

UNIVERSIDAD TÉCNICA DEL NORTE



Facultad de Ingeniería en Ciencias Aplicadas
Carrera de Ingeniería en Sistemas Computacionales

**EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL
SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA
DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA
MAGERIT V3**

Trabajo de grado presentado ante la Universidad Técnica del Norte previo a la
obtención del título de Ingeniera en Sistemas Computacionales

Autora:

Verónica Lizeth Guamán Guamán

Directora:

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

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: | 100355729-3 |
| APELLIDOS Y NOMBRES: | GUAMAN GUAMAN VERÓNICA LIZETH |
| DIRECCIÓN: | CARANQUI |
| EMAIL: | veronicalizeth123@gmail.com |
| TELEFONO MOVIL: | 0939380652 |

| DATOS DE LA OBRA | |
|--------------------------------|---|
| TÍTULO: | EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA MAGERIT V3 |
| AUTOR (ES): | GUAMAN GUAMAN VERONICA LIZETH |
| FECHA: | 2019-07-08 |
| PROGRAMA: | PREGRADO |
| TÍTULO POR EL QUE OPTA: | INGENIERA EN SISTEMAS COMPUTACIONALES |
| ASESOR / DIRECTOR: | MSC. 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 la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 10 días del mes de julio de 2019

EL AUTOR:



Verónica Lizeth Guamán Guamán

Cédula: 100355729-3



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS

Ibarra, 10 de julio de 2019

CERTIFICACIÓN DEL DIRECTOR

Por medio del presente, yo MSc. Daisy Imbaquingo, certifico que la Srta. Verónica Lizeth Guamán Guamán, portador de la cédula de identidad Nro. 100355729-3. Ha trabajado en el desarrollo del proyecto de grado **“EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA MAGERIT V3”**, 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 TRABAJO DE GRADO



UNIVERSIDAD TÉCNICA DEL NORTE

Universidad Acreditada resolución 002-CONEA-2010-129-DC
Resolución No. 001-073-CEAACES-2013-13

DIRECCION DE DESARROLLO TECNOLÓGICO E INFORMÁTICO

DIRECTOR DE LA DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO

CERTIFICA

QUE: La señorita VERÓNICA LIZETH GUAMÁN GUAMÁN con cédula identidad 1003557293 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 “EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA MAGERIT V3”.

QUE: El informe 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 TÉCNICA AL SERVICIO DEL PUEBLO



Av. 17 de Julio 5 – 21 y José María Córdova
Ciudadela Universitaria Barrio El Olivo
Teléfono: (06) 2997800 ext. 7040 Casilla 199
www.utn.edu.ec
Ibarra - Ecuador

Dedicatoria

“Es importante celebrar el éxito, pero es más importante aprender bien de los fracasos.”

Bill Gates

Dedico este proyecto de tesis a mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento. Es por ellos que soy lo que soy ahora. Los amo con mi vida.

A mis hermanos, por sus palabras, el apoyo incondicional y compañía que me han ayudado y llevado hasta donde estoy ahora.

También dedico este trabajo a quienes con su conocimiento han colaborado en la ejecución de este trabajo.

Verónica Lizeth

Agradecimientos

A Dios por haberme guiado a lo largo de la carrera, por ser mi fortaleza en los momentos de debilidad y brindarme una vida llena de aprendizajes.

A la Universidad Técnica del Norte y a mis profesores que cada día formaron en mí una excelente profesional y ser humano.

A mis padres por apoyarme en todo momento, por los valores que me han inculcado y por darme la oportunidad de tener una excelente educación en el transcurso de mi vida.

A mi amiga Cinthia, quien ha estado a mi lado desde el inicio de la carrera, gracias por tu apoyo, por tus esfuerzos por mantener siempre viva la amistad.

A Patricio, por la paciencia, la comprensión y el apoyo constante en mi vida.

Gracias a la vida por este nuevo triunfo, gracias a todas las personas que me apoyaron y creyeron en la realización de esta tesis.

Verónica Lizeth.

