	6.1	Minimizar

Red Interna Biblioteca	[A.11] Acceso no autorizado	6.1	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	6.1	Minimizar
Aplicaciones Ofimática / Académicas	[A.22] Manipulación de programas	6.0	Minimizar
Equipos PC y Didácticos	[I.1] Fuego	6	Minimizar
Equipos PC y Didácticos	[I.*] Desastres industriales	6	Minimizar
Equipos de Redes y Telecomunicaciones	[I.2] Daños por agua	6.0	Evitar
Equipos de Redes y Telecomunicaciones	[A.23] Manipulación del hardware	6.0	Evitar
Equipos de Redes y Telecomunicaciones	[A.25] Robo de equipos	6.0	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.2] Daños por agua	6.0	Evitar
Equipamiento Eléctrico	[I.1] Fuego	6.0	Minimizar
Equipamiento Eléctrico	[I.*] Desastres industriales	6.0	Minimizar
Mobiliario para los equipos	[I.1] Fuego	6.0	Minimizar
Mobiliario para los equipos	[I.*] Desastres industriales	6.0	Minimizar
Espacios Físicos Biblioteca	[N.*] Desastres naturales	6.0	Minimizar
Área de atención y soporte	[N.*] Desastres naturales	6.0	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[A.25] Robo de equipos	6.0	Minimizar
Equipos de Redes y Telecomunicaciones	[N.1] Fuego	5.9	Minimizar
Equipos de Redes y Telecomunicaciones	[N.*] Desastres naturales	5.9	Minimizar

Electrónicos (Nube Microsoft, OneDrive)	[N.1] Fuego	5.9	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[N.*] Desastres naturales	5.9	Minimizar
Espacios Físicos Biblioteca	[A.25] Robo de equipos	5.9	Minimizar
Telefonía	[A.5] Suplantación de la identidad	5.8	Minimizar
Sistema Integrado	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8	Minimizar
Sistema Biblioteca Virtual	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8	Minimizar
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8	Minimizar
Servidores	[E.21] Errores de mantenimiento / actualización de programas (software)	5.8	Minimizar
Telefonía	[A.13] Repudio (negación de actuaciones)	5.7	Minimizar
Telefonía	[A.15] Modificación de la información	5.7	Minimizar
Telefonía	[A.18] Destrucción de la información	5.7	Evitar
Telefonía	[A.19] Revelación de información	5.7	Evitar
Telefonía	[A.24] Denegación de servicio	5.7	Minimizar
Aplicaciones Ofimática / Académicas	[I.5.1] Avería de origen lógico	5.7	Minimizar
Equipos PC y Didácticos	[I.5.2] Avería de origen físico	5.7	Minimizar
Equipos PC y Didácticos	[A.23] Manipulación del hardware	5.7	Evitar
Equipamiento Eléctrico	[A.23] Manipulación del hardware	5.7	Evitar
Mobiliario para los equipos	[A.23] Manipulación del hardware	5.7	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[E.25] Pérdida de equipos	5.7	Minimizar

Red Interna Biblioteca	[E.2] Errores del administrador del sistema / de la seguridad	5.6	Minimizar
Portal Web Biblioteca	[E.21] Errores de mantenimiento / actualización de programas (software)	5.6	Minimizar
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)	5.6	Minimizar
Equipos PC y Didácticos	[N.1] Fuego	5.4	Minimizar
Equipos PC y Didácticos	[N.*] Desastres naturales	5.4	Minimizar
Equipos PC y Didácticos	[I.2] Daños por agua	5.4	Evitar
Equipos de Redes y Telecomunicaciones	[N.2] Daños por agua	5.4	Evitar
Equipos de Redes y Telecomunicaciones	[I.3] Contaminación medioambiental	5.4	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[N.2] Daños por agua	5.4	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[A.23] Manipulación del hardware	5.4	Evitar
Equipamiento Eléctrico	[N.1] Fuego	5.4	Minimizar
Equipamiento Eléctrico	[N.*] Desastres naturales	5.4	Minimizar
Equipamiento Eléctrico	[I.2] Daños por agua	5.4	Evitar
Mobiliario para los equipos	[N.1] Fuego	5.4	Minimizar
Mobiliario para los equipos	[N.*] Desastres naturales	5.4	Minimizar
Mobiliario para los equipos	[I.2] Daños por agua	5.4	Evitar
Espacios Físicos Biblioteca	[A.26] Ataque destructivo	5.4	Minimizar
Área de atención y soporte	[E.25] Pérdida de equipos	5.4	Minimizar
Área de atención y soporte	[A.26] Ataque destructivo	5.4	Minimizar

Equipos de Redes y Telecomunicaciones	[A.11] Acceso no autorizado	5.3	Minimizar
Personal administrativo informático	[A.28] Indisponibilidad del personal	5.3	Minimizar
Aplicaciones Ofimática / Académicas	[E.21] Errores de mantenimiento / actualización de programas (software)	5.2	Minimizar
Base de datos	[E.19] Fugas de información	5.1	Minimizar
Documentación interna	[E.19] Fugas de información	5.1	Minimizar
Servidores internos	[E.15] Alteración de la información	5.1	Minimizar
Servidores internos	[E.18] Destrucción de la información	5.1	Evitar
Servidores internos	[E.19] Fugas de información	5.1	Minimizar
Internet	[E.15] Alteración de la información	5.1	Minimizar
Internet	[E.18] Destrucción de la información	5.1	Evitar
Internet	[E.19] Fugas de información	5.1	Minimizar
Electricidad	[E.18] Destrucción de la información	5.1	Evitar
Electricidad	[A.13] Repudio (negación de actuaciones)	5.1	Minimizar
Electricidad	[A.19] Revelación de información	5.1	Evitar
Sistema Integrado	[E.8] Difusión de software dañino	5.1	Minimizar
Sistema Biblioteca Virtual	[E.8] Difusión de software dañino	5.1	Minimizar
Sistemas operativos	[E.8] Difusión de software dañino	5.1	Minimizar
Servidores	[E.8] Difusión de software dañino	5.1	Minimizar
Equipos de Redes y Telecomunicaciones	[I.4] Contaminación electromagnética	5.1	Minimizar
Equipos de Redes y Telecomunicaciones	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5.1	Minimizar
Red Interna Biblioteca	[E.9] Errores de [re-]encaminamiento	5.1	Minimizar
Red Interna Biblioteca	[E.10] Errores de secuencia	5.1	Minimizar

