UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería En Sistemas Computacionales

ESTUDIO DE LA SEGURIDAD EN BIG DATA, PRIVACIDAD Y PROTECCIÓN DE DATOS MEDIANTE LA ISO/IEC 27007:2017- APLICADO A LOS DATOS ACADÉMICOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Trabajo de grado previo a la obtención del título de Ingeniera en Sistemas Computacionales

Autora:

Cinthia Carolina Hernández Obando

Director

MSc. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2019

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA

UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La 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:	0401555214
APELLIDOS Y NOMBRES:	HERNÁNDEZ OBANDO CINTHIA CAROLINA
DIRECCIÓN:	AV. 17 DE JULIO JUNTO A UTN
EMAIL:	cinthi_carito17@hotmail.com
TELÉFONO MÓVIL:	0981597955

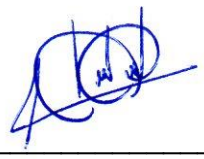
DATOS DE LA OBRA	
TÍTULO:	ESTUDIO DE LA SEGURIDAD EN BIG DATA, PRIVACIDAD Y PROTECCIÓN DE DATOS MEDIANTE LA ISO/IEC 27007:2017- APLICADO A LOS DATOS ACADÉMICOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE.
AUTOR (ES):	HERNÁNDEZ OBANDO CINTHIA CAROLINA
FECHA:	2019-07-11
PROGRAMA:	PREGRADO
TITULO POR EL QUE OPTA:	INGENIERA EN SISTEMAS COMPUTACIONALES
ASESOR /DIRECTOR:	MCs. DAISY IMBAQUINGO

2. CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y la desarrollo sin violar los derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá de la defensa de la Universidad en caso de reclamos por parte de terceros.

Ibarra, a los 11 días del mes de julio del 2019

AUTORA:



Cinthia Carolina Hernández Obando

Ibarra, 12 de julio del 2019

CERTIFICACIÓN DEL DIRECTOR

Por medio del presente, yo MSc. Daisy Imbaquingo, certifico que la Srta. Cinthia Carolina Hernández Obando, portadora de la cédula de identidad Nro. 040155521-4. Ha trabajado en el desarrollo del proyecto de grado denominado **"ESTUDIO DE LA SEGURIDAD EN BIG DATA, PRIVACIDAD Y PROTECCIÓN DE DATOS MEDIANTE LA ISO/IEC 27007:2017 – APLICADO A LOS DATOS ACADÉMICOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE",** previo a la obtención del título de Ingeniera en Sistemas Computacionales, lo cual ha realizado en su totalidad con responsabilidad.

Es todo cuanto puedo certificar en honor a la verdad.

Atentamente,

Msc. Daisy Imbaquingo

DIRECTORA DE TESIS

DIRECTOR DE LA DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO

CERTIFICA

QUE: La señorita CINTHIA CAROLINA HERNÁNDEZ OBANDO con cédula identidad 0401555214 estudiante de la Facultad de Ingeniería en Ciencias Aplicadas – de la Carrera de Ingeniería en Sistemas Computacionales, ha desarrollado con los datos entregados de la Dirección de Desarrollo Tecnológico e Informático, el Proyecto de Tesis "**ESTUDIO DE LA SEGURIDAD EN BIG DATA, PRIVACIDAD Y PROTECCIÓN DE DATOS MEDIANTE LA ISO/IEC 27007:2017 – APLICADO A LOS DATOS ACADÉMICOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE".**

QUE: El estudio del proyecto fue entregado a la Dirección de Desarrollo Tecnológico e Informático el 2 de julio del 2019.

Es todo cuanto puedo certificar, facultando a la interesada hacer uso de este certificado como estime conveniente, excepto para trámites judiciales.

Ibarra, 8 de julio del 2019

Atentamente
CIENCIA Y TECNICA AL SERVICIO DEL PUEBLO

Ing. Juan Carlos García
DIRECTOR

Dedicatoria

La presente tesis la dedico principalmente a mi mamá Verónica Hernández y al Sr. Jaime Trujillo, quienes fueron los pilares fundamentales en mi formación académica, por brindarme su apoyo incondicional, sus consejos, sus valores y por la motivación constante que me ha permitido ser una persona de bien. Pero más que nada, por su amor.

A mi hermano Carlos Trujillo por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias.

Finalmente quiero dedicar esta tesis a todos mis amigos, por apoyarme cuando más los necesito, por extender su mano en momentos difíciles y por el amor brindado cada día, de verdad mil gracias, siempre los llevo en mi corazón.

Cinthia Carolina Hernández Obando

Agradecimiento

Me van a faltar páginas para agradecer a las personas que se han involucrado en la realización de este trabajo, sin embargo, merece un reconocimiento especial mi Madre que con su esfuerzo y dedicación me ayudo a culminar mi carrera universitaria y me dio el apoyo suficiente para no decaer cuando todo parecía complicado e imposible.

Asimismo, agradezco infinitamente a mi hermano y a su padre que con sus palabras me hacían sentir orgullosa de lo que soy y de lo que puedo llegar a ser.

De igual forma, agradezco a mi Directora de Tesis, que gracias a sus consejos y correcciones hoy puedo culminar este trabajo. A los Docentes que me han visto crecer como persona, y gracias a sus conocimientos.

Cinthia Carolina Hernández Obando

Resumen

La Universidad Técnica del Norte es una organización que ha ido creciendo a lo largo de los años. En esta institución prestigiosa se desarrolla software de calidad uno de ellos sirve para la gestión académica de la universidad.

Dentro de la organización de la Universidad Técnica del Norte se encuentra el Departamento de Desarrollo Tecnológico e Informático (DDTI), quienes se encargan de la administración de los sistemas entre ellos el académico. Sin embargo, con el continuo avance tecnológico y la facilidad de ingresar a la red, existen amenazas y vulnerabilidades que pueden ocasionar problemas en la seguridad de la información.

El DDTI se enfrenta a un factor importante a considerar, debido a que cada vez existe mayor cantidad de información para procesar, es necesario explorar alternativas para el manejo de grandes volúmenes de datos. Big Data toma relevancia en este sentido promete el manejo, procesamiento y análisis de grandes volúmenes de datos en pequeños intervalos de tiempo.

En el presente estudio, se realizó una auditoría aplicada al sistema académico referente a la seguridad de la información basándose en la guía de auditoría ISO/IEC 27007:2017, con el fin de determinar el estado actual de la seguridad de los grandes volúmenes de datos que maneja el sistema académico. La guía de auditoría se basa en los controles de la norma ISO/IEC 27002:2017, donde evalúa el cumplimiento del estándar bajo los requisitos del software Ear Pilar que ejecuta un análisis de la situación actual de la empresa evaluando activos, dominios y riesgos utilizando la metodología MAGERIT.

Se comprobó el porcentaje de cumplimento de la norma ISO/IEC 27002:2017 y las no conformidades encontradas, además de los requisitos que posee la Universidad Técnica del Norte para la implementación de Big Data.

Palabras Claves: Sistema Académico, Big Data, Auditoría, ISO

Abstract

Universidad Técnica del Norte is an organization which has grown over the years. In this prestigious institution quality software is developed, one of them, is used for the university academic management.

Within the organization of Universidad Técnica del Norte is the Department of Technological and Computer Development (DDTI), who are responsible for the administration of the systems, including the academic one. However, with the continuous advance and ease of entering the network, there are threats and vulnerabilities that can cause problems in the security of information.

The DDTI is faced with an important factor to consider, because there is a growing amount of information to process, it is necessary to explore alternatives for handling large volumes of data. Big Data takes relevance in this sense promises the handling, processing and analysis of large volumes of data in small time intervals.

In the present study, an audit applied to the academic system about information security was executed based on the audit guide ISO / IEC 27007: 2017, in order to determine the current state of the security of the large volumes of data that manages the academic system. The audit guide is based on the controls of ISO / IEC 27002: 2017, where is evaluated the compliance of the standard under the Ear Pilar software requirements and executes an analysis of the company's current situation evaluating assets, domains, and risks using the MAGERIT methodology.

The percentage compliance of the ISO / IEC 27002: 2017 norm and the non-conformities found was verified, in addition to the requirements that the Universidad Técnica del Norte has for the implementation of Big Data.

Keywords: Academic System, Big Data, Audit, ISO

Tabla De Contenido

Índice De Figuras

Índice De Tablas

INTRODUCCIÓN

Antecedentes

El Sistema de Gestión Académico de la Universidad Técnica del Norte está dedicado a recopilar información de cada uno de los estudiantes para tener un seguimiento adecuado de los mismos, el DDTI[1] es el encargado de administrar los datos académicos y proporcionar los reportes adecuados a cada facultad, a medida que la UTN crece. la información se acumula y se encuentra expuesta a diversas vulnerabilidades y riesgos, por eso surge la necesidad de realizar un estudio de seguridad en grandes volúmenes de datos, conocido como Big Data tomando como referencia la ISO/IEC 27007:2017.

El Sistema de Gestión de Seguridad de la Información (SGSI), según la ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización (Excellence, 2015).

La seguridad de información debe formar parte de todos los procesos de negocio, tanto si los procesos son manuales como automatizados, para que la información cuente con sus tres propiedades confidencialidad, integridad y disponibilidad.

El objetivo de la seguridad de la información es establecer la administración de la seguridad mediante la aprobación de políticas de seguridad, la coordinación de la implantación de la seguridad y la asignación de funciones y responsabilidades dentro de la organización.

Actualmente por motivos de seguridad las organizaciones se han visto en la necesidad de migrar datos a servidores que se encuentran en la nube, ya que permite el ahorro de espacio físico, y la información se encuentra segura y libre de sufrir daños.

La cantidad de datos generados en el entorno educativo crece a un ritmo exponencial, los responsables del DDTI, son conscientes de estos flujos masivos de información es así como surge el termino de Big Data.

El Big Data es una gran fuente de información, permite realizar análisis y descubrimientos continuamente, importante no es la cantidad de datos acumulados, sino lo que realmente haces con estos datos y su posterior análisis (O'neill, s.f.).

[1] DDTI: Siglas del Departamento de Desarrollo Tecnológico e Informático

Justificación e importancia

Impacto tecnológico

La razón del estudio de la seguridad de Big Data de los datos académicos es tener una información segura y libre de amenazas para su posterior análisis y toma de decisiones. En la actualidad existen varias herramientas para controlar la seguridad de los datos, estas facilitan conocer si nuestra información está segura.

Impacto social

Con la propuesta de este estudio se espera ofrecer una solución para que la institución disponga de datos confiables y seguros. También se espera verificar las vulnerabilidades existentes en los activos de información para percibir el impacto que tendrá y establecer los controles necesarios en el ingreso, control y manipulación de la información. Los beneficiaros directos serán todas las personas que pertenecen a la institución.

Prospectiva

La evaluación del sistema académico es indispensable para facilitar el análisis y seguimiento del crecimiento de información en la universidad, esto proporcionará los conocimientos adecuados para una eficiente toma de decisiones. Como solución a esta necesidad, se ha optado por la evaluación del sistema académico para el análisis e interpretación de los datos a través de resultados respaldada en una herramienta de software.

Con este estudio se pretende encontrar una forma viable de implementar una normativa internacional que garantice que la información está segura y de forma confidencial.

Objetivos

Objetivo general

Estudiar la Seguridad en Big Data, privacidad y protección de datos mediante ISO/IEC 27007:2017 Aplicado a los Datos Académicos de la Universidad Técnica del Norte.

Objetivos específicos

- Realizar un estudio de la Seguridad de los datos académicos de la UTN, basado en la norma ISO/IEC 27007:2017.
- Utilizar la norma ISO/IEC 27007:2017 para comprobar el tipo de seguridad que poseen los datos académicos.
- Elaborar un documento con las medidas necesarias que se debe llevar acabo para que los datos académicos sean seguros.

Alcance

El presente proyecto tiene como finalidad evaluar las amenazas y las vulnerabilidades de los datos académicos de la UTN, utilizando la ISO 27007:2017, para poder facilitar el análisis de la información y generar reportes para un mejor entendimiento de la información, que ayudará a la toma decisiones.

Cuando existen grandes volumenes de datos (Big Data) la seguridad es expuesta a riesgos o a una ingeniería social.

El marco de referencia para realizar este estudio será la norma ISO/IEC 27007, debido que es un estándar que proporciona orientación sobre la gestión de un programa de auditoría del sistema de gestión de la seguridad de la información.

Las áreas con las que directamente se estará involucrado este estudio son:

- Big Data
- ISO/IEC 27007:2017

Estas áreas facilitarán el estudio a realizarse para que los datos académicos tengan más seguridad y cuenten con la debida confidencial que los datos ameritan, para poder tomar decisiones eficientes y seguras. Se confirmará que los controles de seguridad de información mitigan de forma correcta los riesgos de la información, verificando todos los controles de seguridad.

CAPÍTULO 1

Marco Teórico

1.1. Información

El término información describe a un conjunto de datos, procesados y ordenados para su comprensión, aportan nuevos conocimientos a un individuo o sistema sobre un, fenómeno determinado. La información es un activo esencial para cualquier organización, juega un papel importante a la hora de tomar decisiones y definir nuevas estrategias de negocios. Al igual que otros activos, la información tiene un valor estratégico y operativo, como consecuencia, estos datos deben ser protegidos ante posibles pérdidas y violaciones de la seguridad y otros riesgos a la que se encuentra expuesta (Garcia, 2011).

La información permite el estado de conocimiento que un individuo o sistema maneja con respecto a determinado fenómeno, lo que influye en las acciones, actitudes o decisiones que se tomen a partir de la nueva información.

1.2. Metadatos

Benjumea (2012) afirma que el término metadatos se refiere a datos que describen el contenido de los archivos o la información de estos, es decir un grupo de datos o recursos. Son datos altamente estructurados que describen características de los datos, como el contenido, calidad, información y otras circunstancias o atributos.

Actualmente los metadatos han adquirido relevancia frente a la cantidad de información que crece de forma exponencial, una gestión oportuna es transcendental para la eficiencia operativa en organizaciones.

1.3. Seguridad de la Información

Según Bertolín (2008), este término hace referencia al conjunto de técnicas y medidas para controlar los datos que se manejan dentro de una organización, la seguridad de la información tiene como fin resguardar la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada. En este sentido, la seguridad de la información implica proporcionar protección a los recursos tanto abstractos como físicos, para

evitar riesgos a nivel tecnológico dentro de una organización.

Conviene aclara que la seguridad absoluta no es posible, no existe un sistema 100% seguro, de forma que el elemento de riesgo siempre está presente, independientemente de las medidas de prevención que tomemos.

1.3.1. Tipos de seguridad

Existen diversos tipos de seguridad que una organización debe vigilar para evitar la pérdida de datos, en la Tabla 1 se los menciona:

Tabla 1: Tipos de Seguridad

Tipos de Seguridad	Descripción
Seguridad Física	Se refiere a la protección de los elementos a nivel físico en un espacio determinado para protegerlos de posibles amenazas tales como desastres naturales o problemas eléctricos.
Seguridad Lógica	Protege lo relacionado con el software o la información contenida en los equipos.
Seguridad de Hardware	Son las medidas que se adoptan para proteger los dispositivos de posibles daños de diversa índole.
Seguridad de Software	Este tipo de seguridad lucha contra las amenazas existentes, implementando mecanismos contra virus, hackers y robo de información sensible.
Seguridad de Red	Resguarda toda la información que esta accesible a través de internet y que podría ser usada de forma malintencionada, este tipo de seguridad lucha contra las amenazas existentes implementando

Seguridad Activa	Es el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.
Seguridad pasiva	Son las medidas que se implementan después de un incidente de seguridad, para minimizar su repercusión y facilitar la recuperación del sistema.

Fuente: Autor

1.4. Auditoría informática.

Es el compendio de técnicas o procedimientos que se utilizan para realizar evaluaciones y controles de un sistema informático con el fin de certificar el correcto funcionamiento de sus actividades en el marco legal. Asimismo, comprende elementos más allá de la evaluación considerando entradas, procesos, registros, modelos de seguridad implantados y métodos de obtención de datos (Quishpe & Vargas, 2013).

Esta práctica se estima fundamental para el correcto desempeño de este tipo de sistemas dentro de una empresa en base a los controles que proporciona para la confiabilidad y resguardo de activos de información.

1.4.1 Tipos de Auditoría

La auditoría es un recurso legal que ha evolucionado en las últimas décadas dando lugar a varias especialidades. En la actualidad existen varios tipos de auditoría que se diferencian básicamente por los objetivos y los agentes que la realizan.

a) Auditoría Fiscal

La auditoría fiscal es realizada por la Administración Tributaria con el fin de denominar las responsabilidades pecuniarias[2] de los contribuyentes, y a su vez la practicada por preprofesionales independientes en orden para dar una opinión sobre la razonabilidad de las cuentas de las entidades públicas por conceptos fiscales. (Miramegias, 2018)

[2] Pecuniarias: denominación de la sanción que consiste en el pago de una multa al Estado como castigo por haber cometido un delito

b) Auditoría de Gestión u Operacional

Es el examen crítico, sistemático e imparcial de una identidad de administración, la cual determina la eficacia con que logra los objetivos establecidos en economía, con que se utiliza y obtiene los recursos, con el objetivo de sugerir las recomendaciones, que mejoraran la gestión en el futuro. (Gonzales, 2018)

c) Auditoría Financiera o de Estados Financieros

Esta Auditoría es el examen integral sobre la estructura, las transacciones y el desempeño de una entidad económica para contribuir a la oportuna prevención de riesgos, la productividad en la utilización de los recursos y el acatamiento permanente de los mecanismos de control implantados por la administración. (Curiel, 2006)

d) Auditoría Informática

La auditoría informática se ocupa de la revisión del uso de las TI[3], en las empresas como factor de ventaja competitiva, cuyo objetivo primordial es emitir una opinión profesional acerca de los estados financieros de una entidad. (Aguirre, 2011)

1.4.2 Clasificación de Auditoría

La filiación del auditor, se clasifican en Auditoría Externa e Interna.

a) Auditoría externa

Se llevan a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre, está la efectúan profesionales que no dependen de la empresa, ni económicamente ni bajo cualquier otro concepto, y a los que se reconoce un juicio imparcial merecedor de la confianza de terceros (Universidad Tecnológica de la Huasteca Hidalguense, 2011).

b) Auditoría interna

Se realizan en nombre de la propia organización, para la revisión por la dirección con otros fines internos, y pueden constituir la base para una auto declaración de conformidad de una organización; además de ello la desarrollan personas que dependen del negocio y actúan

[3] TI: Tecnología de la información significado en inglés, information technology es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas

revisando los aspectos que interesan particularmente a la admisión, aun que pueden efectuar revisiones programadas sobre todos los aspectos operativos (Universidad Tecnológica de la Huasteca Hidalguense, 2011).

1.4.3 Metodologías para Auditar

Los métodos utilizados en el estudio que se presenta fueron: el Análisis-síntesis para conformar la base teórica y metodológica. El Histórico-lógico para analizar el desarrollo lógico e histórico de los principales postulados sobre la auditoría de información sus metodologías y métodos. El Sistémico-estructural para abordar las relaciones entre los aspectos que abordan las diversas metodologías y modelos, a fin de establecer puntos de contacto y diferencias, con un enfoque integral.

En la Tabla 2. Se detallan las metodologías para Auditar según (Guitián, 2014) se clasifican en las siguientes:

Tabla 2: Metodologías para auditar

Metodologías para Auditar	
Metodologías de auditoría de información enfocadas hacia los procesos	
Metodología	**Objetivo**
Metodología de Reynolds (1980)	Analiza las debilidades del sistema de reportes, no puede ser aplicada a otros ámbitos, funciones o procesos.
Metodologías de auditorías de información enfocadas hacia los recursos	
Metodologías de Riley, (1975) y Alderson (1993)	Compara opciones a partir de costos con relación a los beneficios, están orientadas al sistema y al análisis del valor de la información. La metodología hace énfasis en la medición cuantitativa de costos, pero no valora cualitativamente y no considera el análisis del ambiente organizacional ni las necesidades de información.
Metodologías de Auditorias de Información con enfoque Hibrido	
Metodología de Gruber (1983)	Considera la eficiencia y la efectividad con que se usan, manejan y protegen los recursos de información, la confiabilidad del sistema y su conformidad con las obligaciones, regulaciones y normas vigentes. Se considera enfoque hibrido porque abraca análisis

	estratégicos, recursos tecnológicos y las necesidades en función de las tareas.
Metodología de Gillman (1985)	Se enfatiza en el análisis de los SI que en el costo beneficio de los recursos de información e intentan identificar los principales componentes del sistema para mapearlos en relación unos con otros, se considera hibrida porque se focaliza no solo hacia las estrategias y metas, también en la identificación de los recursos y sus flujos por cada servicio.
Metodología InfoMap de Burk & Horton (1988)	Es la más usada y citada, orientada a identificar, mapear y evaluar los recursos de información y proporciona un sistema para identificarlos, mapearlos y evaluarlos al detectar como se usan y contribuyen a cada área de trabajo y a la estrategia económico de la organización.
Metodología de Barker (1990)	Consta de 10 etapas, en las cuales se enfatiza en la fiabilidad del SI. Pero a pesar de que incluye el análisis de las necesidades de información, el inventario de los recursos, y enfatiza en el control de los procesos, monitoreo y prueba, no incluye la elaboración de los mapas con los flujos.
Modelo de Stanat (1992)	Evalúa la efectividad de las redes y SI de la organización, las necesidades actuales, la efectividad de las fuentes y de la distribución de información y el uso de las tecnologías, analiza la información por área de trabajo, la principal ventaja de esta metodología es la evaluación de actitudes y prácticas de los empleados y gerentes con respecto a las fuentes de información.
Metodología de Buchanan & Gibb (1998)	Desarrolla un enfoque estratégico integrado con un acercamiento arriba-abajo, evalúa las fuentes en correspondencia con las tareas que apoyan, los factores claves de éxito, los objetivos, valoran los problemas, a

	partir de su naturaleza y así pueden ser de conciencia, de disponibilidad, de accesibilidad o de apropiación.
Modelo de Orna (1999)	Compuesto por 10 etapas, concibe la auditoría como una plataforma para el cambio mediante el uso adecuado de la información y del conocimiento. Enfatiza en la importancia del estudio de los flujos dentro de la organización, el esclarecimiento de los canales de comunicación, la identificación del conocimiento que cada trabajador posee sobre la información existente y las personas que puedan ser considerados como fuentes de información, para llevar a cabo las funciones organizacionales.
Modelo de Henczel (2001).	Henczel adopta una propuesta parecida a la de Orna, Buchanan & Gibb, Su modelo consta de 7 etapas, se caracteriza por no ser un proceso altamente controlado y estructurado, Se puede utilizar no sólo para identificar las fuentes significativas de información, sino también las actividades que crean conocimiento hacia otras áreas de la organización.
Metodología de Soy i-Aumatell (2003).	No propone un método específico ni un software para el procesamiento y análisis estadístico de los datos, llama la atención los enfoques que propone para llevarla a cabo: de arriba- abajo, (estrategia corporativa-necesidades de información básicas), de abajo- arriba (mapeo y análisis de los RI a través de entrevistas estructuradas u otros métodos), de dentro- afuera (formando grupos de trabajo para identificar oportunidades y riesgos
Modelo integral para auditar organizaciones de información en	Dirigido al análisis de los procesos de información en organizaciones de información y estructurado en 6 etapas. Tiene una perspectiva gerencial y permite llevar a cabo la auditoría evaluando los procesos de

Cuba de Villardefrancos-Álvarez (2005)	tratamiento de la información y los asociados al flujo y uso de esta. Para ello establece indicadores y variables de evaluación.
Procedimiento de Auditorías de Información en Instalaciones Hoteleras (González-Guitián (2011).	Esta propuesta, hasta ahora sin precedentes en el sector del turismo, incluye un instrumento conformado por una serie variables asociadas a 19 indicadores que permiten valorar cuantitativa y cualitativamente la GI en organizaciones de este tipo, pero por su flexibilidad, puede adecuarse a las características propias de organizaciones en otros sectores.

Fuente: (Guitián, 2014)

1.5. Big Data

Según Hernández, Duque & Moreno (2017) el término refiere a diferentes tecnologías asociadas a la administración de grandes volúmenes de datos provenientes de diferentes fuentes y que se generan con rapidez y adicionalmente abarca tanto volumen como variedad de datos y velocidad de acceso y procesamiento. De forma general su composición se fundamenta en siete características, llamadas las siete V del Big Data, las cuales se ilustran en la Figura 1 y se describen a continuación:

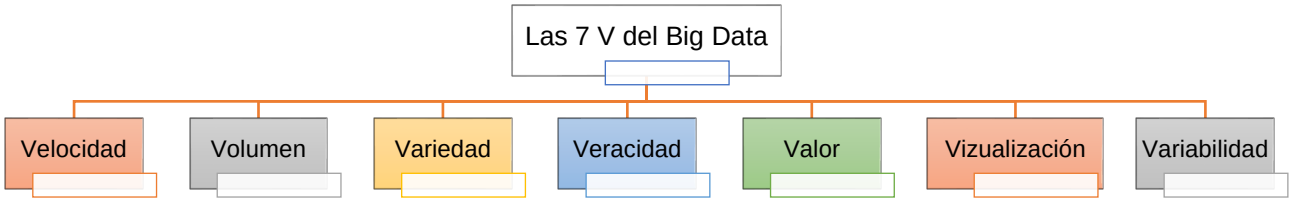


Figura 1: Las 7 V del Big Data
Fuente: Propia

a) **Velocidad**

De acuerdo con Montealegre (2017) la velocidad se refiere al movimiento de los datos por las constantes interconexiones que se efectúan en los procesos de información, es decir, a la rapidez en la que son creados, almacenados y procesados en tiempo real.

b) **Volumen**

Este elemento se refiere según Montealegre (2017) a la cantidad de datos que son generados cada segundo, minuto y días en el entorno de desarrollo y ésta carácter reseña a las cantidades masivas de datos que se almacenan con la finalidad de procesar dicha información, transformando los datos en acciones.

c) **Variedad**

Esta característica hace referencia a las formas, tipos y fuentes en las que se registran los datos, los cuales pueden ser datos estructurados y fáciles de gestionar como son las bases de datos, o datos no estructurados, entre los que se incluyen documentos de texto, correos electrónicos, datos de sensores, audios, vídeos o imágenes que se tienen en los dispositivos móviles de acuerdo a Montealegre (2017).

d) **Veracidad**

Con base a lo expuesto por Montealegre (2017) la veracidad en el Big Data hace referencia a la incertidumbre de los datos, es decir, al grado de fiabilidad de la información recibida.

e) **Valor**

Esta característica según el autor Montealegre (2017) se obtiene de datos que se transforman en información; esta a su vez se convierte en conocimiento, y este en acción o en decisión, por lo que este valor se fundamenta principalmente en la racionabilidad de estos datos.

f) **Visualización**

La visualización de datos se refiere al modo en el que los datos son presentados de manera que sean legibles y accesibles, para encontrar patrones y claves ocultas en el tema a investigar, por lo que se complementa con herramientas de visualización que ayuden a comprender los datos gráficamente y en perspectiva contextual (Montealegre, 2017).

g) **Variabilidad**

Se trata de la capacidad que tienen las compañías en generar un uso eficaz del gran volumen de datos que manejan y una vez conocida la viabilidad de cada empresa, es el momento de detallar el proyecto en una hoja de ruta, y desarrollar el plan de negocio (Montealegre, 2017).

1.5.1. Tipos de Datos en Big Data

Para el análisis y procesamiento de datos con Big Data, se maneja tres tipos de datos, estructurados, no estructurados y semiestructurados.

a) Datos estructurados

Este tipo de datos según ESPAE (2017) son aquellos que se almacenan en campos de tablas de bases de datos relacionales donde su longitud, denominación y formato han sido predefinidos. La organización, estructura, el tipo, su posición y las posibles relaciones entre ellos, es conocida previamente La información se representa por datos elementales, no compuestos por otras estructuras.

b) Datos no estructurados

A diferencia de los datos estructurados, los de este tipo se documentan en el formato en el que ha sido creados, no tienen una estructura predefinida, ni están almacenados en una tabla, por lo que de acuerdo a ESPAE (2017) la información no está representada por datos elementales, sino por una composición cohesionada de unidades estructurales de nivel superior.

c) Datos semiestructurados

ESPAE (2017) define a los datos semiestructurados como datos elementales, no tienen estructura fija a pesar de que tienen algún tipo de estructura implícita o autodefinida que se encuentran encapsulados en ficheros semiestructurados. Es el caso de documentos escritos con lenguaje HTML, XML o SGML.

1.5.2. Ciclo de análisis de Big Data

El objetivo principal de Big Data es mejorar la toma de decisiones en las organizaciones, en la ejecución de proyectos y en la ejecución de decisiones, tomando en cuenta que la toma de decisiones informada es un componente esencial para una organización. Para ello es importante realizar un análisis exhaustivo de la información previo a la toma de decisiones operativas y estratégicas. (Tabesh, Mousavidin, & Hasani, 2019)

En la toma de decisiones importantes los gerentes recolectan datos, para generar varias estrategias y someterlas a evaluaciones, considerando a detalle todos los aspectos necesarios para la toma de decisiones finales. Una vez que una estrategia se pone en marcha, esta es evaluada con el fin de generar resultados que sirven como retroalimentación para la posterior toma de decisiones.

El ciclo de Big Data consta de cuatro fases, mismas que se presentan en la figura 2 y se detallan a continuación:

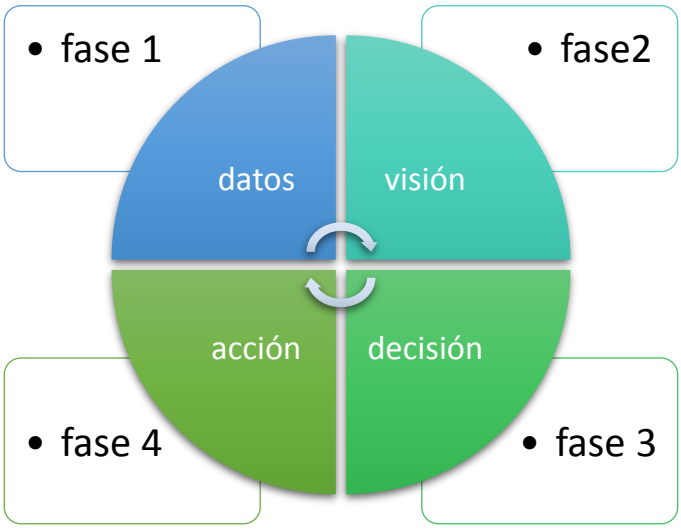


Figura 2: Fases de Big Data.

Fuente: Propia

Fase 1: Es amplia y diversa, en esta fase generalmente se recopilan los datos no estructurados de fuentes internas, externas, fuentes procesadas es decir datos analizados utilizando herramientas analíticas avanzadas y diversos algoritmos para la generación de ideas.

Fase 2: Todo lo percibido en la fase 1 se transforma en decisiones, esto lo suelen hacer los gerentes, ellos generan ideas a partir de los datos analizados, además suelen asignar un significado especifico según amerite el caso.

Fase 3: Las decisiones generadas en la fase 2 se transforman en acciones operativas específicas. En este punto las decisiones se ejecutan.

Fase 4: Las decisiones que se ejecutan se transforman en acciones que generan resultados, el conjunto de datos resultante sirve para retroalimentar al proceso con el fin de mejorar la toma de decisiones futuras.

Como resultado de la ejecución de las cuatro fases descritas es posible obtener un sistema de Big data que puede beneficiar en gran medida a los procesos de la organización.

En la tabla 3 se presenta la información relacionada con las tareas esenciales, los recursos necesarios y los actores involucrados en cada fase del ciclo descrito en la figura 2, correspondiente a Big Data. (Tabesh et al., 2019)

Tabla 3. Fases del ciclo de Big Data

Cuatro fases del ciclo de Big Data				
	Fase 1 **Datos -Visión**	**Fase 2** **Visión -Decisión**	**Fase 3** **Decisión -Acción**	**Fase 4** **Acción - Datos**
Tarea principal	Limpieza de datos y análisis	Interpretación de ideas	Ejecución de decisiones	Recopilación de datos y almacenamiento
Recursos clave/ capacidad	Infraestructura técnica y capacidad	Capacidad de gestión para contextualizar	Capacidad para la ejecución de decisiones	Infraestructura técnica y capacidad
Actores críticos	Gestores de datos científicos	Gerentes	Gerentes	Gestores de datos científicos

Fuente: Propia

1.5.3. Barreras tecnológicas

Big Data requiere ciertas características tecnológicas, mismas que imponen varias restricciones en cuanto a la gestión y análisis de datos se refiere. Dentro de las limitaciones se encuentran las infraestructuras costosas para la adquisición, almacenamiento y análisis de datos. Es indispensable contar con profesionales calificados en el manejo de datos referentes a Big data. (Tabesh et al., 2019)

En la actualidad las empresas necesitan renovar sus infraestructuras en TI, puesto que las herramientas de administración de datos convencionales no tienen la capacidad de actualizar, manejar y analizar grandes volúmenes da datos, de hecho, de todas las empresas que son conscientes de la importancia de los datos, únicamente el 22% dominan la infraestructura tecnológica. (Tabesh et al., 2019)

1.5.4. Calidad de los datos en Big Data

La calidad de los datos es un tema importante, puesto que proporciona información precisa para la toma de decisiones. La calidad es posible con el cumplimiento de algunos requisitos mencionados en la norma ISO/IEC 25012, en esta se vincula la calidad de los datos a un grado en el que un conjunto de datos cumpla con las características de calidad necesarias.

La calidad de los datos depende del contexto de cada proyecto, puesto que se puede analizar en una o más dimensiones. Una de las dimensiones es la propiedad de la calidad de los datos medible que representa varios aspectos como precisión, consistencia entre otros. (Tabesh et al., 2019)

1.5.5. Mala calidad de los datos en Big Data

La calidad de los datos es esencial en Big Data, muchas investigaciones comprobaron que la deficiencia en la calidad de datos en diferentes contextos y niveles produce graves problemas. La mala calidad de los datos produce hallazgos incorrectos y afecta significativamente en la toma de decisiones. Además, se asocia un costo muy alto en cuanto a la perdida de oportunidades, la pérdida de ingresos, la re-ejecución de procesos debido a datos erróneos, entre otros.

Existen varias razones para la mala calidad de datos, estos pueden ser: errores en la entrada de datos, uso de métodos defectuosos para la recopilación de datos, falta de actualización de datos cambiantes en el tiempo, aplicación incorrecta de reglas comerciales, registros duplicados, valores de entrada faltantes o incorrectos, entre otros. (Tabesh et al., 2019)

Las anomalías en los datos se clasifican en sintácticas, semánticas y de cobertura.

a) Anomalías sintácticas

Este tipo de anomalías incluye errores léxicos (es decir diferencias entre la estructura de los elementos de datos y el formato especificado), errores de formato de dominio (errores que ocurren cuando el valor asignado para un atributo no se ajusta al formato de dominio esperado), irregularidades en el uso no uniforme de los valores (como el uso de diferente moneda).

b) Anomalías semánticas

En este tipo de anomalías se encuentran las violaciones de restricciones de integridad (cuando las tuplas no satisfacen una o varias restricciones de integridad), contradicciones (cuando los valores de tupla violan una clase de dependencia entre valores, por ejemplo, una diferencia entre la fecha y edad), entradas duplicadas y datos inválidos.

c) Anomalías de cobertura

Este tipo de anomalías se refieren a valores perdidos y tuplas faltantes.

Para una correcta configuración del sistema de gestión de datos es necesario de una fase de análisis de datos, con el fin de identificar los errores y anomalías que afecten a la calidad de los datos.

La fase de análisis permite seleccionar las dimensiones para cumplir con nuevos objetivos de calidad. Para ello la norma ISO/IEC 25012 proporciona una definición para las dimensiones más discutidas y clasifica a estas desde un punto de vista inherente, la norma centra un énfasis especial en valores de dominio, posibles restricciones, entre otros. Además, la norma describe la configuración que se debe alcanzar para mantener la calidad de los datos en un sistema informático. A continuación, en la tabla 4 se presenta las quince características que se debe cumplir para una calidad de datos adecuada según la norma ISO/IEC 25012.

Tabla 4. Calidad de los datos según ISO/IEC 25012

Característica	Inherente	Dependiente del sistema
Exactitud	X	
Exhaustividad	X	
Consistencia	X	
Corriente	X	
Accesibilidad	X	X
Conformidad	X	X
Confidencialidad	X	X
Eficiencia	X	X
Precisión	X	X
Trazabilidad	X	X
Comprensibilidad	X	X

Disponibilidad	X
Portabilidad	X
Recuperabilidad	X

Fuente: Propia

Es posible medir cada dimensión en base a métricas de calidad. Una métrica de calidad se define como evaluar una dimensión, la evaluación en base a su objetivo cuando se basa en medidas cuantitativas o subjetivo cuando se basa en evaluaciones cualitativas como percepciones, necesidades y experiencia de los interesados. Las métricas de evaluación se clasifican en tres categorías: según el tipo de información se utiliza como indicador de calidad.

Primera categoría: en esta la métrica se basa en el contenido, la misma información se usa como indicador de calidad.

Segunda categoría: en esta la métrica se basa en el contexto, los metadatos son usados como indicadores de calidad sobre las circunstancias en las que se creó o uso la información.

Tercera categoría: en esta la métrica se basa en la calificación, la métrica se basa en ratios explícitos.

1.5.6. Seguridad en Big Data

La seguridad de Big Data se centra en la confidencialidad, integridad y disponibilidad. La confidencialidad es la encargada de proteger a los datos de accesos no autorizados. La integridad se encarga de proteger los datos de cambios no autorizados. La disponibilidad se encarga de que los datos sean accesibles para los usuarios autorizados. Para garantizar la seguridad de la información Big Data requiere el cumplimiento de los controles de la norma ISO/IEC 27002. (TALHA, EL KALAM, & ELMARZOUQI, 2019)

En el campo de Big Data otro de los intereses esenciales es el proteger la información personal y sensible para colocarla como objetivo fundamental de seguridad. La privacidad se considera como una particularidad de la confidencialidad, misma que toma en cuenta elementos adicionales, como la gestión de los usuarios en base a los datos personales, cumplimento de obligaciones legales y reglamentarias, entre otras. (TALHA et al., 2019)

1.5.7. Ciclo de vida de la seguridad en Big Data.

Existen tres fases para la obtención de información relevante en Big Data. La primera consiste en recopilar datos de una variedad de fuentes. La segunda consiste en almacenar la información obtenido en entornos seguros. La tercera consiste en extraer información útil mediante técnicas de extracción de datos. Tratando el tema de seguridad es posible identificar una serie de amenazas en cada una de las fases descritas (TALHA et al., 2019). A continuación, en la figura 3 se presenta los diversos riesgos de seguridad que presenta en cada fase.

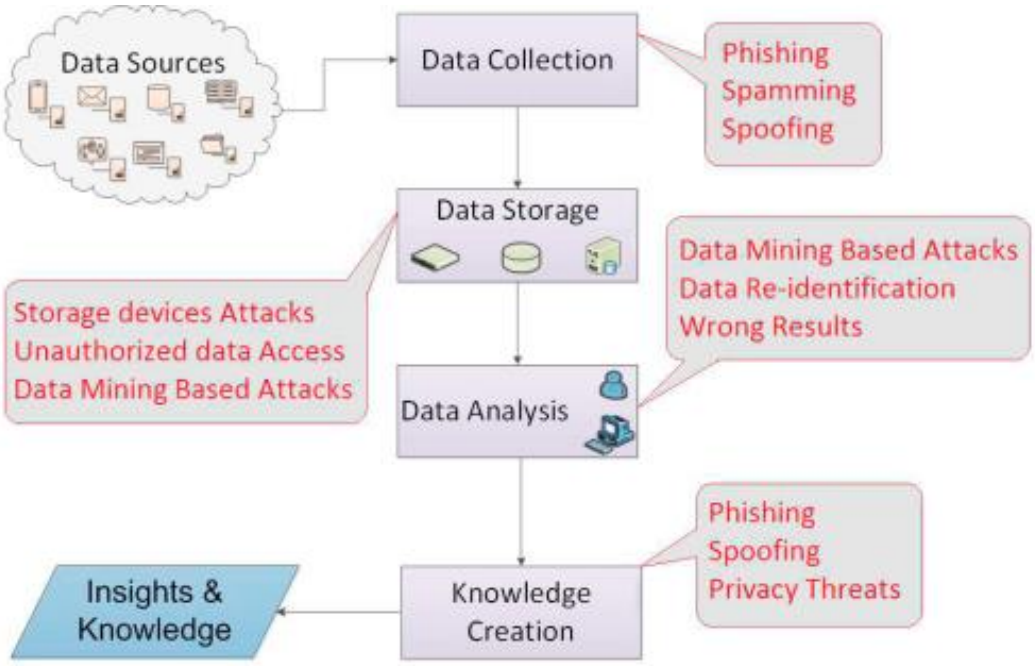


Figura 3: Ciclo de vida y seguridad en Big Data.

Fuente: (TALHA et al., 2019)

Fase de recolección de datos: desde la perspectiva de seguridad, es necesario recolectar información de fuentes confiables, además es imprescindible asegurar que los sitios de recolección sean seguros y protegidos contra fugas (phishing, spamming, apoofing). En esta fase es posible aplicar varias medidas para la recopilación de datos, como el control de acceso y el cifrado de datos confidenciales.

Fase de almacenamiento de datos: toda la información que se recopila en la fase previa se debe almacenar y proteger para garantizar un entorno seguro en la fase de análisis. En esta fase los blancos de ataque pueden ser los discos de almacenamiento, el ataque podría consistir en intentar vulnerar la seguridad para copiar, dañar o robar los discos de almacenamiento, acceder de forma no autorizada para explorar los servidores de datos y extraer información valiosa. Como medida preventiva es posible anonimizar los datos, para ello se emplean técnicas de partición e intercambio con el fin de proteger los datos.