TABLA DE CONTENIDOS

| | |
|--|--------------------------------------|
| AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UTN..... | I |
| CERTIFICACIÓN DEL DIRECTOR | III |
| CERTIFICACION DEL DDTI - UTN. | ¡Error! Marcador no definido. |
| Dedicatoria..... | V |
| Agradecimientos..... | VI |
| Resumen..... | XV |
| Abstract..... | XVI |
| INTRODUCCIÓN | XVII |
| Antecedentes | XVII |
| Justificación e Importancia | XVIII |
| Impacto Tecnológico..... | XVIII |
| Impacto Social | XVIII |
| Prospectiva | XIX |
| Objetivos | XIX |
| Objetivo General..... | XIX |
| Objetivos Específicos | XIX |
| Alcance | XIX |
| CAPÍTULO 1. Marco Teórico..... | 1 |
| 1.1 Conceptos de Auditoría, tipos de auditoria | 1 |
| 1.1.1 Auditoria..... | 1 |
| 1.1.2 Tipos de Auditoría..... | 1 |
| 1.1.3 Clasificación de Auditoria..... | 2 |
| 1.2 Introducción a la Seguridad Informática o seguridad de la información | 3 |
| 1.2.1 ¿Qué es Seguridad Informática?..... | 3 |
| 1.2.2 ¿Qué es Seguridad de la Información?..... | 3 |

| | | |
|-------|--|----|
| 1.2.3 | Requisitos de seguridad de la información..... | 4 |
| 1.2.4 | ¿Dónde interviene la gestión de seguridad de la información?..... | 5 |
| 1.2.5 | Pilares de la Seguridad Informática..... | 5 |
| 1.3 | Conceptos de Vulnerabilidad, Amenaza, Riesgo | 7 |
| 1.3.1 | Vulnerabilidad | 8 |
| 1.3.2 | Amenaza..... | 8 |
| 1.3.3 | Riesgo..... | 8 |
| 1.4 | Clasificación de las amenazas informáticas..... | 9 |
| 1.4.1 | Tipos de amenazas informáticas..... | 9 |
| 1.4.2 | Ataques informáticos..... | 10 |
| 1.5 | Estándares ISO 27000 | 11 |
| 1.5.1 | ¿Qué son los Estándares ISO 27000?..... | 11 |
| 1.5.2 | Estándares que conforman la Familia de la ISO 27000..... | 11 |
| 1.6 | Estándares ISO/IEC 270001 e ISO/IEC 27002..... | 13 |
| 1.6.1 | Estándar ISO/IEC 27001..... | 13 |
| 1.6.2 | Norma ISO 27002 | 14 |
| 1.6.3 | Antecedentes y Contexto del Estándar ISO/IEC 27002:2017 | 15 |
| 1.6.4 | Ciclo de vida de la Norma ISO 27002 | 15 |
| 1.6.5 | Estructura de la Norma ISO 27002 | 16 |
| 1.7 | Metodologías para el Análisis de Riesgos | 18 |
| 1.7.1 | ¿Cuáles son las metodologías para el Análisis de Riesgos?..... | 18 |
| 1.8 | Selección de metodología para análisis de riesgos. | 19 |
| 1.9 | Metodología de Análisis y Gestión de Riesgos de Información (Magerit)..... | 28 |
| 1.9.1 | Introducción | 28 |
| 1.9.2 | Objetivos de Magerit | 30 |
| 1.9.3 | Características de Magerit | 30 |
| 1.9.4 | Estructura MAGERIT | 31 |