Red Interna Biblioteca	[E.19] Fugas de información	5.1	Minimizar
Red Interna Biblioteca	[A.7] Uso no previsto	5.1	Evitar
Red Interna Biblioteca	[A.9] [Re-]encaminamiento de mensajes	5.1	Evitar
Red Interna Biblioteca	[A.10] Alteración de secuencia	5.1	Evitar
Red Interna Biblioteca	[A.14] Interceptación de información (escucha)	5.1	Evitar
Red Interna Biblioteca	[A.15] Modificación de la información	5.1	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.4] Contaminación electromagnética	5.1	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[E.19] Fugas de información	5.1	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[A.26] Ataque destructivo	5.1	Minimizar
Equipamiento Eléctrico	[A.11] Acceso no autorizado	5.1	Minimizar
Personal administrativo informático	[E.15] Alteración de la información	5.1	Minimizar
Personal administrativo informático	[E.19] Fugas de información	5.1	Minimizar
Personal administrativo informático	[E.28] Indisponibilidad del personal	5.1	Minimizar
Personal administrativo informático	[A.18] Destrucción de la información	5.1	Evitar
Servidores internos	[A.6] Abuso de privilegios de acceso	5.1	Evitar
Portal Web Biblioteca	[E.8] Difusión de software dañino	4.9	Minimizar
Licencias	[E.8] Difusión de software dañino	4.9	Minimizar
Equipos PC y Didácticos	[A.11] Acceso no autorizado	4.9	Minimizar
Electricidad	[A.5] Suplantación de la identidad	4.8	Minimizar
Sistema Integrado	[E.20] Vulnerabilidades de los programas (software)	4.8	Minimizar
Sistema Biblioteca Virtual	[E.20] Vulnerabilidades de los programas (software)	4.8	Minimizar

Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	4.8	Minimizar
Servidores	[E.20] Vulnerabilidades de los programas (software)	4.8	Minimizar
Mobiliario para los equipos	[A.25] Robo de equipos	4.8	Minimizar
Equipos PC y Didácticos	[N.2] Daños por agua	4.8	Evitar
Equipos PC y Didácticos	[I.3] Contaminación medioambiental	4.8	Minimizar
Equipos de Redes y Telecomunicaciones	[A.7] Uso no previsto	4.8	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[A.11] Acceso no autorizado	4.8	Minimizar
Equipamiento Eléctrico	[N.2] Daños por agua	4.8	Evitar
Equipamiento Eléctrico	[I.3] Contaminación medioambiental	4.8	Minimizar
Mobiliario para los equipos	[N.2] Daños por agua	4.8	Evitar
Mobiliario para los equipos	[I.3] Contaminación medioambiental	4.8	Minimizar
Portal Web Biblioteca	[E.20] Vulnerabilidades de los programas (software)	4.6	Minimizar
Licencias	[E.20] Vulnerabilidades de los programas (software)	4.6	Minimizar
Electricidad	[A.15] Modificación de la información	4.5	Minimizar
Telefonía	[E.15] Alteración de la información	4.5	Minimizar
Telefonía	[E.18] Destrucción de la información	4.5	Evitar
Telefonía	[E.19] Fugas de información	4.5	Minimizar
Aplicaciones Ofimática / Académicas	[E.8] Difusión de software dañino	4.5	Minimizar
Equipos PC y Didácticos	[I.4] Contaminación electromagnética	4.5	Minimizar
Equipos PC y Didácticos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5	Minimizar

Equipamiento Eléctrico	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5	Minimizar
Mobiliario para los equipos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4.5	Minimizar
Mobiliario para los equipos	[A.26] Ataque destructivo	4.5	Minimizar
Espacios Físicos Biblioteca	[I.3] Contaminación medioambiental	4.5	Minimizar
Espacios Físicos Biblioteca	[A.6] Abuso de privilegios de acceso	4.5	Evitar
Espacios Físicos Biblioteca	[A.7] Uso no previsto	4.5	Evitar
Área de atención y soporte	[I.3] Contaminación medioambiental	4.5	Minimizar
Área de atención y soporte	[A.6] Abuso de privilegios de acceso	4.5	Evitar
Área de atención y soporte	[A.7] Uso no previsto	4.5	Evitar
Servidores internos	[A.7] Uso no previsto	4.5	Evitar
Base de datos	[A.6] Abuso de privilegios de acceso	4.4	Evitar
Documentación interna	[A.6] Abuso de privilegios de acceso	4.4	Evitar
Electrónicos (Nube Microsoft, OneDrive)	[E.1] Errores de los usuarios	4.3	Minimizar
Aplicaciones Ofimática / Académicas	[E.20] Vulnerabilidades de los programas (software)	4.2	Minimizar
Equipamiento Eléctrico	[I.4] Contaminación electromagnética	4.2	Minimizar
Espacios Físicos Biblioteca	[E.25] Pérdida de equipos	4.2	Minimizar
Electricidad	[E.19] Fugas de información	3.9	Minimizar
Equipos PC y Didácticos	[A.7] Uso no previsto	3.9	Evitar
Red Interna Biblioteca	[A.12] Análisis de tráfico	3.8	Evitar

Servidores internos	[E.2] Errores del administrador del sistema / de la seguridad	3.7	Minimizar
Equipamiento Eléctrico	[A.7] Uso no previsto	3.7	Evitar
Mobiliario para los equipos	[A.7] Uso no previsto	3.7	Evitar
Espacios Físicos Biblioteca	[I.4] Contaminación electromagnética	3.6	Minimizar
Área de atención y soporte	[I.4] Contaminación electromagnética	3.6	Minimizar
Servidores internos	[E.1] Errores de los usuarios	3.4	Minimizar
Base de datos	[E.15] Alteración de la información	3.3	Minimizar
Base de datos	[E.18] Destrucción de la información	3.3	Evitar
Documentación interna	[E.15] Alteración de la información	3.3	Minimizar
Documentación interna	[E.18] Destrucción de la información	3.3	Evitar
Electricidad	[E.15] Alteración de la información	3.3	Minimizar
Red Interna Biblioteca	[E.15] Alteración de la información	3.3	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[I.11] Emanaciones electromagnéticas (TEMPEST)	3.3	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[E.15] Alteración de la información	3.3	Minimizar
Electrónicos (Nube Microsoft, OneDrive)	[A.7] Uso no previsto	3.3	Evitar
Personal administrativo informático	[E.18] Destrucción de la información	3.3	Evitar
Equipos PC y Didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)	2.7	Minimizar
Equipos de Redes y Telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)	2.7	Minimizar
Equipamiento Eléctrico	[I.11] Emanaciones electromagnéticas (TEMPEST)	2.7	Minimizar

Personal administrativo informático	[E.19] Fugas de información	1	Minimizar
Personal administrativo informático	[E.28] Indisponibilidad del personal	1	Minimizar
Personal administrativo informático	[A.15] Modificación de la información	1	Minimizar
Personal administrativo informático	[A.18] Destrucción de la información	1	Evitar
Personal administrativo informático	[A.19] Revelación de información	10	Evitar
Personal administrativo informático	[A.28] Indisponibilidad del personal	0,5	Minimizar
Personal administrativo informático	[A.29] Extorsión	0,9	Evitar
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	0,5	Evitar

Nota: Elaboración propia.