Fase de análisis de datos: en esta fase se extrae información importante aplicando técnicas de minería de datos. Es necesario que el entorno de procesamiento sea seguro para evitar el acceso de entidades no autorizadas que pretendan analizar los datos para extraer información civil y/o personal. Existen varias técnicas para la deducción de información personal como la identificación y la correlación, otro factor muy influyente es la mala calidad de los datos, puesto que supone un riesgo para la seguridad. Si se ataca directamente a la integridad de los datos, los resultados obtenidos del análisis son erróneos.

Fase de creación de conocimiento: la información generada en la fase de análisis es muy sensible y debe ser protegida de manera obligatoria. Los riesgos de seguridad de esta fase se relacionan directamente con la fuga de datos (phishing y suplantación de identidad), además de la amenaza de la privacidad de las personas. En esta fase es necesario adoptar una estrategia para el control de acceso y el cifrado de los resultados relevantes.

1.6. Gestión de Riesgos

Los activos de una empresa según Bertolín (2008) deben ser objeto de gestión de riesgos para evitar su pérdida, uso inadecuado y perjudicar los objetivos del negocio en el servicio que brinda el sistema, están clasificados en tres grupos: datos e información los cuales son generados y almacenados por la organización; los sistemas e infraestructura encargados de gestionar dicha información y por último el personal conformado por los individuos que están involucrados en el mantenimiento, cuidado y protección de los dispositivos de hardware y software, así como de la información.

1.7. Vulnerabilidad Informática

Milagros & Steven (2017) manifiesta que son puntos endebles en la seguridad de un sistema informático o de un proceso, sirven de acceso a diversos tipos de amenazas generadoras peligros de integridad, privacidad, confidencialidad y autenticación de datos que pueden poner en peligro la confidencialidad, integridad y autenticación de la información. Cabe destacar, que existen riesgos de distintos tipos, físicos, naturales, de las comunicaciones, software e inclusive humanas.

Los riesgos físicos son aquellos que cubren las posibilidades de acceso al sistema de manera directa desde un equipo con la finalidad de extraer información, para alterarla o eliminarla, mientras que los riesgos naturales o imprevistas como incendios, inundaciones que provoquen pérdida en la información.

Las vulnerabilidades de comunicaciones se dan por acceso indebido de usuarios a un sistema de información conectado a una red global con fines de robar la información. En este sentido, Mieres (2009) manifiesta que los riesgos de software se presentan cuando existen contingencias de vulnerabilidad a causas de diseño o errores involuntarios de los usuarios que afecten a los datos.

1.7.1. Clasificación de las vulnerabilidades.

En la Tabla 6 se detallan las vulnerabilidades según su naturaleza:

Tabla 5: Clasificación de vulnerabilidades

Vulnerabilidades	Descripción
De diseño	Son debilidades que por lo general se encuentran adentro de las descripciones de hardware o software, por lo que representan esquemas mal definidos en las aplicaciones de software, o arquitecturas de red, sistemas de seguridad, infraestructura, entre otros. Las amenazas que se encuentran asociadas a esta vulnerabilidad son mala configuración de equipos, vandalismo o pérdida de datos así lo afirma Pazmiño (2007) .

De configuración	Son los que resultan de la administración de un componente del sistema o un error en la configuración, y adicionalmente pueden surgir como consecuencia de un error humano. Por lo cual, según Pazmiño (2007) las instituciones son propensas a caídas del sistema, pérdida de autenticación y de confidencialidad de la información.
De implementación	Este tipo de vulnerabilidades están relacionadas fundamentalmente a actividades de programación errónea de sistemas, por lo que los riesgos que están asociados son: de mal uso o configuración de equipos, así como pérdida de información y confidencialidad según lo expuesto por Pazmiño (2007).
Organizacionales	Están constituidas por las vulnerabilidades que surgen cuando no existe el registro adecuado de las políticas y prácticas de seguridad para su correcta aplicación en una organización a institución (Pazmiño, 2007).
Tecnológicas	Incluyen debilidades en el diseño, configuración e implementación de un sistema y están presentes por lo general en aplicaciones a servicios de red, arquitectura, y sistemas operativos según Pazmiño (2007).
Físicas	Son aquellas que se encuentran relacionadas a la infraestructura física de una institución que pueden acarrear faltas en control de acceso, protección antisísmica, acondicionamiento para servidores, entre otros (Pazmiño, 2007).
De control	Pazmiño (2007) expresa que están constituidos por controles mal desarrollados o implementados que pueden acarrear caídas en el sistema o pérdidas de la información.

Fuente: Autor

1.8. Normas ISO/IEC 27000

ISO es una organización no gubernamental que facilita la coordinación internacional y la unificación de los estándares industriales y de manera específica ha reservado la serie ISO/IEC 27000 para una gama de normas de gestión de la seguridad de la información de manera similar a lo realizado con las normas de gestión de la calidad, según lo señalado por ISO (2019).

La norma 27000 permite verificar la importancia de la implementación de un sistema de gestión de seguridad de información, una introducción a ellos, además de una descripción de pasos a seguir para las empresas u organizaciones que deseen certificarse con esta familia perteneciente a los estándares ISO.

1.8.1. Estándares que componen la familia de la ISO 27000

La composición general de la familia de la normativa ISO 27000 se fundamenta en varias normativas las cuales se ilustran en la Figura 4 y se describen a continuación:

- **ISO/IEC 27001**.-Es la norma principal de esta familia de normas y en ella se describe los requisitos del sistema de gestión de seguridad de la información.
- **ISO/IEC 27002**.-Describe los objetivos de control en relación con la seguridad de la información.
- **ISO/IEC 27003.-**Se basa en los aspectos más críticos del diseño de un SGSI muestra cómo debe llevar a cabo con cada una de los procesos para la seguridad de la información.
- **ISO/IEC 27004**.-Se define como una guía para la utilización de directrices de Sistemas de Gestión de Seguridad de Información que será pasos a seguir que ayudaran a cumplir con cada uno de ellos y sea menos riesgo para la seguridad de la información.
- **ISO/IEC 27005**.-Proporciona matrices guía en el riesgo de la seguridad de la información para tener un orden adecuado en el manejo de los datos o de la información que va ser respaldada en algún equipo de cómputo que ayude con el almacenamiento de los datos o información.
- **ISO/IEC 27007**.-Proporciona orientación sobre la realización de auditorías, así como orientación sobre la competencia de los auditores de sistemas de gestión de seguridad de la información.

- **ISO/IEC 27039**.-Es una guía para que permite el despliegue operativo de sistemas de detección de intrusos en la información empresarial.
- **ISO/IEC 27040**.-Es una guía para la seguridad en los diferentes medios de almacenaje de la información para que exista un resguardo de la misma, detallando cada paso y poder cumplir con cada uno de estos estándares.

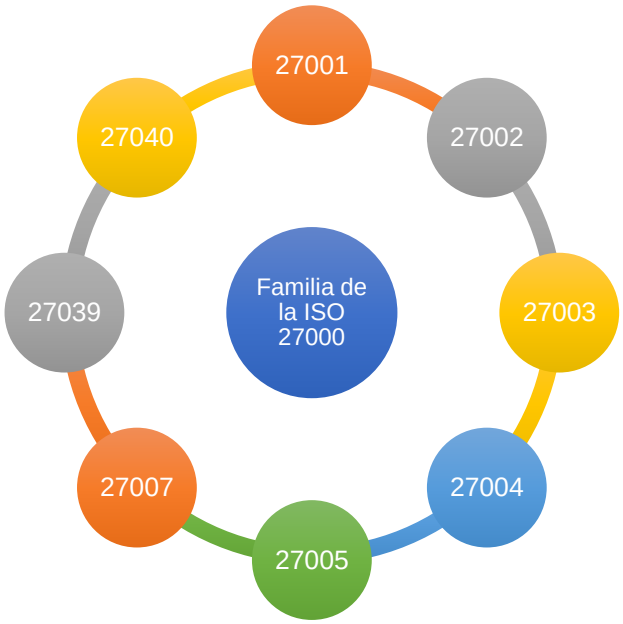


Figura 4: Estándares de conforman la familia de la ISO 27000

Fuente: Autor

1.9. Norma ISO 27001:2013

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información, además, tiene su origen en la BS 7799-2:2002 ya anulada y es la norma con arreglo a la cual se certifican por auditores externos los Sistemas de Gestión de la Seguridad de la Información (SGSI) de las organizaciones. Adicionalmente, enumera en forma de resumen objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por organizaciones en el desarrollo de sus SGSI, a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados de acuerdo a lo expresado por ISO (2019).

1.10. Norma ISO 27002:2017

La ISO 27002:2017 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de seguridad de la información a todos los interesados y responsables de tecnologìa para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad. La norma ISO 27002 se encuentra organizada en base a los 14 dominios, 35 objetivos de control y 114 controles según ISO (2019).

1.11. Norma ISO 27004:2016

La ISO (2019) facilita una serie de mejores prácticas para poder medir el resultado de un Sistema de Gestión de la Seguridad de la Información(SGSI) basado en ISO 27001:2013, este estándar especifica como estructurar el sistema de medición, qué parámetros medir, cuándo y cómo medirlos, y ayuda a las empresas a crear objetivos de rendimiento y criterios de éxito. Asimismo, expone que el tipo de medidas requeridas dependerá del tamaño y complejidad de la organización, de la relación coste beneficio y del nivel de integración de la seguridad de la información en los procesos de la propia organización.

1.12. Norma ISO 27006:2015

Esta norma específica requisitos y proporciona una guía para organismos que brindan auditoría y certificación de sistemas de gestión de seguridad de la información (SGSI), además de los requisitos contenidos en ISO / IEC 17021 e ISO / IEC 27001:2013. El objetivo principal es apoyar la acreditación de los organismos de certificación que proporcionan la certificación SGSI en base a ISO (2019).

Los requisitos contenidos en ISO / IEC 27006: 2007 deben ser demostrados en términos de competencia y confiabilidad por cualquier organismo que proporcione la certificación SGSI, y la guía contenida en ISO / IEC 27006: 2007 proporciona una interpretación adicional de estos requisitos para cualquier organismo que proporcione la certificación SGSI.

1.13. Norma ISO 27007:2017

La norma internacional ISO 27007:2017 forma parte de la familia de normas del Sistema de Gestión de Seguridad de la Información y proporciona una guía para las organizaciones certificadas para auditar el SGSI.

1.13.1. Antecedentes de la Norma ISO 27007:2017

De acuerdo a ISO (2019) es una guía para gestionar un sistema de gestión de seguridad de la información (SGSI), programas de auditoría, realización de auditorías, y en la competencia de los auditores ISMS[4], además de las directrices contenidas en la norma ISO 19011: 2013, además es aplicable a aquellos que necesitan para comprender o llevar a cabo auditorías internas o externas de un SGSI o para gestionar un programa de auditoría ISMS por lo que el alcance de la auditoría debe tener en cuenta los riesgos de seguridad de la información y los riesgos y oportunidades que afectan el SGSI de las partes pertinentes, es decir, el cliente de la auditoría y el auditado.

1.13.2. Principales directrices de la Norma ISO 27007:2017

La norma ISO 27007 se basa en gran medida en ISO 19011, el estándar para auditar sistemas de gestión, que ofrece orientación específica para el Sistema de Gestión de Seguridad de la Información. En la tabla 6 se detallan las principales directrices de la ISO/IEC 27007:2017.

Tabla 6: Principales directrices de la ISO/IEC 27007:2017

Principales directrices de la ISO/IEC 27007:2017
3. Principios de auditoría Aplican los principios de auditoría del Capítulo 4 de la ISO 19011:2011
4. Administración de un programa de auditoría
4.1. General De las directrices de la norma ISO 19011:2011 se aplican las 5.1
4.2. Establecimiento de los objetivos del programa de auditoría De las directrices de la norma ISO 19011:2011 se aplican las 5.2

[4] **ISMS:** Son las siglas en ingles de los Sistemas de Gestión de Seguridad de la Información

4.2.1. Es de 5.2 Establecimiento de los objetivos del programa de auditoría. a) Requisitos de seguridad de la información identificados b) Requisitos de la ISO/IEC 27001 c) Nivel de desempeño del auditado, como se refleja en la aparición de eventos e incidentes de seguridad de la información y la efectividad del SGSI.
4.3. Establecimiento del programa de auditoría
4.3.1. Función y responsabilidades de la persona que administra el programa de auditoría De las directrices de norma ISO 19011:2011, se aplican 5.3.1
4.3.2. Competencia de la persona que administra el programa de auditoría De las directrices de la norma ISO 19011: 2011, se aplican 5.3.2.
4.3.3. Establecimiento de la extensión del programa de auditoría De las directrices de la norma ISO 19011: 2011, se aplican 5.3.3.
5.3.3.1 Establecer el alcance de la auditoría a) El tamaño del SGSI b) La complejidad del SGSI c) Qué tan significativos son los riesgos de seguridad
5. Realización de la auditoría
6.4.3. Realización de la revisión de la documentación, mientras se realiza la auditoría

Fuente: Autor

1.14. Norma ISO 19011:2018

Esta norma proporciona recomendaciones para ayudar a las organizaciones a establecer un programa de auditoría que facilite el cumplimiento de los requisitos establecidos en las diferentes normas ISO. La normativa 27007:2017 y la 19011 trabajan en conjunto para proporcionar más precisión en las directrices o pasos a seguir, al momento de realizar una aduditoria al SGSI.

CAPÍTULO 2

Desarrollo

2.1. Análisis de Situación actual

En la actualidad el sistema académico de la UTN ha experimentado un crecimiento de datos importante, por esta razón se ha estimado la necesidad de evaluar y llevar un control orientado a garantizar integridad, seguridad y confiabilidad de la información, aspectos que requieren ser revisados en base a modelos de control interno para establecer una línea base diagnostica en post de su mejoramiento y eficiencia administrativa de los activos de información. Esto representa un elemento crítico que requiere ser abordado con instrumentos de reajuste y vanguardia acorde con los mecanismos de control vigente.

La auditoría de los activos de información se basa en una normativa vigente dentro de un marco legal que garantice el alto cumplimiento de la seguridad de estos conlleva a la correcta y eficiente administración de estos recursos, que avala la gestión y control de los sistemas.

2.2. Descripción del sistema académico UTN

El sistema académico es una herramienta factible, permite organizar y administrar los datos e información de los estudiantes, docentes y personal administrativo pertenecientes a la institución. a la institución, modernizando de esta forma los procesos académicos.

La información crece cada día a un ritmo exponencial por este hecho se ha visto en la necesidad de trasladar toda la información y sistemas de la institución, a otra plataforma reduciendo así los costos e incrementando la capacidad de almacenamiento en Oracle Cloud para que los usuarios accedan a los recursos que están en línea a través de un servidor remoto.

2.2.1. Proceso general del sistema académico

El sistema académico está conformado por sistemas interrelacionados, que apoyan a la gestión de los procesos de las distintas facultades, centros, posgrados y demás unidades académicas que conforman la Universidad Técnica del Norte. En la figura 5 se muestran los procesos generales del sistema académico.

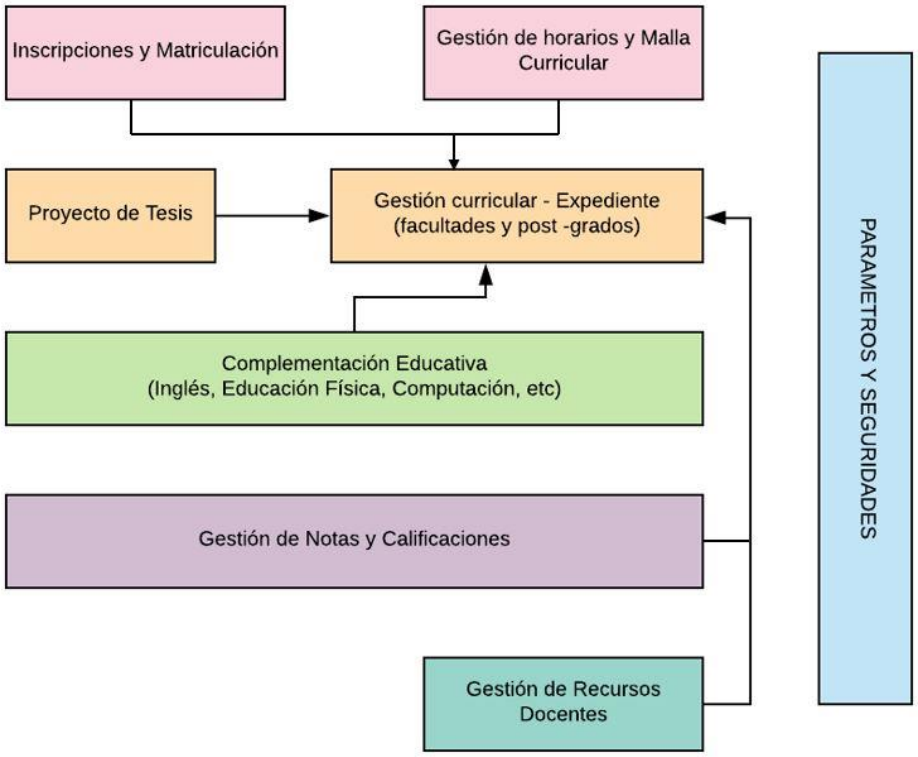


Figura 5: Proceso del Sistema Académico

Fuente: Autor

Los módulos que conforman el sistema académico UTN son los siguientes:

- Inscripciones y Matriculación
- Gestión de horarios y Malla Curricular
- Gestión Curricular
- Gestión de Proyectos de Tesis
- Gestión de Complementación Educativa
- Gestión de Notas y Calificaciones
- Gestión de Recursos Docentes

A continuación, se describen las principales características, facilidades operativas y reportes para la gestión de información que dispone cada uno de los módulos que conforman el sistema académico:

- **Inscripciones y matriculación**

Registra la información de aspirantes que recibirán cursos de preparación académica, para determinar la admisión en calidad de estudiantes en una carrera de las facultades de la UTN.

- **Gestión de horarios y malla curricular**

El principal objetivo de este módulo es definir planes curriculares, que deberá cursar cada estudiante, a medida que aprueba materias o créditos que conforman la malla curricular, considerando las regulaciones y normativas de la UTN, (falta)

- **Gestión curricular – expediente**

Este módulo permite consultar el historial académico de un estudiante en un determinado plan curricular, se proporciona mantenimiento a sus datos personales, de acceso y seguridad, o cualquier información relacionada con su permanencia en la UTN.

- **Gestión de proyectos de tesis**

En este módulo se administra las funcionalidades de información relacionada a proyectos de tesis desde la presentación del anteproyecto, hasta su defensa y calificación.

- **Gestión de complementación educativa**

Administra la información de todos los planes complementarios educativos, requisitos obligatorios en programas de pregrado.

- **Gestión de notas y calificaciones**

Gestiona las calificaciones que utiliza cada materia o crédito de un programa curricular, así como el ingreso de calificaciones parciales y definitivas, con sus respectivos reportes de notas y calificaciones.

- **Gestión de recursos docentes**

Permite ingresar recursos y material de estudio de cada materia, administra la planificación docente, y todas las actividades concernientes, asignación, mantenimiento de la información de su currículo, control de asistencia; entre las funciones más importantes.

2.3. Estructura organizacional

Una estructura organizacional establece un sistema de papeles que desarrollan los miembros de una organización para trabajar de una forma óptima y que alcancen las metas fijadas. En la Figura 6 se observa el Organigrama estructural de la UTN.

2.3.1. Organigrama estructural UTN

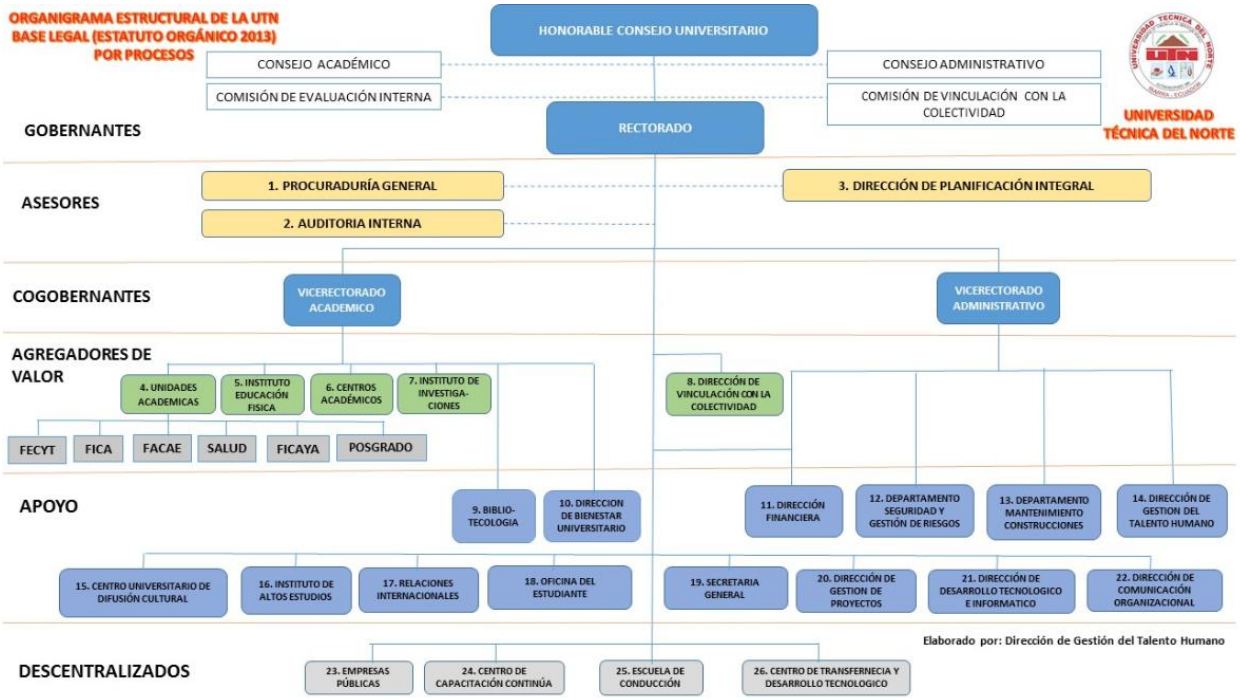


Figura 6: Organigrama Estructural de la UTN

Fuente: https://www.utn.edu.ec/web/uniportal/?page_id=2171

2.3.2. Organigrama del Departamento de Informática

La estructura organizativa del departamento de informática está compuesta por diferentes áreas que se enumeran en la Figura 7.

Figura 7: Organigrama del Departamento Informático – UTN

Fuente: http://repositorio.utn.edu.ec/bitstream/123456789/969/1/OrganigramaDI.pdf

2.3.3. Misión

La dirección de desarrollo tecnológico e informático de la Universidad Técnica del Norte, le corresponde administrar los servicios de informática, computación y comunicaciones, sin perjuicio de las demás funciones que se le recomiende. Ser el ente regulador de las políticas y normativas de carácter institucional; que deben ser llevadas a cabo con rigor, manteniendo el alto espíritu de calidad en todos los funcionarios, con el fin de lograr las expectativas encomendadas al departamento (UTN, 2013).

2.3.4. Visión

Establecer el rumbo estratégico del departamento y ejercer el liderazgo a nivel institucional, regional y nacional en el campo de la informática, computación y telecomunicaciones con tecnología de punta, investigaciones de avanzada e innovación que aportara para la transformación de la UTN (UTN, 2013).

2.3.5. Roles, Responsabilidades y Funciones del Personal de TIC'S

El mayor aporte que genera una definición de roles es que se tendrá establecidas las tareas que realizará cada uno de los miembros del equipo dentro de la organización. En la Tabla 7 se especifica el rol de cada miembro que integra el DDTI.

Tabla 7. Roles DDTI

Puesto	Responsabilidades y Funciones
Jefe de Proyecto	Es el encargado de asignar recursos, gestionar prioridades, coordinar las iteraciones con los clientes y usuarios y mantiene al equipo del proyecto enfocado en los objetivos institucionales. Asimismo, establece un conjunto de prácticas que aseguran la integridad y calidad del proyecto, así como el impulso y desarrollo de proyectos de tecnologías de información y comunicación que la Universidad requiera.
Analista de Sistemas	Es el encargado de capturar, especificar y validar los requisitos, interactuando con el cliente y los usuarios mediante entrevistas, así como la colaboración en la elaboración de las pruebas funcionales y modelos de datos.
Programador	Es el encargado de construir prototipos, elaborar las pruebas funcionales, modelos de datos y las validaciones con el usuario.
Ingeniero de Software	Se encarga de la gestión de requisitos, la configuración y elaboración del modelo de datos, y preparación de las pruebas funcionales y la elaboración de la documentación.

Administrador de la Red	Su rol es el de realizar la adquisición de paquetes de software, licencias y hardware que permitan dar solución a las necesidades tecnológicas, así como tener una red monitoreada las 24 horas y operando al 100%.
Web máster	Su principal función es la de fortalecer la investigación, implementación de nuevas tecnologías para la administración del Geo portal. Asimismo, la participación en soporte y soluciones informáticas de los diferentes planes y proyectos en las áreas de la institución que buscan mejorar las condiciones de procesos.
Ingeniero de Hardware	Gestiona la adquisición de los insumos de software y hardware necesario, establece políticas de operación y control informático, formula plan de contingencia para asegurar la protección del hardware y la información ante algún desastre natural o provocado y se encarga del manejo del catálogo electrónico de equipos informáticos del Sistema Nacional de Compras Públicas.

Fuente: (UTN, 2013)

2.4. Metodología

El método que se utilizará para la evaluación a la seguridad de la información del sistema académico de la UTN y así mismo se definirá el tipo de investigación a emplearse, la necesidad de la obtención de la información y la manera en cómo se recopilará, para su respectivo análisis y validación con ayuda de software y para obtener un resultado valido.

2.4.1. Población y muestra

Es necesario determinar el tamaño adecuado de la muestra que se empleara para el método de muestreo, este permite establecer el número de encuestados para evaluar las aplicaciones y seguridades del Sistema académico de la Universidad Técnica del Norte.

Para el cálculo de la muestra se debe tomar en cuenta tres factores.

- Proporción estimada de la variable a considerar
- Nivel de fiabilidad
- Margen de error aceptable.

Para el tamaño de la muestra se basa en una muestra aleatoria simple, misma que se puede calculada con la siguiente expresión.

$$a = \frac{f^2 \, x \, d(1-d)}{l^2}$$

En donde:

a= tamaño de la muestra

f= nivel de fiabilidad del 95% (valor estándar de 1,96)

d= predominio estimado en la zona del proyecto

l= margen de error de 5% (valor estándar de 0,05)

Con el tamaño de la muestra se debe segmentar la población en: estudiantes, docentes y personal administrativo. La segmentación de la población se la realizo con los datos que posee el Departamento de Informática de la UTN y que se expone en la Tabla 8.

Tabla 8. Usuarios de la Universidad Técnica del Norte

Usuarios	Número	Porcentaje
Estudiantes	9829	89.35%
Docentes	770	7.0%
Personal	401	3.64%
TOTAL	1100	100%

Fuente: (UTN, 2013)

El resultado de aplicar la expresión antes descrita fue una muestra de 337 estudiantes, 35 docentes y 17 personas del personal administrativo. Dentro del personal administrativo se encuentran lo miembros encargados del manejo y la gestión del sistema académico.

2.5. Métodos para la investigación

Existen varios métodos y técnicas para auditorias de sistemas de información, el método que se elija depende mucho de lo que se pretende analizar. Para la presente investigación se analiza las cuatro fases estándar del proceso de revisión:

- Aplicación de estudio preliminar.
- Revisión y evaluación de controles de seguridad.
- Examen detallado de áreas críticas.
- Informe de resultados.

2.5.1. Tipo de investigación.

Para llevar a cabo el proceso de evaluación de amenazas y vulnerabilidades de la información es necesario conocer la infraestructura tecnológica que emplea la Universidad Técnica del Norte, para ello se empleó tres tipos de investigación.

Descriptiva: es necesario trabajar con las actividades, características y procedimientos que la Universidad Técnica del Norte posee y aplica para la determinación de riesgos que involucran la seguridad de la información del sistema académico.

Mixta: las políticas que existan en la Universidad Técnica del Norte se pretende reaccionarlas con encuestas formuladas a los usuarios del sistema académico. Con el fin de verificar las políticas empleadas en la UTN en cuanto a seguridad de la información.

Transversal: la información recolectada será de ayuda para la evaluación técnica del sistema académico, misma que se desarrolla en un tiempo definido.

2.5.2. Métodos de investigación

Método científico: este método aplica al caso de estudio, debido a que se emplea la norma ISO/IEC 27007:2017 como guía para la ejecución de la auditoría. Además, esta norma cita a la norma 27002:2013, con la finalidad de seguir los controles descritos en dicha norma bajo la guía de ejecución del manual de auditoría.

Método deductivo: este método se aplica al caso de estudio, debido a que la norma ISO/IEC 27007:2017 ejecuta la auditoría en base a los controles de la norma 27002:2013, controles que pueden ser aplicados para cualquier organización.

Método inductivo: este método se aplica al caso de estudio, debido a que para la evaluación del sistema académico nos será de utilidad los datos particulares (de investigación), con el fin de determinar las amenazas y vulnerabilidades.

2.5.3. Técnicas para la recopilación de información.

Fichas técnicas: para recopilar la información relevante en cuanto activos físicos como personal humano se planteó una ficha técnica que será de ayuda para la identificación de activos en todo nivel.

Check list: para recopilar información relevante en cuanto a políticas, controles de gestión y operación que emplea el sistema académico se formuló un check list en base a la norma ISO/IEC 27002:2013. Esta herramienta permite validar los controles de la norma y verificar la aplicación de cada control dentro de la UTN.

Encuestas: para recopilar información relevante en cuanto a usabilidad del sistema académico se formuló encuestas a todos los usuarios que forman parte de este, para comprender de mejor forma la funcionalidad real del sistema académico.

Revisión de la documentación: para abarcar otros aspectos que no pueden ser identificados en las dos herramientas anteriores se propone la revisión de documentación como:

- Informes de evaluación de riesgos
- Plan integral de desarrollo informático
- Manuales de usuario del sistema académico.

2.6. Plan de auditoría

Para la ejecución de la auditoría del sistema académico de la Universidad Técnica del Norte se toma en cuenta la norma ISO/IEC 27007:2017.

2.6.1. Sujeto de la Auditoría.

El sujeto de la auditoría es la Universidad Técnica del Norte, Departamento de Informática (DDTI), Sistema Integrado informático Universitario- sistema académico.

2.6.2. Formulación del plan

El plan de estudio se realizó dentro de la UTN, en el Departamento de Desarrollo de Tecnologías de la Información.

2.6.3. Introducción

Este informe de la situación actual de la seguridad de los datos del sistema académico orientado a Big Data de la Universidad Técnica contiene a detalle los aspectos, evaluados en el

sistema académico de la UTN, donde se identificó amenazas y vulnerabilidades existentes, se propuso recomendaciones para, con la finalidad de tomar las decisiones pertinentes en el uso y manejo adecuado del sistema, salvaguardando la información que se genera constantemente.

2.6.4. Antecedentes

La UTN (Universidad Técnica del Norte) como un referente de la región norte del Ecuador desarrolla sus aplicaciones informáticas y las integra en un el SIIU (Sistema Informático Integrado Universitario), con el paso del tiempo el volumen de información ha crecido exponencialmente y con ella la seguridad en los sistemas informáticos se ve expuesta ataques. El DDTI (Departamento de Desarrollo Tecnológico e Informático) es el encargado del manejo de los sistemas que se encuentran almacenados en el SIIU dentro de la UTN y en este último año los sistemas informáticos han sido trasladados a la nube y es ahí donde se encuentran vulnerables, es por eso que para poder detectar las amenazas a las que están expuestos los sistemas se decide utilizar la metodología de Magerit para analizar los activos que hacen parte del almacenamiento, trazabilidad y confidencialidad de la información al momento del uso y manejo del sistema académico, exponiendo las vulnerabilidades utilizadas por las amenazas para eludir la seguridad establecida.

2.6.5. Justificación

a) Descripción del problema

La creciente información en el sistema académico de la Universidad Técnica del Norte determinó la migración de los datos a la nube, por lo que se desconoce el nivel de seguridad actual de los mismos. Este sistema requiere una evaluación y control de seguridad mediante una normativa vigente es por eso, que se hace necesaria una verificación técnica de los procesos y procedimientos de control interno de información dentro del Departamento de Tecnología y en los activos del sistema implementado para salvaguardar los recursos tecnológicos, y plantear acciones que ayudarán a manejar eficientemente, velar por la eficacia de sus procesos y el valor de sus recursos.

b) Solución Propuesta

Debido al problema descrito anteriormente se realizó una auditoría al Sistema de Gestión de Seguridad de Información (SGSI) mediante el uso de la herramienta PILAR que trabaja con la Metodología de Magerit al sistema académico de la Universidad Técnica del Norte, con el objetivo de conocer el estado actual y proporcionar las recomendaciones adecuadas para minimizar los

riesgos y optimizar el manejo del sistema de acuerdo con las buenas prácticas establecidas en la Norma ISO 27007:2017.

c) Ventajas de la solución propuesta

El desarrollo de esta auditoría permitirá conocer las amenazas y vulnerabilidades a las que se encuentra expuesto el sistema académico y el impacto que causaría a la Institución. Adicionalmente, también se obtuvo un documento con recomendaciones para el mejoramiento continuo de los sistemas de información para la toma correcta de decisiones por parte del departamento encargado en la universidad.

2.6.6. Alcance

Para el desarrollo de este proyecto se realizó un levantamiento de información a través de entrevistas al personal de la DDTI, observación de la ejecución de las operaciones, competencias de las personas y dependencias que intervienen en el manejo de las operaciones; así como una evaluación de la seguridad al sistema mediante una herramienta informática.

Con el objetivo de recopilar la suficiente evidencia confiable se aplicó banco de preguntas para la evaluación de controles orientados a comprobar el cumplimiento de políticas con la ayuda de las principales directrices de la normativa ISO/IEC 27007:2017 y de los requerimientos que hace mención en las políticas de uso de la metodología Magerit y de esta manera mitigar los riesgos y salvaguardar la información obtenida.

2.6.7. Objetivo general

Realizar una auditoría de seguridad de la información de los datos del sistema académico de la Universidad Técnica del Norte, con el objeto de establecer su estado actual y emitir las recomendaciones para minimizar y optimizar su uso orientado a Big Data.

2.6.8. Objetivos específicos

- Evaluar el procedimiento de los controles de operación.
- Estudiar la documentación referente a la norma ISO/IEC 27007:2017.
- Realizar un levantamiento de información en el DDTI de los activos que forman parte del sistema académico.
- Analizar y evaluar la información obtenida en la herramienta Pilar y así poder determinar el nivel de seguridad en el sistema académico.

- Elaborar un informe técnico con recomendaciones de los resultados obtenidos en el diagnóstico, de acuerdo con el cumplimiento de las Normas.

2.6.9. Condiciones de ejecución

- **Organización:**

La tesista encargada revisara la información proporcionada por parte del DDTI acerca del Sistema Académico:

- Objetivo del activo
- Objetivo del puesto
- Responsable Principal
- Competencias profesionales
- Normativas de Seguridad

- **Metodología:**

El trabajo cubrió las siguientes actividades:

- Elaborar Plan Preliminar.
- Investigación sobre el sistema académico.
- Evaluación de riesgos
- Elaborar un informe con las recomendaciones.

Las técnicas utilizadas en la investigación son las siguientes:

- Entrevistas al personal técnico.
- Consultas a expertos.
- Observación de campo.

2.6.10. Factores de Riesgos

Como factor de riesgo para no alcanzar los objetivos del presente trabajo de auditoría se tomó en cuenta los siguiente:

- En caso de falta de colaboración por parte de funcionarios o intervención no adecuada de los mismos, deberá tomarse las medidas administrativas.

- El Personal está sujeto a traslados lo que no permitiría mantener una continuidad en el proyecto, y se debería informar para conocer a los nuevos encargados y mantener la continuidad del proyecto.

2.6.11. Áreas para examinar

Las áreas que serán examinadas son las correspondientes al departamento de informática de la UTN.

1. Director del departamento de Informática
2. Analistas de Sistemas
3. Administrador de la red.

2.6.12. Sistema por auditar.

Tabla 9. Servicios del sistema académico.

#	Módulo	Descripción
1	Sistema Académico	Inscripción y matriculación(Registro e información de aspirantes que recibirán los recursos de preparación académica, proceso de matriculación en las diferentes unidades académicas; facultades, institutos o centros, Equiparación y convalidación de asignaturas), gestión curricular y expediente(Calendarios académicos, apertura y cierre de ciclos académicos(años, semestre, entre otros), parámetros y requisitos de eventos y actividades académicas, historiales académicos de estudiantes, fichas socioeconómicas de estudiantes), gestión de mallas curriculares y horarios(mantenimiento físico de edificios de unidades académicas; facultades, institutos, escuelas, especialidades y unidades de apoyo académico: laboratorio, granjas, talleres, entre otros. Parámetros y requisitos de mallas, curriculares y pensum académico, planes curriculares y sílabos, distribución docente, control de horarios), gestión de evaluación académica, asistencia e información gerencial.

Fuente: (UTN, 2013)

2.6.13. Tipo de Auditoría

En definitiva, se realizó una **AUDITORÍA DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN.** Al sistema académico de la Universidad Técnica del Norte, con el objetivo de establecer su estado actual y emitir las recomendaciones necesarias para minimizar los riesgos y optimizar el sistema para el uso adecuado del mismo.

2.6.14. Cronograma de trabajo

Tabla 10. Horas estimadas de ejecución de la auditoría.

PROGRAMA DE AUDITORÍA		
EMPRESA	**UNIVERSIDAD TÉCNICA DEL NORTE. DEPARTAMENTO DE INFORMÁTICA**	
FASE	**ACTIVIDAD**	**HORAS ESTIMADAS**
I	VISITA PRELIMINAR Solicitud de documentación del sistema académico Petición de información organizacional, recursos humanos y estructura orgánica. Desarrollo de encuestas	40
II	EJECUCIÓN DE LA AUDITORÍA Aplicación de encuestas a los estudiantes Aplicación de encuestas a los docentes. Aplicación de encuestas al personal administrativo Aplicación de encuesta a los miembros del DDTI. Identificación y clasificación de activos físicos. Identificación de activos críticos. Identificación de los activos humanos. Evaluación del proceso de los datos, respaldo y seguridad física de los datos.	120
III	REVISIÓN Y PRE- INFORME Revisión y aplicación a detalle de los controles de la norma ISO/IEC 27002:2017 con la ayuda de la guía de la ISO/27007:2017.	60

IV	INFORME Elaboración del informa de auditoría en base a resultados obtenidos	24

Fuente: Propia

2.6.15. Diagrama de GANT

Nombre	Duracion	Inicio	Terminado
Elaboración de encuestas y cuestionarios	2 days?	2/01/19 8:00	3/01/19 17:00
Elaboracion de Plan Preliminar	1 day?	7/01/19 8:00	7/01/19 17:00
Recopilación de infomación	6 days?	8/01/19 8:00	15/01/19 17:00
Análisis de la informacion obtenida	6 days?	16/01/19 8:00	23/01/19 17:00
Evaluacion del sistema academico UTN	4 days?	24/01/19 8:00	29/01/19 17:00
Determinacion del diagnostico	4 days?	30/01/19 8:00	4/02/19 17:00
Elaboracion del documento	4 days?	5/02/19 8:00	8/02/19 17:00

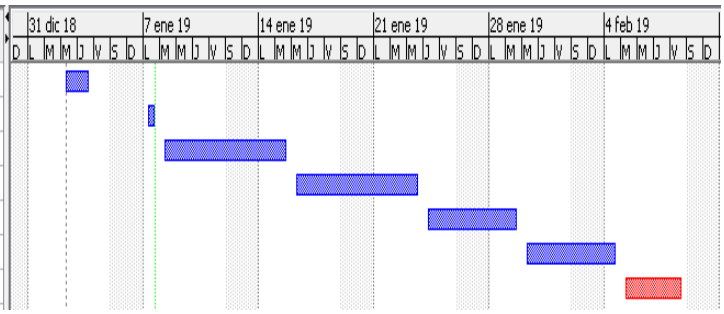


Figura 8: Cronograma de trabajo, plan de auditoría.

Fuente: Propia.

2.7. Ejecución de auditoría

2.7.1. Recopilación de datos.

La finalidad de esta fase es obtener información acerca del sistema académico, para ello se empleó varias herramientas clave para la recopilación de la información.

Las herramientas que se emplearon en la auditoría fueron las entrevistas, mismas que fueron realizadas al director de Informática de la Universidad Técnica del Norte y a diferentes miembros del DDTI. Es importante tomar en cuenta que para la recopilación de información se trató de tomar en cuenta de los miembros con mayor experiencia en el DDTI, tomando en cuenta la disponibilidad de tiempo.

Otra herramienta que se aplico fue la encuesta, misma que fue ejecutada a todos los usuarios del sistema académico, es decir a los estudiantes, docentes, personal administrativo y miembros del DDTI.

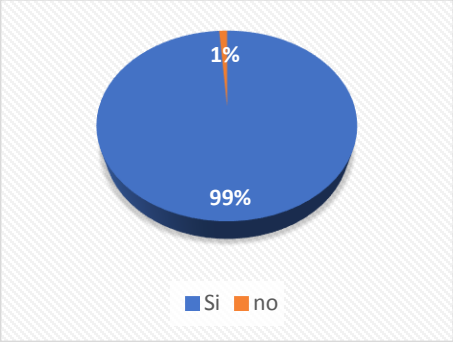
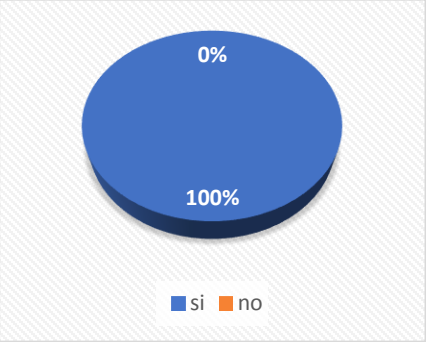
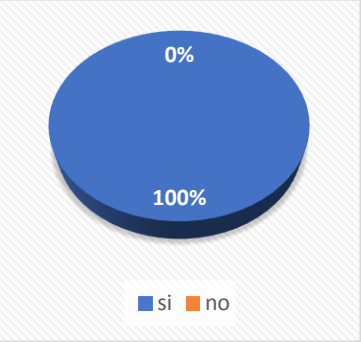
Las encuestas y entrevistas desarrollados se adjuntan en el anexo A y B.