| | |
|---|-----------|
| CAPÍTULO 2. Desarrollo | 33 |
| 2 Marco Contextual | 33 |
| 2.1 Descripción del Sistema Informático Integrado Universitario (SIIU) | 33 |
| 2.1.1 Sistema Académico - Universidad Técnica del Norte | 34 |
| 2.1.2 Sistema de Evaluación Docentes – Universidad Técnica del Norte..... | 34 |
| 2.2 Estructura Organizacional..... | 36 |
| 2.2.1 Organigrama Estructural UTN..... | 36 |
| 2.2.2 Organigrama DDTI - UTN | 37 |
| 2.2.3 Misión | 37 |
| 2.2.4 Visión | 38 |
| 2.3 Roles y Responsabilidades, funciones del personal de DDTI | 38 |
| 2.4 Técnicas de Investigación | 39 |
| 2.4.1 Población y Muestra..... | 39 |
| 2.5 Fuentes y técnicas para la recolección de información | 41 |
| 2.5.1 Tipos de Investigación | 41 |
| 2.5.2 Fuentes y técnicas de recolección de información | 41 |
| 2.5.3 Análisis de encuestas | 42 |
| 2.6 Procedimiento Informático Lógico para el Análisis de Riesgos (PILAR)..... | 60 |
| 2.6.1 Determinación de activos | 64 |
| 2.6.2 Dependencia entre activos..... | 66 |
| 2.6.3 Valoración de activos | 68 |
| 2.6.4 Identificación de amenazas..... | 70 |
| 2.6.5 Valoración de amenazas..... | 71 |
| 2.6.6 Estimación de impacto | 73 |
| 2.6.7 Impacto acumulado..... | 73 |
| 2.6.8 Riesgo acumulado | 75 |
| 2.6.9 Impacto repercutido | 75 |

| | | |
|-------------------------------------|---|------------|
| 2.6.10 | Situación actual del riesgo acumulado | 78 |
| CAPÍTULO 3. Resultados | | 81 |
| 3.1 | Informe de Resultados..... | 81 |
| 3.2 | Evaluación del cumplimiento | 82 |
| 3.3 | Informe de No Conformidades ISO 27002:2017 | 95 |
| 3.4 | Identificación de Vulnerabilidades..... | 105 |
| 3.5 | Informe de Auditoría | 113 |
| CONCLUSIONES | | 115 |
| RECOMENDACIONES | | 116 |
| BIBLIOGRAFÍA | | 117 |
| ANEXOS | | 121 |
| Anexo 1: | Encuesta aplicada a Docentes y Estudiantes | 121 |
| Anexo 2: | Preguntas dirigidas al personal encargado del manejo del sistema..... | 125 |
| Anexo 3: | Encuesta de Valoración de Dimensiones | 126 |
| GLOSARIO | | 127 |

INDICE DE FIGURAS

| | |
|--|----|
| Figura 1: Fases de la Metodología Magerit | XX |
| Figura 2: Seguridad de la información en una empresa. | 5 |
| Figura 3: Pilares de la Seguridad Informática..... | 7 |
| Figura 4: Relación de Vulnerabilidad, Amenazas y Sistemas de Información | 8 |
| Figura 5: Riesgos globales..... | 10 |
| Figura 6: Serie de Estándares de la familia ISO 27000. | 11 |
| Figura 7: Ciclo de Deming PDCA Sistema de Gestión ISO/IEC 27001 | 14 |
| Figura 8: Estructura Norma ISO/IEC 27002:2017 | 17 |
| Figura 9: Marco de trabajo para la gestión de riesgos..... | 29 |
| Figura 10: Proceso de evaluación integral | 34 |
| Figura 11: Organigrama Estructural UTN (2013)..... | 36 |
| Figura 12: Organigrama Dirección Informática UTN..... | 37 |
| Figura 13: Procesos para aplicar MAGERIT | 61 |
| Figura 14: Pantalla principal PILAR- MAGERIT | 63 |
| Figura 15: Información del proyecto. | 63 |
| Figura 16: Activos del sistema de evaluación docente. | 66 |
| Figura 17: Valoración de activos del sistema de evaluación docente. | 68 |
| Figura 18: Valoración del dominio de seguridad UTN | 69 |
| Figura 19: Gráfica de valor/activos..... | 69 |
| Figura 20: Amenazas del sistema de evaluación docente. | 70 |
| Figura 21: Amenazas del sistema de evaluación docente. | 72 |
| Figura 22: Tabla de amenazas y porcentaje de probabilidad de ocurrencia | 72 |
| Figura 23: Impacto acumulado del sistema de evaluación docente..... | 74 |
| Figura 24: Situación actual del impacto acumulado del sistema de evaluación docentes.... | 74 |
| Figura 25: Riesgo acumulado del sistema de evaluación docente. | 75 |