Anexo K: Identificación de Tareas por Salvaguardas para la Biblioteca de la UTN

ACTIVO AFECTADO	RIESGO	TRATAMIENTO	SALVAGUARDA	TIPO DE PROTECCIÓN	TAREA PROPUESTA
Base de datos	[A.11] Acceso no autorizado	Minimizar	[IA] Identificación y autenticación	EL	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario
Documentación interna	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
Servidores internos	[A.13] Repudio (negación de actuaciones)	Minimizar	[K] Protección de claves criptográficas	EL	Implementación del cifrado hash para el almacenamiento de contraseñas
Electrónicos (Nube Microsoft, OneDrive)	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Servidores internos	[E.24] Caída del sistema por agotamiento de recursos	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Servidores internos	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN

Servidores internos	[A.24] Denegación de servicio	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques
Equipos de Redes y Telecomunicaciones	[E.24] Caída del sistema por agotamiento de recursos	Minimizar	[V] Gestión de vulnerabilidades	PR	Desarrollar un manual de emergencia para las redes de comunicaciones
Red Interna Biblioteca	[A.24] Denegación de servicio	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)
Personal administrativo informático	[A.19] Revelación de información	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Equipos de Redes y Telecomunicaciones	[A.24] Denegación de servicio	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)
Área de atención y soporte	[A.25] Robo de equipos	Minimizar	[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
Base de datos	[A.5] Suplantación de la identidad	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso

Documentación interna	[A.5] Suplantación de la identidad	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
Servidores internos	[A.5] Suplantación de la identidad	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
Internet	[I.8] Fallo de servicios de comunicaciones	Minimizar	[BC] Continuidad del negocio	RC	Implementación de un Plan en caso de fallo de Internet
Sistema Integrado	[A.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte
Sistema Biblioteca Virtual	[A.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte

Servidores	[A.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte
Equipos de Redes y Telecomunicaciones	[I.6] Corte del suministro eléctrico	Aceptar	[AUX] Elementos auxiliares	PR	Corrección de la carga de dispositivos electrónicos en la distribución de red eléctrica
Equipos de Redes y Telecomunicaciones	[I.7] Condiciones inadecuadas de temperatura o humedad	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
Equipos de Redes y Telecomunicaciones	[A.26] Ataque destructivo	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Electrónicos (Nube Microsoft, OneDrive)	[I.6] Corte del suministro eléctrico	Aceptar	[AUX] Elementos auxiliares	PR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Electrónicos (Nube Microsoft, OneDrive)	[I.7] Condiciones inadecuadas de temperatura o humedad	Minimizar	[AUX] Elementos auxiliares	PR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Electrónicos (Nube Microsoft, OneDrive)	[I.10] Degradación de los soportes de almacenamiento de la información	Evitar	[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)

Electrónicos (Nube Microsoft, OneDrive)	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de almacenamiento
Electrónicos (Nube Microsoft, OneDrive)	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos
Sistema Integrado	[A.22] Manipulación de programas	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte
Sistema Biblioteca Virtual	[A.22] Manipulación de programas	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte
Sistemas operativos	[A.22] Manipulación de programas	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte
Servidores	[A.22] Manipulación de programas	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Implementación de firewall para la red interna de la Biblioteca de la UTN
Personal administrativo informático	[A.29] Extorsión	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Portal Web Biblioteca	[A.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte
Licencias	[A.8] Difusión de software dañino	Minimizar	[BC] Continuidad del negocio	RC	Desarrollar un Plan de Continuidad del Negocio para Mitigar el Riesgo de Difusión de Software Dañino en las Licencias
Equipos PC y Didácticos	[E.24] Caída del sistema por agotamiento de recursos	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Equipos PC y Didácticos	[E.25] Pérdida de equipos	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
Equipos PC y Didácticos	[A.25] Robo de equipos	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipos de Redes y Telecomunicaciones	[I.1] Fuego	Minimizar	[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)
Equipos de Redes y Telecomunicaciones	[I.*] Desastres industriales	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware

Electrónicos (Nube Microsoft, OneDrive)	[I.1] Fuego	Minimizar	[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)
Electrónicos (Nube Microsoft, OneDrive)	[I.*] Desastres industriales	Minimizar	[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)
Equipos PC y Didácticos	[A.24] Denegación de servicio	Minimizar	[S] Protección de los servicios	PR	Establecimiento de un Plan de renovación de equipos de hardware por vida útil
Sistema operativos	[A.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte
Portal Web Biblioteca	[A.22] Manipulación de programas	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Implementación de firewall para la red interna de la Biblioteca de la UTN
Licencias	[A.22] Manipulación de programas	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Desarrollo de la documentación de programas y archivos
Personal administrativo informático	[A.30] Ingeniería social (picaresca)	Evitar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Servidores internos	[I.9] Interrupción de otros servicios o suministros esenciales	Minimizar	[D] Protección de la información	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)
Servidores internos	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos
Servidores internos	[A.19] Revelación de información	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Internet	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Internet	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos
Internet	[A.19] Revelación de información	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Internet	[A.24] Denegación de servicio	Minimizar	[BC] Continuidad del negocio	RC	Desarrollar e Implementar un Plan de Continuidad del Negocio para Mitigar la Denegación de Servicio en Internet
Electricidad	[I.9] Interrupción de otros servicios o suministros esenciales	Minimizar	[AUX] Elementos auxiliares	PR	Desarrollo de un Plan de Emergencia en caso de fallas eléctricas
Electricidad	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos
Electricidad	[A.24] Denegación de servicio	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de un Plan de Respuesta ante incidentes de Corte de Electricidad
Sistema Integrado	[I.5.1] Avería de origen lógico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Sistema Biblioteca Virtual	[I.5.1] Avería de origen lógico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Portal Web Biblioteca	[I.5.1] Avería de origen lógico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Licencias	[I.5.1] Avería de origen lógico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software

Sistema operativos	[I.5.1] Avería de origen lógico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Sistemas Operativos
Servidores	[I.5.1] Avería de origen lógico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software en Servidores
Equipos de Redes y Telecomunicaciones	[I.5.2] Avería de origen físico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Comunicaciones
Red Interna Biblioteca	[I.8] Fallo de servicios de comunicaciones	Minimizar	[BC] Continuidad del negocio	RC	Implementación de un Plan en caso de fallo de comunicaciones
Red Interna Biblioteca	[E.24] Caída del sistema por agotamiento de recursos	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Red Interna Biblioteca	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos
Electrónicos (Nube Microsoft, OneDrive)	[I.3] Contaminación medioambiental	Minimizar	[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)
Electrónicos (Nube Microsoft, OneDrive)	[I.5.2] Avería de origen físico	Minimizar	[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)

Personal administrativo informático	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Equipos de Redes y Telecomunicaciones	[E.25] Pérdida de equipos	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
Internet	[A.5] Suplantación de la identidad	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Internet	[A.13] Repudio (negación de actuaciones)	Minimizar	[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras
Telefonía	[I.8] Fallo de servicios de comunicaciones	Minimizar	[BC] Continuidad del negocio	RC	Implementación de un Plan en caso de fallo de comunicaciones
Aplicaciones Ofimática / Académicas	[A.8] Difusión de software dañino	Minimizar	[BC] Continuidad del negocio	RC	Implantación de un software de antivirus y antimalware efectivo
Equipos PC y Didácticos	[I.6] Corte del suministro eléctrico	Aceptar	[AUX] Elementos auxiliares	PR	Implementación de UPS para mantener operativos los servicios
Equipos PC y Didácticos	[I.7] Condiciones inadecuadas de temperatura o humedad	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de equipo de aire acondicionado para evitar recalentamiento de equipos