Análisis de la primera encuesta (primera herramienta)

Para el estudio de la gestión de la seguridad de la información, se recopilo información mediante encuestas formuladas hacia los usuarios del sistema académico de la Universidad Técnica del Norte. Con el fin de determinar el volumen de datos que maneja el sistema en mención, además de identificar riesgos latentes. A continuación, se detallan las preguntas formuladas a cada usuario de la muestra calculada.

1) ¿Utiliza el sistema académico de la UTN?

Tabla 11. Primera pregunta de encuesta

Estudiantes	Docentes	Personal Administrativo
		

Fuente: Propia

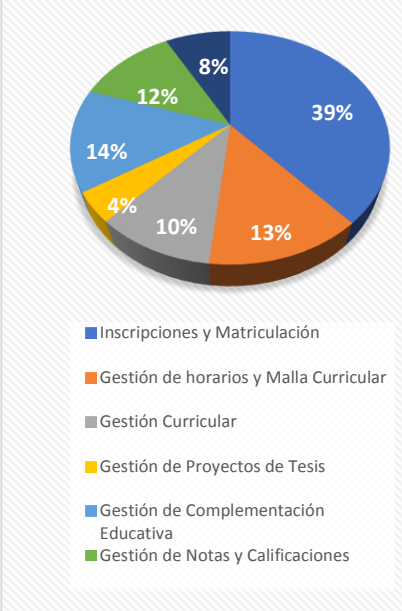
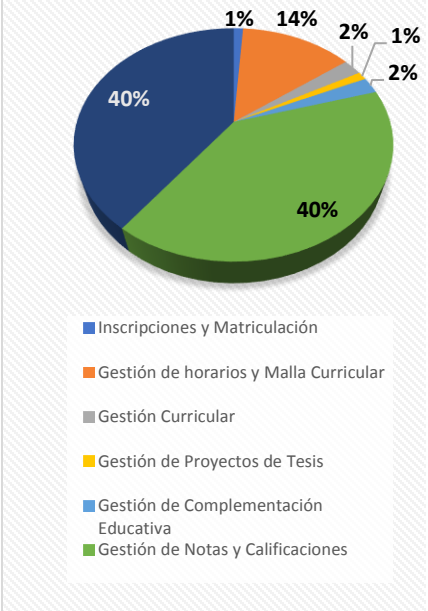
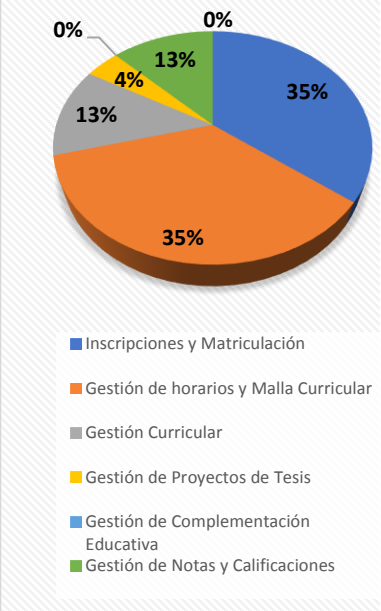
Análisis de resultados

En la tabla 11 se presenta los datos resultantes de la primera pregunta realizada a estudiantes, Docentes y personal administrativo. Los datos muestran que los docentes y el personal administrativo usa a menudo el Sistema académico de la UTN. En otra perspectiva se observa que el 99% de los estudiantes usa a menudo el sistema académico, mientras que un 1 % no lo suele usar. En base a las cifras obtenidas es posible concluir que la mayor parte de los usuarios de la UTN usan con frecuencia el sistema académico.

2) ¿A qué parte del sistema académico tiene acceso?

Tabla 12. Segunda pregunta de encuesta

Acceso	Estudiantes	Docentes	Personal Administrativo
Inscripciones y Matriculas	309	1	17
Gestión de horarios y malla curricular	107	12	17
Gestión Curricular	81	2	6
Gestión de Proyectos de tesis	33	1	2
Gestión de Complementación Educativa	114	2	0
Gestión de Notas y Calificaciones	96	35	6
Gestión de recursos Docentes	64	35	0

Estudiantes	Docentes	Personal administrativo
		

Fuente: Propia

Análisis de resultados

En la tabla 12 se presenta los datos resultantes de la segunda pregunta formulada a estudiantes, docentes y personal administrativo. Los datos muestran que los estudiantes tienen acceso a ciertas áreas del sistema académico, repartidas de la siguiente forma el 39% de los estudiantes tiene acceso a Inscripciones y matriculas, el 13 % que tiene acceso a la gestión de horarios y malla curricular, un 10 % tiene acceso a gestión curricular, un 14 % tiene acceso a gestión de complementación educativa, un 12 % tiene acceso a gestión de notas y calificaciones, un 4 % tiene acceso a gestión de proyectos de tesis y por ultimo un 8% tiene acceso a gestión de recursos docentes. Desde otra perspectiva se tiene que los docentes tienen acceso a varias áreas, repartidas de la siguiente forma: el 40% tiene acceso a gestión de notas y calificaciones, otro 40 % tiene acceso a gestión de recursos docentes, un 14% tiene acceso a gestión de horarios y malla curricular, un 2% tiene acceso a gestión curricular, otro 2% tiene acceso gestión de complementación educativa, un 1% tiene acceso a inscripciones y matriculas y por ultimo un 1% tiene acceso a gestión de proyectos de tesis. Desde otra perspectiva se tiene al personal administrativo, mismo que tiene acceso a varias áreas del sistema académico, repartidos de la siguiente forma: un 35 % tiene acceso a inscripciones y matriculas, otro 35% tiene acceso a gestión de horarios y malla curricular, un 13% tiene acceso a gestión curricular, un 31% tiene acceso a gestión de horarios y malla curricular y por último un 4% tiene acceso a gestión de proyectos de tesis. De los resultados obtenidos se concluye que tanto los estudiantes, docentes y personal administrativo tiene acceso a todas las áreas del sistema académico, excepto el personal administrativo que no tiene acceso a gestión de recursos docentes y gestión de complementación educativa.

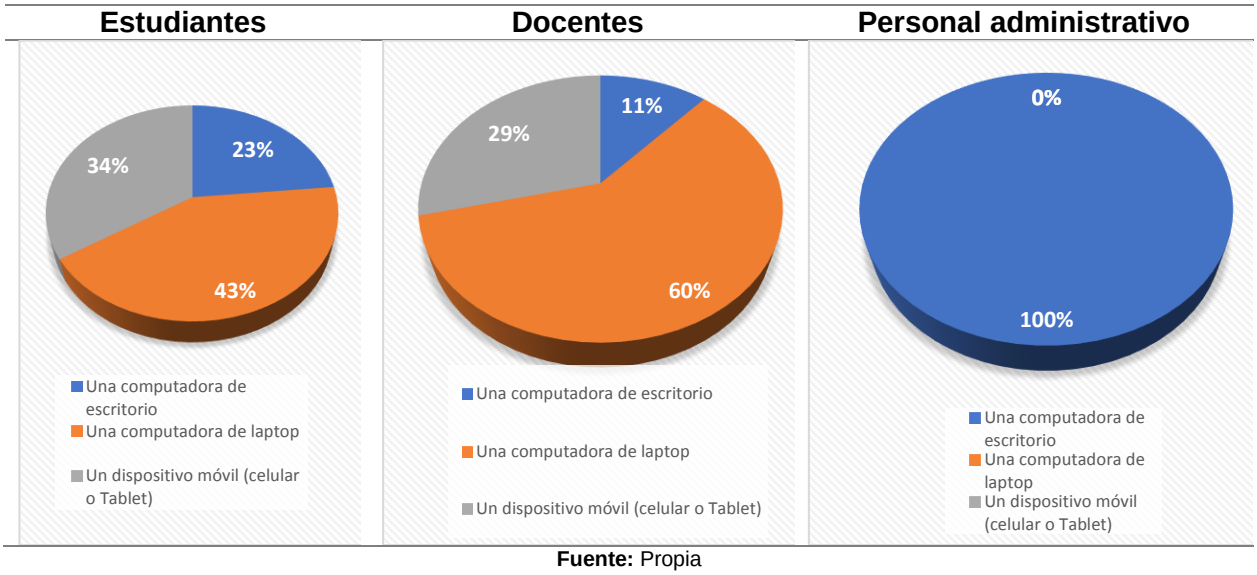
3) ¿Su acceso a esta parte del sistema académico lo hace mediante qué dispositivo?

Tabla 13. Tercera pregunta de encuesta

Dispositivo	Estudiantes	Docentes	Personal Administrativo
Una computadora de escritorio	134	6	17
Una laptop	243	31	0
Celular o Tablet	195	15	0

Fuente: Propia

Tabla 14. Tercera pregunta, tabulación de encuesta



Fuente: Propia

Análisis de resultados

En la tabla 13 y 14 se presenta los resultados obtenidos de la tercera pregunta realizada a estudiantes, docentes y personal administrativo. Es posible observar que la mayor parte de usuarios ingresa al sistema académico desde una laptop, distribuidos de la siguiente forma 43% estudiantes, 60% docentes. Otro dispositivo que usan los usuarios son las computadoras de escritorio, mismas que son empleadas para el ingreso al sistema de académico distribuidos de la siguiente forma: 23% estudiantes y 11% docentes. Existe otro dispositivo que emplean los usuarios, son los celulares y Tablet que según su ingreso al sistema académico se distribuyen en: 34% estudiantes y 29% docentes. De los resultados obtenidos es posible concluir que la mayor parte de usuarios usan laptops, celulares y tabletas inteligentes para ingresar al sistema académico.

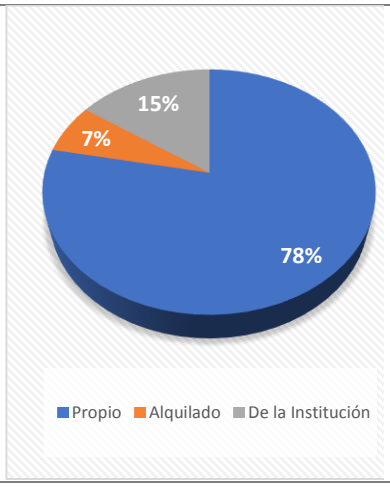
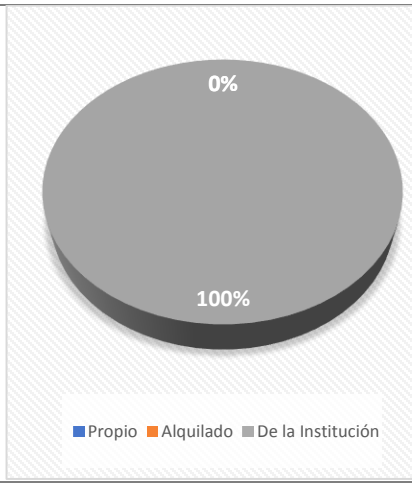
4) ¿El dispositivo que usa para el acceso al sistema académico es?

Tabla 15. Cuarta pregunta, encuesta

Dispositivo	Estudiantes	Docentes	Personal Administrativo
Propio	297	35	0
Alquilado	25	0	0
De la institución	58	0	17

Fuente: Propia

Tabla 16. Cuarta pregunta, tabulación de encuesta

Estudiantes	Docentes	Personal administrativo
		

Fuente: Propia

Análisis de resultados

En la tabla 15 y 16 se presenta los resultados obtenidos de la cuarta pregunta realizada a estudiantes, docentes y personal administrativo. Es posible observar que los dispositivos propios que son empleados para ingresar al sistema académico se distribuyen de la siguiente forma: 78% estudiantes, 100% docentes y 100% personal administrativo. Sin embargo, existe un 15% de estudiantes que emplean equipos de la UTN para ingresar al sistema académico, mientras que un 7% alquila un computador para el acceso al sistema académico. De los resultados obtenidos se concluye que la mayor parte de los usuarios del sistema académico emplean equipos propios para ingresar al mismo.

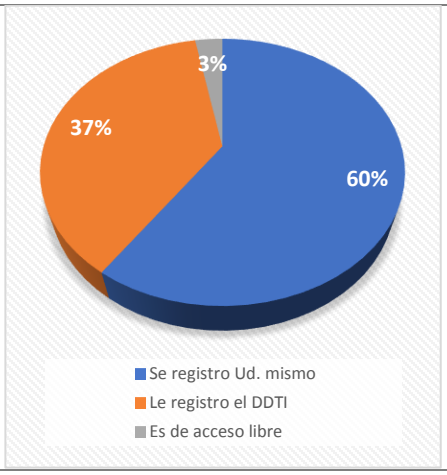
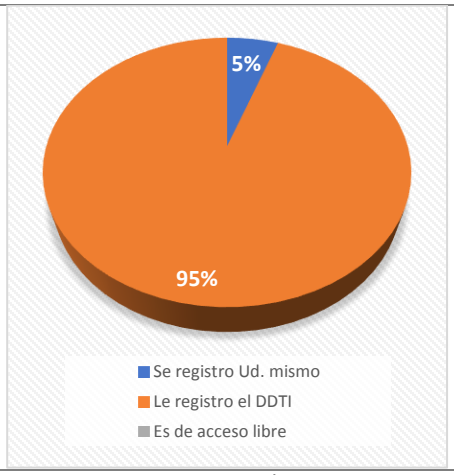
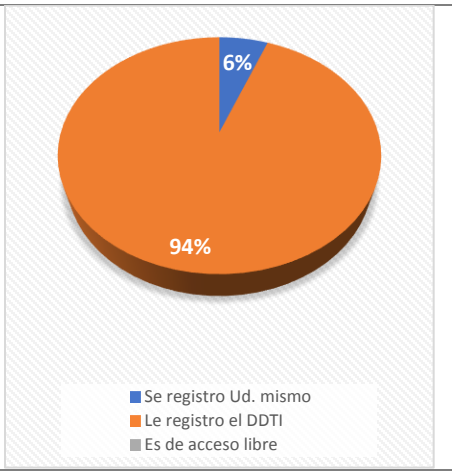
5) ¿Cómo hizo para poder ingresar a esta parte del sistema académico?

Tabla 17. Quinta pregunta, encuesta

	Estudiantes	Docentes	Personal Administrativo
Se registro usted mismo	143	2	1
Le registro el DDT	90	35	16
Es de acceso libre	57	0	0

Fuente: Propia

Tabla 18. Quinta pregunta, tabulación de encuesta

Estudiantes	Docentes	Personal administrativo
		

Fuente: Propia

Análisis de resultados

En la tabla 17 y 18 se presentan los resultados obtenidos de la quinta pregunta realizada a estudiantes, docentes y personal administrativo. Se observa para ingresar al sistema académico existe una parte de usuarios que fueron registrados por miembros del DDTI, distribuidos de la siguiente forma: 37% estudiantes, 95% docentes y 94% personal administrativo. Por otra parte, existe otro grupo de usuarios que afirman que se registraron ellos mismo en el sistema para tener acceso al sistema académico, distribuidos de la siguiente forma: 60% estudiantes, 5% docentes y 6% personal administrativo. Además, existe un pequeño grupo de estudiantes que afirman que el acceso al sistema académico es libre.

Se concluye que la mayor parte de usuarios fueron registrados por el DDTI para obtener el acceso al sistema académico, sin embargo, existe un gran parte de usuarios que se registraron por su cuenta para tener acceso al sistema.

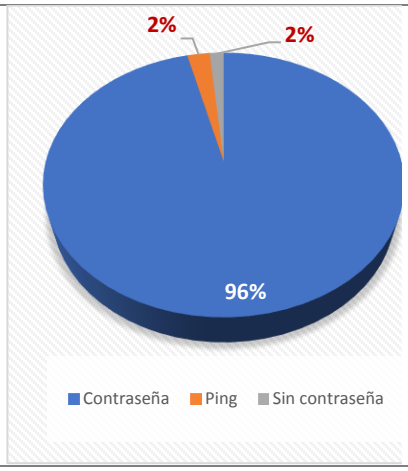
6) ¿Al portal que Ud. accede tiene un nivel de seguridad (contraseña o pin)?

Tabla 19. Sexta pregunta, encuesta

Tipo de seguridad	Estudiantes	Docentes	Personal Administrativo
Contraseña	324	35	17
Pin	8	0	0
Sin contraseña	5	0	0

Fuente: Propia

Tabla 20. Sexta pregunta, tabulación de encuesta

Estudiantes	Docentes	Personal administrativo
		

Fuente: Propia

Análisis de resultados

En la tabla 19 y 20 se presentan los resultados obtenidos de la sexta pregunta realizada a estudiantes, docentes y personal administrativo. La mayor parte de usuarios afirma que posee un pin o una contraseña para acceder al sistema académico, mismos que se distribuyen de la siguiente forma: 96% estudiantes, 100% docentes y 100% personal administrativo. Por otra parte, existe un 2% de estudiantes que afirman que no tienen ningún pin o contraseña para acceder al sistema académico. Se concluye que la mayor parte de usuarios poseen una contraseña o pin de seguridad para acceder al sistema académico.

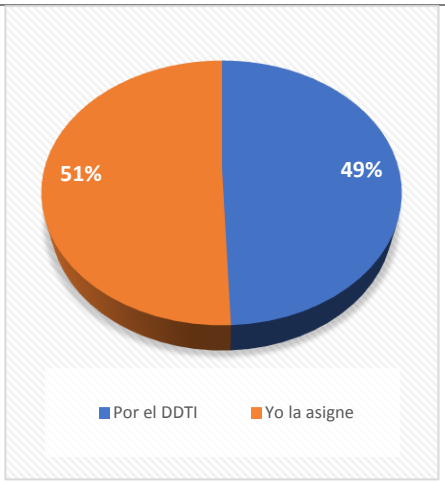
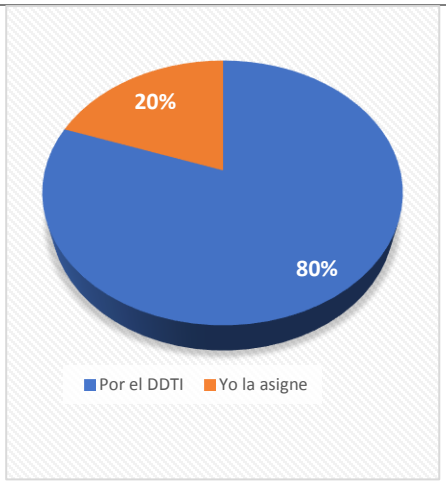
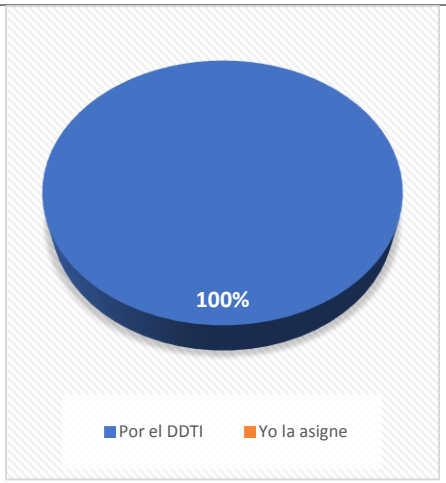
7) En el caso de tener contraseña o ping. ¿Cómo fue asignada?

Tabla 21. Séptima pregunta, encuesta

Asignada por	Estudiantes	Docentes	Personal Administrativo
Por el DDTI	113	33	17
Yo la asigne	116	8	0

Fuente: Propia

Tabla 22. Séptima pregunta, tabulación de encuesta

Estudiantes	Docentes	Personal administrativo
		

Fuente: Propia

Análisis de resultados

En la tabla 21 y 22 se presentan los resultados obtenidos de la séptima pregunta realizada a estudiantes, docentes y personal administrativo. De los resultados obtenidos existe una gran parte de los usuarios repartidos de la siguiente forma: 49% estudiantes, 80% docentes y 100% personal administrativo, que afirman que las claves o contraseñas fueron proporcionadas por el DDTI. Desde otra perspectiva se tiene que un 51% de estudiantes y un 20% de docentes afirman que las claves que poseen para ingresar al sistema académico las generaron ellos mismo. En conclusión, la mayor parte de claves que poseen los usuarios fueron asignadas por el DDTI.

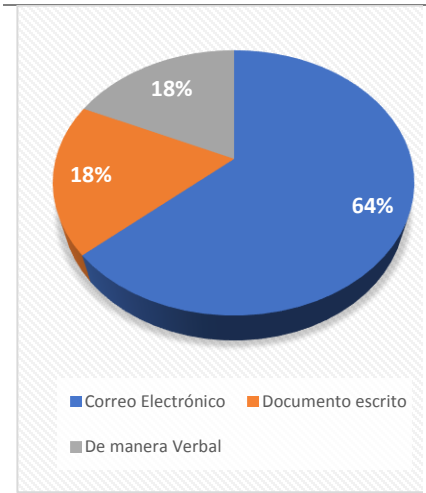
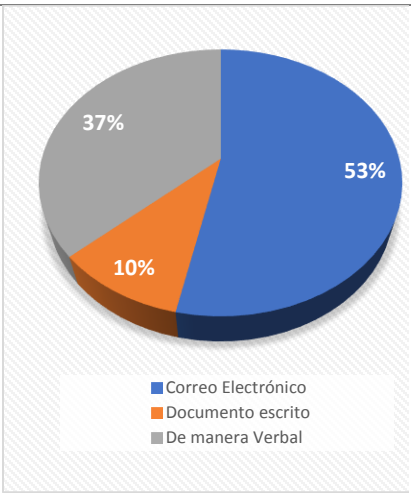
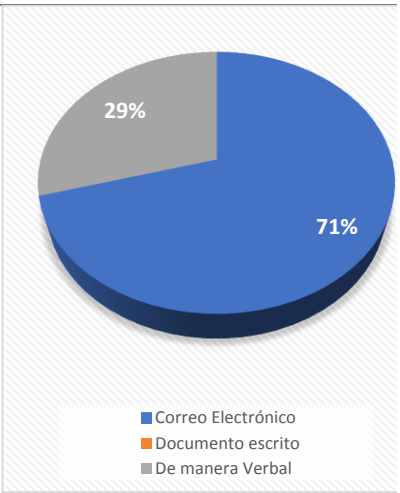
8) De ser por parte del DDTI. ¿Cómo le hizo llegar su contraseña o ping a Ud.?

Tabla 23. Octava pregunta, encuesta

La contraseña se entregó por	Estudiantes	Docentes	Personal Administrativo
Correo electrónico	193	16	12
Documento escrito	56	3	0
De forma verbal	55	11	5

Fuente: Propia

Tabla 24. Octava pregunta, tabulación de encuesta

ESTUDIANTES	DOCENTES	Personal administrativo
		

Fuente: Propia

Análisis de resultados

En la tabla 23 y 24 se presentan los resultados obtenidos de la octava pregunta realizada a estudiantes, docentes y personal administrativo. Existe un 64% de estudiantes, 53% de docentes y un 71% del personal administrativo, que afirman que la contraseña fue entregada por correo electrónico. Por otro lado, existe un 18% de estudiantes, 37% de docentes y un 29% del personal administrativo, afirman que se le informo la contraseña de manera verbal. Desde otra perspectiva se tiene un 18% de estudiantes y 10% de docentes que afirman que la contraseña les llego de forma escrita. En conclusión, la mayor parte de los usuarios del sistema académico recibieron la contraseña mediante correo electrónico.

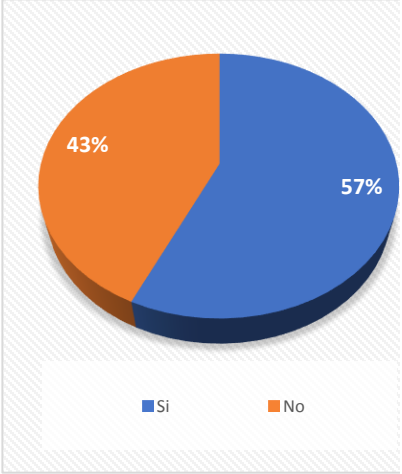
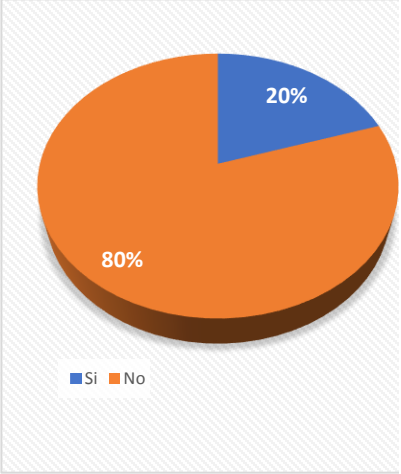
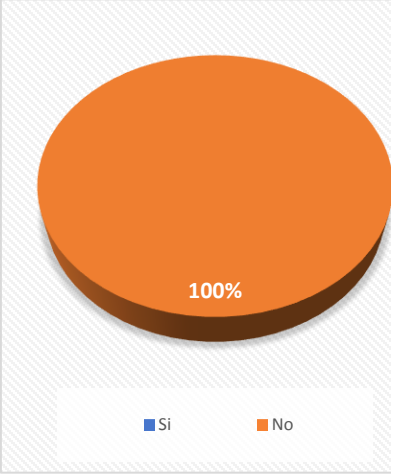
9) En caso de ser por asignación propia. ¿Al asignar la contraseña se le impusieron ciertos parámetros para ser aceptada?

Tabla 25. Novena pregunta, encuesta

Existe parámetros	Estudiantes	Docentes	Personal Administrativo
Si	145	1	0
No	110	4	1

Fuente: Propia

Tabla 26. Novena pregunta, tabulación de encuesta

ESTUDIANTES	DOCENTES	PERSONAL ADMINISTRATIVO
		

Fuente: Propia

Análisis de resultados

En la tabla 25 y 26 se presentan los resultados obtenidos de la novena pregunta realizada a estudiantes, docentes y personal administrativo. Existe un 57% de estudiantes y un 20% de docentes que afirman que en la creación de contraseñas propias les impusieron ciertos parámetros de seguridad para ser aceptada. Por otro lado, existe un 43% de estudiantes, 80% de docentes y el 100% del personal administrativo que afirman que durante la creación de contraseñas propias no tuvo que aceptar ningunos parámetros de seguridad para la creación de la contraseña. En conclusión, la mayor parte de usuarios crearon contraseñas sin ningún parámetro de seguridad.

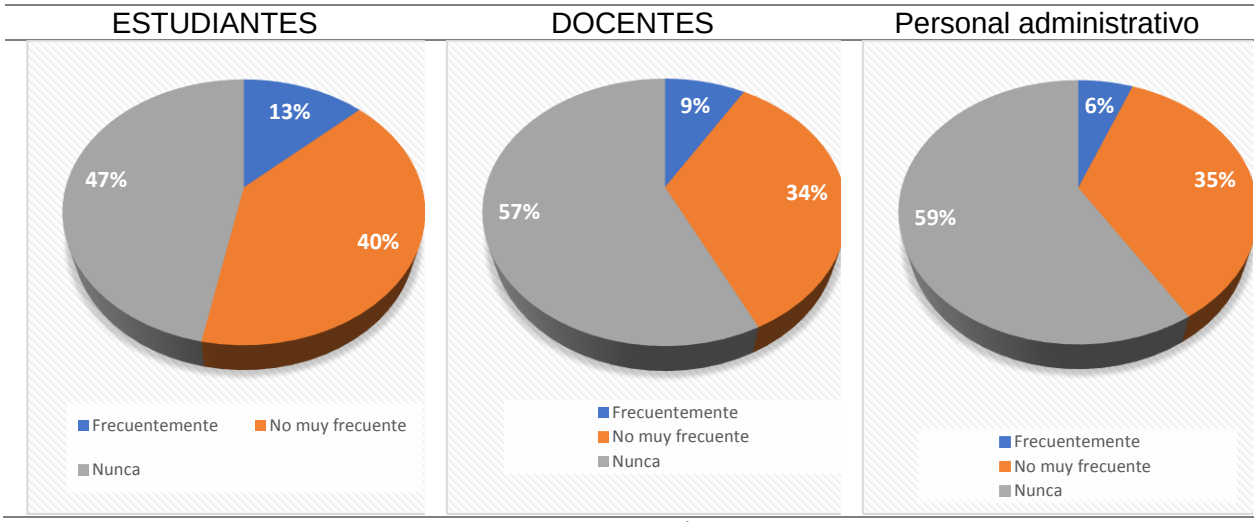
10) En los dos casos de asignación de contraseña. ¿Cada cuánto le asignan o le piden asignar una nueva contraseña?

Tabla 27. Decima pregunta, encuesta

Frecuencia de cambio de contraseña	Estudiantes	Docentes	Personal Administrativo
Frecuentemente	44	3	1
No muy frecuente	135	12	6
Nunca	158	20	10

Fuente: Propia

Tabla 28. Decima pregunta, tabulación de encuesta



Fuente: Propia

Análisis de resultados

En la tabla 27 y 28 se presentan los resultados obtenidos de la décima pregunta realizada a estudiantes, docentes y personal administrativo. Existe un 47% de estudiantes, 57% de docentes y un 59% del personal administrativo, que afirman el sistema nunca pide el cambio de contraseña. Por otro lado, existe un 40% de estudiantes, 34% de docentes y un 35% del personal administrativo, afirman el sistema les pide el cambio de contraseña no muy frecuentemente. Desde otra perspectiva se tiene un 13% de estudiantes, 9% de docentes y un 6% del personal administrativo que el sistema pide el cambio de contraseña muy frecuentemente. En conclusión, existe un porcentaje muy alto de usuarios a los que el sistema no pide un cambio de contraseña cada determinado tiempo, como medida de seguridad.

Análisis de la segunda encuesta (segunda herramienta)

Para el estudio de la gestión de la seguridad de la información, se recopilo información mediante una segunda encuesta formulada exclusivamente para el departamento de informática de la Universidad Técnica del Norte. Con el fin de conocer la privacidad y protección de datos según los parámetros de la norma ISO/IEC 27002:2017.

1) ¿Existen documento(s) de políticas de seguridad de S.I.?

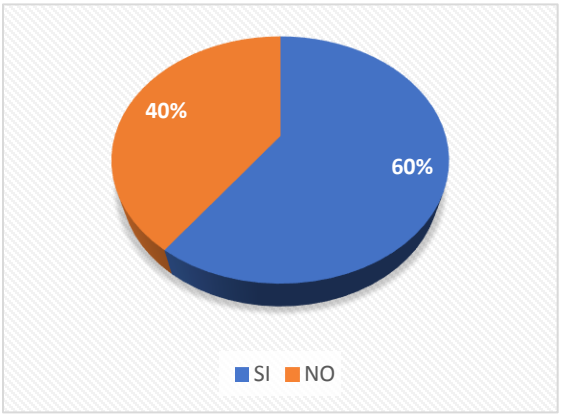


Figura 9: Pregunta 1, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 9 se presentan los resultados obtenidos de la primera pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 60% de miembros del DDTI que afirman que, si existen documentos de políticas de seguridad de la información, mientras que un 40% afirma que no existe documentos de políticas de seguridad de la información. En conclusión, es posible decir que si existe documentos de políticas para seguridad de la información.

2) ¿Existe normativa relativa a la seguridad de S.I.?

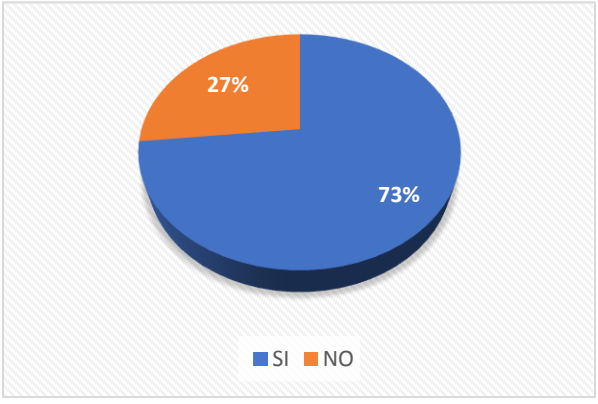


Figura 10: Pregunta 2, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 10 se presentan los resultados obtenidos de la segunda pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 73% de miembros del DDTI que afirman que, si existe una normativa relativa de seguridad de la información, mientras que un 40% afirma que no existe una normativa relativa de seguridad de la información. En conclusión, es posible decir que si existe una normativa relativa a la seguridad de la información.

3) ¿Existen procedimientos relativos a la seguridad de S.I.?

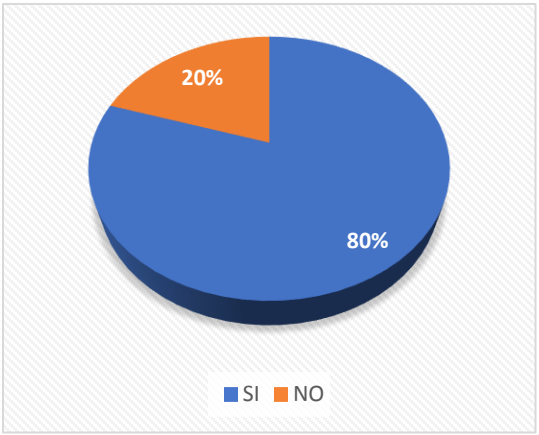


Figura 11: Pregunta 3, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 11 se presentan los resultados obtenidos de la tercera pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 80% de miembros del DDTI que afirman que, existen procedimientos para la seguridad de la información, mientras que un 20% afirma que no existe procedimientos relativos a la seguridad de la información. En conclusión, es posible decir que si existe procedimientos para la seguridad de la información.

4) **¿Existe un responsable de las políticas, normas y procedimientos?**

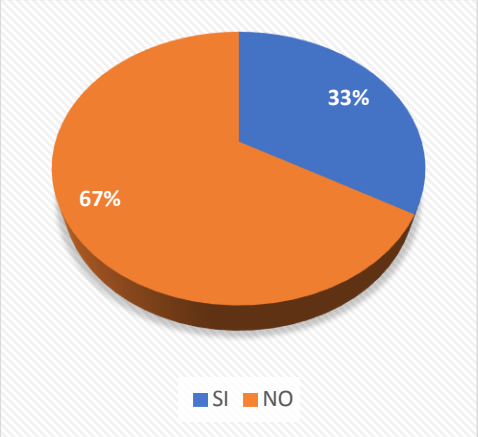


Figura 12: Pregunta 4, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 12 se presentan los resultados obtenidos de la cuarta pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 33% de miembros del DDTI que afirman que, existe una persona responsable de las políticas, normas y procedimientos para la seguridad de la información, mientras que un 67% afirma que no existe una persona encargada de las políticas, normas y procedimientos para la seguridad de la información. En conclusión, es posible decir que no existe una persona encargada de las políticas, normas y procedimientos para la seguridad de la información.

5) **¿Existen mecanismos para la comunicación a los usuarios de las normas?**

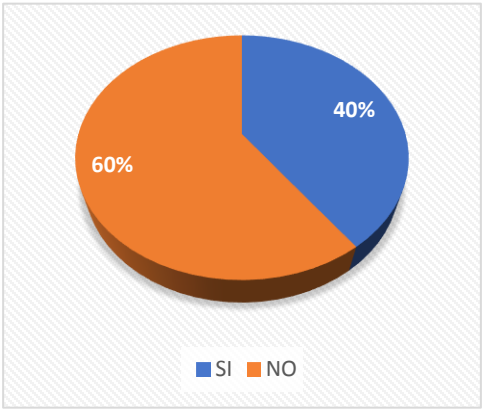


Figura 13: Pregunta 5, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 13 se presentan los resultados obtenidos de la quinta pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 40% de miembros del DDTI que afirman que, si existe una difusión de las normas referentes a la seguridad de la información, mientras que un 60% afirma que no existe una difusión de las normas referentes a la seguridad de la información. En conclusión, es posible decir que no existe una difusión adecuada de las normas referentes a la seguridad de la información.

6) ¿Existen controles regulares para verificar la efectividad de las políticas?

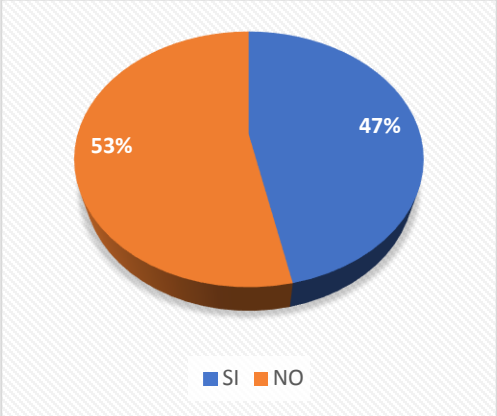


Figura 14: Pregunta 6, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 14 se presentan los resultados obtenidos de la sexta pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 47% de miembros del DDTI que afirman que, si existe controles que verifiquen la efectividad de políticas de seguridad de la información, mientras que un 53% afirma que no existe controles que verifiquen la efectividad de políticas de seguridad de la información. En conclusión, es posible decir que no existe controles que permitan comprobar la efectividad de políticas de seguridad de la información existentes en el DDTI.

7) **¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?**

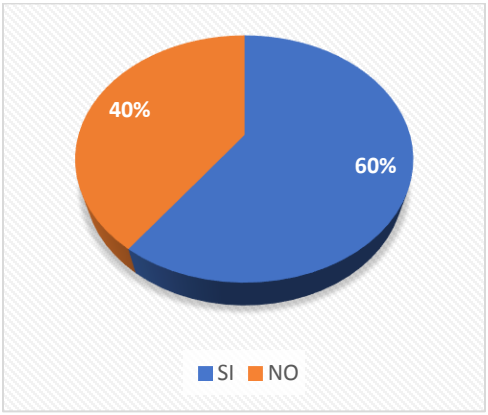


Figura 15: Pregunta 7, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 15 se presentan los resultados obtenidos de la séptima pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 60% de miembros del DDTI que afirman que, si existe roles y responsabilidad definidos para las personas implicadas en la seguridad de la información, mientras que un 40% afirma que no existe roles y responsabilidad definidos para las personas implicadas en la seguridad de la información. En conclusión, es posible decir que si existe roles y responsabilidad definidos para los miembros del DDTI implicadas en la seguridad de la información.

8) **¿Existe un responsable encargado de evaluar la adquisición y cambios de S.I.?**

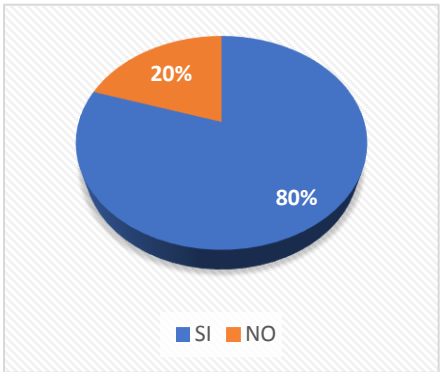


Figura 16: Pregunta 8, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 16 se presentan los resultados obtenidos de la octava pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 80% de miembros del DDTI que afirman que, si existe un encargado de evaluar las adquisiciones y cambios de la seguridad de la información, mientras que un 20% afirma que no existe un encargado de evaluar las adquisiciones y cambios de la seguridad de la información. En conclusión, es posible decir que si existe un encargado de evaluar las adquisiciones y cambios de la seguridad de la información en él DDTI.

9) **¿Existen condiciones contractuales de seguridad con terceros y Outsourcing?**

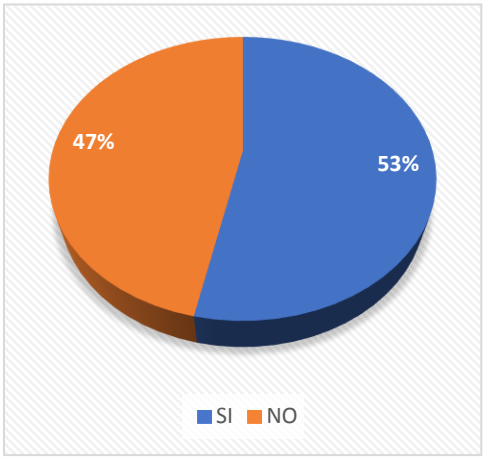


Figura 17: Pregunta 9, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 17 se presentan los resultados obtenidos de la novena pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 53% de miembros del DDTI que afirman que, si existe condiciones contractuales de seguridad con terceros y outsourcing, mientras que un 47% afirma que no existe condiciones contractuales de seguridad con terceros y outsourcing. En conclusión, es posible decir que si existe condiciones contractuales de seguridad con terceros y outsourcing para la seguridad de la información.

10) ¿Existen criterios de seguridad en el manejo de terceras partes?

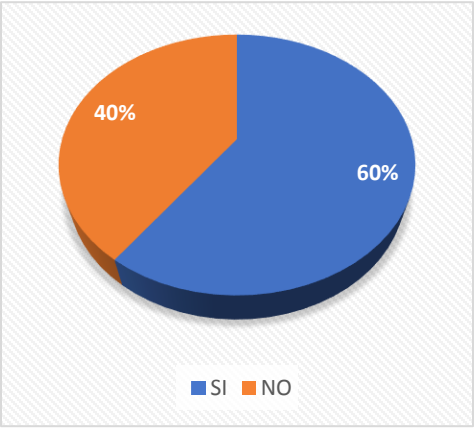


Figura 18: Pregunta 10, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 18 se presentan los resultados obtenidos de la décima pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 60% de miembros del DDTI que afirman que, si existe criterios de seguridad para el manejo del sistema por parte de terceros, mientras que un 40% afirma que no existe criterios de seguridad para el manejo del sistema por parte de terceros. En conclusión, es posible decir que si existe criterios de seguridad para el manejo del sistema por parte de terceros para salvaguardar la seguridad de la información.

11) ¿Existen programas de formación en seguridad para los empleados, clientes y terceros?