| | |
|--|-----|
| Figura 26: Tabla de Nivel de Riesgo | 77 |
| Figura 27: Situación actual del riesgo acumulado del sistema de evaluación docente. | 78 |
| Figura 28: Riesgo Acumulado/dimensión | 79 |
| Figura 29: Cumplimiento de controles ISO 27002:2017 | 95 |
| Figura 30: Observaciones y recomendaciones de los controles ISO 27002:2017 | 96 |
| Figura 31: Utilización de la herramienta SiteVerify | 106 |
| Figura 32 Escaneo con Nmap | 107 |
| Figura 33: Puertos habilitados Nmap | 108 |
| Figura 34: Utilización de comando –Sv para identificar servicios y versiones | 109 |
| Figura 35: Reporte de Vulnerabilidad de OpenSSH en CVE Details | 110 |
| Figura 36: Reporte de Vulnerabilidad puerto 80 y 9071 en Exploit Database | 111 |
| Figura 37: SqlMap en Kali Linux | 112 |

ÍNDICE DE TABLAS

| | |
|--|----|
| Tabla 1: Normativa ISO 27000..... | 12 |
| Tabla 2: Comparación Metodologías MAGERIT y CRAMM..... | 21 |
| Tabla 3: Roles y responsabilidades del personal de DDTI-UTN..... | 38 |
| Tabla 4: Usuarios Universidad Técnica del Norte..... | 40 |
| Tabla 5: Primera pregunta encuesta | 42 |
| Tabla 6: Segunda pregunta encuesta | 43 |
| Tabla 7: Tercera pregunta encuesta | 44 |
| Tabla 8: Cuarta pregunta encuesta..... | 45 |
| Tabla 9: Quinta pregunta encuesta | 46 |
| Tabla 10: Sexta pregunta encuesta..... | 47 |
| Tabla 11: Séptima pregunta encuesta..... | 48 |
| Tabla 12: Octava pregunta encuesta | 49 |
| Tabla 13: Novena pregunta encuesta | 50 |
| Tabla 14: Décima pregunta encuesta..... | 51 |
| Tabla 15: Onceava pregunta encuesta | 52 |
| Tabla 16: Doceava pregunta encuesta..... | 53 |
| Tabla 17: Treceava pregunta encuesta..... | 54 |
| Tabla 18: Catorceava pregunta encuesta..... | 55 |
| Tabla 19: Quinceava pregunta encuesta..... | 56 |
| Tabla 20: Dieciseisava pregunta encuesta..... | 57 |
| Tabla 21: Diecisieteava pregunta encuesta..... | 58 |
| Tabla 22: Dimensiones de Valoración..... | 59 |
| Tabla 23: Escala de Valoración..... | 60 |
| Tabla 24: Clasificación de Activos..... | 64 |
| Tabla 25: Probabilidad de ocurrencia..... | 71 |

| | |
|--|-----|
| Tabla 26: Nivel de riesgo | 77 |
| Tabla 27: Evaluación de cumplimiento de controles ISO 27002:2017 | 82 |
| Tabla 29: Identificación de puertos..... | 108 |

Resumen

La evaluación docente es un proceso importante dentro de las universidades ecuatorianas, permite mejorar las metodologías empleadas en la enseñanza y los posibles fallos en la educación y de esta manera lograr la acreditación universitaria exigida actualmente por organismos de control como el Consejo de Educación Superior del Ecuador (CES).

Con el continuo crecimiento de las tecnologías de la información y el uso de sistemas en todo tipo de empresas, procesos, productos y servicios, el manejo de las mismas se vuelve incontrolable por los volúmenes de información generados. La Universidad Técnica del Norte posee una plataforma tecnológica académica con varios módulos que están a disposición de docentes, estudiantes y personal administrativo. Uno de ellos es el de evaluación docente en el que intervienen estudiantes, docentes y personal administrativo.