Equipos PC y Didácticos	[A.26] Ataque destructivo	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipamiento Eléctrico	[A.25] Robo de equipos	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipamiento Eléctrico	[A.26] Ataque destructivo	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Espacios Físicos Biblioteca	[N.1] Fuego	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
Espacios Físicos Biblioteca	[N.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	PR	Corregir las falencias en las paredes y techos para evitar humedad
Espacios Físicos Biblioteca	[I.1] Fuego	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)
Espacios Físicos Biblioteca	[I.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	MI	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)

Espacios Físicos Biblioteca	[I.*] Desastres industriales	Minimizar	[V] Gestión de vulnerabilidades	MI	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)
Espacios Físicos Biblioteca	[A.27] Ocupación enemiga	Aceptar	[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
Área de atención y soporte	[N.1] Fuego	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
Área de atención y soporte	[N.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	PR	Corregir las falencias en las paredes y techos para evitar humedad
Área de atención y soporte	[I.1] Fuego	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)
Área de atención y soporte	[I.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de políticas de uso para los usuarios de la Biblioteca de la UTN
Área de atención y soporte	[I.*] Desastres industriales	Minimizar	[V] Gestión de vulnerabilidades	MI	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)

Área de atención y soporte	[A.27] Ocupación enemiga	Aceptar	[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
Servidores internos	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
Red Interna Biblioteca	[A.5] Suplantación de la identidad	Minimizar	[AC] Control de acceso lógico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
Red Interna Biblioteca	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Restricciones de acceso a Equipos y Servidores mediante asignación de perfiles de usuario
Electrónicos (Nube Microsoft, OneDrive)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Aplicaciones Ofimática / Académicas	[A.22] Manipulación de programas	Minimizar	[SW] Protección de las aplicaciones informáticas	CR	Desarrollo de la documentación de programas y archivos

Equipos PC y Didácticos	[I.1] Fuego	Minimizar	[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)
Equipos PC y Didácticos	[I.*] Desastres industriales	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware
Equipos de Redes y Telecomunicaciones	[I.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidad	CR	Establecimiento de políticas de uso para los usuarios de la Biblioteca de la UTN
Equipos de Redes y Telecomunicaciones	[A.23] Manipulación del hardware	Evitar	[HW] Protección de los equipos informáticos	PR	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipos de Redes y Telecomunicaciones	[A.25] Robo de equipos	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Electrónicos (Nube Microsoft, OneDrive)	[I.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
Equipamiento Eléctrico	[I.1] Fuego	Minimizar	[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)

Equipamiento Eléctrico	[I.*] Desastres industriales	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de buenas prácticas para la adquisición de Hardware
Mobiliario para los equipos	[I.1] Fuego	Minimizar	[HW] Protección de los equipos informáticos	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)
Mobiliario para los equipos	[I.*] Desastres industriales	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)
Espacios Físicos Biblioteca	[N.*] Desastres naturales	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Área de atención y soporte	[N.*] Desastres naturales	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Electrónicos (Nube Microsoft, OneDrive)	[A.25] Robo de equipos	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipos de Redes y Telecomunicaciones	[N.1] Fuego	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores

Equipos de Redes y Telecomunicaciones	[N.*] Desastres naturales	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Electrónicos (Nube Microsoft, OneDrive)	[N.1] Fuego	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
Electrónicos (Nube Microsoft, OneDrive)	[N.*] Desastres naturales	Minimizar	S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)
Espacios Físicos Biblioteca	[A.25] Robo de equipos	Minimizar	[A] Registro y auditoría	MN	Implementación de registro de acceso a la Biblioteca
Telefonía	[A.5] Suplantación de la identidad	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
Sistema Integrado	[E.21] Errores de mantenimiento / actualización de programas (software)	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Sistema Biblioteca Virtual	[E.21] Errores de mantenimiento / actualización de programas (software)	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN

Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Servidores	[E.21] Errores de mantenimiento / actualización de programas (software)	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Telefonía	[A.13] Repudio (negación de actuaciones)	Minimizar	[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras
Telefonía	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Telefonía	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos
Telefonía	[A.19] Revelación de información	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Telefonía	[A.24] Denegación de servicio	Minimizar	[BC] Continuidad del negocio	PR	Establecimiento de un Plan de Respuesta ante incidentes de Telefonía

Aplicaciones Ofimática / Académicas	[I.5.1] Avería de origen lógico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Equipos PC y Didácticos	[I.5.2] Avería de origen físico	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Equipos PC y Didácticos	[A.23] Manipulación del hardware	Evitar	[HW] Protección de los equipos informáticos	PR	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipamiento Eléctrico	[A.23] Manipulación del hardware	Evitar	[HW] Protección de los equipos informáticos	PR	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Mobiliario para los equipos	[A.23] Manipulación del hardware	Evitar	[HW] Protección de los equipos informáticos	PR	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Electrónicos (Nube Microsoft, OneDrive)	[E.25] Pérdida de equipos	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
Red Interna Biblioteca	[E.2] Errores del administrador del sistema / de la seguridad	Minimizar	[BC] Continuidad del negocio	RC	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN

Portal Web Biblioteca	[E.21] Errores de mantenimiento / actualización de programas (software)	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Equipos PC y Didácticos	[N.1] Fuego	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
Equipos PC y Didácticos	[N.*] Desastres naturales	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Equipos PC y Didácticos	[I.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Equipos de Redes y Telecomunicaciones	[N.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	PR	Corregir las falencias en las paredes y techos para evitar humedad
Equipos de Redes y Telecomunicaciones	[I.3] Contaminación medioambiental	Minimizar	[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)

Electrónicos (Nube Microsoft, OneDrive)	[N.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
Electrónicos (Nube Microsoft, OneDrive)	[A.23] Manipulación del hardware	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de almacenamiento
Equipamiento Eléctrico	[N.1] Fuego	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
Equipamiento Eléctrico	[N.*] Desastres naturales	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Equipamiento Eléctrico	[I.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
Mobiliario para los equipos	[N.1] Fuego	Minimizar	[PPE] Protección física de los equipos	EL	Instalación de detectores de humo, alarmas contra incendios, extintores
Mobiliario para los equipos	[N.*] Desastres naturales	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)

Mobiliario para los equipos	[I.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica)
Espacios Físicos Biblioteca	[A.26] Ataque destructivo	Aceptar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Área de atención y soporte	[E.25] Pérdida de equipos	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
Área de atención y soporte	[A.26] Ataque destructivo	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipos de Redes y Telecomunicaciones	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a la Red.
Personal administrativo informático	[A.28] Indisponibilidad del personal	Minimizar	[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras
Aplicaciones Ofimática / Académicas	[E.21] Errores de mantenimiento /	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN

	actualización de programas (software)				
Base de datos	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Documentación interna	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Servidores internos	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Servidores internos	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de servidores
Servidores internos	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Internet	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo

Internet	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de Internet
Internet	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad con el proveedor de Internet de la Biblioteca de la UTN
Electricidad	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de Electricidad
Electricidad	[A.13] Repudio (negación de actuaciones)	Minimizar	[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras
Electricidad	[A.19] Revelación de información	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Sistema Integrado	[E.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte
Sistema Biblioteca Virtual	[E.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte

Sistemas operativos	[E.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte
Servidores	[E.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte
Equipos de Redes y Telecomunicaciones	[I.4] Contaminación electromagnética	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
Equipos de Redes y Telecomunicaciones	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Red Interna Biblioteca	[E.9] Errores de [re-]encaminamiento	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
Red Interna Biblioteca	[E.10] Errores de secuencia	Minimizar	[V] Gestión de vulnerabilidades	CR	Implementación de Controles de Validación y Monitoreo de Secuencias
Red Interna Biblioteca	[E.19] Fugas de información	Minimizar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Red Interna Biblioteca	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Red Interna Biblioteca	[A.9] [Re-]encaminamiento de mensajes	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Red Interna Biblioteca	[A.10] Alteración de secuencia	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Red Interna Biblioteca	[A.14] Interceptación de información (escucha)	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Red Interna Biblioteca	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Electrónicos (Nube Microsoft, OneDrive)	[I.4] Contaminación electromagnética	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
Electrónicos (Nube Microsoft, OneDrive)	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Electrónicos (Nube Microsoft, OneDrive)	[A.26] Ataque destructivo	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Equipamiento Eléctrico	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
Personal administrativo informático	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Personal administrativo informático	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Personal administrativo informático	[E.28] Indisponibilidad del personal	Minimizar	[P] Gestión del Personal	PR	Implementación de Acuerdos de Compromiso y responsabilidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Personal administrativo informático	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos por parte del personal administrativo

Servidores internos	[A.6] Abuso de privilegios de acceso	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Portal Web Biblioteca	[E.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte
Licencias	[E.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte
Equipos PC y Didácticos	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
Electricidad	[A.5] Suplantación de la identidad	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para el uso de contraseñas seguras en las cuentas de acceso
Sistema Integrado	[E.20] Vulnerabilidades de los programas (software)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades en el software utilizado

Sistema Biblioteca Virtual	[E.20] Vulnerabilidades de los programas (software)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades en el software utilizado
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades de los Sistemas operativos
Servidores	[E.20] Vulnerabilidades de los programas (software)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades en el software utilizado
Mobiliario para los equipos	[A.25] Robo de equipos	Minimizar	[PPS] Protección del perímetro físico	EL	Implementación de controles de acceso físico, biométrico y de vigilancia en las instalaciones
Equipos PC y Didácticos	[N.2] Daños por agua	Evitar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de emergencia ante desastres naturales (Fuego, daños por agua, temblores)
Equipos PC y Didácticos	[I.3] Contaminación medioambiental	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de emergencia ante Contaminación medioambiental

Equipos de Redes y Telecomunicaciones	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Electrónicos (Nube Microsoft, OneDrive)	[A.11] Acceso no autorizado	Minimizar	[AC] Control de acceso lógico	EL	Establecimiento de una normativa para la administración de cuentas de acceso a los Equipos PC y Servidores
Equipamiento Eléctrico	[N.2] Daños por agua	Evitar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de emergencia ante desastres naturales (Fuego, daños por agua, temblores)
Equipamiento Eléctrico	[I.3] Contaminación medioambiental	Minimizar	[S] Protección de los servicios	PR	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento, electricidad)
Mobiliario para los equipos	[N.2] Daños por agua	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de emergencia ante desastres naturales (Fuego, daños por agua, temblores)
Mobiliario para los equipos	[I.3] Contaminación medioambiental	Minimizar	[S] Protección de los servicios	PR	Establecimiento de un Plan de emergencia ante Contaminación medioambiental
Portal Web Biblioteca	[E.20] Vulnerabilidades de los programas (software)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades en el software utilizado

Licencias	[E.20] Vulnerabilidades de los programas (software)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades en el software utilizado
Electricidad	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Telefonía	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Telefonía	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de Telefonía
Telefonía	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad con el proveedor de telefonía de la Biblioteca de la UTN
Aplicaciones Ofimática / Académicas	[E.8] Difusión de software dañino	Minimizar	[SW] Protección de las aplicaciones informáticas	PR	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte
Equipos PC y Didácticos	[I.4] Contaminación electromagnética	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware

Equipos PC y Didácticos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Equipamiento Eléctrico	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Mobiliario para los equipos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Mantenimiento de Hardware y Software
Mobiliario para los equipos	[A.26] Ataque destructivo	Minimizar	[BC] Continuidad del negocio	RC	Establecimiento de una normativa para imponer sanciones ante daños a los activos
Espacios Físicos Biblioteca	[I.3] Contaminación medioambiental	Minimizar	[S] Protección de los servicios	PR	Establecimiento de un Plan de emergencia ante Contaminación medioambiental
Espacios Físicos Biblioteca	[A.6] Abuso de privilegios de acceso	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Espacios Físicos Biblioteca	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Área de atención y soporte	[I.3] Contaminación medioambiental	Minimizar	[S] Protección de los servicios	PR	Establecimiento de un Plan de emergencia ante Contaminación medioambiental
Área de atención y soporte	[A.6] Abuso de privilegios de acceso	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Área de atención y soporte	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Servidores internos	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Base de datos	[A.6] Abuso de privilegios de acceso	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Documentación interna	[A.6] Abuso de privilegios de acceso	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Electrónicos (Nube Microsoft, OneDrive)	[E.1] Errores de los usuarios	Minimizar	[P] Gestión del Personal	PR	Establecimiento de un Programa de Capacitación Continua
Aplicaciones Ofimática / Académicas	[E.20] Vulnerabilidades de los programas (software)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades en el software utilizado
Equipamiento Eléctrico	[I.4] Contaminación electromagnética	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
Espacios Físicos Biblioteca	[E.25] Pérdida de equipos	Minimizar	[HW] Protección de los equipos informáticos	PR	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware
Electricidad	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad con el proveedor de Electricidad de la Biblioteca de la UTN

Equipos PC y Didácticos	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Red Interna Biblioteca	[A.12] Análisis de tráfico	Evitar	[D] Protección de la información	PR	Implementación de Encriptación del Tráfico de Red.
Servidores internos	[E.2] Errores del administrador del sistema / de la seguridad	Minimizar	[BC] Continuidad del negocio	RC	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Equipamiento Eléctrico	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Mobiliario para los equipos	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad para la Biblioteca de la UTN
Espacios Físicos Biblioteca	[I.4] Contaminación electromagnética	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
Área de atención y soporte	[I.4] Contaminación electromagnética	Minimizar	[PPE] Protección física de los equipos	EL	Establecimiento de un Protocolo de ubicación correcta para los equipos de hardware
Servidores internos	[E.1] Errores de los usuarios	Minimizar	[P] Gestión del Personal	PR	Establecimiento de un Programa de Capacitación Continua

Base de datos	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Base de datos	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información en el servicio de Datos de Información
Documentación interna	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Documentación interna	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información de Documentación Interna por parte del personal a cargo
Electricidad	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Red Interna Biblioteca	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Electrónicos (Nube Microsoft, OneDrive)	[I.11] Emanaciones electromagnéticas (TEMPEST)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Electrónicos (Nube Microsoft, OneDrive)	[E.15] Alteración de la información	Minimizar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo

Electrónicos (Nube Microsoft, OneDrive)	[A.7] Uso no previsto	Evitar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la UTN
Personal administrativo informático	[E.18] Destrucción de la información	Evitar	[D] Protección de la información	PR	Aseguramiento de respaldos de información por parte del personal a cargo
Equipos PC y Didácticos	[I.11] Emanaciones electromagnéticas (TEMPEST)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Equipos de Redes y Telecomunicaciones	[I.11] Emanaciones electromagnéticas (TEMPEST)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Equipamiento Eléctrico	[I.11] Emanaciones electromagnéticas (TEMPEST)	Minimizar	[V] Gestión de vulnerabilidades	CR	Establecimiento de un Plan de simulacros ante desastres naturales (Incendio, sismo, tormenta eléctrica)
Personal administrativo informático	[E.19] Fugas de información	Minimizar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Personal administrativo informático	[E.28] Indisponibilidad del personal	Minimizar	[P] Gestión del Personal	PR	Implementación de Acuerdos de Compromiso y responsabilidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Personal administrativo informático	[A.15] Modificación de la información	Minimizar	[D] Protección de la información	PR	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la UTN
Personal administrativo informático	[A.18] Destrucción de la información	Evitar	[D] Protección de la información	RC	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos por parte del personal administrativo
Personal administrativo informático	[A.19] Revelación de información	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN
Personal administrativo informático	[A.28] Indisponibilidad del personal	Minimizar	[A] Registro y auditoría	MN	Implementación de registro de actividades mediante bitácoras
Personal administrativo informático	[A.29] Extorsión	Evitar	[P] Gestión del Personal	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Personal administrativo informático	[A.30] Ingeniería social (picaresca)	Evitar	[D] Protección de la información	PR	Implementación de Acuerdos de confidencialidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN

Nota: Elaboración propia.

Anexo L: Descripción Tareas Propuestas para el cumplimiento de Salvaguardas en la Biblioteca de la UTN

N°	Nombre	Descripción	Actividades	Presupuesto	Personal	Tiempo (meses)	Factibilidad

1	Implementación del cifrado hash para el almacenamiento de contraseñas	Contratación de un sistema en la nube para el almacenamiento de contraseñas con encriptación segura mediante cifrado hash	$500.00	Encargado del Área de Informática y Digitalización	1	Media
2	Diseño de un Sistema de Gestión de Seguridad de la Información para la Biblioteca de la 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.		Un profesional en seguridad informática / equipo de trabajo especializado en informática	8	Media Baja
3	Establecimiento de un Plan de Mantenimiento de Hardware y Software	Desarrollar un Plan para el Mantenimiento de Software en los Equipos y PC	$0.00	Encargado del Área de Informática y Digitalización	1	Media

4	Establecimiento de un Plan de Respuesta ante incidentes de ciberataques	Desarrollar un Plan ante posibles ataques de ciberataques	Definir una política sobre ciberseguridad Definir una estrategia de continuidad y recuperación de perdidas Contención del incidente Respaldo de información y cambio de contraseñas Concientización sobre el ataque generado	$4,000.00	Profesionales altamente capacitados en ciberseguridad	8	Media Baja
5	Desarrollar un manual de emergencia para las redes de comunicaciones	Desarrollo de un conjunto de actividades a realizar en caso de fallos del Router.		$800.00	Profesional en el Área de Telecomunicaciones	3	Media
6	Implementación de un Sistema de detección y prevención de intrusiones (IDS/IPS)	Un Sistema de Detección de Intrusiones (IDS) constituye un elemento de software integrado en el marco de seguridad destinado a identificar acciones impropias que se originan tanto de un dispositivo como de la red. En contraste, un Sistema de Prevención de Intrusiones (IPS) representa un componente de		$4,000.00	Profesional en Seguridad Informática	4	Media

		software dentro del modelo de seguridad diseñado para evitar acciones inapropiadas que se originan en la red.					
7	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de atención y soporte	Garantizar la seguridad de los sistemas implica disminuir las vulnerabilidades a través de la eliminación de elementos no esenciales, como software, servicios, usuarios, entre otros, que no son necesarios para el funcionamiento del sistema.	Configuración de contraseñas para iniciar dispositivos y ajustes en la BIOS. Creación de particiones seguras para el sistema operativo. Habilitación y limitación de actualizaciones de software. Implementación de herramientas de seguridad como antivirus. Definición de protocolos de red. Garantía de seguridad	$2,500.00	Profesionales expertos en Informática	5	Alta

			en el control de acceso remoto.				
8	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, sobrecargas y apagones.		$1,200.00	Profesional en el Área Eléctrica	3	Media

9	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento)	Implementación de un conjunto de procesos y medidas diseñadas para garantizar la calidad, confiabilidad y seguridad de los servicios externalizados.	$800.00	Profesional en el Área de Telecomunicaciones	2	Media
10	Aseguramiento de respaldos de información en el servicio de almacenamiento	Fortalecer significativamente la seguridad y confiabilidad de sus respaldos de información en el servicio de almacenamiento, asegurando la protección efectiva de los datos.	$500.00	Profesional en el Área de Informática	1	Media Baja
11	Establecer manuales de respaldo y duplicado de los sistemas, programas y archivos	Desarrollo de informes con información relevante a la descripción y configuración de programas y sistemas instalados en los Equipos PC.	$800.00	Encargado del Área de Informática y Digitalización	2	Media Alta

12	Desarrollar un Plan de Continuidad del Negocio para Mitigar el Riesgo de Difusión de Software Dañino en las Licencias	Implementación de medidas preventivas y correctivas para garantizar la integridad de los sistemas y minimizar los impactos en caso de una amenaza.	Este plan integral permitirá a la empresa mitigar el riesgo de difusión de software dañino en las licencias, protegiendo la integridad de sus sistemas y garantizando la continuidad del negocio en caso de una amenaza.	$1,200.00	Profesional en Seguridad Informática	3	Media Alta
13	Establecimiento de un Plan de Seguimiento y Monitoreo de Equipos de hardware	Implementación de un conjunto de prácticas para supervisar y mantener el rendimiento, la integridad y la disponibilidad de los dispositivos físicos en la infraestructura tecnológica de la Biblioteca.		$1,200.00	Profesional en Sistemas y Hardware	2	Media Alta

14	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)	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		$1,200.00	Equipo técnico especializado en desastres y catastros	6	Alta
15	Establecimiento de buenas prácticas para la adquisición de Hardware	Establecimiento de buenas prácticas para la adquisición de hardware implica la creación de pautas y procesos efectivos para garantizar que la empresa adquiera equipos que cumplan con sus necesidades operativas y se alineen con estándares de calidad y seguridad.	Realizar una evaluación detallada de los requisitos de hardware, teniendo en cuenta las necesidades presentes y futuras de la Biblioteca.	$0	Encargado del Área de Informática y Digitalización	2	Media Alta
16	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (almacenamiento en la nube)	Implementación de medidas estratégicas para garantizar la seguridad, disponibilidad y confiabilidad de los datos almacenados.	Realizar una evaluación exhaustiva de los proveedores de almacenamiento en la nube, considerando su reputación, historial de seguridad y	$1,200.00	Equipo técnico especializado en informática y seguridad	2	Media

			cumplimiento normativo.				
17	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.		$500.00	Encargado del Área de Informática y Digitalización	1	Media Alta
18	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.		$800.00	Encargado del Área de Informática y Digitalización	2	Media Alta
19	Desarrollar e Implementar un Plan de Continuidad del Negocio para Mitigar la Denegación de Servicio en Internet	Establecer estrategias y procedimientos que permitan mantener la operatividad, la seguridad y la disponibilidad de los servicios online en caso de un ataque.		$600.00	Profesional en el Área de Telecomunicaciones	2	Media Alta