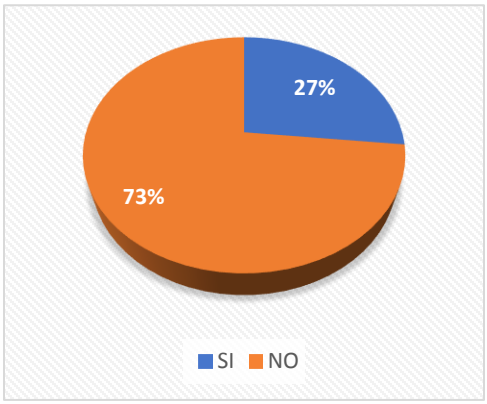


Figura 19: Pregunta 11, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 19 se presentan los resultados obtenidos de la décima primera pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 27% de miembros del DDTI que afirman que, existen programas de formación de seguridad de la información para los empleados de la UTN y terceros, mientras que un 73% afirma que no existen programas de formación de seguridad de la información para los empleados de la UTN y terceros. En conclusión, es posible decir que no existen programas de formación de seguridad de la información para los empleados de la UTN y terceros.

12) ¿Existe un acuerdo de confidencialidad de la información a la que se accede?

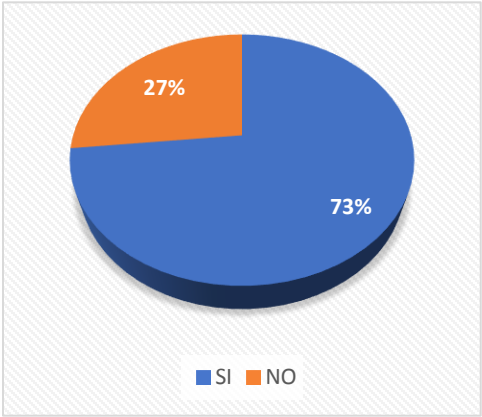


Figura 20: Pregunta 12, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 20 se presentan los resultados obtenidos de la décima segunda pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 73% de miembros del DDTI que afirman que, existe un acuerdo de confidencialidad de la información con los miembros que manejan la información del DDTI, mientras que un 27% afirma que no existe un acuerdo de confidencialidad de la información con los miembros que manejan la información del DDTI. En conclusión, es posible decir que existe un acuerdo de confidencialidad de la información con los miembros que manejan la información del DDTI.

13) ¿Se revisa la organización de la seguridad periódicamente por una empresa externa?

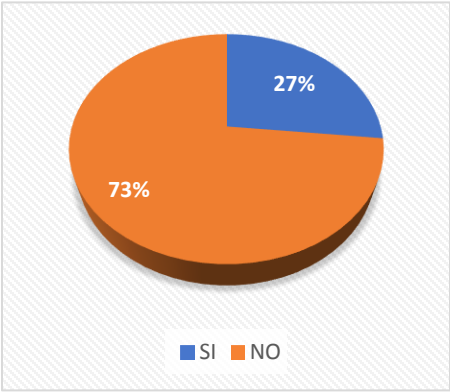


Figura 21: Pregunta 13, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 21 se presentan los resultados obtenidos de la décima tercera pregunta de la segunda encuesta realizada a los miembros del DDTI. Existe un 27% de miembros del DDTI que afirman que, la organización de seguridad de la UTN es revisada periódicamente por una empresa externa, mientras que un 73% afirma que no existe la organización de seguridad de la UTN y no es revisada periódicamente por una empresa externa. En conclusión, es posible decir que no existe la organización de seguridad de la UTN y que no es revisada periódicamente por una empresa externa.

14) ¿Existe un inventario de activos actualizado?

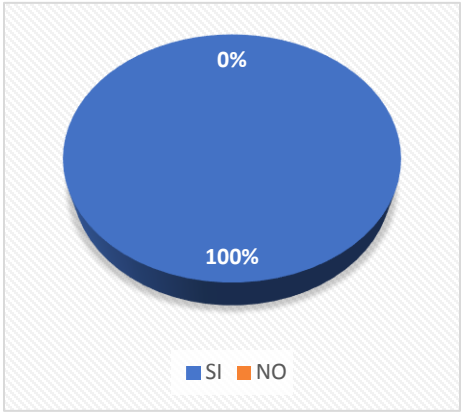


Figura 22: Pregunta 14, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 22 se presentan los resultados obtenidos de la décima cuarta pregunta de la segunda encuesta realizada a los miembros del DDTI. Todos los miembros del DDTI están de acuerdo en que existe un inventario de activos actualizado.

15) ¿El Inventario contiene activos de datos, software, equipos y servicios?

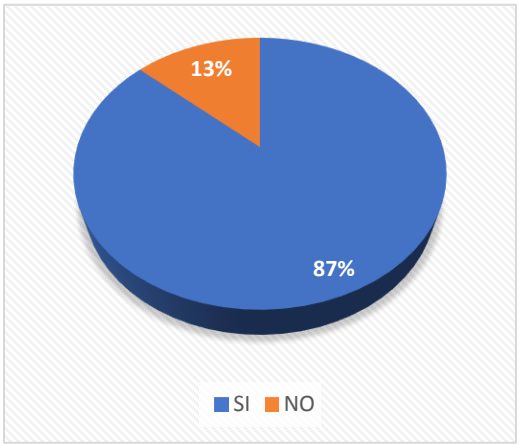


Figura 23: Pregunta 15, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 23 se presentan los resultados obtenidos de la décima quinta pregunta de la segunda encuesta realizada a los miembros del DDTI. El 87% de los miembros del DDTI afirman que el inventario actualizado contiene activos de datos, software, equipos y servicios, mientras que el 13% afirma que existen otro tipo de activos a los mencionados. En conclusión, se puede decir que en el inventario actualizado que posee el DDTI no incluye todos los activos que posee la red de datos de la UTN.

16) ¿Se dispone de una clasificación de la información según la criticidad de esta?

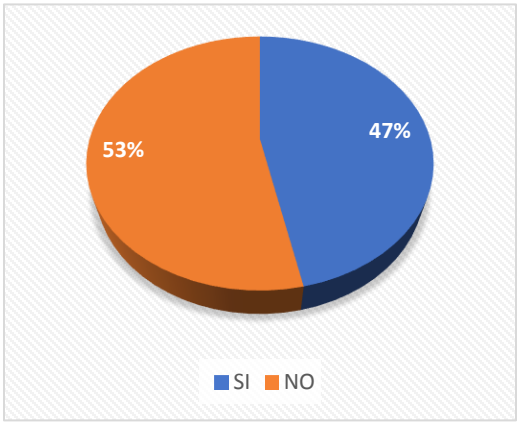


Figura 24: Pregunta 16, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 24 se presentan los resultados obtenidos de la décima sexta pregunta de la segunda encuesta realizada a los miembros del DDTI. El 47% de los miembros del DDTI afirman que existe una clasificación de la información según la criticidad, mientras que el 53% afirma que no existe una clasificación de la información según la criticidad. En conclusión, no existe una clasificación de la información en cuanto a criticidad.

17) ¿Existe un responsable de los activos?

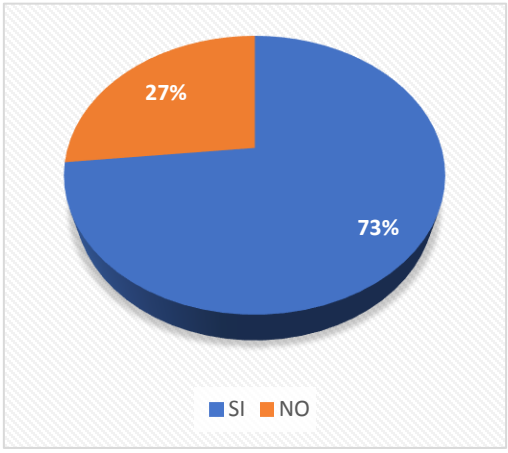


Figura 25: Pregunta 17, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 25 se presentan los resultados obtenidos de la décima séptima pregunta de la segunda encuesta realizada a los miembros del DDTI. El 73% de los miembros del DDTI afirman que existe una persona del DDTI responsable de los activos de la red de la UTN, mientras que el 27% afirma que no existe una persona del DDTI responsable de los activos de la red de la UTN. En conclusión, existe un miembro del DDTI que está a cargo de todos los activos de la UTN.

18) ¿Existen procedimientos para clasificar la información?

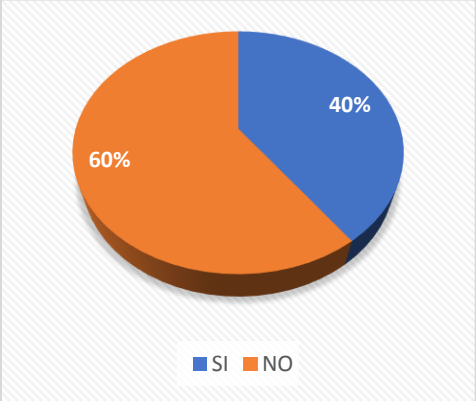


Figura 26: Pregunta 18, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 26 se presentan los resultados obtenidos de la décima octava pregunta de la segunda encuesta realizada a los miembros del DDTI. El 40% de los miembros del DDTI afirman que existe procedimientos para clasificar la información que maneja el sistema académico, mientras que el 60% afirma que no existe procedimientos para clasificar la información que maneja el sistema académico. En conclusión, no existe los procedimientos adecuados para la clasificación de la información del sistema académico.

19) ¿Existen procedimientos de etiquetado de la información?

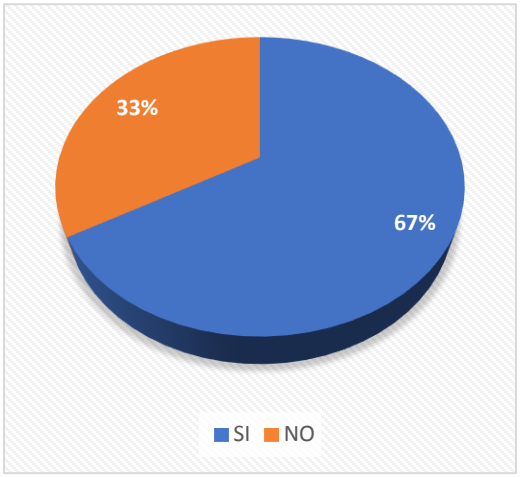


Figura 27: Pregunta 19, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 27 se presentan los resultados obtenidos de la décima novena pregunta de la segunda encuesta realizada a los miembros del DDTI. El 67% de los miembros del DDTI afirman que existe procedimientos para el etiquetado de la información tanto física como digital, mientras que el 33% afirma que no existe procedimientos para el etiquetado de la información tanto física como digital. En conclusión, no se evidencia ningún tipo de procedimiento para el etiquetado de la información del sistema académico.

20) ¿Se tienen definidas responsabilidades y roles de seguridad?

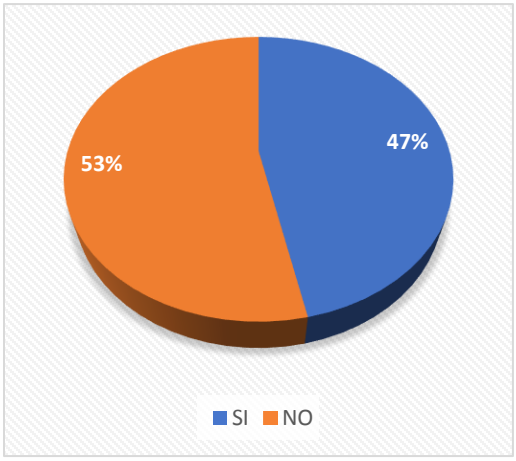


Figura 28: Pregunta 20, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 28 se presentan los resultados obtenidos de la pregunta veinte de la segunda encuesta realizada a los miembros del DDTI. El 47% de los miembros del DDTI afirman que el DDTI tiene responsabilidades y roles de seguridad, mientras que el 53% afirma que no existe responsabilidades y roles de seguridad. En conclusión, no se evidencia ningún tipo de responsabilidades designadas correspondientes a roles de seguridad en el DDTI.

21) ¿Se tiene en cuenta la seguridad en la selección y baja del personal?

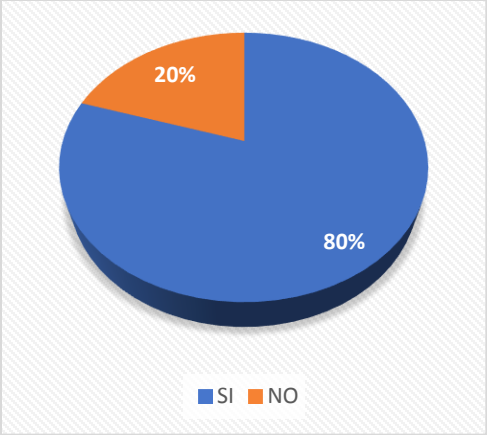


Figura 29: Pregunta 21, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 29 se presentan los resultados obtenidos de la pregunta veinte y uno de la segunda encuesta realizada a los miembros del DDTI. El 80% de los miembros del DDTI afirman que tanto para la elección de una nueva persona para el DDTI como para el despido se tiene medidas de seguridad para salvaguardar la información interna de la UTN, mientras que el 20% afirma que tanto para la elección de una nueva persona para el DDTI como para el despido no se tiene medidas de seguridad para salvaguardar la información interna de la UTN. En conclusión, se evidencia que existen medida para el personal que entra y sale de la UTN.

22) ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?

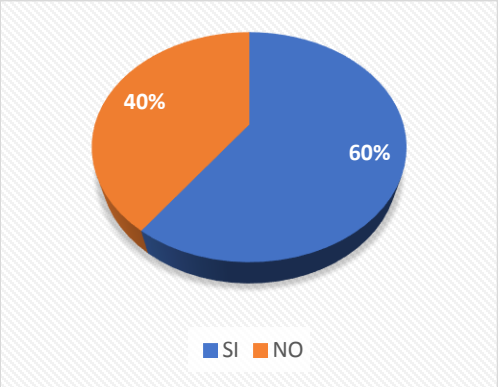


Figura 30: Pregunta 22, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 30 se presentan los resultados obtenidos de la pregunta veinte y dos de la segunda encuesta realizada a los miembros del DDTI. El 60% de los miembros del DDTI afirman que existen condiciones de confidencialidad y responsabilidades en los contratos existente en el DDTI, mientras que el 20% afirma que no existen condiciones de confidencialidad y responsabilidades en los contratos existente en el DDTI. En conclusión, se evidencia que en los contratos del DDTI se incluyen condiciones de confidencialidad y responsabilidades.

23) ¿Se imparte la formación adecuada de seguridad y tratamiento de activos?

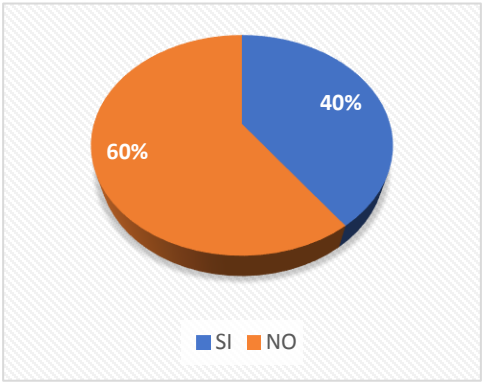


Figura 31: Pregunta 23, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 31 se presentan los resultados obtenidos de la pregunta veinte y tres de la segunda encuesta realizada a los miembros del DDTI. El 40% de los miembros del DDTI afirman que se capacita acerca de la seguridad y tratamiento de activos, mientras que el 60% afirma que no se capacita acerca de la seguridad y tratamiento de activos. En conclusión, se evidencia que el personal del DDTI no recibe la formación adecuada de seguridad de la información y tratamiento de activos.

24) ¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?

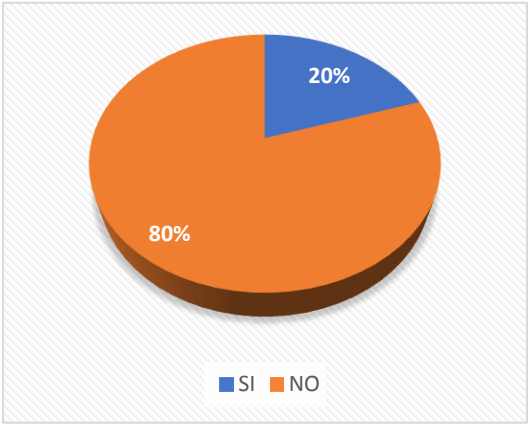


Figura 32: Pregunta 24, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 32 se presentan los resultados obtenidos de la pregunta veinte y cuatro de la segunda encuesta realizada a los miembros del DDTI. El 20% de los miembros del DDTI afirman que existe un canal y procedimientos claros para seguir en caso de un incidente de seguridad, mientras que el 80% afirma que no existe un canal y procedimientos claros para seguir en caso de un incidente de seguridad. En conclusión, se evidencia que en el caso de un incidente de seguridad no existe procedimientos establecidos para actuar frente al inconveniente.

25) ¿Se recogen los datos de los incidentes de forma detallada?

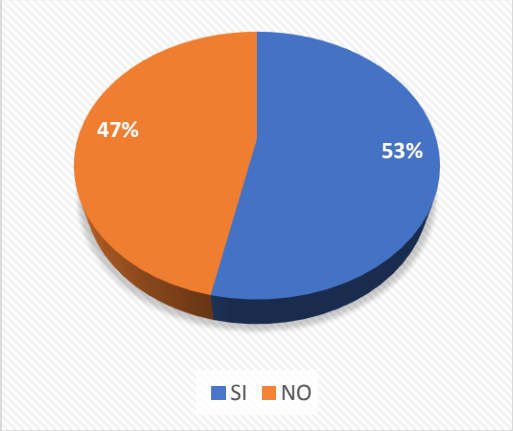


Figura 33: Pregunta 25, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 33 se presentan los resultados obtenidos de la pregunta veinte y cinco de la segunda encuesta realizada a los miembros del DDTI. El 53% de los miembros del DDTI afirman que se recolecta los datos de los incidentes producidos en el sistema académico de forma detallada, mientras que el 47% afirma que no se recolecta los datos de los incidentes producidos en el sistema académico de forma detallada. En conclusión, se evidencia que los datos de forma detallada de los incidentes producidos en el sistema académico.

26) ¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?

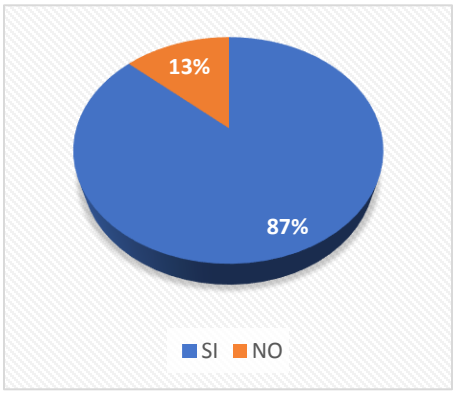


Figura 34: Pregunta 26, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 34 se presentan los resultados obtenidos de la pregunta veinte y seis de la segunda encuesta realizada a los miembros del DDTI. El 87% de los miembros del DDTI afirman que los usuarios suelen informar acerca de las vulnerabilidades observadas y sospechadas, mientras que el 13% afirma que los usuarios no suelen informar acerca de las vulnerabilidades observadas y sospechadas. En conclusión, se evidencia que los usuarios a menudo informan de las vulnerabilidades encontradas y potenciales.

27) ¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?

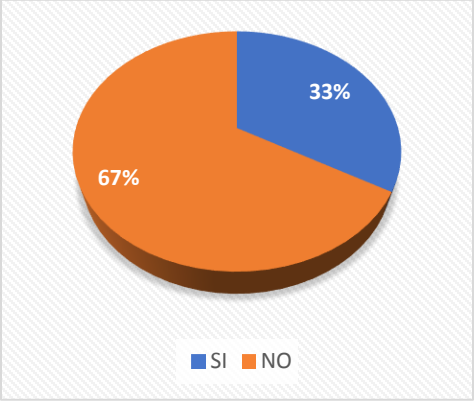


Figura 35: Pregunta 27, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 35 se presentan los resultados obtenidos de la pregunta veinte y siete de la segunda encuesta realizada a los miembros del DDTI. El 33% de los miembros del DDTI afirman que se informa a los usuarios que no deben probar las vulnerabilidades del sistema académico, mientras que el 67% afirma que no se informa a los usuarios que no deben probar las vulnerabilidades del sistema académico. En conclusión, se evidencia que no se informa sobre la prueba de vulnerabilidades por parte de los usuarios.

28) ¿Existe un proceso disciplinario de la seguridad de la información?

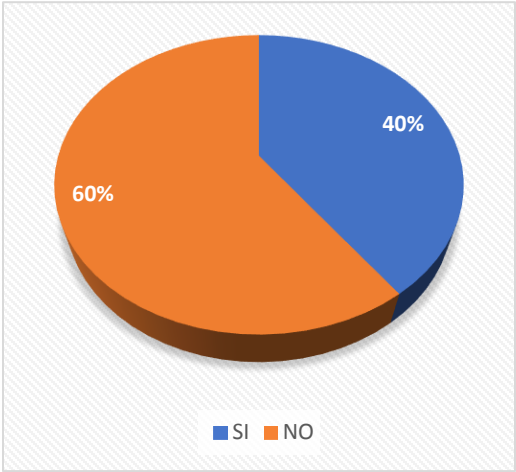


Figura 36: Pregunta 28, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 36 se presentan los resultados obtenidos de la pregunta veinte y ocho de la segunda encuesta realizada a los miembros del DDTI. El 40% de los miembros del DDTI afirman que existe un proceso disciplinario de seguridad de la información, mientras que el 60% afirma que no existe un proceso disciplinario de seguridad de la información. En conclusión, se evidencia que el DDTI no posee un proceso disciplinario de seguridad de la información.

29) ¿Existe perímetro de seguridad física (una pared, puerta con llave)?

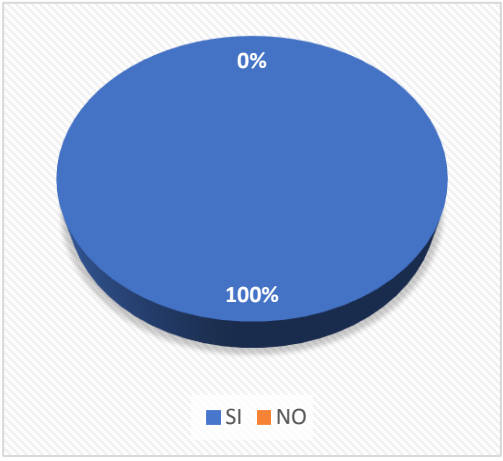


Figura 37: Pregunta 29, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 37 se presentan los resultados obtenidos de la pregunta veinte y nueve de la segunda encuesta realizada a los miembros del DDTI. Todos los usuarios afirmaron que existe un perímetro de seguridad física que resguarde los dispositivos físicos que almacenan la información.

30) ¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?

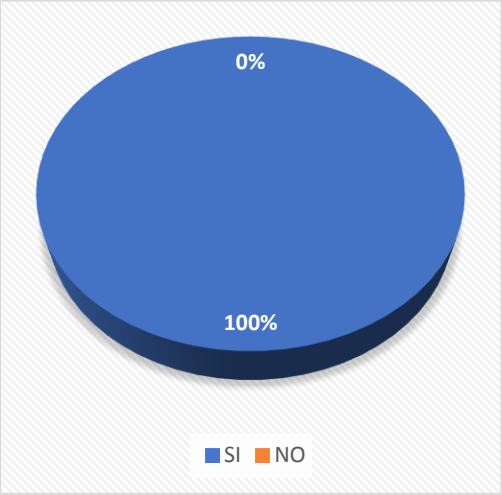


Figura 38: Pregunta 30, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 38 se presentan los resultados obtenidos de la pregunta treinta de la segunda encuesta realizada a los miembros del DDTI. Todos los usuarios afirmaron que existen controles de entrada que protege el acceso del personal no autorizado hacia al área del DDTI.

31) ¿En las áreas seguras existen controles adicionales al personal propio y ajeno?

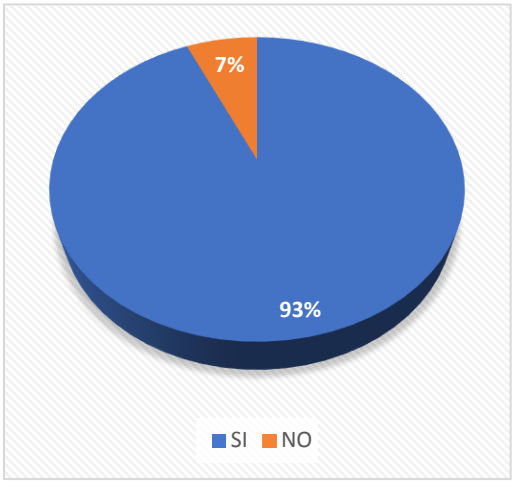


Figura 39: Pregunta 31, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 39 se presentan los resultados obtenidos de la pregunta treinta y uno de la segunda encuesta realizada a los miembros del DDTI. El 93% de los miembros del DDTI afirman que en las áreas seguras existen controles adicionales para el personal propio y ajeno al DDTI, mientras que el 7% afirma que en las áreas seguras no existen controles adicionales para el personal propio y ajeno al DDTI. En conclusión, se evidencia que existe controles adicionales para el personal propio y ajeno en las áreas seguras.

32) ¿Las áreas de carga y expedición están aisladas de las áreas de S.I.?

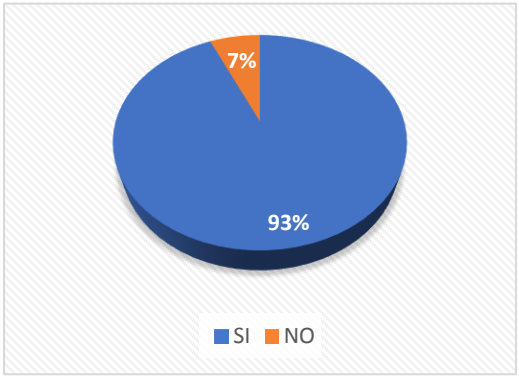


Figura 40: Pregunta 32, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 40 se presentan los resultados obtenidos de la pregunta treinta y dos de la segunda encuesta realizada a los miembros del DDTI. El 93% de los miembros del DDTI afirman que las áreas de carga y expedición están aisladas del área del sistema de información, mientras que el 7% afirma que las áreas de carga y expedición no están aisladas del área del sistema de información. En conclusión, se evidencia que el área del sistema de información se encuentra aislado de las áreas de carga y expedición.

33) ¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?

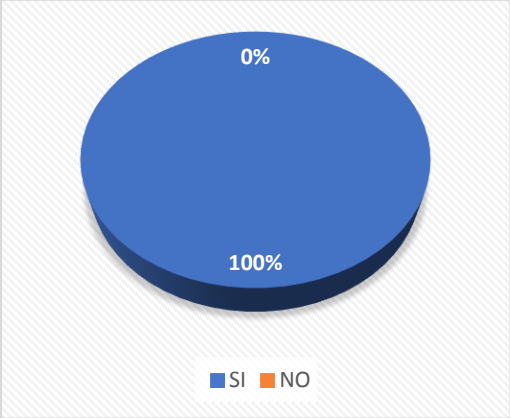


Figura 41: Pregunta 33, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 41 se presentan los resultados obtenidos de la pregunta treinta y tres de la segunda encuesta realizada a los miembros del DDTI. Todos los miembros del DDTI afirmaron que la ubicación de los servidores de información se encuentra ubicados estratégicamente para evitar accesos innecesarios por parte de externos.

34) ¿Existe seguridad en el cableado general del DataCenter, frente a daños e intercepciones?

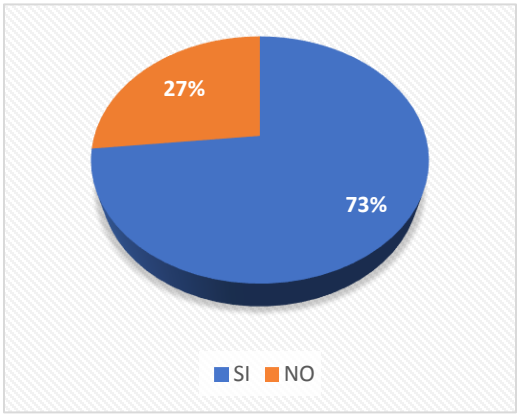


Figura 42: Pregunta 34, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 42 se presentan los resultados obtenidos de la pregunta treinta y cuatro de la segunda encuesta realizada a los miembros del DDTI. El 73% de los miembros del DDTI afirman que existe seguridad en el cableado del DataCenter frente a daños e intercepciones, mientras que el 27% afirma que no existe seguridad en el cableado del DataCenter frente a daños e intercepciones. En conclusión, se evidencia que el cableado de la data center se encuentra seguro frente a daños e intercepciones.

35) ¿Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente?

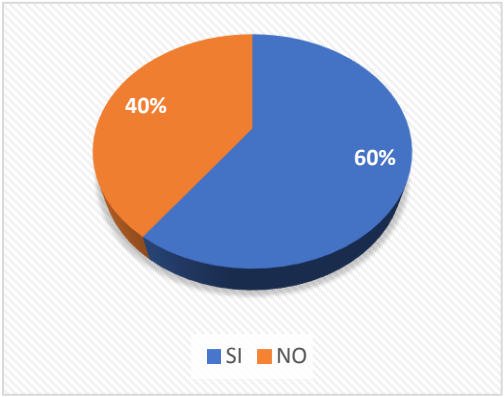


Figura 43: Pregunta 35, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 43 se presentan los resultados obtenidos de la pregunta treinta y cinco de la segunda encuesta realizada a los miembros del DDTI. El 60% de los miembros del DDTI afirman que existe medidas de seguridad para equipos retirados y ubicados en el exterior al DDTI, mientras que el 40% afirma que no existe medidas de seguridad para equipos retirados y ubicados en el exterior al DDTI. En conclusión, se evidencia que el DDTI posee medidas de seguridad para equipos retirados y ubicados en el exterior.

36) ¿Todos los procedimientos operativos identificados en la política de seguridad están documentados?

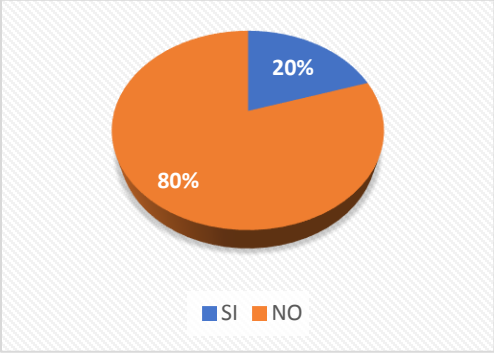


Figura 44: Pregunta 36, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 44 se presentan los resultados obtenidos de la pregunta treinta y seis de la segunda encuesta realizada a los miembros del DDTI. El 20% de los miembros del DDTI afirman que los procedimientos identificados en la seguridad se encuentran documentados, mientras que el 80% afirma que los procedimientos identificados en la seguridad no se encuentran documentados. En conclusión, se evidencia que los procedimientos identificados en la política de seguridad de la información del sistema académico no se encuentran documentados.

37) ¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?

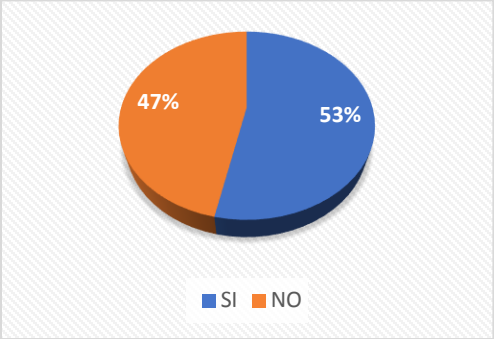


Figura 45: Pregunta 37, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 45 se presentan los resultados obtenidos de la pregunta treinta y ocho de la segunda encuesta realizada a los miembros del DDTI. El 53% de los miembros del DDTI afirman que existe establecidas responsabilidades para asegurar la respuesta rápida, ordenada y efectiva frente a un incidente de seguridad, mientras que el 47% afirma que no existe establecidas responsabilidades para asegurar la respuesta rápida, ordenada y efectiva frente a un incidente de seguridad. En conclusión, se evidencia que existe establecidas responsabilidades para asegurar la respuesta rápida, ordenada y efectiva frente a un incidente de seguridad en el sistema académico.

38) ¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?

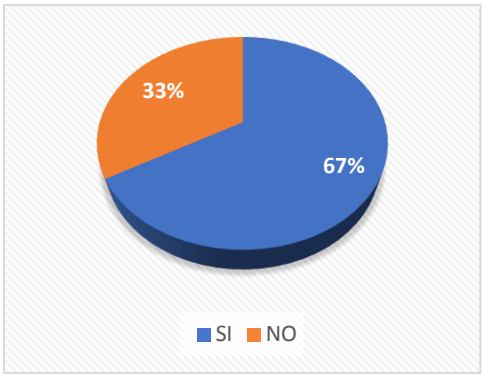


Figura 46: Pregunta 38, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 46 se presentan los resultados obtenidos de la pregunta treinta y nueve de la segunda encuesta realizada a los miembros del DDTI. El 67% de los miembros del DDTI afirman que existe un método para reducir el mal accidental e intencional de los sistemas de la UTN, mientras que el 33% afirma que no existe un método para reducir el mal accidental e intencional de los sistemas de la UTN. En conclusión, se evidencia que existe un método específico para reducir el mal uso accidental y deliberado del sistema académico.

39) ¿Existe una separación de los entornos de desarrollo y producción?

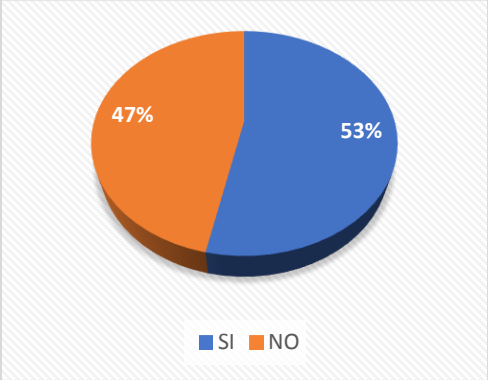


Figura 47: Pregunta 39, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 47 se presentan los resultados obtenidos de la pregunta cuarenta de la segunda encuesta realizada a los miembros del DDTI. El 53% de los miembros del DDTI afirman que existe separación entre entornos de desarrollo y producción, mientras que el 47% afirma que no existe separación entre entornos de desarrollo y producción. En conclusión, se evidencia que existe una separación en el entorno de desarrollo y producción del DDTI.

40) ¿Existen contratistas externos para la gestión de los Sistemas de información?

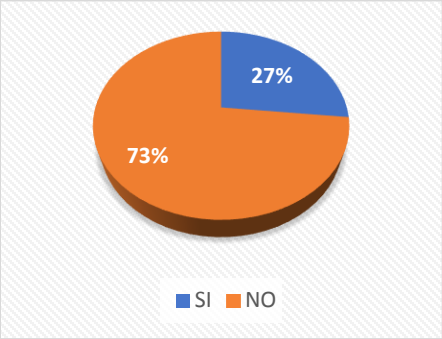


Figura 48: Pregunta 40, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 48 se presentan los resultados obtenidos de la pregunta cuarenta y uno de la segunda encuesta realizada a los miembros del DDTI. El 27% de los miembros del DDTI afirman que existe contratistas externos para la gestión de los sistemas de información, mientras que el 73% afirma que no existe contratistas externos para la gestión de los sistemas de información. En conclusión, se evidencia que no existe relación con contratistas externos para la gestión de los sistemas de información.

41) ¿Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento?

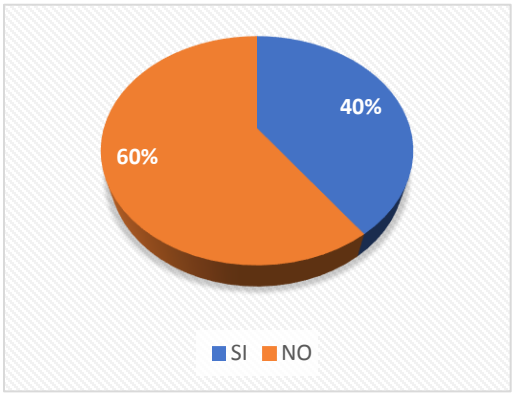


Figura 49: Pregunta 41, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 49 se presentan los resultados obtenidos de la pregunta cuarenta y dos de la segunda encuesta realizada a los miembros del DDTI. El 40% de los miembros del DDTI afirman que existe un plan de capacidad que asegura la adecuada capacidad de proceso y almacenamiento, mientras que el 60% afirma que no existe un plan de capacidad que asegura la adecuada capacidad de proceso y almacenamiento. En conclusión, se evidencia que no existe un plan de capacidad que asegura la adecuada capacidad de proceso y almacenamiento para el sistema académico.

42) ¿Existen Controles contra software maligno?

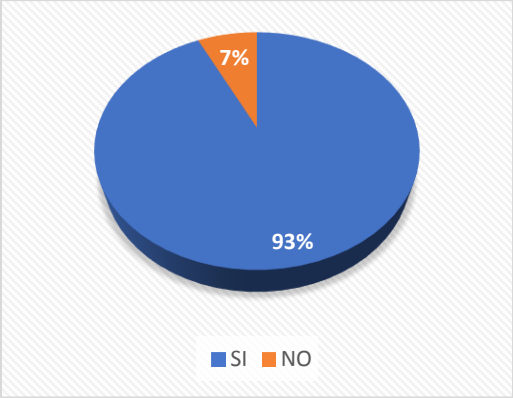


Figura 50: Pregunta 42, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 50 se presentan los resultados obtenidos de la pregunta cuarenta y tres de la segunda encuesta realizada a los miembros del DDTI. El 93% de los miembros del DDTI afirman que existe controles contra software maligno, mientras que el 7% afirma que no existe controles contra software maligno. En conclusión, se evidencia que existe controles contra software maligno en el sistema académico.

43) ¿Realizan copias de backup de la información?

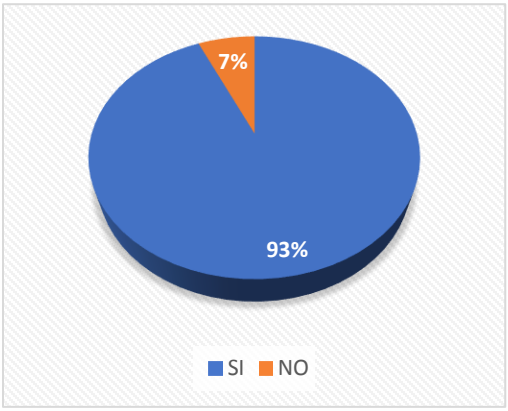


Figura 51: Pregunta 43, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 51 se presentan los resultados obtenidos de la pregunta cuarenta y cuatro de la segunda encuesta realizada a los miembros del DDTI. El 93% de los miembros del DDTI afirman que se si se realizan copias de seguridad de la información del sistema académico, mientras que el 7% afirma que no se realizan copias de seguridad de la información del sistema académico. En conclusión, se evidencia que se realizan copias de seguridad de la información del sistema académico.

44) ¿Existen logs (registro de actividad de un sistema) para las actividades realizadas por los operadores y administradores?

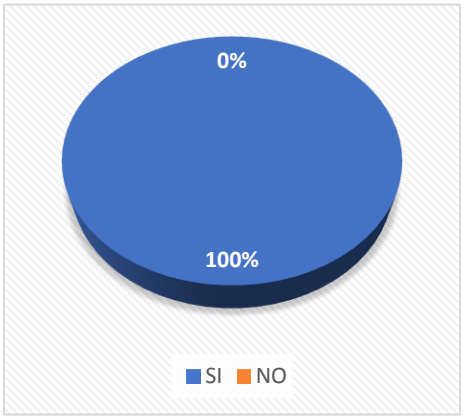


Figura 52: Pregunta 44, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 52 se presentan los resultados obtenidos de la pregunta cuarenta y cinco de la segunda encuesta realizada a los miembros del DDTI. Todos los miembros del DDTI afirman que existe logs para el registro de actividad del sistema académico, tanto para operadores como para administradores.

45) ¿Existe algún control en las redes?

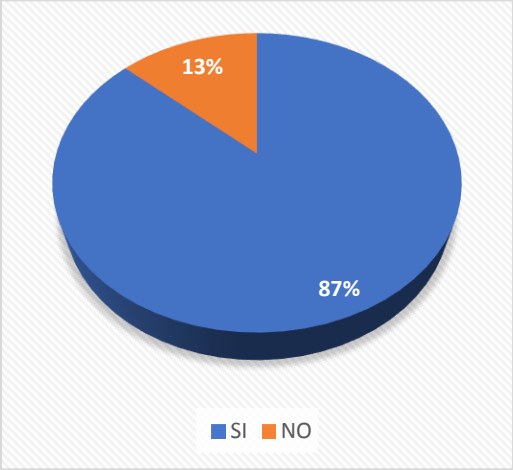


Figura 53: Pregunta 45, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 52 se presentan los resultados obtenidos de la pregunta cuarenta y seis de la segunda encuesta realizada a los miembros del DDTI. El 87% de miembros del DDTI afirman que existe control de las redes de la UTN, mientras que el 13% afirma que no existe ningún control de las redes de la UTN. En conclusión, es posible afirman que existe el control de las redes de comunicación del sistema académico.

46) ¿Hay establecidos controles para realizar la gestión de los medios informáticos? (Cintas, discos, removibles, informes impresos)?

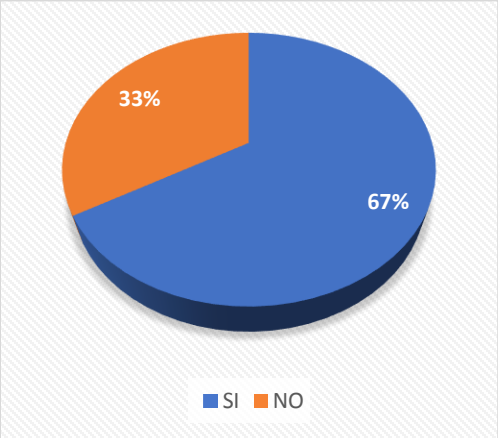


Figura 54: Pregunta 46, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 54 se presentan los resultados obtenidos de la pregunta cuarenta y siete de la segunda encuesta realizada a los miembros del DDTI. El 67% de miembros del DDTI afirman que existen controles para la gestión de los medios informáticos, mientras que el 33% afirma que no existen controles para la gestión de los medios informáticos. En conclusión, es posible afirman que existen controles para la gestión de los medios informáticos del sistema académico.

47) ¿Se monitorean las actividades relacionadas a la seguridad?