El sistema de evaluación docente se encuentra alojado en una plataforma web y necesita cumplir con ciertos requerimientos para preservar el activo más importante que son los datos obtenidos de la evaluación docente por lo que se realizó un estudio de vulnerabilidades para conocer la situación actual establecer si cumple con las normas de seguridad de la información mediante la norma ISO 27002:2017.

Se realizó un análisis de riesgos, siguiendo la metodología MAGERIT. Para ello se han identificado todos los activos que posee la organización y se han valorado. A continuación, se han analizado las posibles amenazas a las que está expuesta la organización y se ha obtenido el impacto y riesgo potencial de cada uno de los activos identificados.

Por último, se realizó una lista de comprobación para evaluar el cumplimiento de la norma de seguridad de la información de la ISO 27002:2017 con la finalidad de conocer el estado actual y proponer recomendaciones adecuadas del caso mejorar el funcionamiento del sistema de evaluación docente.

Palabras clave: evaluación docente, vulnerabilidades, ISO, Magerit, EAR/Pilar

Abstract

The teacher evaluation is an important process within Ecuadorian universities, it allows to improve the methodologies employed in teaching profession and possible failures in education and in this way achieve the university accreditation currently required by organism of control as the Higher Education Council of Ecuador (CES).

With the continuous growth of information technologies and the use of systems in all types of companies, products and services, the management of the same becomes uncontrollable by the volumes of information generated. Técnica del Norte University has technological platform academic with several modules that are available to teachers, students and administrative staff. One of them is the teacher evaluation in which are intervene students, teachers and administrative staff.

The teacher evaluation system is hosted on a web platform and needs to comply with certain requirements to preserve the most important assets which are the data obtain from the teaching evaluation so a vulnerability study was carried out to know the current situation to establish whether it complies with the safety standards of the information by using the ISO 27002:2017.

A risk analysis was carried out, following the methodology MAGERIT. For it, all the assets that owns the organization were identified and have been valued. Then there have been analyzed the possible threats to which the organization is exposed and there have been obtained the impact and potential risk of each of the identified assets.

Finally, a check list was realized to evaluate the fulfillment of the safety standards of the information of the ISO 27002:2017 with the purpose of knowing the current state and proposing appropriate recommendations to improve the functioning of the teacher evaluation system.

Keywords: Teacher evaluation, vulnerabilities, ISO, MAGERIT, EAR/Pilar

INTRODUCCIÓN

Antecedentes

El Sistema de Evaluación Docente de la Universidad Técnica del Norte, es parte del Sistema académico el cual permite evaluar a docentes por parte de los estudiantes la calidad de la educación mediante varias actividades como: investigación, docencia o gestión académica, esto se realiza con el fin de fortalecer el proceso de enseñanza conforme a la visión que proyecta la Universidad. Por tal razón los datos que se recopilan de las evaluaciones se encuentran expuestos a riesgos y vulnerabilidades físicas y lógicas, por lo que es necesario realizar la investigación y formular alternativas para resolver los posibles riesgos tomando como referencia la norma ISO/IEC 27002:2017 ¹ y la metodología Magerit V3².

Según (Manuel Muñoz, 2015) “Un SGSI³ es para una organización, el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información”.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo, adaptándose a los cambios internos de la organización, así como los externos del entorno. (Manuel Muñoz, 2015)

Se usará la norma ISO/IEC 27002:2017, esta normativa establece directrices y principios generales para iniciar, implementar, mantener y mejorar una gestión de seguridad de la información en una organización. Los objetivos definidos en esta norma proveen directrices generales sobre las metas generadas para una gestión de la seguridad de la información.

¹ ISO/IEC 27002:2017: Tecnología de la Información. Código de prácticas para los controles de seguridad de la información.

² MAGERIT: Metodología de Análisis de Riesgos de los Sistemas de Información.