20	Desarrollo de un Plan de Emergencia en caso de fallas eléctricas	Desarrollo de un conjunto de actividades a realizar en caso de fallas de energía o fallo de los equipos UPS.		$1,250.00	Profesional en el Área Eléctrica	3	Media
21	Establecimiento de un Plan de Respuesta ante incidentes de Corte de Electricidad	Establecer estrategias y procedimientos que permitan mantener la operatividad, la seguridad y la disponibilidad de los servicios en caso de un corte de electricidad.	Desarrollar un conjunto de medidas para garantizar la continuidad operativa y la seguridad de la empresa en caso de interrupciones en el suministro eléctrico	$800.00	Profesional en el Área Eléctrica	2	Media
22	Establecimiento de un Plan de Mantenimiento de Sistemas Operativos	Establecer un Plan de Mantenimiento de Sistemas Operativos implica desarrollar un conjunto de prácticas y procedimientos para garantizar la seguridad, estabilidad y eficiencia de los sistemas operativos utilizados por la Biblioteca.		$0	Encargado del Área de Informática y Digitalización	3	Media

23	Establecimiento de un Plan de Mantenimiento de Comunicaciones	Establecer un Plan de Mantenimiento de Comunicaciones implica desarrollar un conjunto de estrategias y procedimientos para asegurar la continuidad, seguridad y eficiencia de las redes y sistemas de comunicación utilizados por la Biblioteca		$800.00	Equipo encargado en Área de Redes y Sistemas	2	Media Alta
24	Implementación de un Plan en caso de fallo de comunicaciones	Implementación de un Plan en caso de fallo de comunicaciones implica establecer estrategias y procedimientos para asegurar la continuidad operativa y la pronta recuperación en situaciones donde las comunicaciones se vean comprometidas.		$1,200.00	Equipo encargado en Área de Redes y Sistemas	3	Media Alta
25	Implementación de registro de actividades mediante bitácoras	Desarrollo y almacenamiento de un registro digital de todos los procesos y actividades realizadas en la Biblioteca de la UTN	Registro de mantenimiento a equipos y aplicaciones Registro de llamadas Registro de incidentes de activos	$1,100.00	Encargado del Área de Informática y Digitalización	1	Alta

			Registro de acceso a espacios físicos				
26	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 especializado para instalación de los equipos de ventilación	6	Media
27	Establecimiento de un Plan de simulacros ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga eléctrica, etc.)	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
28	Desarrollo de lista de contactos de emergencia (policía, bomberos, emergencia)	Desarrollo de afiches con los números de contactos de emergencia tales como: policía, bomberos, servicios de		$300.00	Encargado del Área de Informática y Digitalización	1	Muy Alta

		emergencia (911), hospital, ambulancia y rescate general.				
29	Establecimiento de un Plan de emergencia ante desastres industriales (Fuego, daños por agua, explosiones, sobrecarga 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 los desastres potenciales que se puedan presentar.	$800.00	Equipo Técnico especializado en equipos tecnológicos	6	Alta

30	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)	$800.00	Equipo técnico especializado en desastres y catastros	6	Alta
31	Establecimiento de un Plan de Respuesta ante incidentes de Telefonía	Establecimiento de un Plan de Respuesta ante incidentes de Telefonía implica desarrollar un conjunto de estrategias y procedimientos para garantizar la continuidad operativa y la recuperación rápida en situaciones donde los servicios de telefonía se vean afectados.	$500.00	Profesional en el Área de Telecomunicaciones	2	Media

32	Implementación de Acuerdos de confidencialidad con el proveedor de Internet de la Biblioteca de la UTN	Implementación de acuerdos formales que protejan la seguridad y confidencialidad de la información transmitida a través de los servicios de Internet.	$500.00	Profesional en el Área de Telecomunicaciones	1	Media Alta
33	Aseguramiento de respaldos de información en el servicio de Electricidad	Implementar medidas para garantizar la integridad y disponibilidad de los datos críticos relacionados con la gestión y operación del servicio eléctrico.	$800.00	Profesional en el Área Eléctrica	2	Media

34	Establecer un proceso de hardening para los Equipos PC de la Biblioteca de la UTN y el área de oficinas y soporte	Garantizar la seguridad de los sistemas implica disminuir las vulnerabilidades a través de la eliminación de elementos no esenciales, como software, servicios, usuarios, entre otros, que no son necesarios para el funcionamiento del sistema.	Configuración de contraseñas para iniciar dispositivos y ajustes en la BIOS. Creación de particiones seguras para el sistema operativo. Habilitación y limitación de actualizaciones de software. Implementación de herramientas de seguridad como antivirus. Definición de protocolos de red. Garantía de seguridad en el control de acceso remoto.	$2,500.00	Profesionales expertos en el Área de Informática	5	Alta
35	Implementación de Controles de Validación y Monitoreo de Secuencias	Identificar las secuencias de procesos o eventos críticos para el funcionamiento del sistema o la operación, determinando su importancia y relevancia.		$800.00	Profesional en el Área de Seguridad Informática	3	Media

36	Establecimiento de un Plan de Gestión de seguridad de la Información para la Biblioteca de la 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	Profesional en el Área de seguridad informática / equipo de trabajo especializado en informática	8	Media Baja
37	Implementación de Acuerdos de Compromiso y responsabilidad a los miembros encargados del Área de Informática y Digitalización de la Biblioteca de la UTN	Establecer claramente las responsabilidades y funciones específicas de los miembros del Área de Informática y Digitalización, delineando sus roles en la gestión y protección de la información.		$0.00	Encargado del Área de Informática y Digitalización	1	Media
38	Establecer un programa sistemático para identificar y evaluar regularmente las	Desarrollar un enfoque estructurado para detectar y abordar posibles brechas de seguridad en las aplicaciones y sistemas.	Crear un inventario completo de todo el software utilizado en la organización, incluyendo sistemas operativos,	$1,200.00	Profesionales en el Área de Desarrollo de Software	3	Media Alta

	vulnerabilidades en el software utilizado		aplicaciones de usuario y software de infraestructura.				
39	Establecer un programa sistemático para identificar y evaluar regularmente las vulnerabilidades de los Sistemas operativos	Desarrollar un enfoque estructurado para detectar y abordar posibles riesgos de seguridad en los sistemas operativos utilizados.		$800.00	Profesionales en el Área de Seguridad Informática	1	Media
40	Establecimiento de un Plan de emergencia ante desastres naturales (Fuego, daños por agua, temblores)	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 (Fuego, daños por agua y temblores)		$800.00	Equipo técnico especializado en desastres y catastros	6	Alta