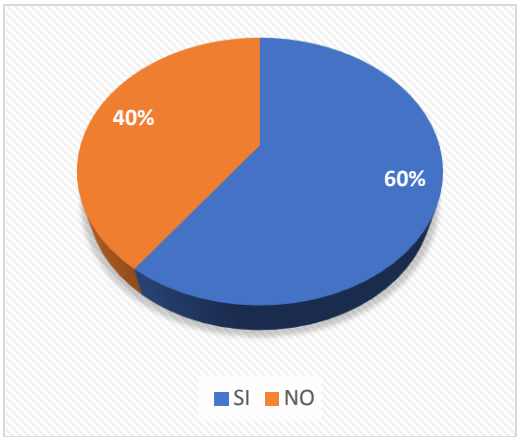


Figura 55: Pregunta 47, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 55 se presentan los resultados obtenidos de la pregunta cuarenta y ocho de la segunda encuesta realizada a los miembros del DDTI. El 60% de miembros del DDTI afirman que existe monitoreo de las actividades relacionadas con la seguridad, mientras que el 40% afirma que no existe monitoreo de las actividades relacionadas con la seguridad. En conclusión, es posible afirmar que el DDTI monitorea las actividades relacionadas con la seguridad.

48) ¿Existe una política de control de accesos?

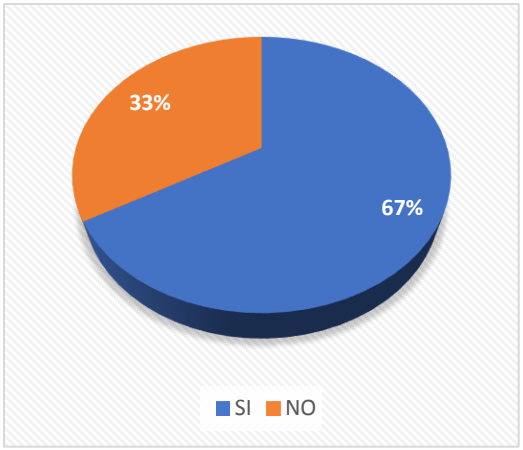


Figura 56: Pregunta 48, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 56 se presentan los resultados obtenidos de la pregunta cuarenta y nueve de la segunda encuesta realizada a los miembros del DDTI. El 67% de miembros del DDTI afirman que existe una política de control de acceso al sistema académico, mientras que el 33% afirma que no existe una política de control de acceso al sistema académico. En conclusión, es posible afirmar que existe una política establecida para el control de accesos al sistema académico.

49) ¿Se controla y restringe la asignación y uso de privilegios en entornos multiusuario?

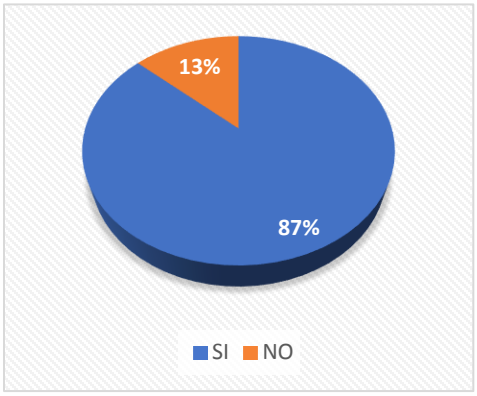


Figura 57: Pregunta 49, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 57 se presentan los resultados obtenidos de la pregunta cincuenta de la segunda encuesta realizada a los miembros del DDTI. El 87% de miembros del DDTI afirman que el DDTI controla y restringe la asignación y el uso de privilegios para multi usuarios, mientras que el 13% afirma que el DDTI no controla y restringe la asignación y el uso de privilegios para multi usuarios. En conclusión, es posible afirma que el DDTI controla y restringe la asignación y el uso de privilegios para multi usuarios.

50) ¿Se asegura la ruta (path) desde el terminal al servicio tanto internos como externos?

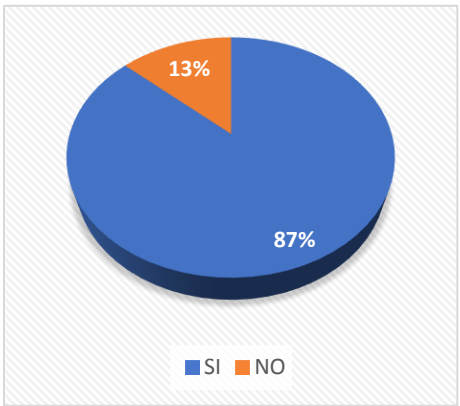


Figura 58: Pregunta 50, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 58 se presentan los resultados obtenidos de la pregunta cincuenta y uno de la segunda encuesta realizada a los miembros del DDTI. El 87% de miembros del DDTI afirman que el DDTI asegura la ruta desde el terminal al servicio para usuarios internos como para externos, mientras que el 13% afirma que el DDTI no asegura la ruta desde el terminal al servicio para usuarios internos como para externos. En conclusión, es posible afirma que el DDTI asegura la ruta desde el terminal al servicio para usuarios internos como para externos.

51) ¿Existe un control del routing (dispositivo para la interconexión de redes informáticas) de las redes internas y externas?

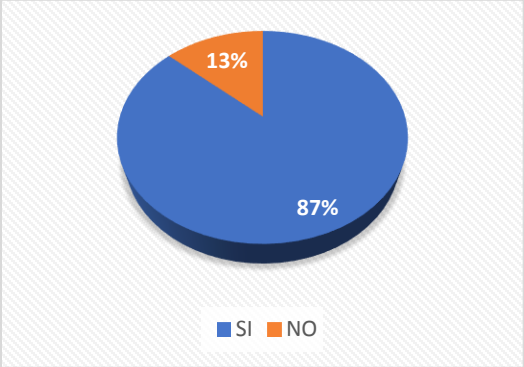


Figura 59: Pregunta 51, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 59 se presentan los resultados obtenidos de la pregunta cincuenta y dos de la segunda encuesta realizada a los miembros del DDTI. El 87% de miembros del DDTI afirman que existe un control de routing tanto para redes internas y externas de la UTN, mientras que el 13% afirma que no existe un control de routing tanto para redes internas y externas de la UTN. En conclusión, es posible afirma que existe un control de routing tanto para redes internas y externas de la UTN.

52) ¿Existe seguridad en los ficheros de los sistemas?

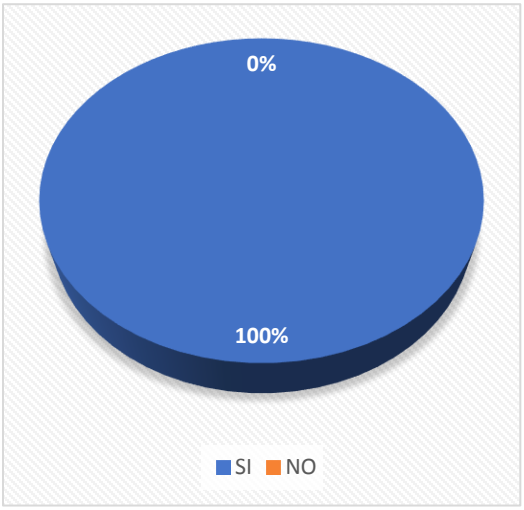


Figura 60: Pregunta 52, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 60 se presentan los resultados obtenidos de la pregunta cincuenta y tres de la segunda encuesta realizada a los miembros del DDTI. Todos los miembros del DDTI afirman que existe seguridad en los ficheros del sistema académico de la UTN.

53) ¿Existe seguridad en los procesos de desarrollo, testing y soporte?

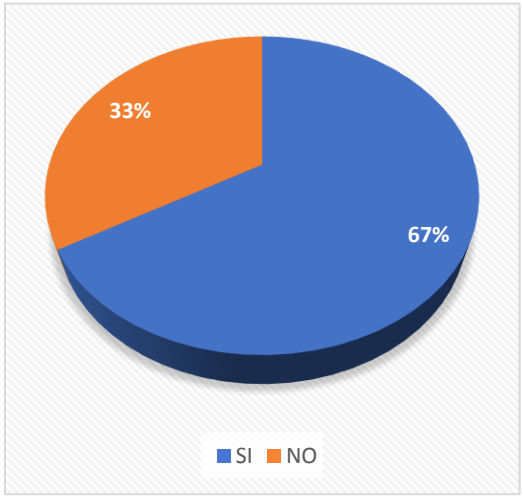


Figura 61: Pregunta 53, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 61 se presentan los resultados obtenidos de la pregunta cincuenta y cuatro de la segunda encuesta realizada a los miembros del DDTI. El 67% de los miembros del DDTI afirman que existe seguridad en los procesos de desarrollo, testing y soporte de la UTN, mientras que el 33% afirma que no existe seguridad en los procesos de desarrollo, testing y soporte de la UTN. En conclusión, es posible decir que existe seguridad en los procesos de desarrollo, testing y soporte de la UTN.

54) ¿Existe la gestión de los cambios en los Sistemas Operativos (S.O.)?

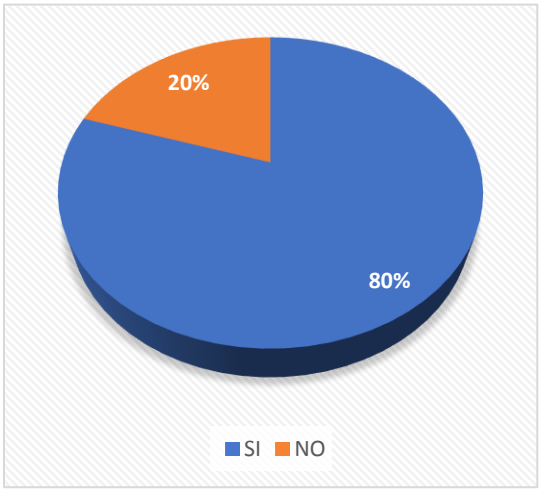


Figura 62: Pregunta 54, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 64 se presentan los resultados obtenidos de la pregunta cincuenta y cinco de la segunda encuesta realizada a los miembros del DDTI. El 80% de los miembros del DDTI afirman que existe la gestión de cambios en los sistemas operativos de la UTN, mientras que el 20% afirma que no existe la gestión de cambios en los sistemas operativos de la UTN. En conclusión, es posible decir que existe la gestión de cambios en los sistemas operativos de la UTN.

55) ¿Se controlan las vulnerabilidades de los equipos?

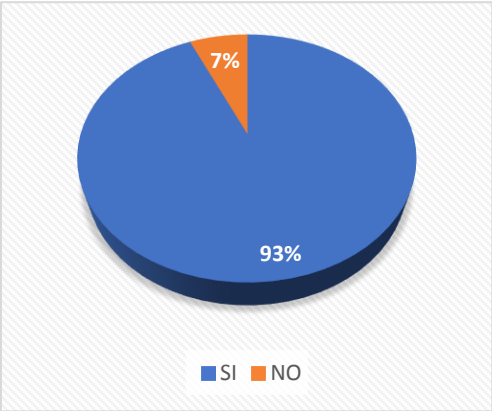


Figura 63: Pregunta 55, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 63 se presentan los resultados obtenidos de la pregunta cincuenta y seis de la segunda encuesta realizada a los miembros del DDTI. El 93% de los miembros del DDTI afirman que existe un control de las vulnerabilidades de los equipos que posee la UTN, mientras que el 7% afirma que no existe un control de las vulnerabilidades de los equipos que posee la UTN. En conclusión, es posible decir que existe un control de las vulnerabilidades de los equipos que posee la UTN.

56) ¿Se comunican los eventos de seguridad?

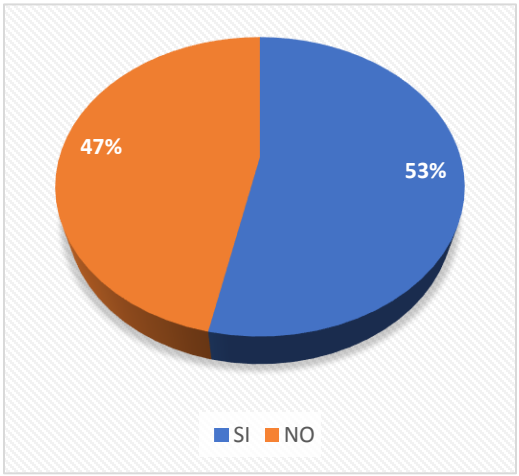


Figura 64: Pregunta 56, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 64 se presentan los resultados obtenidos de la pregunta cincuenta y siete de la segunda encuesta realizada a los miembros del DDTI. El 53% de los miembros del DDTI afirman que existe comunicación por parte del DDTI de los eventos de seguridad, mientras que el 47% afirma que no existe comunicación por parte del DDTI de los eventos de seguridad. En conclusión, es posible decir que existe comunicación por parte del DDTI de los eventos de seguridad.

57) ¿Existe definidas las responsabilidades antes de un incidente?

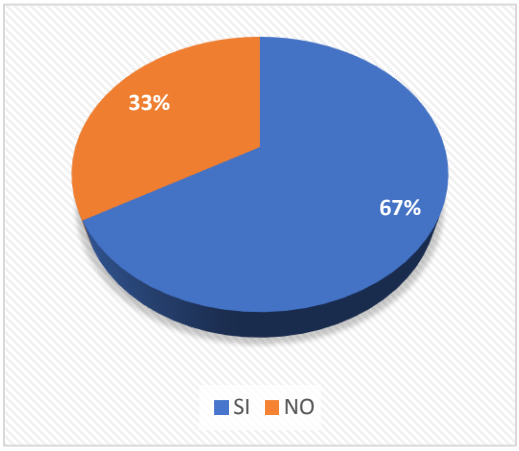


Figura 65: Pregunta 57, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 65 se presentan los resultados obtenidos de la pregunta cincuenta y ocho de la segunda encuesta realizada a los miembros del DDTI. El 67% de los miembros del DDTI afirman que existe asignación de responsabilidades ante incidentes ocurridos en el sistema académico, mientras que el 33% afirma que no existe asignación de responsabilidades ante incidentes ocurridos en el sistema académico. En conclusión, es posible decir que existe asignación de responsabilidades ante incidentes ocurridos en el sistema académico.

58) ¿Existen procesos para la gestión de la continuidad?

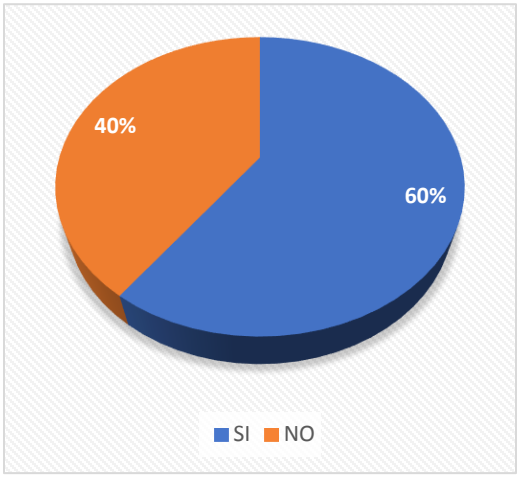


Figura 66: Pregunta 58, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 66 se presentan los resultados obtenidos de la pregunta cincuenta y nueve de la segunda encuesta realizada a los miembros del DDTI. El 60% de los miembros del DDTI afirman que existe procesos definidos para la gestión de la continuidad, mientras que el 40% afirma que no existe procesos definidos para la gestión de la continuidad. En conclusión, es posible decir que existe procesos definidos para la gestión de la continuidad del sistema académico.

59) ¿Existe un diseño, redacción e implantación de planes de continuidad?

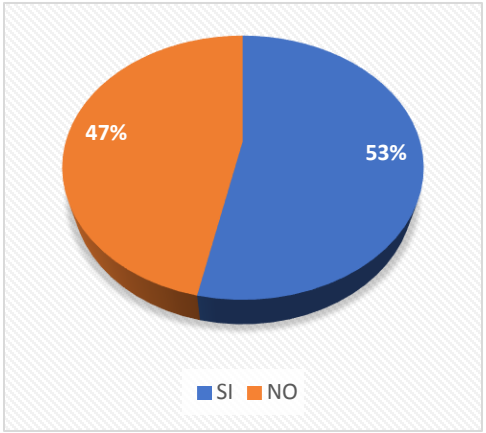


Figura 67: Pregunta 59, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 67 se presentan los resultados obtenidos de la pregunta sesenta de la segunda encuesta realizada a los miembros del DDTI. El 53% de los miembros del DDTI afirman que existe el diseño, redacción y revisión de planes de continuidad, mientras que el 40% afirma que no existe el diseño, redacción y revisión de planes de continuidad. En conclusión, es posible decir que existe el diseño, redacción y revisión de planes de continuidad.

60) ¿Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas?

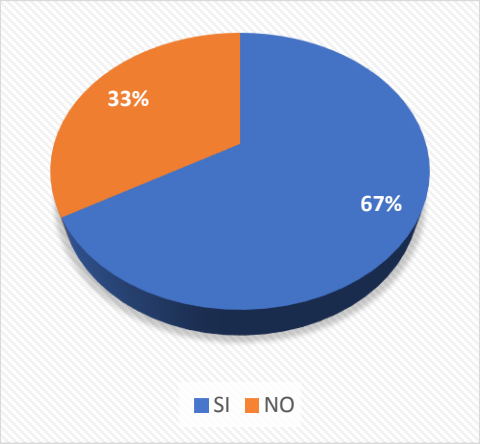


Figura 68: Pregunta 60, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 68 se presentan los resultados obtenidos de la pregunta sesenta y uno de la segunda encuesta realizada a los miembros del DDTI. El 67% de los miembros del DDTI afirman que el DDTI cuenta con el cumplimiento de la legislación por parte de los sistemas, mientras que el 33% afirma que el DDTI cuenta no con el cumplimiento de la legislación por parte de los sistemas. En conclusión, es posible decir que el DDTI cuenta con el cumplimiento de la legislación por parte de los sistemas.

61) ¿Existe el resguardo de los registros de la organización?

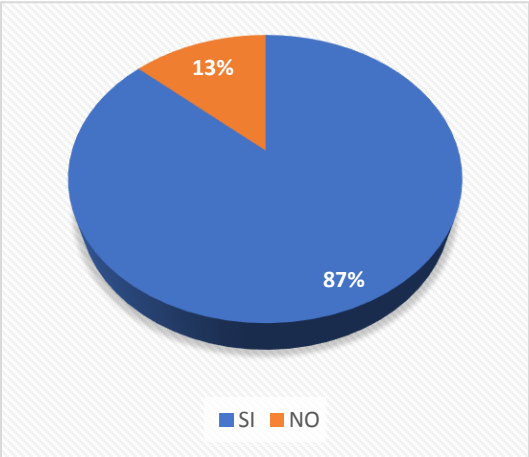


Figura 69: Pregunta 61, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 69 se presentan los resultados obtenidos de la pregunta sesenta y dos de la segunda encuesta realizada a los miembros del DDTI. El 87% de los miembros del DDTI afirman que existe el resguardo de los registros de la organización, mientras que el 33% afirma que no existe el resguardo de los registros de la organización. En conclusión, es posible decir que si existe el resguardo de los registros de la organización por parte del DDTI.

62) ¿Existe una revisión de la política de seguridad y de la conformidad técnica?

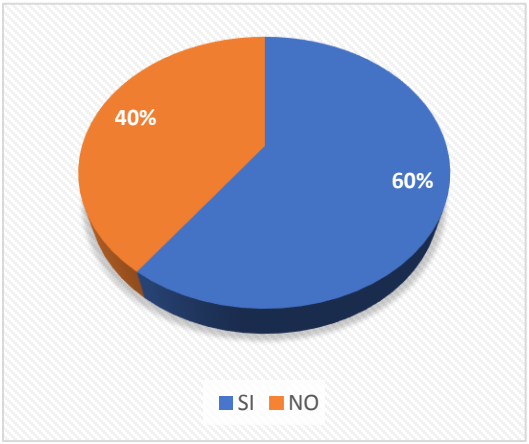


Figura 70: Pregunta 62, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 70 se presentan los resultados obtenidos de la pregunta sesenta y tres de la segunda encuesta realizada a los miembros del DDTI. El 60% de los miembros del DDTI afirman que existe una revisión de la política de seguridad y de la conformidad técnica del sistema académico, mientras que el 40% afirma que no existe una revisión de la política de seguridad y de la conformidad técnica del sistema académico. En conclusión, es posible decir que si existe una revisión de la política de seguridad y de la conformidad técnica del sistema académico.

63) ¿Existen consideraciones sobre las auditorías de los sistemas?

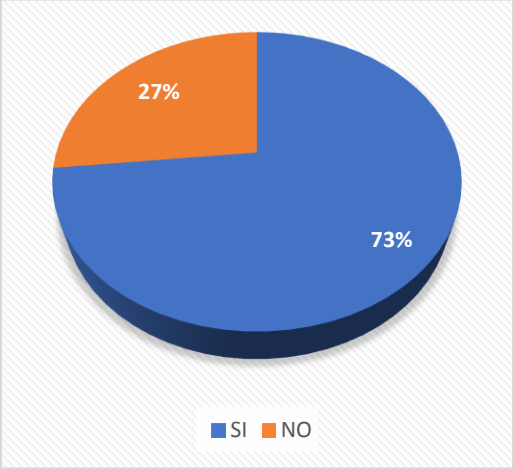


Figura 71: Pregunta 63, encuesta 2.

Fuente: Propia.

Análisis de resultados

En la figura 71 se presentan los resultados obtenidos de la pregunta sesenta y tres de la segunda encuesta realizada a los miembros del DDTI. El 73% de los miembros del DDTI afirman que existe consideración sobre las auditorias de los sistemas de la UTN, mientras que el 27% afirma que no existe consideración sobre las auditorias de los sistemas de la UTN. En conclusión, es posible decir que si existe consideración sobre las auditorias de los sistemas de la UTN.

2.7.2. Técnica de evaluación de la seguridad de la información

Aplicación de la Norma ISO 27002:2017

Para la evaluación de seguridad realizada en el sistema académico de la Universidad Técnica del Norte, se analiza toda la información recopilada de las encuestas y la información proporcionada por la UTN. La revisión de la información se la realiza en base a los controles que posee la norma ISO/IEC 27002:2017 que se describen a continuación:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información
- Seguridad en recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y de entorno
- Seguridad de las operaciones
- Seguridad en las telecomunicaciones
- Adquisición, desarrollo y mantenimiento del sistema
- Relaciones con proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio.
- Cumplimiento

Metodología para el análisis y gestión de riesgos de la información.

Dentro de guía para la ejecución de la auditoría planteada en la norma ISO 27007:2017 menciona que se debe emplear una herramienta para la gestión y el análisis de riesgos de la información. Para el presente caso de estudio se elige la metodología MAGERIT que se describe a continuación.

Magerit

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de

gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (MAGERIT, 2012, pág. 7)

Al utilizar Magerit se analiza el impacto que puede tener la institución educativa en el caso de violación a la seguridad, se busca identificar las posibles amenazas que puede afectar la integridad de la información, y las vulnerabilidades que sirven de acceso para dichas amenazas, pudiendo así establecer medidas preventivas y correctivas para salvaguardar la información.

Magerit trabaja mediante un proceso analítico en base a un software llamando Pilar, con toda la información recolectada de los activos que hacen parte del sistema académico de la UTN para ser ingresados al software y ser analizados mediante las normativas ISO/IEC 27007:2017, siendo el instrumento de las mejores prácticas para el análisis del Sistema de Gestión de seguridad de Información.

Gestión de riesgos

Para la gestión de riesgos MAGERIT propone un proceso definido como se observa en la figura 72 y se procede a describir a continuación:

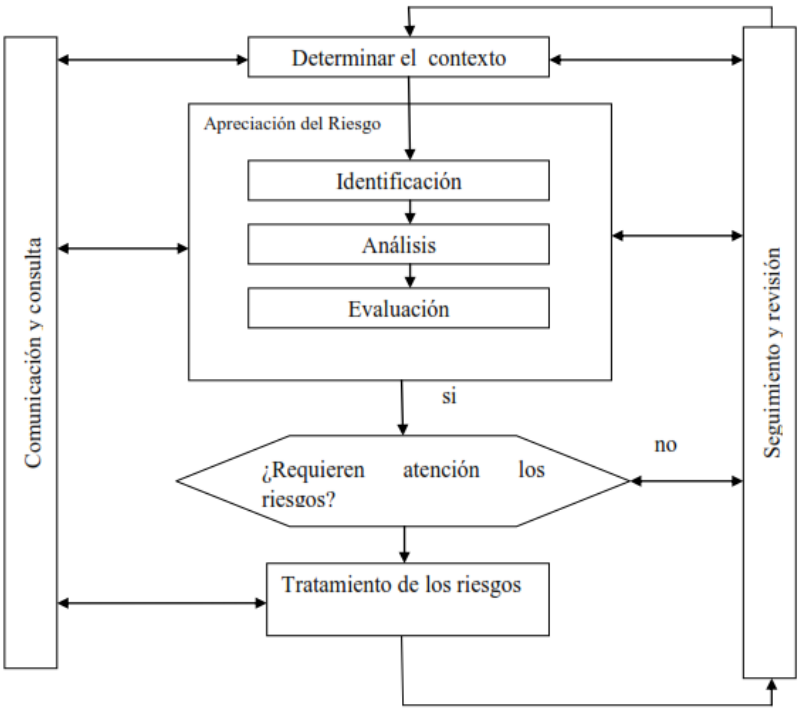


Figura 72: Proceso de gestión de riesgos MAGERIT

Fuente: (CCN-CERT, 2013)

Determinación del contexto: Se refiere a la determinación de parámetros y condiciones tanto internos como externos que permiten elegir una política que se empleara para la gestión de riesgos.

Identificación de riesgos: La identificación de riesgos se trata de encontrar una relación entre los posibles riesgos que se asocia a cada activo.

Análisis de riesgos: El análisis de riesgos califica a los riesgos encontrados en la identificación de riesgos. La calificación que se otorga a cada riesgo es de forma cualitativa o cuantitativamente, una vez calificados todos los riesgos será posible tener una visión mejor estructurada de los riesgos más importantes.

Tratamiento de los riesgos: El tratamiento de los riesgos se refiere a todas las acciones empleadas que tienen la finalidad de modificar de alguna forma la situación de riesgo existente.

Comunicación y consulta: La comunicación y consulta tiene como fin encontrar un balance entre seguridad y productividad.

Seguimiento y revisión: Luego del análisis se tendrá recomendaciones para implementarlas en el caso de estudio, en este caso el sistema académico de la Universidad Técnica del Norte.

Análisis de riesgos

El análisis de riesgo toma importancia debido a que en la actualidad todo sistema está expuesto a riesgos, así como cada parte que componen el mismo; por lo tanto, es posible afirma que no existe un entorno 100% seguro. La organización debe estar alerta a cualquier situación extraña que se pueda presentar y que le afecte de forma negativa de manera parcial o total. Con el análisis de riesgo se espera:

- Identificar los activos esenciales que posee el sistema académico de la Universidad Técnica del Norte.
- Identificar las posibles amenazas a las que se encuentran expuestos los activos del sistema académico.
- Conocer el impacto acumulado si se llegara a materializar alguna de las amenazas identificadas.

A continuación, en la figura 73 se presenta el análisis de riesgos descrito en bloques.

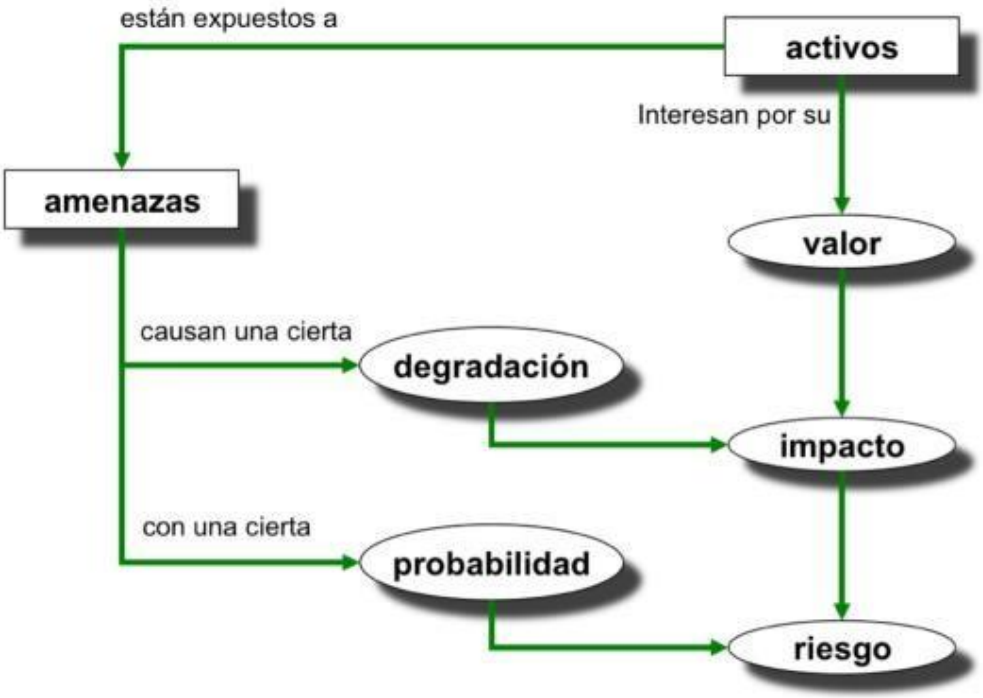


Figura 73: Análisis de riesgos MAGERIT

Fuente: (CCN-CERT, 2013)

Para emplear el análisis de riesgos se empleó la información recolectada mediante la observación física, las dos encuestas realizadas y la información proporcionada por la Universidad Técnica del Norte. El resultado del análisis de riesgo permitirá conocer el valor de los activos y como se encuentra protegidos ante las posibles amenazas.

2.7.3. Procedimiento lógico para el análisis de riesgos mediante Pilar.

El Procedimiento Informático Lógico para el análisis de Riesgos denominada EAR PILAR es una herramienta que aplica la metodología MAGERIT para el análisis de riesgos. Con la ayuda de Pilar es posible ejecutar todas las actividades necesarias para el análisis de gestión de riesgos, siguiendo la secuencia lógica.

Identificación de activos

El activo se define como algo valioso para el sistema académico y tiene la finalidad de brindar la continuidad del negocio. Estos se pueden clasificar en:

a) **Activos de información:** en los activos de información se encuentran bases de datos, manuales, procedimientos, políticas, normativas, etc.

b) **Documentos impresos:** en este grupo se encuentran todos los documentos impresos como reportes, contratos, informes y todo documento impreso con una importancia alta para el sistema académico.
c) **Activos de software:** en este grupo se encuentra todas las herramientas de desarrollo y software creados ya sean propios o adquiridos por terceros.
d) **Activos Físicos:** en este grupo se encuentran todos los activos en cuanto a hardware se refiere.
e) **Activos humanos:** en este grupo se encuentran todos los activos que interactúan con el sistema académico, como estudiantes, docentes, personal administrativo.

Imagen y reputación de la empresa

a) **Servicios:** en este grupo se encuentran todos los servicios contratados a terceros. Es importante tomar en cuenta que todos los activos no tienen el mismo nivel de importancia dentro de la organización, por lo tanto, los mecanismos de seguridad que se empleen deberán ser de acuerdo a las amenazas potenciales de cada activo.

Valoración de activos

Para realizar la valoración de activos es necesario conocer el sistema académico a fondo, para identificar los activos esenciales dentro del proceso. Una vez identificados los activos esenciales se procede a valorarlos de forma cuantitativa, es decir se asigna un valor especifico a cada activo según su nivel de importancia dentro del sistema académico.

Identificación de amenazas

La identificación de amenazas se lo realizara para cada uno de los activos. Para identificar cada amenaza es necesario revisar las encuestas y la información proporcionada por la Universidad Técnica del Norte, además de todas las amenazas Pilar ofrece amenazas asignadas a cada activo que se va ingresando, clasificándolas en dos grupos:

a) **Amenazas deliberadas:** se dice que es una amenaza deliberada cuando la acción es con intención maliciosa.
b) **Amenazas Accidentales:** se dice que es una amenaza accidental cuando la acción es sin intención maliciosa, sin embargo, produce un daño.

Valoración de amenazas

La valoración de amenazas engloba dos conceptos:

a) **Probabilidad de ocurrencia**: es la cantidad de veces que ocurre una amenaza.
b) **Porcentaje de degradación:** es el daño que causa la ocurrencia de una amenaza.

Pilar emplea los parámetros descritos en la tabla 29

Tabla 29. Frecuencia de ocurrencia

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

Fuente: Propia

El porcentaje de degradación se describe como la razón entre la amenaza y la dimensión, el resultado es medible entre 0 y 100%.

Estimación de impacto

El impacto se describe como el porcentaje de daño que se produjo en los diferentes activos del sistema académico. Para la determinación adecuada del impacto Pilar considera tres factores:

- Cuando la ocurrencia de una amenaza afecta a todo un proceso o a una parte de este.
- Cuando la ocurrencia de una amenaza afecta a partes clave de la información.
- Una vez ocurrida la amenaza, esta es permanente o temporal.

Los impactos traen consigo impactos cualitativos o cuantitativos. Por ejemplo:

El impacto de una falla en la Universidad Técnica del Norte, tomando en cuenta que no cuenta con redundancia eléctrica. La falla produce una mala imagen de la universidad.

Es posible establecer relación causa efecto entre las consecuencias de los riesgos y las salvaguardas, debido a que, si existen muchas fallas ocurriendo al mismo tiempo, produciría un efecto en cadena, al que le corresponderían muchas perdidas y daños.

Impacto acumulado

El impacto acumulado es referido a cada activo, cada amenaza y la dimensión de valoración. El valor resultante se describe en función de la degradación y el valor acumulado. El impacto acumulado es de utilidad para determinar que salvaguardas se debe aplicar en el proceso evaluado.

Impacto repercutido

El impacto repercutido permite conocer las consecuencias que tiene los accidentes ocurridos en el sistema de información.

Calculo del nivel de riesgo

Para el cálculo de nivel de riesgos es necesario identificar los riesgos por activos. Para la identificación de riesgos se puede llevar a cabo por diversos métodos como:

- Análisis FODA
- Encuestas
- Entrevistas
- Arboles de fallos
- Arboles de eventos
- Método Delphi
- Análisis probabilístico.

Para la presente investigación se usaron 2 de las herramientas descritas a detalle en los literales 2.7.1. y 2.7.2.

Valoración de riesgos

La valoración de activos es un proceso que posee una secuencia determinada. La secuencia que se tiene que seguir es la siguiente:

- Identificación de activos
- Identificación de amenazas
- Estimación de vulnerabilidades por cada activo.

Existen cuatro rangos de valoración de activos tal como se muestra en la Tabla 30.

a) **Critico:** significa que el riesgo es muy elevado, por lo que es necesario emplear salvaguardas extra para mitigar el riesgo.

b) **Alto:** significa que el riesgo es alto, por lo que es necesario emplear algunas salvaguardas para mitigar riesgos.
c) **Medio:** significa que el riesgo es medio, por lo que se puede considerar emplear algunas salvaguardas para mitigar riesgos.
d) **Bajo:** significa que el riesgo es bajo, por lo que no es necesario emplear salvaguardas para mitigar riesgos.

Tabla 30. Nivel de riesgos

0	<	Nivel de riesgo bajo	<	3
3	<	Nivel de riesgo medio	<	6
6	<	Nivel de riesgo alto	<	9
9	<	Nivel de riesgo critico	<	12

Fuente: Propia

El riesgo más importante es el que pasa desapercibido, puesto que en este tipo de riesgos no se toman medidas, por lo tanto, no se debe omitir la existencia de ningún riesgo.

2.7.4. Aplicación de Pilar

A continuación, se muestra la evaluación del sistema académico con PILAR.

En la figura 74 se presenta la pantalla inicial del software PILAR, es este es posible elegir uno de los análisis, para el caso de estudio se eligió análisis cualitativo. A continuación, en la figura 75 se complementa los datos de la creación del proyecto.

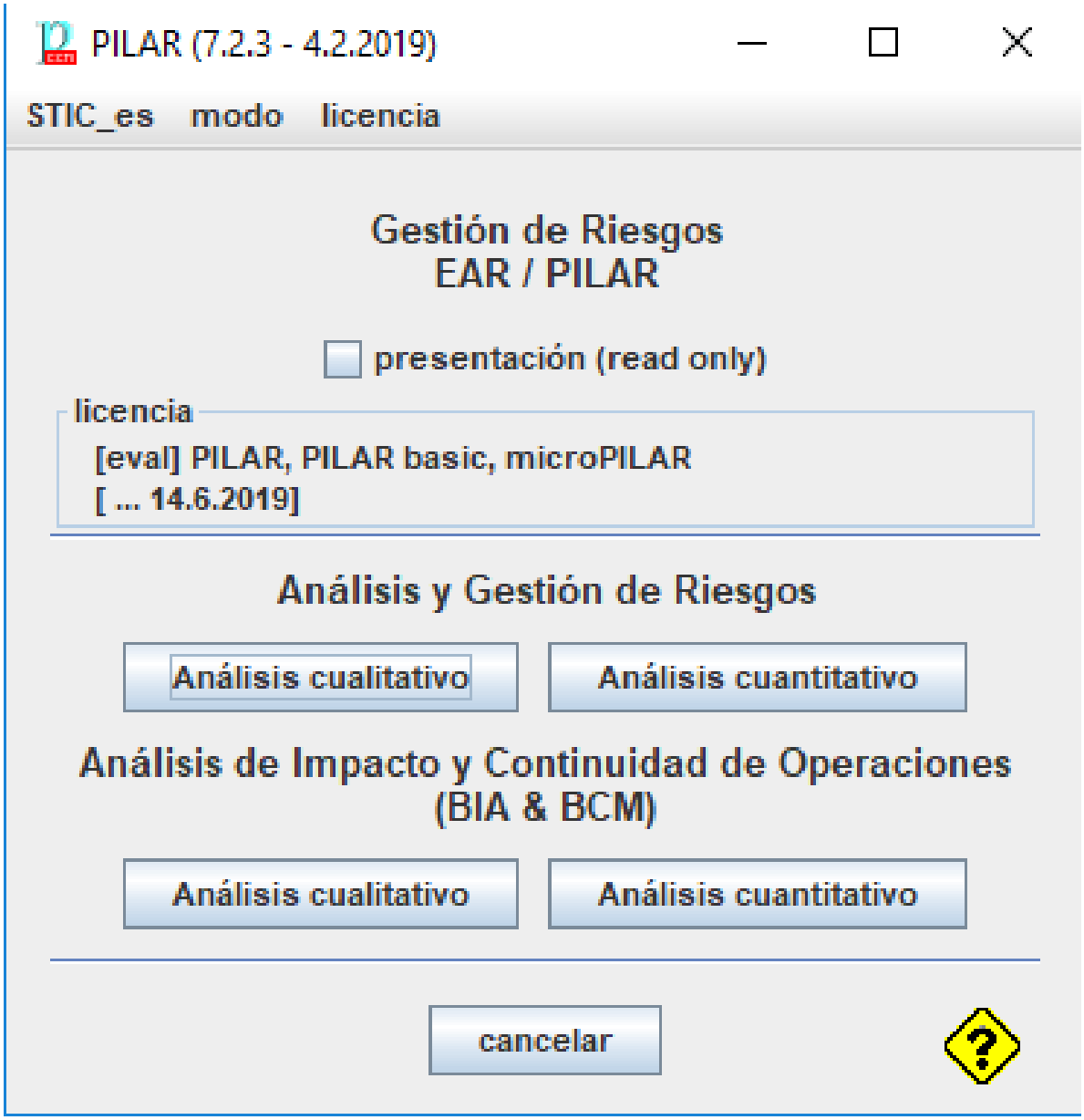


Figura 74: Pantalla inicial de software PILAR

Fuente: Propia

En la figura 75 se observa la pantalla para la creación de un nuevo proyecto, en este se tendrá que llenar datos relevantes acerca del autor, a que institución pertenece, una breve descripción de lo que hará el programa entre otras cosas.

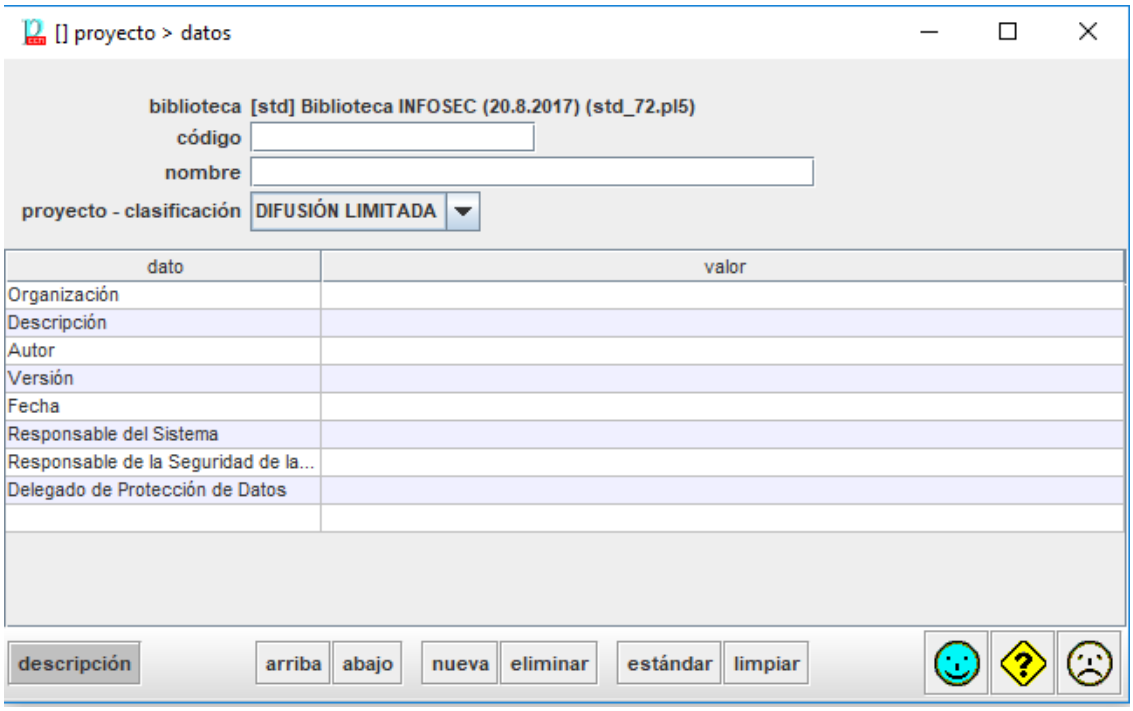


Figura 75: Creación de nuevo proyecto

Fuente: Propia

2.7.5. Identificación de activos

Una vez creado el proyecto se procede a determinar los activos del sistema académico. Para ello fue necesario revisar toda la documentación proporcionada por parte de la UTN y la ficha técnica propuesta, con el fin de conocer el funcionamiento sistema, cuáles son los usuarios que usan el sistema, y finalmente determinar todos los activos que posee la UTN para el funcionamiento de sistema académico.