³ SGSI: Sistema de Gestión de Seguridad de la Información

La metodología Magerit mide la vulnerabilidad por la frecuencia histórica cuantitativa de la materialización de la amenaza sobre el activo, cuando es factible (fiabilidad de un componente hardware, número de fallos de software); o bien por la potencialidad cualitativa de dicha materialización, cuya primera aproximación lleva a emplear una escala vista en las amenazas potenciales (consideradas ahora reales, es decir agresiones). No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a los riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas). (Jácome León, Pusedá Chulde, & Imbaquingo Esparza, 2017)

Justificación e Importancia

Impacto Tecnológico

Dentro de la Universidad Técnica del Norte al igual que cualquier organización se usan sistemas informáticos, siendo un activo fundamental la información, que necesita protección ante amenazas que afectan diariamente la disponibilidad e integridad de la organización, para evitar riesgos altos, daños operantes y económicos para la organización.

Por esto, se debe establecer procedimientos y controles de seguridad. Los procedimientos establecidos se obtienen del análisis de riesgos empleado para identificar los riesgos presentes y afrontarlos de manera adecuada. De esta forma se reduce las amenazas, disminuye los costos y asegura el cumplimiento de la normativa. Es importante el apoyo de la institución, para que el estudio tenga el efecto deseado.

Impacto Social

Con la propuesta de esta metodología se espera ofrecer una solución para que las instituciones públicas o privadas dispongan de un método que les permita identificar posibles amenazas que afectan a los activos, además de verificar las vulnerabilidades, con la finalidad de determinar el impacto que tendrá en la institución las posibles amenazas encontradas.

Prospectiva

Con este estudio se pretende mantener y verificar la seguridad de la información del sistema de Evaluación Docentes, mediante las características básicas de disponibilidad, integridad y confiabilidad y el cumplimiento de la norma ISO/IEC 27002:2017, a través de la metodología MAGERIT. Se tomó en cuenta éste sistema ya que facilita la gestión y desempeño de los docentes dentro de las aulas, para mejorar el sistema de educación, siendo principales usuarios los estudiantes que cada semestre evalúa a cada uno de ellos.

Objetivos

Objetivo General

- Evaluar la seguridad de la información al sistema de Evaluación de Docentes de la Universidad Técnica del Norte basado en la ISO 27002:2017 con la metodología Magerit V3.

Objetivos Específicos

- Diagnosticar la situación real con respecto al proceso de análisis de riesgos en el Sistema de Evaluación Docente.
- Evaluar las vulnerabilidades encontradas, de acuerdo con los riesgos y su impacto mediante la Metodología Magerit V3.
- Elaborar un documento con los riesgos encontrados, referente al Sistema de Evaluación de Docentes en base al análisis y aplicación de la metodología.

Alcance

El presente proyecto tiene como finalidad evaluar la seguridad de la información del Sistema de Evaluación de Docentes de la Universidad Técnica del Norte, se iniciará con la recopilación de la información la que permitirá evaluar los controles más importantes de la norma ISO 27002:2017, que contribuyan con la elaboración de un análisis de la situación actual del sistema. Además, se toma en cuenta los parámetros descritos en ella, para establecer soluciones adecuadas a las falencias encontradas, cumpliendo con los requerimientos de la Norma ISO 27002:2017, conjuntamente con la aplicación de la metodología Magerit, en todas sus fases, mismas que se representan en la figura 1.