41	Establecimiento de un Plan de emergencia ante Contaminación medioambiental	Desarrollar un conjunto de procedimientos y estrategias para responder de manera efectiva y rápida a situaciones que puedan generar contaminación ambiental.		$500.00	Profesionales especializados en el Área del Medioambiente	2	Media
42	Aseguramiento de servicios de subcontratación por parte de las empresas proveedoras (internet, mantenimiento, electricidad)	Implementar medidas para garantizar la calidad, seguridad y continuidad de los servicios contratados.	Realizar una evaluación exhaustiva al seleccionar proveedores, asegurándose de su experiencia, reputación y capacidad para cumplir con los estándares requeridos.	$800.00	Profesional en el Área de Telecomunicaciones	2	Media
43	Aseguramiento de respaldos de información en el servicio de Telefonía	Establecimiento de un Plan de Respuesta ante incidentes de Telefonía implica desarrollar un conjunto de estrategias y procedimientos para garantizar la continuidad operativa y la recuperación rápida en situaciones donde los servicios de telefonía se vean afectados.		$500.00	Profesional en el Área de Telecomunicaciones	2	Media

44	Implementación de Acuerdos de confidencialidad con el proveedor de telefonía de la Biblioteca de la UTN	Implementación de acuerdos formales que protejan la seguridad y confidencialidad de la información transmitida a través de los servicios de Telefonía.		$500.00	Profesional en el Área de Telecomunicaciones	1	Media Alta
45	Implementación de Acuerdos de confidencialidad con el proveedor de Electricidad de la Biblioteca de la UTN	Implementación de acuerdos formales que protejan la seguridad y confidencialidad de la información transmitida a través de los servicios Eléctricos.		$500.00	Profesional en el Área de Electricidad	1	Media Alta
46	Implementación de Encriptación del Tráfico de Red.	Evaluar los requisitos y las necesidades específicas de seguridad para determinar qué tráfico de red debe estar encriptado.	Seleccionar protocolos de encriptación seguros y apropiados para cifrar el tráfico de red, como HTTPS para la web, VPN para conexiones remotas, y TLS/SSL para comunicaciones seguras.	$800.00	Profesional en el Área de Seguridad Informática	2	Media Alta

47	Establecimiento de un Plan de Gestión de Seguridad para los equipos mobiliarios de la Biblioteca de la UTN	Desarrollar un conjunto de medidas y procedimientos para garantizar la seguridad y protección de los activos mobiliarios.	Crear un inventario detallado de todos los equipos mobiliarios de la biblioteca, incluyendo descripciones, ubicaciones y valores.	$0.00	Encargado del Área de Informática y Digitalización	2	Media
48	Aseguramiento de respaldos de información en el servicio de Datos de Información	Implementar un conjunto de prácticas y procedimientos para garantizar la integridad y disponibilidad de la información crítica de la Biblioteca.	Identificar y clasificar la documentación interna crítica para el funcionamiento de la organización, determinando su importancia y relevancia.	$0.00	Encargado del Área de Informática y Digitalización	1	Media Alta
			TOTAL	$50,350.00			

Nota: Elaboración propia

Anexo M: Material didáctico utilizado para la socialización del Plan de Gestión de Riesgos en la Biblioteca de la UTN

Nota: Elaboración propia

Nota: Elaboración propia

Nota: Elaboración propia

Anexo N: Material POP para los funcionarios y estudiantes de la Biblioteca de la UTN

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

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE SOFTWARE

Cuestionario Inicial

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Plan de Gestión de Riesgos Tecnológicos para la Biblioteca 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 y Áreas Tecnológicas como la "Biblioteca de la 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 Biblioteca de la UTN "Área de Informática y Digitalización" 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 criterio, el informe del Plan de Gestión de Riesgos Tecnológicos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización" 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 norma ISO/IEC 31000 para el desarrollo del Plan de Gestión de Riesgos Tecnológicos en el departamento de Biblioteca de la UTN "Área de Informática y Digitalización" 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 Biblioteca de la UTN "Área de Informática y Digitalización" 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 criterio, 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 Biblioteca de la UTN "Área de Informática y Digitalización"?**
    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 Biblioteca de la UTN "Área de Informática y Digitalización" 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 Biblioteca de la UTN "Área de Informática y Digitalización"?**
    1) Totalmente de acuerdo
    2) De acuerdo
    3) Indiferente o neutro
    4) En desacuerdo
    5) Totalmente en desacuerdo

Comentario
(opcional):_____
_____
_____

9. **¿A su criterio, el Plan de Gestión de Riesgos Tecnológicos desarrollado para el departamento de Biblioteca de la UTN "Área de Informática y Digitalización", ¿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 Biblioteca de la UTN "Área de Informática y Digitalización", ¿cuál sería?**

Anexo P: Acta de entrega del Plan de Gestión de Riesgos a Biblioteca

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERIA EN SOFTWARE

CSOFT

ACTA ENTREGA DEL INFORME DEL PLAN DE GESTIÓN DE RIESGOS DE LA BIBLIOTECA DE LA UTN

En la ciudad de Ibarra a los 25 días del mes de enero del año 2024, se entrega a la Directora de Biblioteca de la UTN la Msc. Bethy Chávez, los siguientes documentos:

- Informe del Plan de Gestión de Riesgos
- Documento de Excel
- Archivo .mgr
- Presentación de la socialización

Considerando que las partes manifiestan su total conformidad, se ratifica y aceptan todo su contenido, entendiendo su alcance y significado.

Recibe conforme:	Entrega conforme:
Msc. Bethy Chávez	*Victor Hugo Terán Ballesteros*
Directora de Biblioteca	Estudiante

Anexo Q: Certificado de recepción por parte de la directora de Biblioteca

REPUBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE
Acreditada Resolución Nro. 173-SE-33-CACES-2020
DIRECCIÓN DE BIBLIOTECA

Magister Bethy Mireya Chávez Martínez, DIRECTORA DE BIBLIOTECA DE LA UNIVERSIDAD TÉCNICA DEL NORTE, a petición verbal de la interesada,

CERTIFICA:

Que el señor **Víctor Hugo Terán Ballesteros** con número de cédula **1004786396**, realizó la entrega del CONTENIDO y FORMATO del trabajo de titulación denominado: **EVALUACIÓN DE RIESGOS DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA BIBLIOTECA DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON EL SOFTWARE PILAR, UTILIZANDO LA NORMA ISO/IEC 31000.**

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente como lo estime conveniente.

Ibarra, 25 de enero de 2024

Atentamente,

UNIVERSIDAD TECNICA DEL NORTE BIBLIOTECA Ibarra Ecuador

MSc. Bethy Chávez
DIRECTORA DE BIBLIOTECA

Ciudadela Universitaria Barrio El Olivo
Av.17 de Julio 5-21 y Gral. José María Córdova
Ibarra-Ecuador
Teléfono: (06) 2997-800 RUC: 1060001070001
www.utn.edu.ec