Para ingresar los activos en PILAR es posible usar capas, para diferenciar el tipo de activo del que estamos tratando. Por ejemplo, existe una capa para los activos esenciales, como son la información base de datos etc.

En la figura 76 se presenta el ingreso de activos en PILAR, cada activo pertenece a una capa en específico.

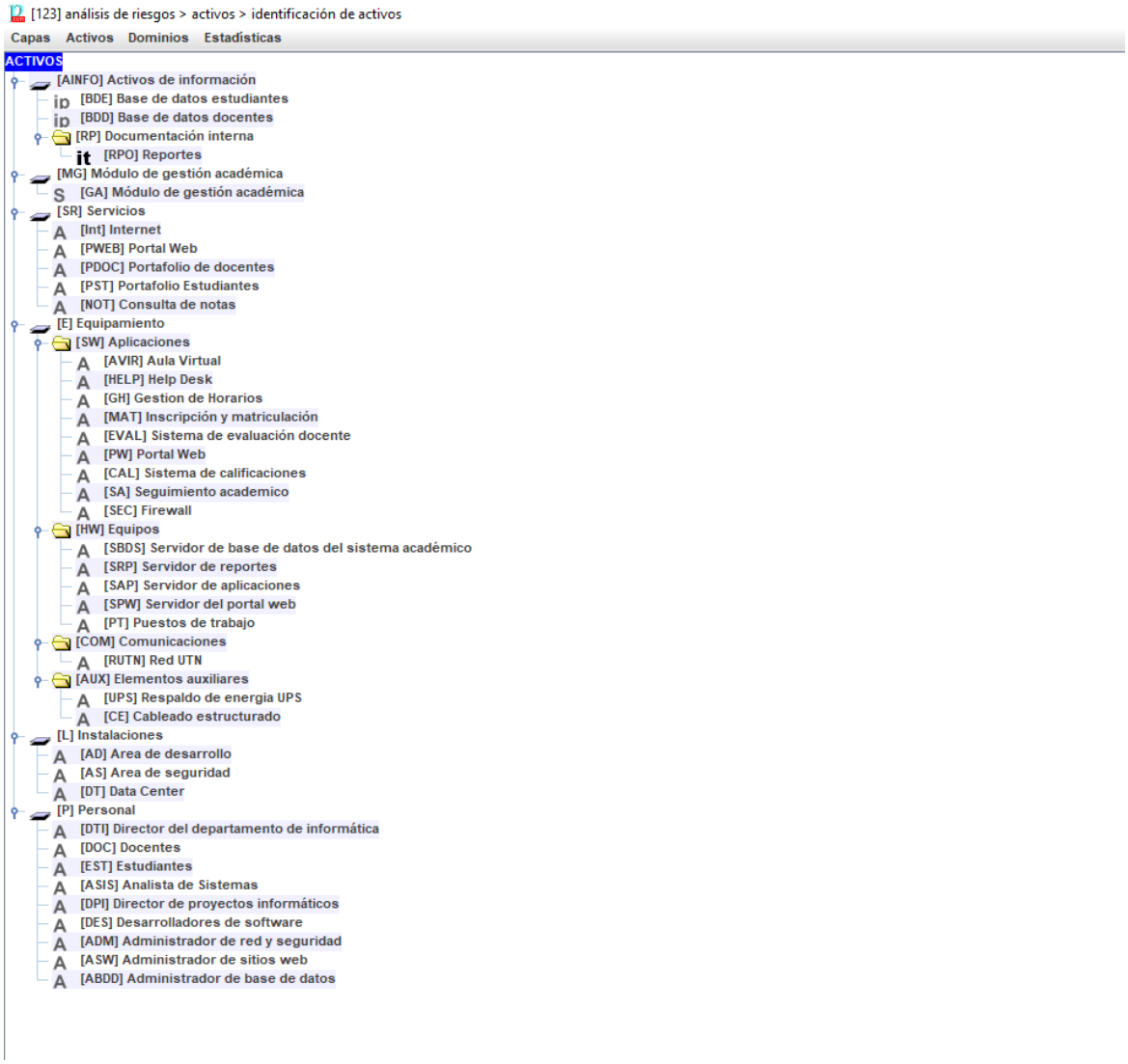


Figura 76: Identificación de activos

Fuente: Propia

2.7.6. Valoración de activos

Para la valoración de activos se toma en cuenta la criticidad del activo dentro de lo que se está evaluando, es decir que tan importante es un activo dentro de la organización y que implicaría que el activo sufra daños por la materialización de una amenaza.

Es importante recordar que para la valoración de activos PILAR toma en cuenta 5 parámetros importantes relacionados con la información.

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticidad
- Trazabilidad

En la figura 77 se presenta la valoración de activos en PILAR, cada activo está valorado con los 5 parámetros relacionados con la información.

[123] análisis de riesgos > activos > valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[AINFO] Activos de información					
[BDE] Base de datos estudiantes	[7]	[8]	[6]	[7]	[9]
[BDD] Base de datos docentes	[7]	[8]	[6]	[7]	[9]
[RP] Documentación interna					
[MG] Módulo de gestión académica					
[GA] Módulo de gestión académica	[9]	[9]	[9]	[9]	[9]
[SR] Servicios					
[Int] Internet	[9]	[7]	[7]	[6]	[9]
[PWEB] Portal Web	[10]	[9]	[8]	[9]	[7]
[PDOC] Portafolio de docentes	[10]	[9]	[8]	[6]	[10]
[PST] Portafolio Estudiantes	[9]	[9]	[9]	[6]	[8]
[NOT] Consulta de notas	[7]	[7]	[9]	[9]	[9]
[E] Equipamiento					
[SW] Aplicaciones					
[AVIR] Aula Virtual	[9]	[9]	[9]	[7]	[7]
[HELP] Help Desk	[10]	[5]	[5]	[9]	[2]
[GH] Gestion de Horarios	[9]	[9]	[6]	[8]	[7]
[MAT] Inscripción y matriculación	[9]	[8]	[9]	[6]	[7]
[EVAL] Sistema de evaluación docente	[7]	[8]	[7]	[6]	[8]
[PW] Portal Web	[9]	[8]	[5]	[9]	[6]
[CAL] Sistema de calificaciones	[9]	[9]	[8]	[6]	[7]
[SA] Seguimiento academico	[9]	[9]	[8]	[7]	[7]
[SEC] Firewall	[9]	[9]	[9]	[9]	[9]
[HW] Equipos					
[SBDS] Servidor de base de datos del sistema académico	[9]	[9]	[9]	[9]	[9]
[SRP] Servidor de reportes	[9]	[8]	[8]	[7]	[7]
[SAP] Servidor de aplicaciones	[8]	[7]	[7]	[7]	[7]
[SPW] Servidor del portal web	[9]	[8]	[8]	[8]	[8]
[PT] Puestos de trabajo	[7]	[7]	[7]	[8]	[7]
[COM] Comunicaciones					
[RUTN] Red UTN	[9]	[9]	[9]	[9]	[9]
[AUX] Elementos auxiliares					
[UPS] Respaldo de energia UPS					
[CE] Cableado estructurado					
[L] Instalaciones					
[AD] Area de desarrollo	[8]	[8]	[7]	[7]	[10]
[AS] Area de seguridad	[8]	[8]	[8]	[8]	[7]
[DT] Data Center	[10]	[9]	[9]	[9]	[9]
[P] Personal					
[DTI] Director del departamento de informática	[9]	[8]	[8]	[8]	[8]
[DOC] Docentes	[9]	[9]	[9]	[9]	[9]
[EST] Estudiantes	[6]	[6]	[6]	[6]	[6]
[ASIS] Analista de Sistemas	[7]	[7]	[5]	[5]	[7]
[DPI] Director de proyectos informáticos	[8]	[8]	[8]	[8]	[8]
[DES] Desarrolladores de software	[9]	[7]	[9]	[7]	[9]
[ADM] Administrador de red y seguridad	[8]	[8]	[7]	[8]	[8]
[ASW] Administrador de sitios web	[8]	[7]	[7]	[8]	[8]
[ABDD] Administrador de base de datos	[8]	[9]	[6]	[8]	[7]

Figura 77: Valoración de activos

Fuente: Propia

2.7.7. Identificación de amenazas.

Una vez valorados los activos, PILAR asocia amenazas posibles para cada activo ingresado. En la figura 78 se presenta los riesgos asociados para cada activo del sistema académico.

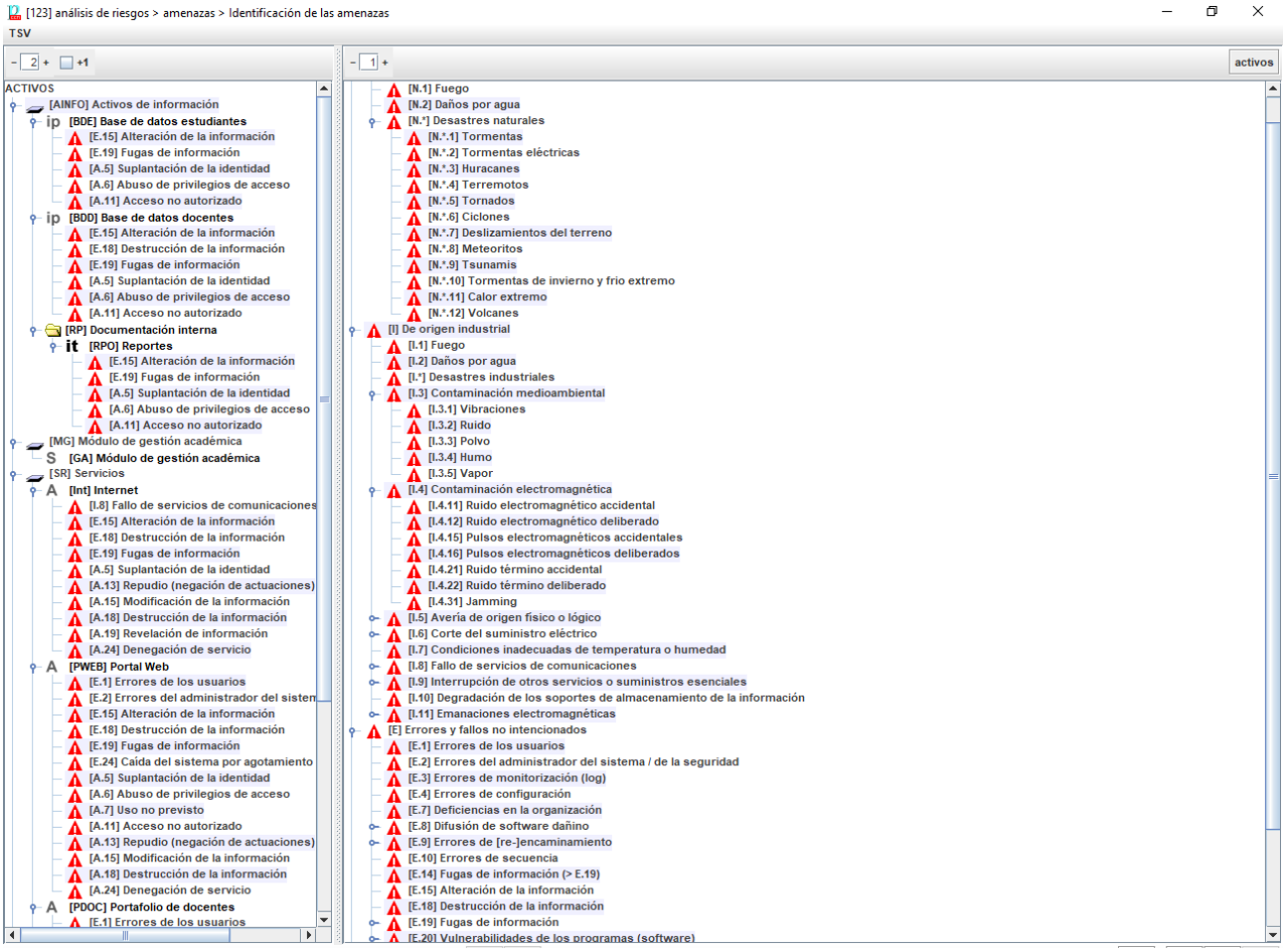


Figura 78: Identificación de Amenazas

Fuente: Propia

2.7.8. Valoración de amenazas.

Una vez identificadas las amenazas, PILAR establece valores recomendados para el sistema académico de la UTN.

[123] análisis de riesgos > amenazas > amenazas

Editar Exportar Importar TSV

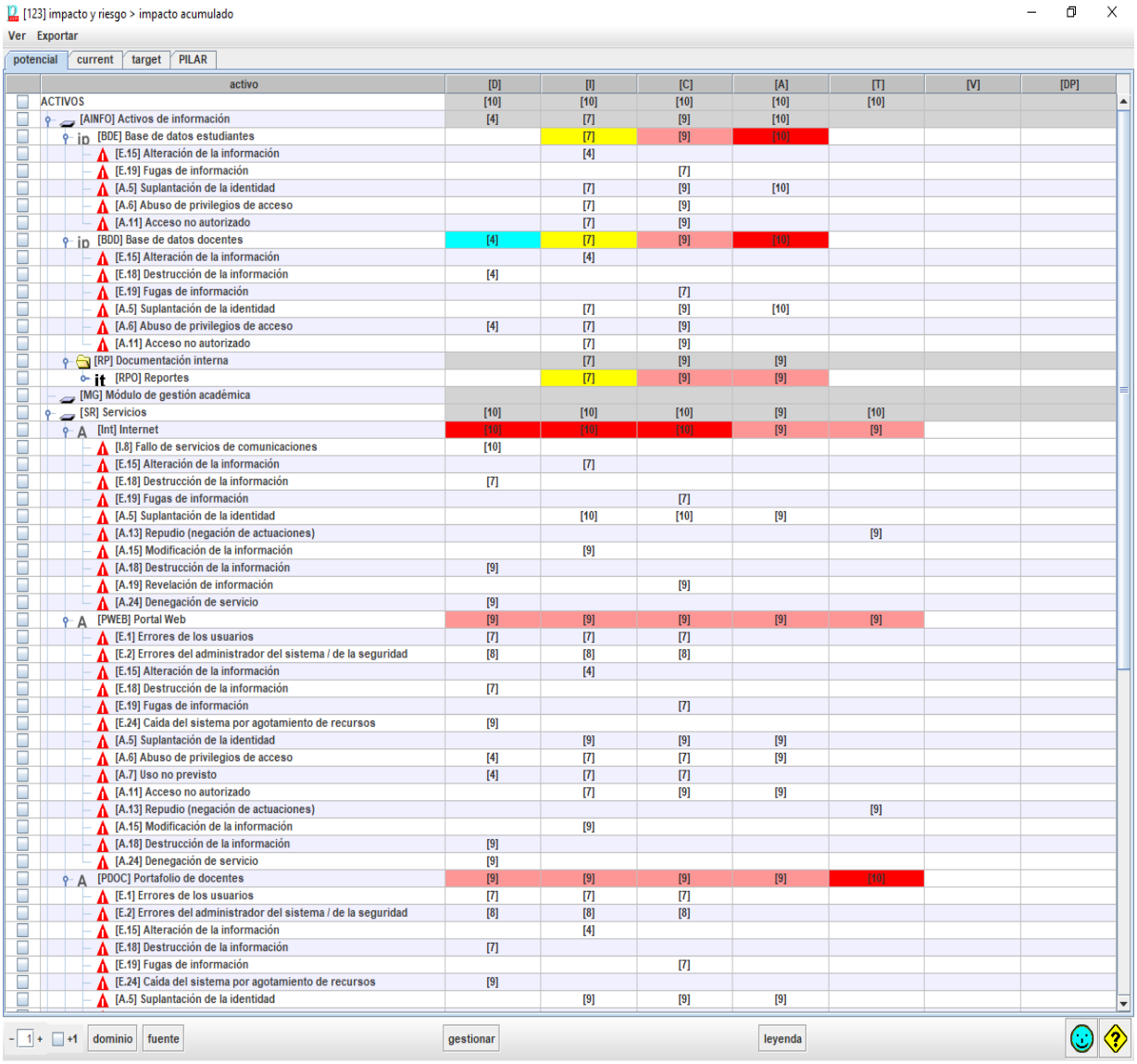
activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS									
[AINFO] Activos de información									
[BDE] Base de datos estudiantes			0	10%	50%	100%			
[BDD] Base de datos docentes			1%	10%	50%	100%			
[RP] Documentación interna									
[RPO] Reportes			0	10%	50%	100%			
[MG] Módulo de gestión académica									
[GA] Módulo de gestión académica									
[SR] Servicios									
[Int] Internet			100%	100%	100%	100%	100%		
[I.8] Fallo de servicios de comunicaciones		1	100%						
[E.15] Alteración de la información		1		10%					
[E.18] Destrucción de la información		1	10%						
[E.19] Fugas de información		1			10%				
[A.5] Suplantación de la identidad		0,2		100%	100%	100%			
[A.13] Repudio (negación de actuaciones)		1					100%		
[A.15] Modificación de la información		1		50%					
[A.18] Destrucción de la información		1	50%						
[A.19] Revelación de información		1			50%				
[A.24] Denegación de servicio		1	50%						
[PWEB] Portal Web			50%	50%	50%	100%	100%		
[E.1] Errores de los usuarios		1	10%	10%	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%				
[E.15] Alteración de la información		1		1%					
[E.18] Destrucción de la información		1	10%						
[E.19] Fugas de información		1			10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%						
[A.5] Suplantación de la identidad		1		50%	50%	100%			
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%	100%			
[A.7] Uso no previsto		1	1%	10%	10%				
[A.11] Acceso no autorizado		1		10%	50%	100%			
[A.13] Repudio (negación de actuaciones)		5					100%		
[A.15] Modificación de la información		10		50%					
[A.18] Destrucción de la información		1	50%						
[A.24] Denegación de servicio		10	50%						
[PDOC] Portafolio de docentes			50%	50%	50%	100%	100%		
[E.1] Errores de los usuarios		1	10%	10%	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%				
[E.15] Alteración de la información		1		1%					
[E.18] Destrucción de la información		1	10%						
[E.19] Fugas de información		1			10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%						
[A.5] Suplantación de la identidad		1		50%	50%	100%			
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%	100%			
[A.7] Uso no previsto		1	1%	10%	10%				
[A.11] Acceso no autorizado		1		10%	50%	100%			
[A.13] Repudio (negación de actuaciones)		5					100%		
[A.15] Modificación de la información		10		50%					
[A.18] Destrucción de la información		1	50%						
[A.24] Denegación de servicio		10	50%						
[PST] Portafolio Estudiantes			50%	50%	50%	100%	100%		
[E.1] Errores de los usuarios		1	10%	10%	10%				
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%				
[E.15] Alteración de la información		1		1%					
[E.18] Destrucción de la información		1	10%						

Figura 79: Valoración Amenazas

Fuente: Propia

2.7.9. Impacto acumulado.

A continuación, en la figura 80, se muestra el impacto acumulado en los activos del sistema académico.



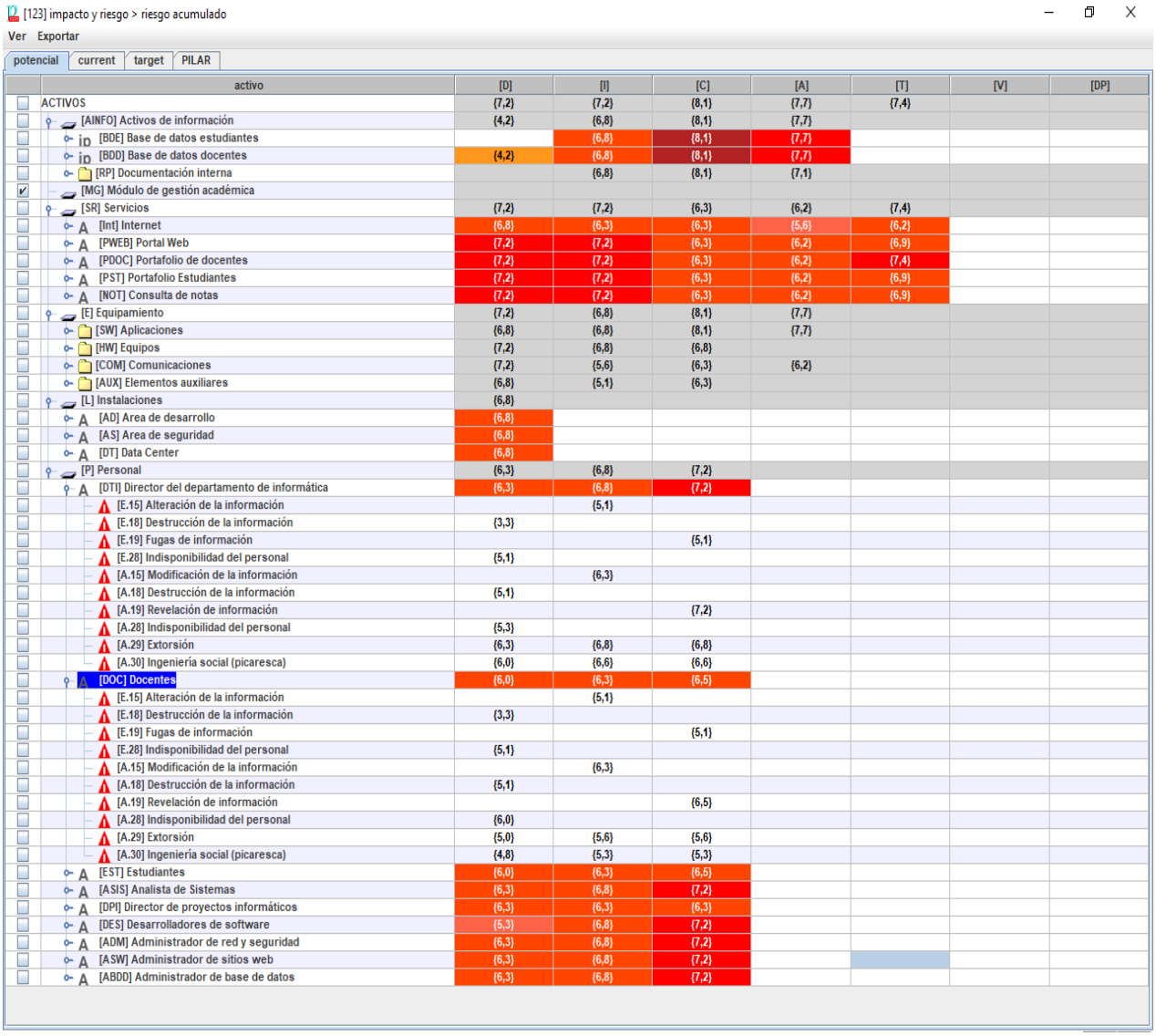
activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[10]	[10]	[10]	[10]	[10]		
[AINFO] Activos de información	[4]	[7]	[9]	[10]			
[BDE] Base de datos estudiantes		[7]	[9]	[10]			
[E.15] Alteración de la información		[4]					
[E.19] Fugas de información			[7]				
[A.5] Suplantación de la identidad		[7]	[9]	[10]			
[A.6] Abuso de privilegios de acceso		[7]	[9]				
[A.11] Acceso no autorizado		[7]	[9]				
[BDD] Base de datos docentes	[4]	[7]	[9]	[10]			
[E.15] Alteración de la información		[4]					
[E.18] Destrucción de la información	[4]						
[E.19] Fugas de información			[7]				
[A.5] Suplantación de la identidad		[7]	[9]	[10]			
[A.6] Abuso de privilegios de acceso	[4]	[7]	[9]				
[A.11] Acceso no autorizado		[7]	[9]				
[RP] Documentación interna		[7]	[9]	[9]			
[RPO] Reportes		[7]	[9]	[9]			
[MG] Módulo de gestión académica							
[SR] Servicios	[10]	[10]	[10]	[9]	[10]		
[Int] Internet	[10]	[10]	[10]	[9]	[9]		
[I.8] Fallo de servicios de comunicaciones	[10]						
[E.15] Alteración de la información		[7]					
[E.18] Destrucción de la información	[7]						
[E.19] Fugas de información			[7]				
[A.5] Suplantación de la identidad		[10]	[10]	[9]			
[A.13] Repudio (negación de actuaciones)					[9]		
[A.15] Modificación de la información		[9]					
[A.18] Destrucción de la información	[9]						
[A.19] Revelación de información			[9]				
[A.24] Denegación de servicio	[9]						
[PWEB] Portal Web	[9]	[9]	[9]	[9]	[9]		
[E.1] Errores de los usuarios	[7]	[7]	[7]				
[E.2] Errores del administrador del sistema / de la seguridad	[8]	[8]	[8]				
[E.15] Alteración de la información		[4]					
[E.18] Destrucción de la información	[7]						
[E.19] Fugas de información			[7]				
[E.24] Caída del sistema por agotamiento de recursos	[9]						
[A.5] Suplantación de la identidad		[9]	[9]	[9]			
[A.6] Abuso de privilegios de acceso	[4]	[7]	[7]	[9]			
[A.7] Uso no previsto	[4]	[7]	[7]				
[A.11] Acceso no autorizado		[7]	[9]	[9]			
[A.13] Repudio (negación de actuaciones)					[9]		
[A.15] Modificación de la información		[9]					
[A.18] Destrucción de la información	[9]						
[A.24] Denegación de servicio	[9]						
[PDOC] Portafolio de docentes	[9]	[9]	[9]	[9]	[10]		
[E.1] Errores de los usuarios	[7]	[7]	[7]				
[E.2] Errores del administrador del sistema / de la seguridad	[8]	[8]	[8]				
[E.15] Alteración de la información		[4]					
[E.18] Destrucción de la información	[7]						
[E.19] Fugas de información			[7]				
[E.24] Caída del sistema por agotamiento de recursos	[9]						
[A.5] Suplantación de la identidad		[9]	[9]	[9]			

Figura 80: Impacto acumulado

Fuente: Propia

2.7.10. Riesgo acumulado.

A continuación, en la figura 81, se muestra el riesgo acumulado en los activos del sistema académico.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{7,2}	{7,2}	{8,1}	{7,7}	{7,4}		
[AINFO] Activos de información	{4,2}	{6,8}	{8,1}	{7,7}			
[BDE] Base de datos estudiantes		{6,8}	{8,1}	{7,7}			
[BDD] Base de datos docentes	{4,2}	{6,8}	{8,1}	{7,7}			
[RP] Documentación interna		{6,8}	{8,1}	{7,1}			
[MG] Módulo de gestión académica							
[SR] Servicios	{7,2}	{7,2}	{6,3}	{6,2}	{7,4}		
[Int] Internet	{6,8}	{6,3}	{6,3}	{5,6}	{6,2}		
[PWEB] Portal Web	{7,2}	{7,2}	{6,3}	{6,2}	{6,9}		
[PDOC] Portafolio de docentes	{7,2}	{7,2}	{6,3}	{6,2}	{7,4}		
[PST] Portafolio Estudiantes	{7,2}	{7,2}	{6,3}	{6,2}	{6,9}		
[NOT] Consulta de notas	{7,2}	{7,2}	{6,3}	{6,2}	{6,9}		
[E] Equipamiento	{7,2}	{6,8}	{8,1}	{7,7}			
[SW] Aplicaciones	{6,8}	{6,8}	{8,1}	{7,7}			
[HW] Equipos	{7,2}	{6,8}	{6,8}				
[COM] Comunicaciones	{7,2}	{5,6}	{6,3}	{6,2}			
[AUX] Elementos auxiliares	{6,8}	{5,1}	{6,3}				
[L] Instalaciones	{6,8}						
[AD] Area de desarrollo	{6,8}						
[AS] Area de seguridad	{6,8}						
[DT] Data Center	{6,8}						
[P] Personal	{6,3}	{6,8}	{7,2}				
[DTI] Director del departamento de informática	{6,3}	{6,8}	{7,2}				
[E.15] Alteración de la información		{5,1}					
[E.18] Destrucción de la información	{3,3}						
[E.19] Fugas de información			{5,1}				
[E.28] Indisponibilidad del personal	{5,1}						
[A.15] Modificación de la información		{6,3}					
[A.18] Destrucción de la información	{5,1}						
[A.19] Revelación de información			{7,2}				
[A.28] Indisponibilidad del personal	{5,3}						
[A.29] Extorsión	{6,3}	{6,8}	{6,8}				
[A.30] Ingeniería social (picaresca)	{6,0}	{6,6}	{6,6}				
[DOC] Docentes	{6,0}	{6,3}	{6,5}				
[E.15] Alteración de la información		{5,1}					
[E.18] Destrucción de la información	{3,3}						
[E.19] Fugas de información			{5,1}				
[E.28] Indisponibilidad del personal	{5,1}						
[A.15] Modificación de la información		{6,3}					
[A.18] Destrucción de la información	{5,1}						
[A.19] Revelación de información			{6,5}				
[A.28] Indisponibilidad del personal	{6,0}						
[A.29] Extorsión	{5,0}	{5,6}	{5,6}				
[A.30] Ingeniería social (picaresca)	{4,8}	{5,3}	{5,3}				
[EST] Estudiantes	{6,0}	{6,3}	{6,5}				
[ASIS] Analista de Sistemas	{6,3}	{6,8}	{7,2}				
[DPI] Director de proyectos informáticos	{6,3}	{6,3}	{6,3}				
[DES] Desarrolladores de software	{5,3}	{6,8}	{7,2}				
[ADM] Administrador de red y seguridad	{6,3}	{6,8}	{7,2}				
[ASW] Administrador de sitios web	{6,3}	{6,8}	{7,2}				
[ABDD] Administrador de base de datos	{6,3}	{6,8}	{7,2}				

Figura 81: Riesgo acumulado

Fuente: Propia

2.7.11. Situación actual del sistema académico.

A continuación, en la figura 82, se muestra la situación actual del sistema académico, además de la situación objetivo que plantea PILAR al adoptar las salvaguardas.

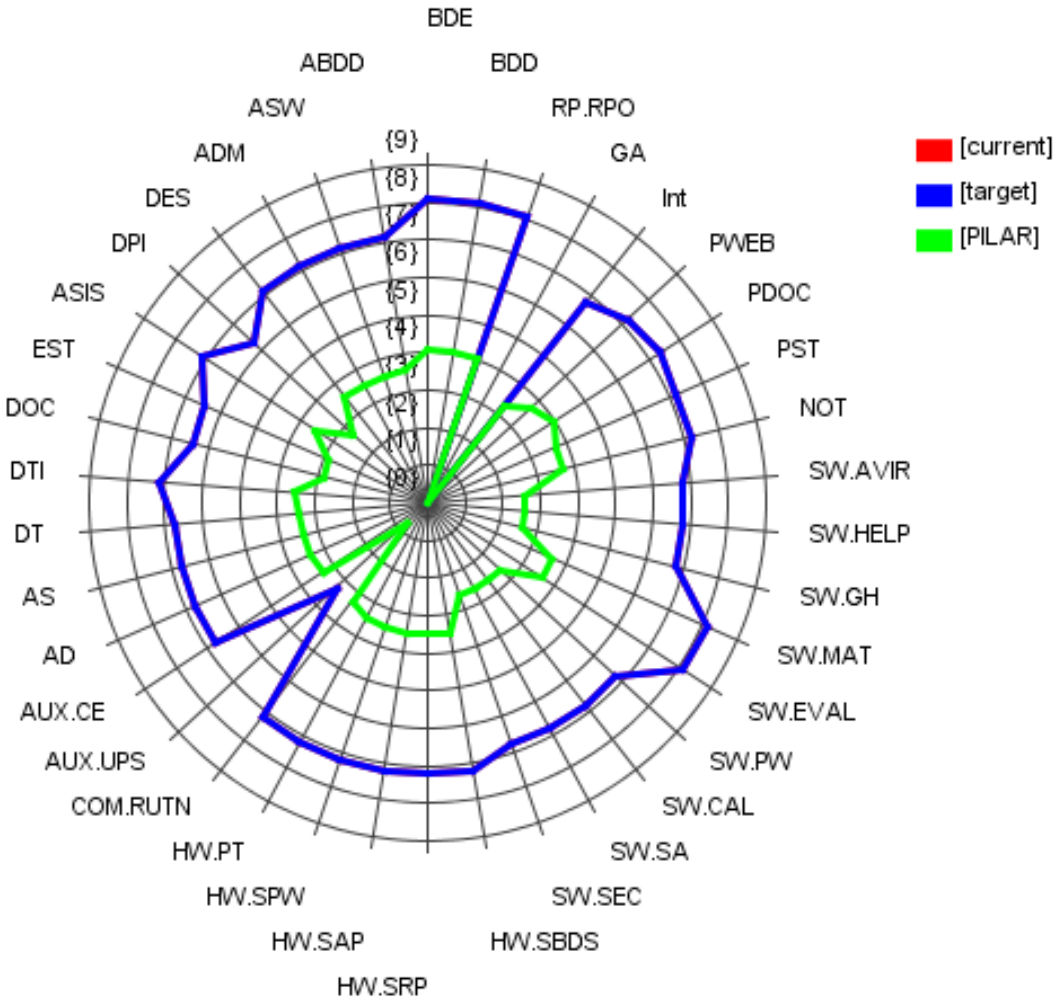


Figura 82: Situación actual del riesgo acumulado del sistema académico.

Fuente: Propia

CAPÍTULO 3

INFORME DE RESULTADOS

En esta sección se procede a evaluar el cumplimiento de seguridad de la información del sistema académico de la Universidad Técnica del Norte enfocado a grandes volúmenes de datos. La ISO/IEC 27007:2017 proporciono una guía para llevar a cabo la auditoría, usando los controles de la norma ISO/IEC 27002:2017, misma que proporciona una base de controles para la evaluación.

A lo largo de la presente investigación se identificaron los activos, las amenazas y vulnerabilidades del sistema académico, la información hallada será de utilidad para identificar las oportunidades y posibilidades de mejora.

3.1. Evaluación de cumplimiento

Es importante verificar el cumplimiento de los controles de la norma ISO/IEC 27002:2017 para comprobar que los datos que maneja el sistema académico de la UTN se encuentran seguros. De esta forma es posible conocer si la UTN garantiza los parámetros de seguridad de los usuarios de esta. Además, la comprobación del cumplimiento de la norma ISO/IEC 27002:2017 es uno de los parámetros necesarios para Big Data.

Para la evaluación del cumplimiento se hace referencia a los controles de seguridad de la información descritos en la norma ISO/IEC 27002:2017, para la revisión del cumplimiento se sigue los procedimientos de la norma ISO/IEC 27007:2017. A continuación, se presenta el check list creado para la evaluación del cumplimiento.

Tabla 31. Cumplimiento de controles ISO/IEC 27002/2017

Aspecto general	**5**	**Políticas de seguridad de la información**	Cumplimiento		Observaciones
Objetivo de control	**5.1**	Dirección de gestión de seguridad de la información.	**SI**	**NO**	
Controles	5.1.1	Políticas de seguridad de la información	X		Se evidencia un plan de desarrollo informático UTN 2018-2022. El documento describe algunas políticas de seguridad de la información con base al plan de desarrollo informático de la UTN.
	5.1.2	Revisión de las políticas para la seguridad de la información.	X		Existen revisión de las políticas de seguridad de la información, pero no se evidencia por escrito.
Aspecto general	**6**	**Organización de la seguridad de la información**	**Cumplimiento**		**Observaciones**
Objetivo de control	**6.1**	Organización interna	**SI**	**NO**	
Controles	6.1.1	Roles y responsabilidades de seguridad de la información	X		Existe roles y responsabilidades definidos para los miembros del personal del departamento de informática de la UTN, sin embargo, algunas actividades se desarrollan de manera esporádica.

	6.1.2	Separación de funciones	X		Cada integrante del departamento de informática DDTI, posee responsabilidades definidas en cuanto a los activos y software
	6.1.3	Contacto con las autoridades	X		Los usuarios del sistema académico pueden establecer contacto con los miembros del DDTI mediante la plataforma QUIPUX
	6.1.4	Contacto con los grupos de interés especial		X	No existe contacto con proveedores importantes en cuanto a la seguridad de la información.
	6.1.5	Gestión de proyectos de seguridad de la información		X	No se evidencia que exista la inclusión de la seguridad de la información para nuevos proyectos que se podrían implementar en el sistema académico.
Objetivo de control	**6.2**	Dispositivos móviles y teletrabajo	**SI**	**NO**	**Observaciones**
Control	6.2.1	Política de dispositivos móviles		X	El sistema académico no posee políticas para el ingreso al sistema académico mediante dispositivos móviles.

Aspecto general	**7**	**Seguridad en recursos humanos**	**Cumplimiento**		**Observaciones**
Objetivo de control	**7.1**	Antes del empleo	**SI**	**NO**	
Controles	7.1.1	Investigaciones de antecedentes	X		Para el ingreso de una persona nueva al departamento del DDTI, la UTN solicita la respectiva hoja de vida con todos los documentos habilitantes.
	7.1.2	Términos y condiciones de empleo		X	En el contrato de trabajo no se detalla las funciones específicas que va a realizar el nuevo miembro del DDTI.
Objetivo de control	**7.2**	Durante el empleo	**SI**	**NO**	**Observaciones**
Controles	7.2.1	Responsabilidades de la dirección	X		El DDTI posee un manual de funciones, en el documento se detallan los roles y responsabilidades, así como la confidencialidad.
	7.2.2	Concienciación, educación y formación en seguridad de la información.		X	No existe un plan de capacitación adecuado, referente al tema de seguridad de la información.

	7.2.3	Proceso disciplinario		X	El DDTI no dispone de un proceso establecido para sancionar a los miembros que hayan infringido o atentado contra la seguridad de la información.
Objetivo de control	**7.3**	Finalización o cambio de empleo	**SI**	**NO**	**Observación**
	7.3.1	Responsabilidades ante la finalización o cambio de empleo		X	La UTN no dispone de un procedimiento establecido para el seguimiento en cuanto a la confidencialidad de la información, una vez finalizado el contrato de empleo.
Aspecto general	**8**	**Gestión de activos**	**Cumplimiento**		**Observaciones**
Objetivo de control	**8.1**	Responsabilidad de los activos	**SI**	**NO**	
Controles	8.1.1	Inventario de activos	X		Existe un inventario a detalle de los diferentes activos presentes en los diversos módulos que posee el sistema académico.
	8.1.2	Propiedad de los activos	X		Existe un encargado de los activos del sistema académico, sin embargo, no existe un propietario de estos.

	8.1.3	Uso aceptable de los activos	X		Existen algunos miembros del DDTI encargado del manejo exclusivo de la información del sistema académico.
	8.1.4	Devolución de activos	X		Existe un registro directo de los activos que son devueltos al DDTI.
Aspecto general	**8.2**	Clasificación de la información	**SI**	**NO**	**Observaciones**
Controles	8.2.1	Clasificación de la información		X	La información que es ingresada al sistema académico no tiene una clasificación adecuada para su almacenamiento ordenado.
	8.2.2	Etiquetado de la información	X		Existen etiquetas que identifican a cada grupo de datos ingresados en el sistema académico.
	8.2.3	Manejo de los activos		X	No existe un procedimiento definido para el procesamiento, almacenado y comunicación de la información del sistema académico.

Aspecto general	**9**	**Control de acceso**	**Cumplimiento**		**Observaciones**
Objetivo de control	**9.1**	Requisitos de acceso para el control de acceso.	**SI**	**NO**	
Controles	9.1.1	Política de control de acceso		X	No se evidencia políticas de control de acceso para el sistema académico de la UTN.
	9.1.2	Acceso a redes y servicios de red		X	No existe políticas para el acceso a la red de la UTN.
Objetivo de control	**9.2**	Gestión de acceso de los usuarios	**SI**	**NO**	**Observaciones**
Controles	9.2.1	Registro y retiro de usuario	X		El DDTI realiza una revisión permanente de los usuarios mediante el módulo de auditorio del sistema académico.
	9.2.2	Provisión de acceso a usuarios		X	No existe un procedimiento para la prohibición de acceso a los usuarios del sistema académico.
	9.2.3	Gestión de privilegios de derechos de acceso.	X		Existe una gestión de privilegios de acceso, controlado por el servidor de BD.
	9.2.4	Gestión de la información secreta de autentificación de los usuarios		X	No existe políticas de confidencialidad para proteger las claves de los usuarios.

	9.2.5	Revisión de los derechos de acceso de usuario		X	No existe un seguimiento de accesos usuarios que ya nos son parte de la institución.
	9.2.6	Retiro y ajuste de los derechos de acceso		X	No se elimina las cuentas de acceso al sistema académico, una vez que los estudiantes ya no son parte de la UTN.
Objetivo de control	**9.3**	Responsabilidades de los usuarios	**SI**	**NO**	**Observación**
Control	9.3.1	Uso de la información secreta de autentificación		X	No se evidencia un proceso definido para el ingreso al sistema académico. Las claves las administra el servidor de BD.
Objetivo de control	**9.4**	Control de acceso a sistemas y aplicaciones	**SI**	**NO**	**Observaciones**
Controles	9.4.1	Restricción de acceso a la información.	X		Existe una restricción de acceso según el nivel de privilegios de usuario
	9.4.2	Procedimientos seguros de inicio de sesión		X	No existe una política que garantice el acceso seguro al sistema académico. El ingreso se lo hace mediante contraseña.