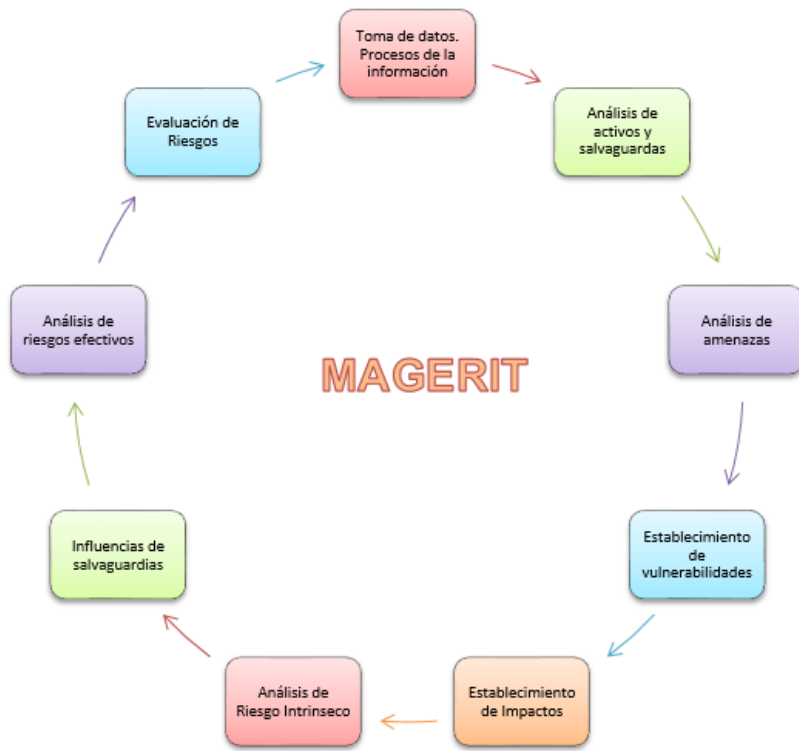


Figura 1: Fases de la Metodología Magerit
 Fuente: Elaboración Propia

CAPÍTULO 1

Marco Teórico

1.1 CONCEPTOS DE AUDITORÍA, TIPOS DE AUDITORIA

1.1.1 Auditoria

La auditoría se desarrolla basándose en normas, procedimientos y técnicas definidas formalmente por institutos establecidos a nivel nacional e internacional.

Etimológicamente la palabra auditoria proviene del latín audire, que significa 'oir', y tiene su origen en los primeros auditores que ejercían su función juzgando verdad o falsedad. También se dice que viene del verbo en inglés to Audit, que significa 'revisar' o 'intervenir'.

Según la real academia de la lengua española, define auditoria como: "Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse". (Real Academia de la Lengua Española, 2018)

1.1.2 Tipos de Auditoría

a) Auditoría Fiscal

La auditoría fiscal es realizada por la Administración Tributaria con el fin de denominar las responsabilidades pecuniarias⁴ de los contribuyentes, y a su vez la practicada pre-profesionales independientes en orden para dar una opinión sobre la razonabilidad de las cuentas de las entidades públicas por conceptos fiscales. (Miramegias, 2018)

b) Auditoria 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

⁴ Pecuniarias: denominación de la sanción que consiste en el pago de una multa al Estado como castigo por haber cometido un delito

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 Auditoria 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) Auditoria Informática

La auditoría informática se ocupa de la revisión del uso de las TI⁵, 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)

1.1.3 Clasificación de Auditoria

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

⁵ 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

organización; además de ello la desarrollan personas que dependen del negocio y actúan 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).

1.2 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA O SEGURIDAD DE LA INFORMACIÓN

Dentro de una organización a diario se genera cantidades enormes de información de diversas fuentes como bases de datos, correos electrónicos documentos en papel, etc. La información cumple un ciclo de vida que tiene un periodo de validez, es decir la información que hoy puede ser crítica, con el pasar del tiempo podría dejar de ser importante y necesaria.

1.2.1 ¿Qué es Seguridad Informática?

La seguridad informática se relaciona con procesos, procedimientos y metodologías que ayudan a salvaguardar los datos y la información privada de una organización. Los procesos se van estructurando con el uso de normas, protocolos, estándares y metodologías que servirán para minimizar riesgos en una infraestructura tecnológica.

Según el autor (Gabriel Baca Urbina, 2016) define la seguridad informática como: la disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta.

Es decir, en caso de existir una amenaza a la seguridad, se debe buscar la forma de recuperar la información sea que haya sido robada o dañada.

1.2.2 ¿Qué es Seguridad de la Información?