	9.4.3	Sistemas de gestión de contraseñas		X	Las contraseñas son gestionadas por la BD y no existe una política para ello.
	9.4.4	Uso de programas utilitarios privilegiados		X	El acceso a las funcionalidades de los computadores es total, sin ningún tipo de restricción.
	9.4.5	Control de acceso al código fuente del programa	X		Solo los miembros del DDTI autorizados tienen acceso al código fuente del sistema académico.
Aspecto general	**10**	**Criptografía**	**Cumplimiento**		**Observaciones**
Objetivo de control	**10.1**	Controles criptográficos	**SI**	**NO**	
Controles	10.1.1	Política de uso de los controles criptográficos	X		Existe procedimientos documentados en el sistema de gestión de procesos.
	10.1.2	Gestión de llaves		X	Las llaves se gestión directamente en la base de datos según su configuración. No existe ninguna política que respalde la creación de llaves.

Aspecto general	11	Seguridad Física y de entorno	Cumplimiento		Observaciones
Objetivo de control	**11.1**	Áreas seguras	**SI**	**NO**	
Controles	11.1.1	Perímetro de seguridad física	X		Existe un área exclusiva para el alojamiento del equipamiento físico, correspondiente al sistema académico.
	11.1.2	Controles físicos de entrada	X		Se evidencia un biométrico de acceso para los miembros del DDTI.
	11.1.3	Seguridad de oficinas, despachos e instalaciones	X		Existe un área exclusiva para el DDTI, aislado de los estudiantes.
	11.1.4	Protección contra amenazas externas y ambientales		X	No existe procedimientos definidos contra eventualidades externas.
	11.1.5	Trabajo en áreas seguras	X		Existe un Área predefinida para el desarrollo de software
	11.1.6	Áreas de carga y entrega	X		El Área de desarrollo está separado del Área de carga y entrega.

Objetivo de control	11.2	Equipos	SI	NO	Observaciones
Controles	11.2.1	Ubicación y protección de equipos		X	No existe políticas para la prohibición de alimentos en los puestos de trabajo.
	11.2.2	Instalaciones de suministro		X	No existe redundancia eléctrica para garantizar la continuidad de operación del DDTI.
	11.2.3	Seguridad del cableado	X		Se evidencia un cableado estructurado resistente a daños.
	11.2.4	Mantenimiento de los equipos	X		Se evidencia un plan de mantenimiento específico para el DATA CENTER. Además, existe un convenio con proveedores externos para la reparación de posibles fallas.
	11.2.5	Eliminación de activos		X	No existe un procedimiento defino para la eliminación de activos.
	11.2.7	Reutilización o eliminación segura de equipos		X	No existe un procedimiento definido para la eliminación de software en activos devueltos.

	11.2.8	Equipos de usuario desatendido		X	No existe evidencia de la protección y almacenamiento adecuado de los activos sin usar.
	11.2.9	Política de puesto de trabajo despejado y pantalla limpia		X	No existe una protección de computadores sin actividad durante un tiempo determinado.

Aspecto general	**12**	**Seguridad de las operaciones**	**Cumplimiento**		
Objetivo de control	**12.1**	Procedimientos y responsabilidades operacionales	**SI**	**NO**	**Observaciones**
Controles	12.1.1	Documentación de procedimientos de operación	X		Existe propuestas de trabajos de pregrado referentes a los procedimientos de operación.
	12.1.2	Gestión de cambios	X		Para posibles cambios existe una planificación en base a la retroalimentación que ofrece la plataforma Quipux.
	12.1.3	Gestión de capacidades	X		Las funciones designadas a los miembros del DDTI son diseñadas para evitar los cambios masivos.

	12.1.4	Separación de ambientes de desarrollo, pruebas y producción	X		Se evidencia que el ambiente de desarrollo y producción se encuentran separados, sin embargo, el ambiente de pruebas es el mismo sitio de trabajo por la naturaleza de la actividad.
Objetivo de control	**12.2**	Protección de malware	**SI**	**NO**	**Observación**
Control	12.2.1	Controles contra un malware	X		La UTN posee Eset EndPoint corporativos, además existe un firewall para el acceso a internet.
Objetivo de control	**12.3**	Copias de seguridad	**SI**	**NO**	**Observación**
Control	12.3.1	Copias de seguridad de la información	X		Las copias de seguridad se realizan a diario. Además, se realiza copias de seguridad semestralmente.
Objetivo de control	**12.4**	Registros y monitoreo	**SI**	**NO**	**Observaciones**
Controles	12.4.1	Registro de eventos		X	No existe un procedimiento definido para el registro de eventos.
	12.4.2	Protección de la información de registro	X		Se protege los registros contra accesos no autorizados.

	12.4.3	Registros de administración y operación		X	No existe una revisión planificada de las actividades de los administradores del sistema académico.
	12.4.4	Sincronización de reloj	X		Todos los dispositivos del sistema académico se encuentran sincronizados con la misma hora.
Objetivo de control	**12.5**	Control de software operacional	**SI**	**NO**	**Observaciones**
Control	12.5.1	Instalación del software en los sistemas operativos	X		La UTN posee sistemas operativos con sus respectivas licencias.
Objetivo de control	**12.6**	Gestión de la vulnerabilidad técnica	**SI**	**NO**	**Observaciones**
Controles	12.6.1	Gestión de vulnerabilidades técnicas		X	No existe procedimientos para fallos técnicos. En caso de fallar el sistema académico no existe herramientas de backup.
	12.6.2	Restricción en la instalación del software		X	No existe restricciones para la instalación de software no permitido en los dispositivos del sistema académico.

Objetivo de control	**12.7**	Consideraciones sobre la auditoría de sistemas de información	**SI**	**NO**	**Observación**
Control	12.7.1	Controles de auditoría de sistemas de información	X		Las auditorias está gestionado por el módulo de auditoría. Todo el proceso se encuentra documentado en trabajos de pregrado.
Aspecto general	**13**	**Seguridad en las telecomunicaciones**	**Cumplimiento**		**Observaciones**
Objetivo de control	**13.1**	Gestión de la seguridad de redes	**SI**	**NO**	
Controles	13.1.1	Controles de red	X		El control mediante el portal educativo, empleando filtrado MAC.
	13.1.2	Seguridad de los servicios de red	X		Los servicios de red cuentan con seguridad CISCO ASA.
	13.1.3	Separación en las redes	X		La red de la UTN es segmentada en varias VLAN.
Aspecto general	**14**	**Adquisición, desarrollo y mantenimiento del sistema**	**Cumplimiento**		**Observaciones**
Objetivo de control	**14.1**	Requisitos de seguridad de los sistemas de información	**SI**	**NO**	
Control	14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	X		Los registros de seguridad de la información se documentan en los manuales de procedimientos de desarrollo.

Objetivo de control	**14.2**	Seguridad en el desarrollo en los procesos de soporte	**SI**	**NO**	**Observaciones**
Controles	14.2.1	Política de desarrollo seguro	X		La metodología RUP es empleada para el desarrollo del sistema académico.
	14.2.2	Procedimientos de control de cambios en sistemas	X		Los futuros cambios se gestionan con el módulo de planificación del sistema integral informático
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo		X	No existe un procedimiento establecido para las pruebas del sistema académico tras modificarlo de alguna forma.
Objetivo de control	14.3	Datos de prueba	**SI**	**NO**	**Observación**
Control	14.3.1	Protección de los datos de prueba		X	No existe directrices para usar datos reales en las pruebas de software.

Aspecto general	**15**	**Relaciones con proveedores**	**Cumplimiento**		
Objetivo de control	**15.1**	Gestión de la provisión de servicios del proveedor	**SI**	**NO**	**Observaciones**
Controles	15.1.1	Monitoreo y revisión de los servicios de proveedores		X	No existe un procedimiento para el seguimiento de proveedores externos.

	15.1.2	Gestión de cambios en los servicios de proveedores	X		Los contratos de proveedores se encuentran en proveeduría.
Aspecto general	**16**	**Gestión de incidentes de seguridad de la información**	**Cumplimiento**		**Observaciones**
Objetivo de control	**16.1**	Gestión de los incidentes de seguridad de la información y mejora	**SI**	**NO**	
Controles	16.1.1	Responsabilidades y procedimientos		X	El software Help Desk que posee la UTN no lo tiene implementado.
	16.1.2	Informe de los eventos de seguridad de la información		X	No existe un proceso definido para la recopilación de errores del sistema académico de la UTN.
	16.1.3	Informe de debilidades de seguridad de la información		X	No existe un procedimiento establecido para el informe de errores por parte de los proveedores.
	16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información		X	No existe un análisis de los incidentes ocurridos para clasificarlos como incidentes o errores.

	16.1.5	Respuesta a incidentes de seguridad de la información	X		Los posibles incidentes y errores se manejan bajo la plataforma Quipux.
	16.1.6	Aprendizaje de los incidentes de seguridad de la información		X	No existe una revisión detallada de los incidentes para crear un plan de mejora en base errores.
	16.1.7	Recopilación de evidencias	X		Los incidentes son recopilados por la plataforma Quipux
Aspecto general	**17**	**Aspectos de seguridad de la información para la gestión de la continuidad del negocio**	**Cumplimiento**		**Observaciones**
Objetivo de control	**17.1**	Continuidad de seguridad de la información	**SI**	**NO**	
Controles	17.1.1	Planificación de la continuidad de seguridad de la información		X	El plan de continuidad presente es a baja escala, no se toma en cuenta catástrofes, danos, tampoco la seguridad de la información.
	17.1.2	Implementación de la continuidad de seguridad de la información		X	No existe un plan de continuidad de seguridad de la información en base a eventos adversos.
	17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información.		X	No existe una evaluación de la efectividad de la seguridad de la información

Objetivo de control	**17.2**	Redundancias	**SI**	**NO**	**Observación**
Control	17.2.1	Disponibilidad de las instalaciones de procesamiento de la información		X	La UTN no dispone de infraestructura necesaria para brindar redundancia en los elementos esenciales del sistema académico
Aspecto general	**18**	**Cumplimiento**	**Cumplimiento**		
Objetivo de control	**18.1**	Cumplimiento de los requisitos legales contractuales	**SI**	**NO**	**Observaciones**
Controles	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	X		Se aplica el reglamento interno de la UTN y la ley de educación superior.
	18.1.2	Derechos de propiedad intelectual	X		Cada software y trabajo de titulación de la UTN cuenta con documentos de derechos de autor.
	18.1.3	Protección de los registros	X		Toda la información ingresada en el sistema académico es almacenada en una base de datos especifica.
	18.1.4	Protección y privacidad de la información de carácter personal		X	No existe documentos de confidencialidad de la información del sistema académico.

Objetivo de control	18.2	Revisiones de seguridad de la información	SI	NO	Observaciones
Controles	18.2.1	Revisión independiente de seguridad de la información		X	No existe revisión de terceros cuando exista cambios significativos en el sistema académico.
	18.2.2	Cumplimiento de las políticas y normas de seguridad	X		En el DDTI se revisa el cumplimiento de normas de seguridad del personal.
	18.2.3	Comprobación del cumplimiento técnico		X	En el DDTI no se revisa el cumplimiento de procedimientos de seguridad de la información

Fuente: Propia

3.2. Evaluación de resultados de cumplimiento

Como se mencionó anteriormente para comprobar el cumplimiento de los controles de la norma ISO/IEC 27002:2017 se realizó un check list. Los resultados resumidos de los controles evaluados se presentan en la figura 83.

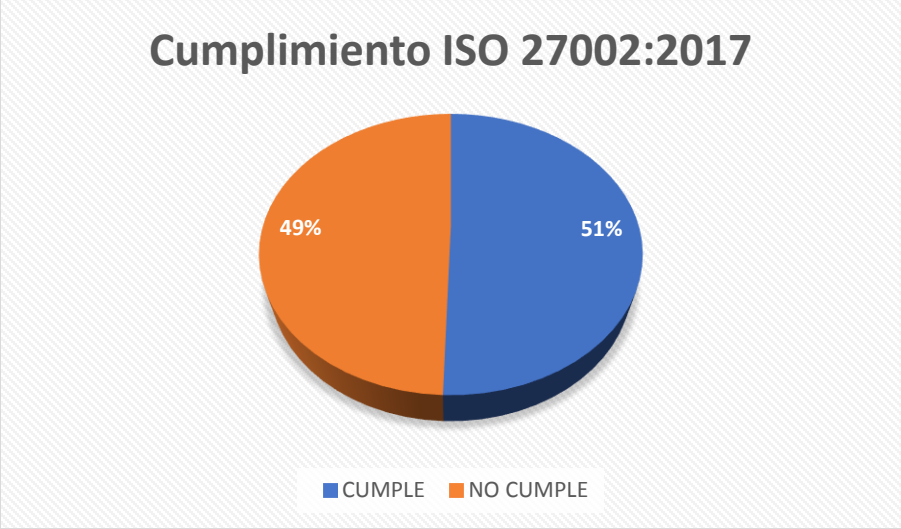


Figura 83: Cumplimiento de controles ISO/IEC 27002:2017.

Fuente: Propia

3.3. Activos de información

La universidad técnica del Norte dispone de varios activos lógicos de información e infraestructura lógica. Los dispositivos que se encontraron fueron los siguientes.

3.4. Infraestructura lógica

La UTN cuenta con servidores.

La UTN dispone de un dispositivo de seguridad perimetral CISCO ASA.

La UTN posee más de 49 zonas de acceso inalámbrico,

La UTN posee redes de comunicación.

La UTN posee un router principal, correspondiente al ISP.

3.5. Sistema de comunicación

La UTN cuenca con una central que administra más de 213 extensiones telefónicas, distribuidas a lo largo del campus.

3.6. Sistemas de seguridad de control de acceso.

La UTN posee varios dispositivos que contribuyen al control de acceso entre ellos destacan:

- Lectores biométricos
- Extintores
- Alarmas
- Cámaras de seguridad

Existe controles de autentificación para ingresar al sistema académico, para docentes y estudiantes, Los docentes poseen un ping, mismo que se envía al correo institucional. Los estudiantes cuentan una clave de 5 dígitos, correspondientes a los 5 últimos dígitos del carné.

3.7. Dispositivos de computo

La UTN cuenta con más de 1000 computadores, distribuidos a lo largo del campus.

3.8. Informe de ejecución

3.8.1. No conformidades

Una no conformidad se refiere al incumplimiento de un requisito o control de una norma establecida como referencia para evaluar un aspecto especifico de una organización. Los requisitos se los conoce como una necesidad o expectativa establecida de carácter obligatorio. Por lo tanto, para el presente caso de estudio se realizará una tabla de no conformidades en la cual se presentará los controles de la norma ISO/IEC 27002:2017 que no cumple el sistema académico en tema de seguridad de la información.

A continuación, en la tabla 32 se presentan las no conformidades encontradas en el sistema académico.

Tabla 32. No conformidades auditoría sistema académico.

Código	Controles	Observación	No conformidad	Recomendación
6.1.4	Contacto con los grupos de interés especial	No existe contacto con proveedores importantes en cuanto a la seguridad de la información	No existe ningún tipo de contacto con grupos especializados en seguridad de la información.	Establecer contacto con grupos especializados en seguridad de la información, mediante boletines foros y propuestas.
6.1.5	Gestión de proyectos de seguridad de la información	No se evidencia que exista la inclusión de la seguridad de la información para nuevos proyectos que se podrían implementar en el sistema académico.	En los proyectos tecnológicos futuros a ser implementados, no se toma en cuenta de la seguridad de la información como un aspecto relevante.	Designar a un analista del DDTI para que trabaje en propuestas referente a la seguridad de la información para futuros proyectos.
6.2.1	Política de dispositivos móviles	El sistema académico no posee políticas para el ingreso al sistema académico mediante dispositivos móviles.	No existe ninguna política de acceso para estudiantes que ingresen al sistema académico desde sus móviles.	Crear una política tomando en cuenta el acceso al sistema académico desde dispositivos móviles.
7.1.2	Términos y condiciones de empleo	En el contrato de trabajo no se detalla las funciones específicas que va a realizar el nuevo miembro del DDTI.	El sistema de contratación está bien definido, sin embargo, no existe la especificación a detalle de las actividades a desarrollar en el DDTI.	Detallar de forma adecuada en los términos y condiciones del contrato del nuevo trabajador, que actividades va a desarrollar en el DDTI.

7.2.2	Concienciación, educación y formación en seguridad de la información.	No existe un plan de capacitación adecuado, referente al tema de seguridad de la información.	No existe concienciación acerca de la seguridad de la información a los usuarios del sistema académico	Elaborar un plan de capacitación enfocado a la seguridad de la información. Además, documentar todo lo registrado.
7.2.3	Proceso disciplinario	El DDTI no dispone de un proceso establecido para sancionar a los miembros que hayan infringido o atentado contra la seguridad de la información	No existe sanciones para empleados que violen de alguna forma la seguridad de la información del sistema académico.	Elaborar el proceso disciplinario riguroso para empleados que incumplan las políticas de seguridad. Además, documentar las evidencias.
7.3.1	Responsabilidades ante la finalización o cambio de empleo	La UTN no dispone de un procedimiento establecido para el seguimiento en cuanto a la confidencialidad de la información, una vez finalizado el contrato de empleo.	No existe evidencias en cambios de personal del DDTI	Crear un plan para el cambio o cese de cambios de personal del DDTI. Documentar el proceso de forma ordenada.
8.2.1	Clasificación de la información	La información que es ingresada al sistema académico no tiene una clasificación adecuada para su almacenamiento ordenado.	La información se almacena de forma unificada	Clasificar la información previa al almacenamiento en la BD, para facilitar el procesamiento posterior de la información.

8.2.3	Manejo de los activos	No existe un procedimiento definido para el procesamiento, almacenado y comunicación de la información del sistema académico	No se encontró un procedimiento para la recolección y almacenamiento de la información	Crear procedimientos debidamente documentados para el manejo de activos de información.
9.1.1	Política de control de acceso	No se evidencia políticas de control de acceso para el sistema académico de la UTN.	No existe evidencias de políticas para el control de acceso para el sistema académico.	Crear o adaptar políticas de seguridad de la información de forma exclusiva para el sistema académico.
9.1.2	Acceso a redes y servicios de red	No existe políticas para el acceso a la red de la UTN.	No existe control de acceso a las redes de la UTN.	Crear un plan de acceso a la red de la UTN.
9.2.2	Provisión de acceso a usuarios	No existe un procedimiento para la prohibición de acceso a los usuarios del sistema académico.	No se evidencia una política de prohibición de acceso a ciertos usuarios del sistema académico.	Crear una política para la prohibición de usuarios según condiciones.
9.2.4	Gestión de la información secreta de autentificación de los usuarios	No existe políticas de confidencialidad para proteger las claves de los usuarios.	No existe evidencia de la información de los usuarios del sistema académico	Crear un documento de confidencialidad para que los empleados se comprometan a la confidencialidad de los datos.
9.2.5	Revisión de los derechos de acceso de usuario	No existe un seguimiento de accesos usuarios que ya nos son parte de la institución.	No existe una revisión de los usuarios que ya no son parte de la institución.	Crear un plan de seguimiento de usuarios del sistema académico.

9.2.6	Retiro y ajuste de los derechos de acceso	No se elimina las cuentas de acceso al sistema académico, una vez que los estudiantes ya no son parte de la UTN.	No se evidencia la eliminación de cuentas de usuarios que ya no son parte de la UTN	Crear un procedimiento para la eliminación de usuarios del sistema académico.
9.3.1	Uso de la información secreta de autentificación	No se evidencia un proceso definido para el ingreso al sistema académico. Las claves las administra el servidor de BD.	No se evidencia ninguna guía para el acceso al sistema académico.	Crear una guía para el ingreso al sistema académico.
9.4.2	Procedimientos seguros de inicio de sesión	No existe una política que garantice el acceso seguro al sistema académico. El ingreso se lo hace mediante contraseña.	No existe mecanismos técnicos de inicio seguro de sesión.	Crear un plan para acceso seguro de usuarios, así como para el desbloqueo de sesiones.
9.4.3	Sistemas de gestión de contraseñas	Las contraseñas son gestionadas por la BD y no existe una política para ello.	No existe una política para la gestión de contraseñas	Crear una política para la creación de contraseñas, para que no sea de forma aleatoria.
9.4.4	Uso de programas utilitarios privilegiados	El acceso a las funcionalidades de los computadores es total, sin ningún tipo de restricción.	Se puede instalar cualquier programa en los computadores de la UTN	Bloquear la instalación de algunos programas de los computadores de la UTN.
10.1.2	Gestión de llaves	Las llaves se gestión directamente en la base de datos según su configuración. No existe ninguna política que respalde la creación de llaves.	No existe políticas ni tampoco gestión de llaves.	Crear una política para la gestión de llaves.

11.1.4	Protección contra amenazas externas y ambientales	No existe procedimientos definidos contra eventualidades externas.	No existe ningún procedimiento para actuar frente a desastres	Crear una guía contra prevención de riesgos frente a desastres.
11.2.1	Ubicación y protección de equipos	No existe políticas para la prohibición de alimentos en los puestos de trabajo.	En los puestos de trabajo existe elementos que pueden dañar los dispositivos. Por ejemplo, bebidas.	Crear una política para prevención y protección de dispositivos de trabajo.
11.2.2	Instalaciones de suministro	No existe redundancia eléctrica para garantizar la continuidad de operación del DDTI.	No existe una fuente de alimentación alternativa para garantizar el funcionamiento continuo.	Adquirir una planta de energía propia, para la selección es posible respaldarlo con un análisis costo beneficio.
11.2.5	Eliminación de activos	No existe un procedimiento defino para la eliminación de activos	Los activos se eliminan de forma inadecuada	Crear procedimientos para la eliminación de activos en cuanto software como hardware.
11.2.7	Reutilización o eliminación segura de equipos	No existe un procedimiento definido para la eliminación de software en activos devueltos.	No existe una eliminación optima de software para los equipos reutilizados.	Crear un procedimiento para la reutilización de equipos, referidos al software o hardware.
11.2.8	Equipos de usuario desatendido	No existe evidencia de la protección y almacenamiento adecuado de los activos sin usar.	Los equipos en desuso se almacenan en un lugar cualquiera.	Asignar un espacio determinado, aislado y con las debidas seguridades.

11.2.9	Política de puesto de trabajo despejado y pantalla limpia	No existe una protección de computadores sin actividad durante un tiempo determinado.	Los computadores no disponen de seguridad durante un periodo de inactividad	Crear procedimientos para seguridad en los puestos de trabajo.
12.4.1	Registro de eventos	No existe un procedimiento definido para el registro de eventos.	No existe planificación para la implementación de Help Desk. No existe un registro documentado de incidentes.	Crear un plan de gestión para la implementación de Help Desk.
12.4.3	Registros de administración y operación	No existe una revisión planificada de las actividades de los administradores del sistema académico.	No existe un monitoreo de los administradores del sistema académico	Crear un plan de monitoreo para controlar a los administradores del sistema académico.
12.6.1	Gestión de vulnerabilidades técnicas	No existe procedimientos para fallos técnicos. En caso de fallar el sistema académico no existe herramientas de backup.	No existe ningún procedimiento para la gestión de vulnerabilidades.	Crear un procedimiento para la gestión de vulnerabilidades de todos los módulos del sistema académico.
12.6.2	Restricción en la instalación del software	No existe restricciones para la instalación de software no permitido en los dispositivos del sistema académico.	Los usuarios tienen acceso completo a todas las características de los computadores de la UTN.	Crear un proceso formal para la estación de software en los computadores de la UTN.
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No existe un procedimiento establecido para las pruebas del sistema académico tras modificarlo de alguna forma.	No existe revisión por un agente externo ante grandes cambios en el sistema académico	Si los cambios en el sistema académico son grandes contratar a un agente externo para comprobar la funcionalidad de los cambios.

14.3.1	Protección de los datos de prueba	No existe directrices para usar datos reales en las pruebas de software.	No existe ningún procedimiento valido para la protección de los datos de prueba.	Crear un procedimiento valido para que los datos de prueba se traten como datos reales en cuanto a la confidencialidad y protección.
15.1.1	Monitoreo y revisión de los servicios de proveedores	No existe un procedimiento para el seguimiento de proveedores externos.	No existe políticas para la seguridad de la información aplicada a los proveedores	Crear políticas y procedimientos para preservar la seguridad de la información por parte de los proveedores.
16.1.1	Responsabilidades y procedimientos	El software Help Desk que posee la UTN no lo tiene implementado.	La UTN posee Help Desk, pero no lo aplica.	Crear un plan de ejecución para que Help Desk sea operativo.
16.1.2	Informe de los eventos de seguridad de la información	No existe un proceso definido para la recopilación de errores del sistema académico de la UTN.	no existe un registro adecuado de incidencias.	Crear procedimientos para la documentación detallada de incidentes ocurridos en el sistema académico.
16.1.3	Informe de debilidades de seguridad de la información	No existe un procedimiento establecido para el informe de errores por parte de los proveedores.	Al no existir un procedimiento para la seguridad de la información para proveedores. Tampoco existe un procedimiento para reportar inconvenientes de seguridad de la información.	Crear procedimientos para que los proveedores entreguen informe de errores en caso de existir.

16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	No existe un análisis de los incidentes ocurridos para clasificarlos como incidentes o errores.	Los inconvenientes que ocurren sobre el sistema académico no son analizados para determinar cómo se lo clasifica	Crear un procedimiento para el análisis de incidentes del sistema académico, con la finalidad de clasificarlos de forma adecuada.
16.1.6	Aprendizaje de los incidentes de seguridad de la información	No existe una revisión detallada de los incidentes para crear un plan de mejora en base errores.	Los incidentes que ocurren se evidencian, pero no se analizan.	Crear un procedimiento para analizar a detalle los errores con el fin de crear soluciones y evitar que se produzca el mismo error.
17.1.1	Planificación de la continuidad de seguridad de la información	El plan de continuidad presente es a baja escala, no se toma en cuenta catástrofes, danos, tampoco la seguridad de la información.	El plan de continuidad carece de solidez	Analizar y crear un nuevo plan de continuidad, tomando en cuenta los factores importantes que no están tomados en cuenta.
17.1.2	Implementación de la continuidad de seguridad de la información	No existe un plan de continuidad de seguridad de la información en base a eventos adversos.	No existe una planificación para la revisión del plan de continuidad de la seguridad de la información.	Crear una planificación para la revisión de las políticas de seguridad de la información.
17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información.	No existe una evaluación de la efectividad de la seguridad de la información	No se asegura la continuidad de seguridad de la información	Establecer un plan que asegure la continuidad de la seguridad de la información.

17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	La UTN no dispone de infraestructura necesaria para brindar redundancia en los elementos esenciales del sistema académico	No existe ningún plan que garantice la continuidad del sistema académico.	Crear un plan de continuidad del sistema académico.
18.1.4	Protección y privacidad de la información de carácter personal	No existe documentos de confidencialidad de la información del sistema académico.	No existe un documento de confidencialidad de los datos del sistema académico.	Crear un documento que garantice la confidencialidad del sistema académico.
18.2.1	Revisión independiente de seguridad de la información	No existe revisión de terceros cuando exista cambios significativos en el sistema académico.	No existe una revisión de agentes independientes al sistema académico.	Designar a una persona para la evaluación de grandes cambios del sistema académico. Si hace falta contratar a terceros
18.2.3	Comprobación del cumplimiento técnico	En el DDTI no se revisa el cumplimiento de procedimientos de seguridad de la información	No existe revisan técnica de los procedimientos relacionados a la seguridad de la información.	Crear un plan para revisar de forma técnica los procedimientos relacionados con la seguridad de la información.

Fuente: Propia

3.8.2. Evaluación de vulnerabilidades de red.

Es necesario realizar un análisis de vulnerabilidades de red del sistema académico de la UTN, para ello se analizó el portafolio de docentes que es parte del sistema en mención, correspondiente al siguiente dominio:

http://cloud1.utn.edu.ec/ords/f?p=116:LOGIN_DESKTOP::::::

La herramienta que se empleó para ejecutar el análisis fue Kali Linux. Esta herramienta es una distribución de la línea de Linux, líder en pruebas de hacking y penetración ética, por ello es muy usado en auditorias de seguridad informática. Kali Linux contiene más de 600 programas para hackeo, entre las cuales destacan nmap para el escaneo de puertos, wireshark el cual es un sniffer entre otros.

Dirección IP

Es necesario hallar la dirección ip del dominio correspondiente al portafolio docente, para ello se ejecuta el comando de la figura 84.

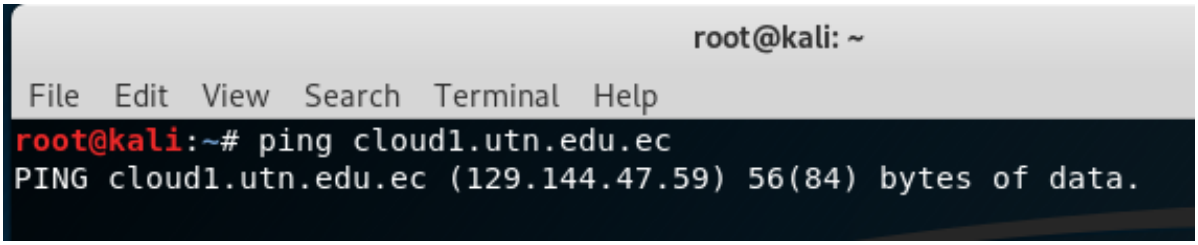


Figura 84: Portafolio docente ip-dominio.

Fuente: Propia

Escaneo de puertos

Una vez obtenida la dirección ip es posible realizar un escaneo de los puertos abiertos, mediante la herramienta zenmap. Esta herramienta es la versión grafica de nmap, es muy útil para ejecutar diferentes tipos de análisis de puertos.

A continuación, en la figura 85 se observa la elección del análisis en zenmap.

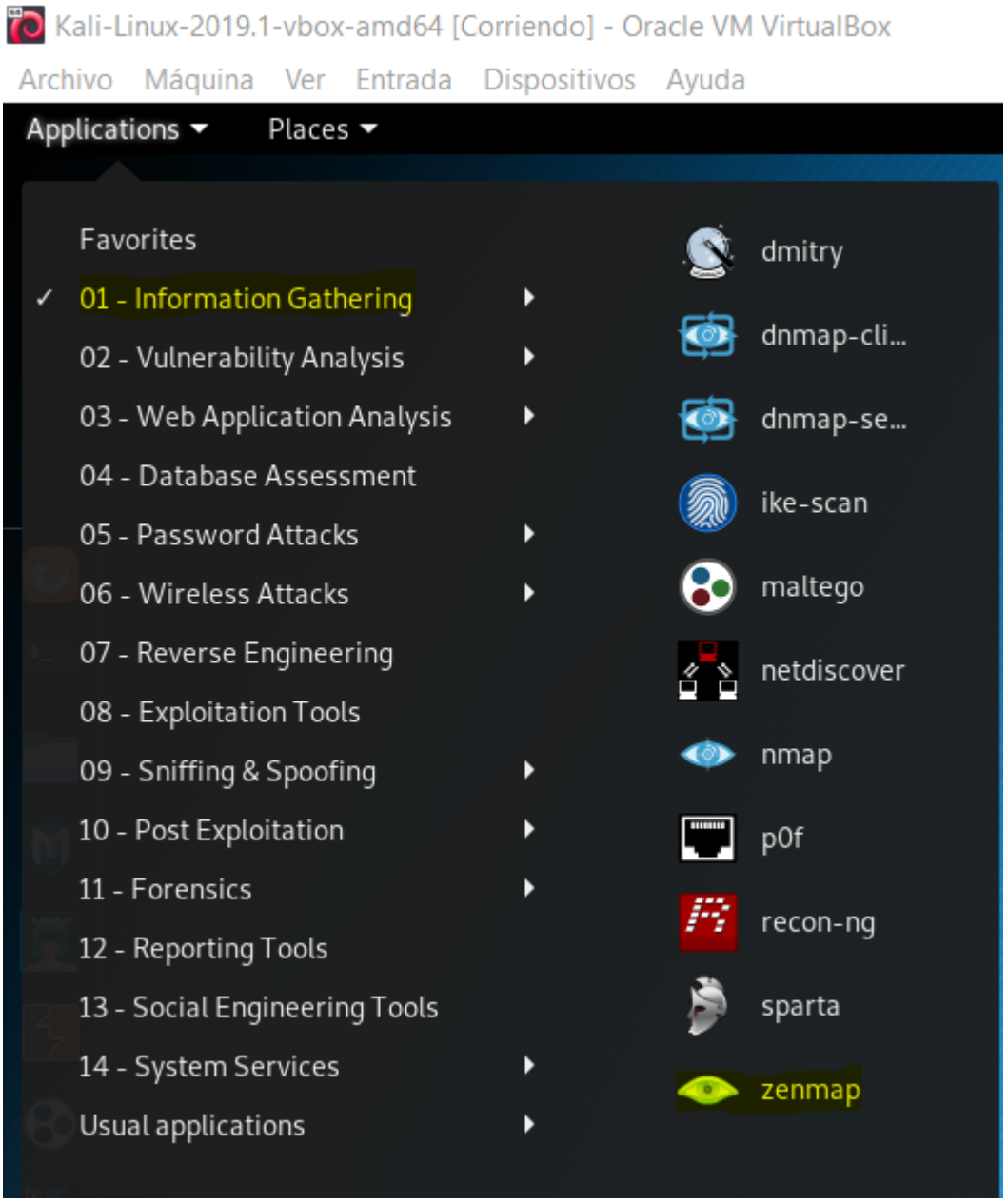


Figura 85: Opciones análisis zenmap.

Fuente: Propia

Para ejecutar el análisis se escogió un escaneo intenso, la sintaxis del comando es:

Comando: nmap -T4 -A -v <dirección>

Este comando inicia un análisis razonablemente rápido, T4 indica a la herramienta que escanee los puertos TCP más comunes. -A indica al programa que identifique los servicios, versiones y el sistema operativo. -v nos da información variada a medida que el análisis avance. A continuación, en la figura 86 se presenta la ejecución del análisis.

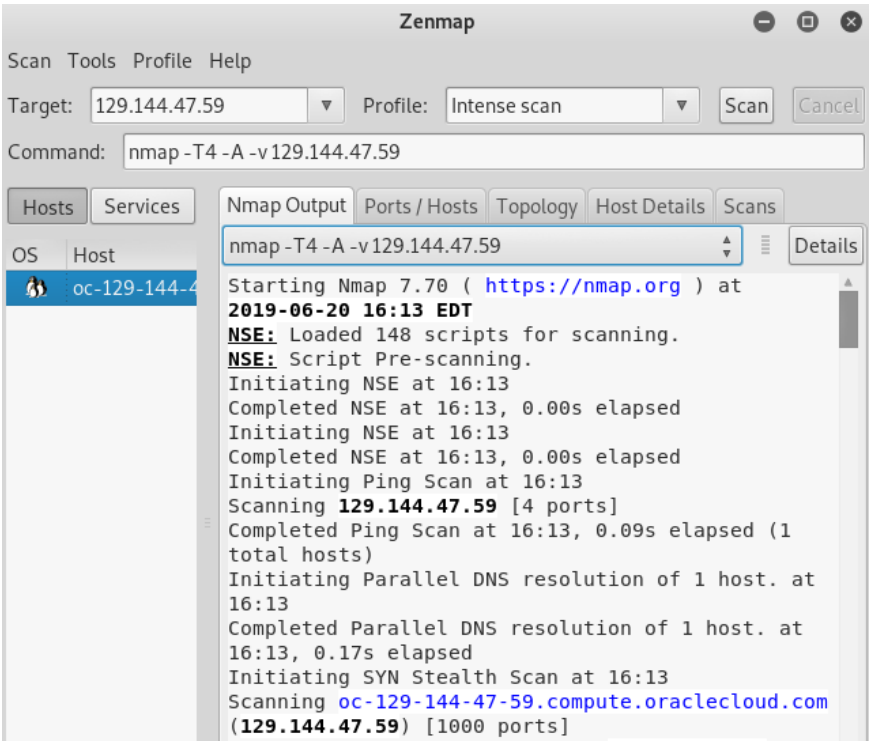


Figura 86: Ejecución de análisis en zenmap.

Fuente: Propia

Como resultado del escaneo se encontró algunos puertos abiertos, mismos que se pueden observar en la figura 87.

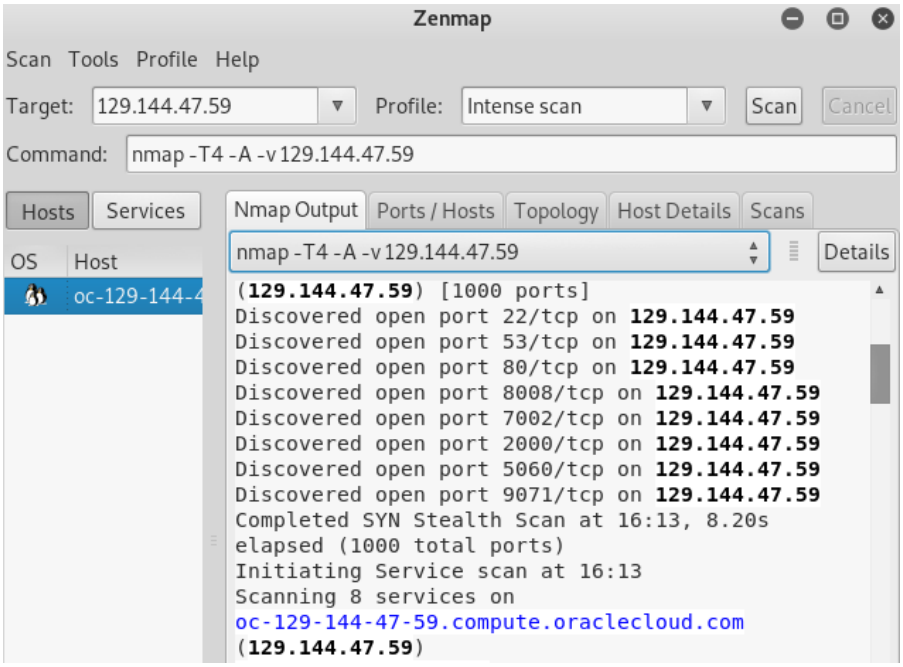


Figura 87: Puertos abiertos en zenmap.

Fuente: Propia

La herramienta proporciona un informe detallado del estado del puerto(abierto-cerrado), el servicio que ofrece y la versión del servicio como se observa en la figura 88.

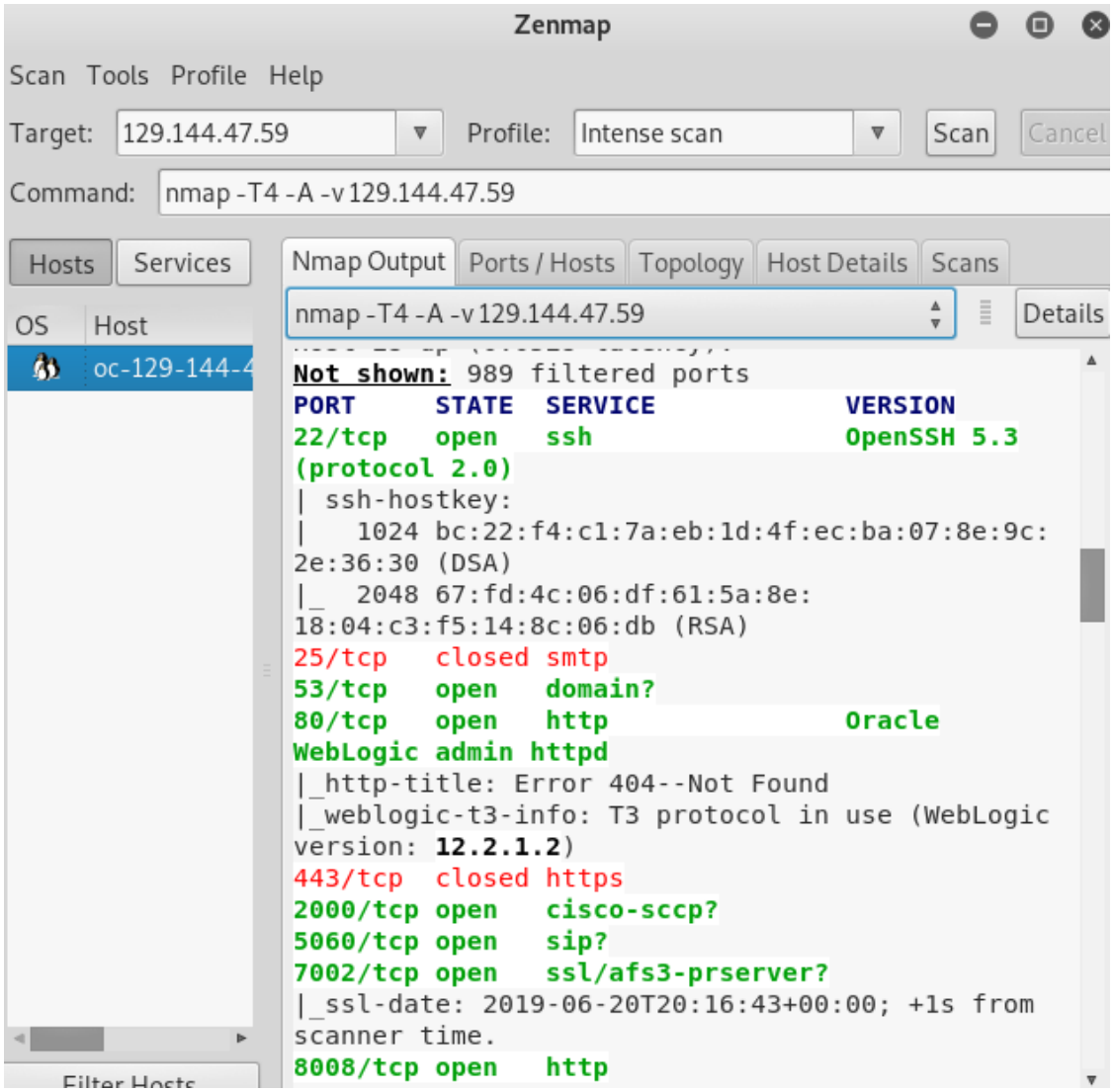


Figura 88: Detalle de puertos abiertos en zenmap.

Fuente: Propia

En el informe final fue posible constatar que existen 11 puertos de los cuales 8 se encuentran abiertos y 3 cerrados como se puede observar en la figura 89.

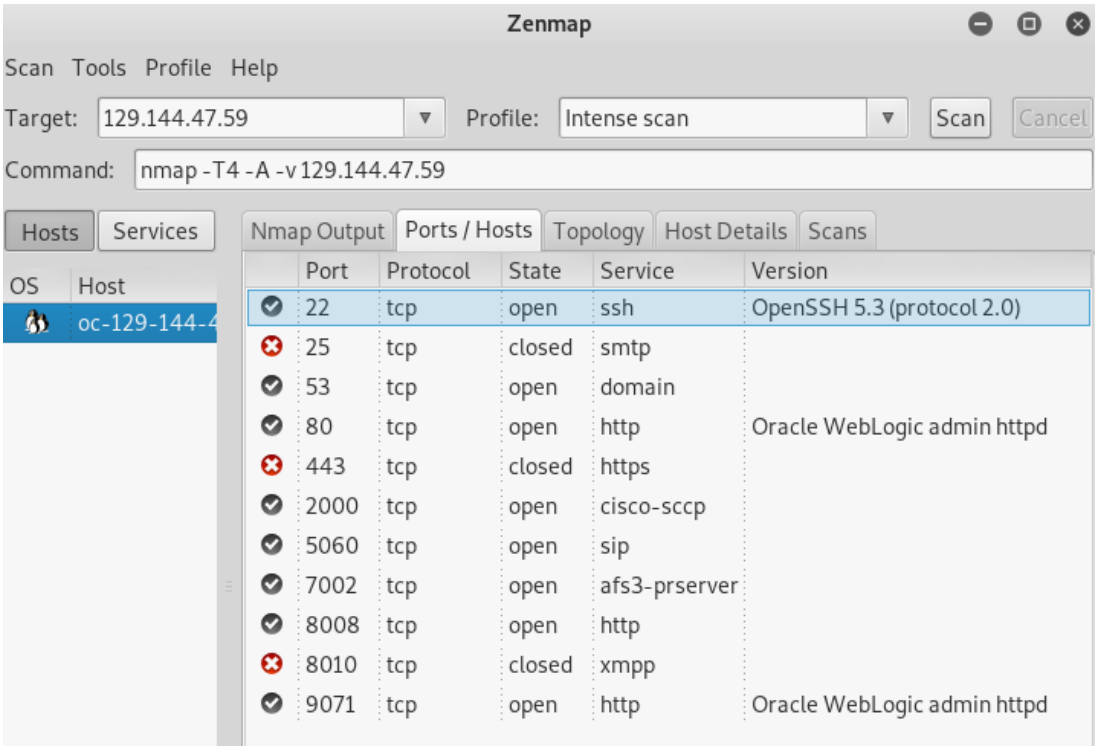


Figura 89: Detalle de puertos abiertos y cerrados en zenmap.

Fuente: Propia

Además de los puertos, la herramienta proporciona la topología del sitio de análisis como se puede observar en la figura 90.

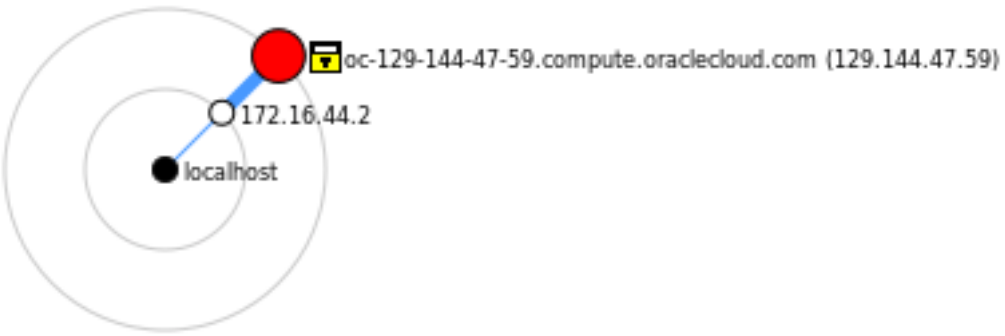


Figura 90: Topología de análisis en zenmap.

Fuente: Propia

Otro de los parámetros que proporciona la herramienta son os detalles de la dirección analizada, el sistema operativo como se puede observar en la figura 91.

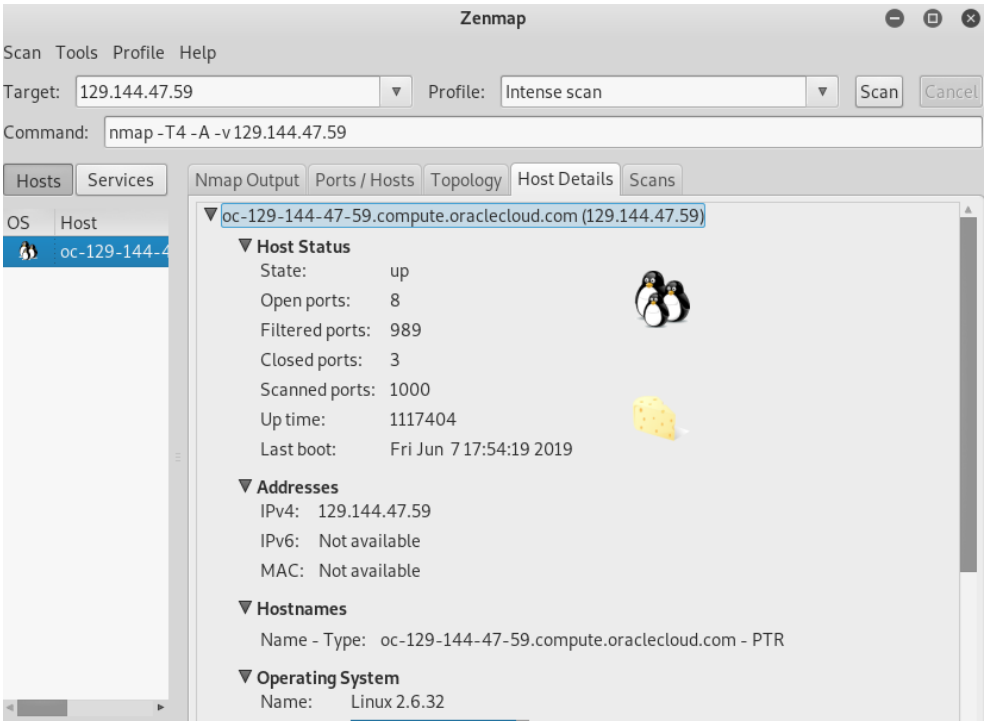


Figura 91: Información de dirección analizada en zenmap.
Fuente: Propia

Posterior al escaneo de puertos se procedió a escoger los puertos 22, 80 y 7002 para analizarlos. A continuación, en la tabla 33 se muestra la identificación de los puertos abiertos elegidos para el análisis.

Tabla 33. Función de los puertos.

Puerto	Nombre	Función
22	ssh	Servicio de Shell seguro. Es útil para acceder a maquinas remotas a través de la red y manejar el sistema mediante un intérprete de comandos, además de copiar información de forma segura.
80	http	Protocolo de transferencia de hipertexto (HTTP) para los servicios del World wide web(www). Este protocolo de comunicación permite la transferencia de información de World Wide Web.
7002	TCP	Garantiza que la entrega de datos sea en el mismo orden del que fueron enviados.

Fuente: Propia

Análisis de puertos abiertos

Para el análisis de los puertos abiertos se ejecutó el siguiente comando:

Comando: nmap –script nmap-vulners -sv -p22 129.144.xx.xx

Este comando permite evaluar las vulnerabilidades, vulners indica que se ejecutara el script para el ataque de vulnerabilidades, sv indica que se entregaran de modo detallado las vulnerabilidades detectadas y p22 indica que se realizara el ataque al puerto 22. A continuación, en la figura 92 se presenta los resultados obtenidos.

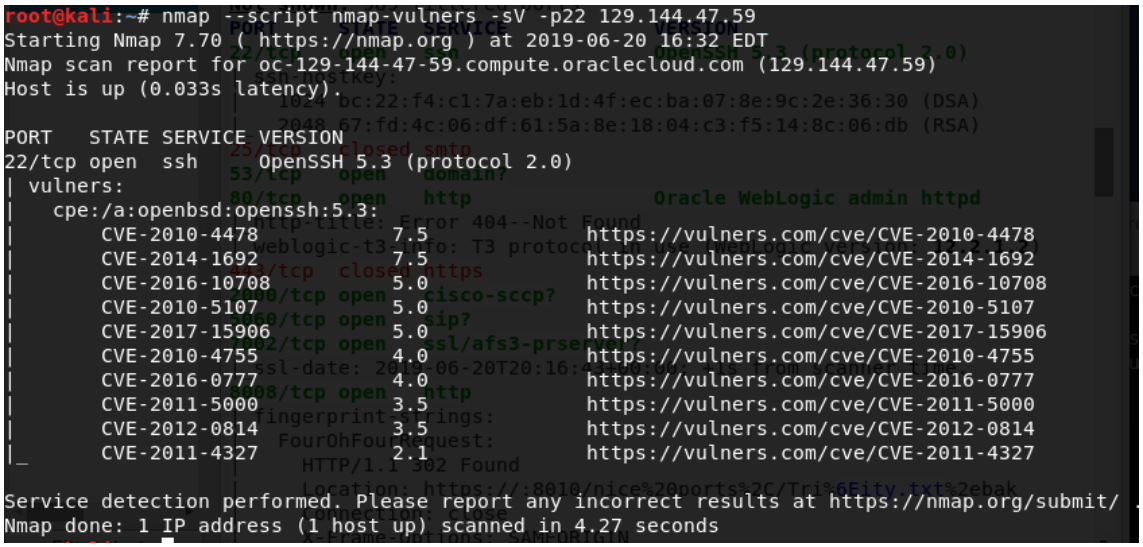


Figura 92: Ejecución de vulnerabilidades del puerto 22.

Fuente: Propia

En la figura 92 se observa que se genera varios informes CVE. Es posible realizar un ataque con la información CVE, pero no se lo hizo debido a que es información delicada y se necesita autorización previa para hacerlo. No fue posible realizar un ataque SQL debido a que la base de datos del sistema académico esta sobre Oracle, lo que significa que los parámetros son distintos a SQL.

Para poder visualizar las vulnerabilidades se tiene que dirigir a la dirección CVE-2017-15906 https://vulners.com/cve/CVE-2017-15906. A continuación, en la figura 93 se presenta el resultado obtenido en la dirección descrita. Es posible observar que el puerto 22 se encuentra expuesto contra ataques, es decir los ataques puedan darse por el puerto en mención mediante conexión remota.

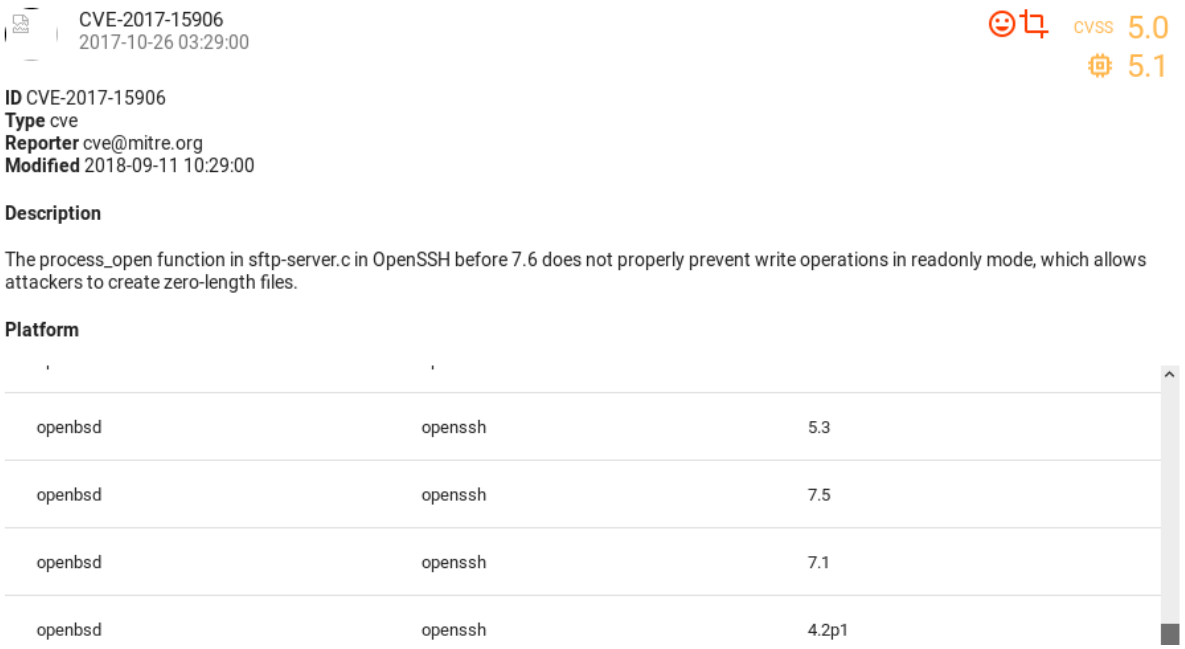


Figura 93: Informe de vulnerabilidades zenmap.

Fuente: Propia

El proceso se repite para los dos puertos restantes. A continuación, se presenta el análisis con el puerto 80.

```
root@kali:~# nmap --script nmap-vulners -sV -p80 129.144.47.59
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-20 16:37 EDT
Nmap scan report for oc-129-144-47-59.compute.oraclecloud.com (129.144.47.59)
Host is up (0.0089s latency).

PORT   STATE    SERVICE VERSION
80/tcp filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
```

Figura 94: Ejecución de vulnerabilidades del puerto 80.

Fuente: Propia

En el puerto 80 no se pudo observar nada ya que este filtrado en un mecanismo de seguridad.

A continuación, se presenta el análisis con el puerto 7002.

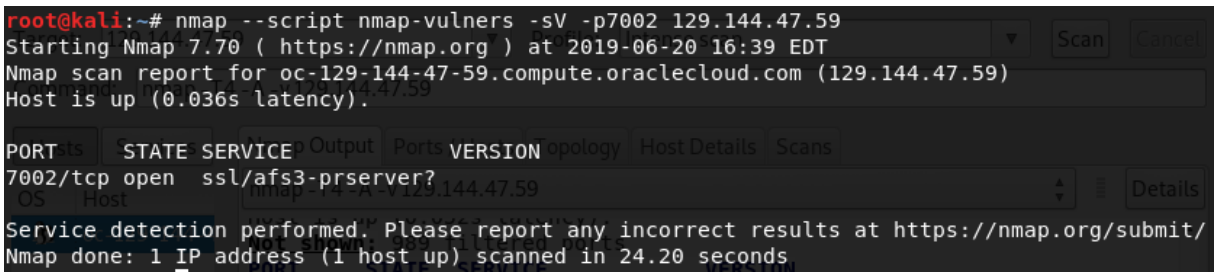


Figura 95: Ejecución de vulnerabilidades del puerto 7002.

Fuente: Propia

En el puerto 7002 no se pudo observar nada ya que este filtrado en un mecanismo de seguridad.

3.8.3. Informe de Auditoría

Nombre de la entidad Auditada: Universidad Técnica del Norte (Sistema académico).

Fecha del informe: 09/07/2019

AUDITORÍA AL SISTEMA ACADÉMICO

OBJETIVO

Realizar una auditoría de seguridad de la información de los datos del sistema académico de la Universidad Técnica del Norte, con el objeto de establecer su estado actual y emitir las recomendaciones para minimizar y optimizar su uso orientado a Big Data.

Lugar de la Auditoría: Departamento de Desarrollo Tecnológico e informático (DDTI).

Grupo de trabajo: Cinthia Carolina Hernández Obando

Herramientas Utilizadas

- Guía de auditoría ISO/IEC 27007:2017
- Norma ISO/IEC 27002:2017
- Software EAR PILAR

ALCANCE

Para el desarrollo de este proyecto se realizó un levantamiento de información a través de entrevistas al personal de la DDTI, observación de la ejecución de las operaciones, competencias de las personas y dependencias que intervienen en el manejo de las operaciones; así como una evaluación de la seguridad al sistema mediante una herramienta informática.

Con el objetivo de recopilar la suficiente evidencia confiable se aplicó banco de preguntas para la evaluación de controles orientados a comprobar el cumplimiento de políticas con la ayuda de las principales directrices de la normativa ISO/IEC 27007:2017 y de los requerimientos que hace mención en las políticas de uso de la metodología Magerit y de esta manera mitigar los riesgos y salvaguardar la información obtenida.

3.8.4. BIG DATA y el sistema académico.

Big Data es una herramienta muy potente para una organización, sin embargo, es esencial conocer varios aspectos de la Universidad Técnica del Norte para determinar si es posible implementar Big Data, y si es o no necesario. Para ello se formulan las siguientes preguntas:

¿La UTN necesita usar todos los datos que almacena?

La mayor parte de datos que maneja la UTN suelen usarse en periodos largos de tiempo, es decir no es continuo.

¿El tiempo es un factor determinante para la UTN?

El tiempo es un factor determinante en periodos determinados, sin embargo, la mayor parte del tiempo no es un factor determinante

¿Cómo se encuentran estructurados los datos?

Los datos no poseen una clasificación adecuada como se demostró en la evaluación del sistema académico.

¿La base de datos es estática o dinámica?

La base de datos es dinámica.

¿La UTN posee los dispositivos tecnológicos necesarios para implementar Big Data?

La infraestructura que posee actualmente la UTN es una pequeña parte de lo que se requiere para la implementación de Big Data por ello es necesario fortalecerla a un nivel más alto de redundancia si se llegara a implementar Big Data.

A continuación, se presenta las necesidades de Big Data versus lo que posee la UTN.

Tabla 34. Data center Big data vs Data center UTN.

Parámetro	Data Center Big Data	Data Center UTN
Refrigeración de alto rendimiento	X	X
Espacio físico	X	X
Sistema control y seguridad	X	
Cableado estructurado	X	X
Tier 1		
Tier 2	X	
Tier 3	X	
Cumplimiento con la norma ISO 27002:2017	X	Parcial
Ingenieros de software	X	X

Fuente: Propia

En la tabla 34 se observa que la UTN posee algunas características necesarias en la implementación de Big Data, sin embargo, la UTN carece de los requerimientos más importantes como lo es el nivel Tier 2 o Tier 3. Estos niveles se refieren a la redundancia de dispositivos de la data center, con la finalidad de ser resistente ante fallos.

Un factor muy importante para la implementación de Big Data es cumplir con los controles de la norma ISO/IEC 27002:2017 referente a seguridad de la información, sin embargo, la UTN únicamente cumple con la mitad de los controles del estándar en mención.

En base a la respuesta de las preguntas formuladas anteriormente se evidencia que la UTN almacena datos en periodos largos de tiempo, el tiempo es un factor determinante en ciertos periodos establecidos mas no siempre y la infraestructura que actualmente posee es las más básica en términos de Big Data. Por lo que no es necesario la implementación de Big

Data puesto que esta responde bien cuando se requiere procesar grandes cantidades de datos en tiempos relativamente cortos, respondiendo a las 3v (variabilidad, veracidad y velocidad), además por las características que demanda Big Data se requiere una infraestructura más robusta y una madurez en seguridad de la información elevada, lo cual la UTN no posee como se evidencio en la evaluación de vulnerabilidades. La UTN cuenta con pocos recursos destinados a seguridad de la información, esto se refleja en el 51% de cumplimento de los controles establecidos en la norma ISO/IEC 27002:2017 contra el 49% de controles que incumple.

3.8.5. Resultados y Hallazgos de la auditoria

El sistema académico de la Universidad Técnica del Norte maneja un gran volumen de datos como se lo comprobó en las encuestas de la primera y segunda herramienta, además existen varias vulnerabilidades identificadas en la parte de los usuarios que en este caso son los estudiantes, puesto que la gran parte de ellos tiene acceso a casi todas las funcionalidades del sistema académico y las contraseñas de acceso son algunos dígitos del carné estudiantil. Por lo que la perdida de este implica un fácil acceso para hackers y personas que quieran obtener información privilegiada.

Todo esto se deriva de un inexistente departamento especializado en seguridad de la información, como consecuencia de ello el departamento de informática carece de políticas de seguridad de la información que se incluyan en los proyectos funcionales y futuros. Todo esto conlleva al incumplimiento de un 49% de los controles necesarios para la seguridad de la información, esto se puede apreciar de forma detallada en sección 3.1 en adelante.

CONCLUSIONES

La guía de ejecución de auditoría ISO/IEC 27007:2017 es muy útil para enfocarse en aspectos específicos de seguridad de la información, basándose en los controles de la norma ISO/IEC 27002:2017.

La identificación de activos del sistema académico y los riesgos son indispensables para conocer las vulnerabilidades a las que se encuentra expuesta la información, basados en el estándar ISO/IEC 27002:2017 bajo la guía de la ISO/IEC 27007:2017.

El sistema académico evidencia 51% de controles cumplidos, este porcentaje es bastante bajo, considerando que el porcentaje de incumplimiento de la norma ISO/IEC 27002:2017 es del 49%.

La aplicación de la metodología MAGERIT permitió identificar los activos, vulnerabilidades y riesgos más importantes del sistema académico, correspondiente a la Universidad Técnica del Norte.

Como resultado de la ejecución de vulnerabilidades de red se encontró que existen varios puertos abiertos, estos se encuentran expuestos a ataques.

Al momento de evaluar vulnerabilidades con la herramienta de Kali Linux, no fue posible ejecutar un análisis de SQL, debido a que la base de datos del sistema académico esta sobre Oracle, mismo que posee parámetros diferentes a SQL.

La infraestructura que posee actualmente la Universidad Técnica del Norte es una pequeña parte para la implementación de Big Data, sin embargo, existe una carencia de dos aspectos esenciales para la implementación de Big Data. Estos aspectos son el nivel Tier II o Tier III y el cumplimiento de todos los controles de la norma ISO/IEC 27002:2017.

Para seguridad de la información en Big Data son importantes tres factores esenciales: confidencialidad, integridad y disponibilidad. Estos son definidos en la norma ISO/IEC 27002, por lo que el cumplimiento de los controles es esencial cuando se habla de Big Data.

RECOMENDACIONES

Llevar un control continúo de las políticas de acceso adoptadas en la herramienta de seguridad perimetral, ya que su debido monitoreo ayudará a detectar y prevenir posibles ataques que pongan en peligro la información e integridad de esta.

Establecer un plan de seguimiento y planificación en temas de seguridad de la información, partiendo de las sugerencias descritas en la tabla de no conformidades. Para obtener una retroalimentación, para la creación de políticas en base a falencias halladas.

Implementar políticas de seguridad interna, basadas en el estándar ISO 27002, acorde con las necesidades del Departamento de Desarrollo Tecnológico e Informático, para mejorar la confiabilidad, disponibilidad e integridad de la información.

Supervisar los puertos abiertos encontrados y filtrarlos en un mecanismo de seguridad para que el sistema no sea vulnerado.

Como complemento a esta investigación se sugiere realizar un estudio de ‘’ Implementación de estrategias de Big data desde una perspectiva gerencial’’, en base a la presente investigación para tener un enfoque más preciso en la posible aplicación de Big Data en la Universidad técnica del Norte.

BIBLIOGRAFÍA

Acasado. (2014). *ISO/IEC 27007*. Obtenido de http://www.isotools.cl/isoiec-27007/

Alomoto, D., & Carrera, A. (2018). Estudio de Mapeo Sistemático de Las Tendencias. *Trabajo de Grado*. Quito, Ecuador.

Arias, J., & Aristizábal, C. (2011). El dato, La Información, el conocimiento y su productividad en empresas del sector público. *SCIELO*, 97.

Benjumea, M. (2012). Los metadatos. *MINISTERIO DE EDUCACIÓN NACIONAL - REPUBLICA DE COLOMBIA*, 1.

Bertolín, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Paraninfo.

Calder, A., & Watkins, S. (2013). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002.* Kogan Page Ltd.

Clements, P. (1996). *Coming attractions in Software Architecture. Technical Report.* CMU.

Comer, D. (2015). *Redes globles de información con internet y TCP/IP.* México: Prentice Hall.

Dávila, S. (2017, 03 29). No ha existido crecimiento en la industria del software, según Aesoft. *El Comercio*, p. 8.

Definición de Datos - Significado y definición de Datos. (s.f.). Obtenido de https://sistemas.com/datos.php

Duarte, L. L. (28 de Octubre de 2013). *La informática, datos e información.* Obtenido de https://prezi.com/ddeollkz8cjv/la-informatica-datos-e-informacion/

ESPAE. (2017, 01 04). *ESPAE.ESPOL.* Retrieved from http://www.espae.espol.edu.ec/wp-content/uploads/2016/12/industriasoftware.pdf

Excellence, I. (28 de 07 de 2015). *Blog especializado en Sistemas de Gestión* . Obtenido de http://www.pmg-ssi.com/2015/07/que-es-sgsi/

Excellence, ISOTools. (3 de Agosto de 2017). *Norma ISO 27002: El dominio política de seguridad*. Obtenido de https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Freire Cobo, L. E. (1 de Octubre de 2015). Obtenido de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/30314

Garcia, F. (2011). El concepto de la información. *REVISTA CIENTÍFICAS COMPLUTENSES*, 305-307.

Hernández, E., Duque, N., & Moreno, J. (2017). Big Data: una exploración de investigaciones, tecnologías y casos de aplicación. *TecnoLógicas*, 2-24.

Hernández, Fernández, & Baptista. (2010). *Metodología de la Investigación. .* México D.F: McGraw Hill.

INEC. (2015). *Tecnologías de la Información y Telecomunicaciones.* Quito: INEC.

ISO. (2011). *Baja California*. Obtenido de http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm

ISO. (2019, 03 15). *ISO*. Retrieved from https://www.iso.org/standard/54534.html

ISOTools. (19 de Marzo de 2015). *Blog Calidad y Excelencia*. Obtenido de https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

Li, K., Jiang, H., Yang, L., & Cuzzocrea, A. (2015). *Big Data: Algorithms, Analytics, and Applications, Chapman &. CRC Press, 2015.* Chapman & CRC Press.

MAGERIT. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I.* Madrid.

Maté Jiménez, C. (01 de 12 de 2014). *Big data. Un nuevo paradigma de análisis de datos*. Obtenido de https://repositorio.comillas.edu/xmlui/handle/11531/4873

Mieres, J. (2009). *Ataques informáticos. Debilidades de seguridad comúnmente explotadas.* Obtenido de Ucting: http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

Milagros, P., & Steven, Y. (2017). Análisis de vulnerabilidades en la infraestructura tecnológica de una empresa, utilizando herramientas de test de intrusión. *Trabajo de Grado*. Guayaquil, Ecuador: Universidad de Guayaquil.

MINTEL. (30 de Agosto de 2014). Obtenido de https://www.telecomunicaciones.gob.ec: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/08/Libro_plan_tti_REGISTRO-OFICIAL_30_AGOSTO.pdf

Montealegre, A. (2017). Tesis de Pregrado. *Importancia de la solución Big Data en la Aplicación de*. Bogotá, Colombia: Universidad Libre de Colombia.

Norma ISO 19011 – Principios de auditoría. (2 de Noviembre de 2015). Obtenido de https://www.escuelaeuropeaexcelencia.com/2015/11/norma-iso-19011-principios-de-auditoria/

O'neill, K. (s.f.). Obtenido de https://www.cyberclick.es/numerical-blog/big-data-que-es-y-como-usarlo-en-marketing

Pazmiño, P. (2007). Análisis de los riesgos y vulnerabilidades de la red de datos de Escuela Politécnica Nacional. *Trabajo de Grado*. Quito, Ecuador: EPN.

PriteshGupta.com. (s.f.). *El portal de ISO 27001 en Español*. Obtenido de http://www.iso27000.es/aviso.html

Prom Perú. (2011). *Perfil de Mercado de Software en Ecuador.* Lima.

Quishpe, B., & Vargas, M. (2013). Modelo de auditoría informática basada en riesgos en ámbitos financieros. Aplicación de un caso de estudio a una cooperativa de ahorro y crédito. *Trabajo de Grado*. Quito, Ecuador: Universidad Politécnica Nacional.

Rodriguez, M. (2010). *Métodos de investigación : diseño de proyectos y desarrollo de tesis en ciencias administrativas, organizacionales y sociales.* Sinaloa: Universidad Autónoma de Sinaloa.

Tamayo, & Tamayo, M. (2007). *El Proceso de la Investigación Científica: Incluye evaluación y administración de proyectos de investigación .* México: Limusa.

Taylor, S., & Bogdan, R. (1987). *Introducción a los métodos cualitativos de investigación : la búsqueda de significados.* Barcelona: Paidos.

UTN, D. d. (2013).

VIEITES, Á. G. (2014). *ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA.* MEXICO: ALFA-OMEGA.

Yañes, C. (08 de 11 de 2017). *TIPOS DE SEGURIDAD INFORMÁTICA*. Obtenido de https://www.ceac.es/blog/tipos-de-seguridad-informatica

Aguirre, B. J. (2011). Auditoria Informática. MEXICO: UNAM.

Curiel, G. (2006). Auditoria de Estados Financieros. Naucalpan de Juárez: PEARSON.

Gonzales, E. F. (2018). Auditoria Operativa. Quito: Universidad Central del Ecuador.

Guitián, G. (2014). Metodologías y modelos para auditar la información. Análisis reflexivo. Revistas Científicas Complutenses, 234-235.

Miramegias. (11 de 11 de 2018). Miramegias. Obtenido de Miramegias: http://www.miramegias.com/auditoria/files/apuntes/ut12.pdf

Universidad Tecnológica de la Huasteca Hidalguense. (2011). Auditoria. Mexico: UTHH.

CCN-CERT. (2013). Libro I Magerit 3, Método. Madrid, España.

CCN-CERT. (2013). Libro II Magerit 3, Catálogo de elementos. Madrid, España.

CCN-CERT. (2013). Libro III Magerit 3, Guías de Técnicas. Madrid, España.

Tabesh, P., Mousavidin, E., & Hasani, S. (2019). Implementing big data strategies: A managerial perspective. Business Horizons, 62(3), 347–358. https://doi.org/10.1016/j.bushor.2019.02.001

TALHA, M., EL KALAM, A. A., & ELMARZOUQI, N. (2019). Big Data: Trade-off between Data Quality and Data Security. Procedia Computer Science, 151, 916–922. https://doi.org/10.1016/j.procs.2019.04.127

ANEXOS

Anexo A: Encuesta aplicada a los usuarios del Sistema Académico

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIA APLICADAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

ENCUESTA APLICADA A LOS USUARIOS DEL SISTEMA ACADÉMICO.

Objetivo: Conocer la opinión sobre el uso del Sistema Académico de la UTN.
Indicaciones: Contestar de forma clara a las siguientes interrogantes.

1. ¿Utiliza el sistema académico de la UTN?

   Si ☐
   No ☐

2. ¿A qué parte del sistema académico tiene acceso?
   - Inscripciones y Matriculación ☐
   - Gestión de horarios y Malla Curricular ☐
   - Gestión Curricular ☐
   - Gestión de Proyectos de Tesis ☐
   - Gestión de Complementación Educativa ☐
   - Gestión de Notas y Calificaciones ☐
   - Gestión de Recursos Docentes ☐

3. ¿Su acceso a esta parte del sistema académico lo hace mediante qué dispositivo?
   - Una computadora de escritorio ☐
   - Una computadora de laptop ☐
   - Un dispositivo móvil (celular o Tablet) ☐

4. ¿El dispositivo que usa para el acceso al sistema académico es?
   - Propio ☐
   - Alquilado ☐
   - De la Institución ☐
5. ¿Cómo hizo para poder ingresar a esta parte del sistema académico?
   - Se registró Ud. mismo ☐
   - Le registro el DDTI ☐
   - Es de acceso libre ☐
6. ¿Al portal que Ud. accede tiene un nivel de seguridad (contraseña o pin)?
   - Contraseña ☐
   - Ping ☐
   - Sin contraseña ☐
7. En el caso de tener contraseña o ping. ¿Cómo fue asignada?
   - Por el DDTI ☐
   - Yo la asigne ☐
8. De ser por parte del DDTI. ¿Cómo le hizo llegar su contraseña o ping a Ud.?
   - Correo Electrónico ☐
   - Documento escrito ☐
   - De manera Verbal ☐
9. En caso de ser por asignación propia. ¿Al asignar la contraseña se le impusieron ciertos parámetros para ser aceptada?

   Si ☐

   No ☐
10. En los dos casos de asignación de contraseña. ¿Cada cuánto le asignan o le piden asignar una nueva contraseña?

    Frecuentemente ☐

    No muy frecuente ☐

    Nunca ☐

Anexo B: Encuesta aplicada al personal que labora dentro del Departamento de Desarrollo de Tecnologías de la Información.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIA APLICADAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

ENCUESTA DIRIGIDA AL PERSONAL QUE LABORA DENTRO DEL DEPARTAMENTO DE DESARROLLO DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UTN.

TEMA: "Estudio de la seguridad en Big Data, privacidad y protección de datos mediante la ISO/IEC 27007:2017- aplicado a los datos académicos de la Universidad Técnica del Norte"

Objetivo: Conocer la opinión de los empleados de DDTI acerca de la seguridad en Big Data, privacidad y protección de datos de acuerdo con los parámetros de la norma ISO/IEC 27002:2017, en los datos académicos de la Universidad Técnica del Norte.

Indicaciones: Contestar de forma clara a las siguientes interrogantes.

1. ¿Existen documento(s) de políticas de seguridad de S.I.?

Si ☐
No ☐

2. ¿Existe normativa relativa a la seguridad de S.I.?

Si ☐
No ☐

3. ¿Existen procedimientos relativos a la seguridad de S.I.?

Si ☐
No ☐

4. ¿Existe un responsable de las políticas, normas y procedimientos?

Si ☐
No ☐

5. ¿Existen mecanismos para la comunicación a los usuarios de las normas?

Si ☐

No ☐

6. ¿Existen controles regulares para verificar la efectividad de las políticas?

Si ☐

No ☐

7. ¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?

Si ☐

No ☐

8. ¿Existe un responsable encargado de evaluar la adquisición y cambios de S.I.?

Si ☐

No ☐

9. ¿Existen condiciones contractuales de seguridad con terceros y Outsourcing?

Si ☐

No ☐

10. ¿Existen criterios de seguridad en el manejo de terceras partes?

Si ☐

No ☐

11. ¿Existen programas de formación en seguridad para los empleados, clientes y terceros?

Si ☐

No ☐

12. ¿Existe un acuerdo de confidencialidad de la información a la que se accede?

Si ☐

No ☐

13. ¿Se revisa la organización de la seguridad periódicamente por una empresa externa?

Si ☐

No ☐

14. ¿Existe un inventario de activos actualizado?

Si ☐

No ☐

15. ¿El Inventario contiene activos de datos, software, equipos y servicios?

Si ☐

No ☐

16. ¿Se dispone de una clasificación de la información según la criticidad de esta?

Si ☐

No ☐

17. ¿Existe un responsable de los activos?

Si ☐

No ☐

18. ¿Existen procedimientos para clasificar la información ?

Si ☐

No ☐

19. ¿Existen procedimientos de etiquetado de la información?

Si ☐

No ☐

20. ¿Se tienen definidas responsabilidades y roles de seguridad?

Si ☐

No ☐

21. ¿Se tiene en cuenta la seguridad en la selección y baja del personal?

Si ☐

No ☐

22. ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?

Si ☐

No ☐

23. ¿Se imparte la formación adecuada de seguridad y tratamiento de activos?

Si ☐

No ☐

24. ¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?

Si ☐

No ☐

25. ¿Se recogen los datos de los incidentes de forma detallada?

Si ☐

No ☐

26. ¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?

Si ☐

No ☐

27. ¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?

Si ☐

No ☐

28. ¿Existe un proceso disciplinario de la seguridad de la información?

Si ☐

No ☐

29. ¿Existe perímetro de seguridad física (una pared, puerta con llave)?

Si ☐

No ☐

30. ¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?

Si ☐

No ☐

31. ¿En las áreas seguras existen controles adicionales al personal propio y ajeno?

Si ☐

No ☐

32. ¿Las áreas de carga y expedición están aisladas de las áreas de S.I.?

Si ☐

No ☐

33. ¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?

Si ☐

No ☐

34. ¿Existe seguridad en el cableado general del DataCenter, frente a daños e intercepciones?

Si ☐

No ☐

35. ¿Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente?

Si ☐

No ☐

36. ¿Todos los procedimientos operativos identificados en la política de seguridad están documentados?

Si ☐

No ☐

37. ¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?

Si ☐

No ☐

38. ¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?

Si ☐

No ☐

39. ¿Existe una separación de los entornos de desarrollo y producción?

Si ☐

No ☐

40. ¿Existen contratistas externos para la gestión de los Sistemas de Información?

Si ☐

No ☐

41. ¿Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento?

Si ☐

No ☐

42. ¿Existen Controles contra software maligno?

Si ☐

No ☐

43. ¿Realizan copias de backup de la información?

Si ☐

No ☐

44. ¿Existen logs (registro de actividad de un sistema) para las actividades realizadas por los operadores y administradores?

Si ☐

No ☐

45. ¿Existe algún control en las redes?

Si ☐

No ☐

46. ¿Hay establecidos controles para realizar la gestión de los medios informáticos? (Cintas, discos, removibles, informes impresos)?

Si ☐

No ☐

47. ¿Se monitorean las actividades relacionadas a la seguridad?

Si ☐

No ☐

48. ¿Existe una política de control de accesos?

Si ☐

No ☐

49. ¿Se controla y restringe la asignación y uso de privilegios en entornos multiusuario?

Si ☐

No ☐

50. ¿Se asegura la ruta (path) desde el terminal al servicio tanto internos como externos?

Si ☐

No ☐

51. ¿Existe un control del routing (dispositivo para la interconexión de redes informáticas) de las redes internas y externas?

Si ☐

No ☐

52. ¿Existe seguridad en los ficheros de los sistemas?

Si ☐

No ☐

53. ¿Existe seguridad en los procesos de desarrollo, testing y soporte?

Si ☐

No ☐

54. ¿Existe la gestión de los cambios en los Sistemas Operativos (S.O.)?

Si ☐

No ☐

55. ¿Se controlan las vulnerabilidades de los equipos?

Si ☐

No ☐

56. ¿Se comunican los eventos de seguridad?

Si ☐

No ☐

57. ¿Existe definidas las responsabilidades antes de un incidente?

Si ☐

No ☐

58. ¿Existen procesos para la gestión de la continuidad?

Si ☐

No ☐

59. ¿Existe un diseño, redacción e implantación de planes de continuidad?

Si ☐

No ☐

60. ¿Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas?

Si ☐

No ☐

61. ¿Existe el resguardo de los registros de la organización?

Si ☐

No ☐

62. ¿Existe una revisión de la política de seguridad y de la conformidad técnica?

Si ☐

No ☐

63. ¿Existen consideraciones sobre las auditorías de los sistemas?

Si ☐

No ☐

La presente información es de uso confidencial, y es recolectada con el propósito de Estudiar la Gestión de la Seguridad Informática en grandes volúmenes de datos (Big Data)", del Sistema academico de la Universidad Técnica del Norte mediante ISO/IEC 27002:2017. Agradezco su colaboración que es muy valiosa para el presente estudio.

Gracias por su colaboración

GLOSARIO

Auditoria de seguridad: es el estudio y examen independiente de registros historicos y actividades especificas de un sistema de informacion, tiene como objetivo comprobar la solidez y cumplimiento de controles del sistema de informacion, para detectar brechas en la seguridad y recomendar algunos procesos, controles y estructuras de seguridad para solucionar la brecha en mencion.

Ataque: es cualquier accion deliberada que tiene como objetivo vulnera la brecha de seguridad.

Autenticidad: es la preservación de la identidad.

Degradación: es la pérdida del valor de un activo al materializarse una amenaza.

Confidencialidad: es asegurar la información para que pueda ser vista solo por los usuarios que tienen autorización a la misma.

Disponibilidad: es asegurar que la información esté disponible para los usuarios que tengan autorización, cuando ellos lo requieran.

Estado de riesgo: se trata de caracterizar los activos por el riesgo residual, es decir que ocurre después de que las salvaguardas han sido ejecutadas.

Evento de seguridad: es cuando la amenaza existe y puede afectar a los activos.

Frecuencia: es la cantidad de veces que ocurre una amenaza en un determinado tiempo.

Gestión de riesgos: consiste en la implementación de medidas de seguridad para impedir, reducir y controlar los riesgos identificados. La gestión de riesgos se basa en los resultados obtenidos del análisis de riesgos.

Impacto: es la consecuencia que tiene sobre un activo por la materialización de una amenaza.

Impacto residual: es el impacto remanente que existe luego de las medidas de seguridad.

Integridad: garantizar la exactitud y veracidad de la información según los métodos de procesamiento.

Plan de seguridad: es un conjunto de procesos de seguridad que permite ejecutar las decisiones para la prevención de riesgos.

Riesgo: es la estimación de cuan expuesto esta un activo ante la materialización de amenazas.

Riesgo acumulado: toma en cuenta el valor propio del activo y el valor de los activos que dependen de él, para combinarlo con la degradación que causa una amenaza y la frecuencia estimada.

Riesgo repercutido: es el cálculo entre el valor propio del activo, la degradación y la frecuencia estimada de la materialización de amenazas.

Seguridad: es la habilidad de los sistemas de información para resistir a los accidentes o ataques provocados con el fin de afectar a la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados y de los servicios que dichas redes y sistemas ofertan.

Trazabilidad: es la habilidad de determinar en todo momento que cambio se realizó y quien lo realizo.

Valor de un activo: es la estimación del costo inducido por la materialización de una amenaza.

Vulnerabilidad: es la determinación de la exposición de un activo ante una amenaza, es posible determinarlo por dos medidas: frecuencia de ocurrencia y degradación causada.

Algoritmo: es una secuencia lógica que forman una ecuación matemática útil para el análisis de datos.

Data Scientist: es el analista de datos, es decir es la persona encargada de capturar los insights dentro de los grandes volúmenes de datos.

Big Data: es una herramienta útil para manejar un conjunto muy grande de datos, responde a los tres v: volumen de datos importante, variedad de los datos, velocidad a la que llegan los datos.