Las organizaciones públicas o privadas, al igual que las personas, dependen de muchas maneras de la tecnología de la información, como un punto esencial para lograr todas sus metas de negocio o para poder desarrollar actividades en su vida cotidiana, todos tienen que

enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas. (Tarazona, T Cesar H, 2011)

La seguridad de la información debe tener 3 cualidades:

- a) Crítica: al momento de operar la información puede correr riesgos.
- b) Valiosa: los datos que se manejan dentro de una organización son confidenciales y no pueden ser divulgados.
- c) Sensible: ya que al sistema solo podrán ingresar personas que estén autorizadas en el manejo.

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. (Asociación Española para la Calidad, 2012)

1.2.3 Requisitos de seguridad de la información

Es esencial que la organización identifique sus requisitos de seguridad. Según (INEN, 2017) existen tres fuentes principales de requisitos de seguridad:

- a) La evaluación de los riesgos de la organización: teniendo en cuenta los objetivos y estrategia de negocio globales de la organización. A través de una evaluación de los riesgos se identifican las amenazas de los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su impacto potencial (INEN, 2017).
- b) El conjunto de requisitos legales, estatutarios, reglamentarios y contractuales que debería satisfacer a la organización, sus socios comerciales, contratistas y proveedores de servicios, así como el entorno sociocultural (INEN, 2017).
- c) El conjunto de principios, objetivos y requisitos de negocio que la organización ha desarrollado para el manejo, procesamiento, almacenamiento, comunicación y archivo de la información que da soporte a sus operaciones (INEN, 2017).

Los recursos utilizados en la implementación de los controles han de estar equilibrados, con el nivel de daños probables que resultarían de problemas de seguridad, en ausencia de dichos controles. Los resultados de una evaluación de riesgos ayudarán a guiar y determinar las acciones de gestión más adecuadas y las prioridades para la gestión de riesgos de seguridad de la información, así como para la implementación de los controles seleccionados para protegerse contra estos riesgos. (INEN, 2017)

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

La seguridad de la información es parte de la gestión global del riesgo de una entidad, los aspectos que se superponen con la ciberseguridad, así mismo con la gestión de la continuidad del negocio y la tecnología de la información.

En la figura 2 se puede apreciar como la gestión del riesgo engloba varios aspectos teniendo en cuenta el riesgo que puede afectar al rendimiento de una empresa.



Figura 2: Seguridad de la información en una empresa.

Fuente: ISO-27000 (International Organization for Standardization, 2017).

La seguridad informática trata de salvaguardar la información que se obtiene mediante los datos de la organización, asignando una persona acreditada para el manejo de la información, el robo de esta información podría causar daños y perjuicios a la organización ya que podría ser mal usada en manos de personas no autorizadas

1.2.5 Pilares de la Seguridad Informática

Según (Romo, Daniel; Valarezo, 2012) la seguridad de la información está apoyada en 3 pilares fundamentales de la seguridad:

a) Confidencialidad

Certifica que solo los usuarios con accesos autorizados puedan acceder a la información. La seguridad que se implementará debe asegurar que solo las personas que tengan acceso a la información fueron autorizadas. Una medida que mitiga este tipo de riesgo es la firma de contratos de confidencialidad o inclusión de este tipo de cláusulas en el contrato de servicio. (Ministerio de Energía, 2017)

b) Integridad

Hace referencia a que la información sea correcta y no se modifique, ni haya errores. La información puede ser corrompida y se puede basar decisiones en torno a la información, lo cual da la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad (Hidalguense, 2011).

c) Disponibilidad

Según (Chilán & Williams, 2017) la disponibilidad es cuando se asegura que los usuarios autorizados tienen el acceso debido a la información siendo la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La información es el núcleo dentro de una organización, se indica la relación que existe dentro de la misma, por ello es necesario mantener un nivel aceptable de protección para estos componentes y minimizar los riesgos a los que puede estar expuesta cualquier tipo de entidad.

Es decir, la seguridad de la información tiene como misión principal cuidar del buen funcionamiento de los datos y de la transmisión de los mismos en un entorno seguro utilizando protocolos de seguridad y técnicas para evitar riesgos como se aprecia en la figura 3.

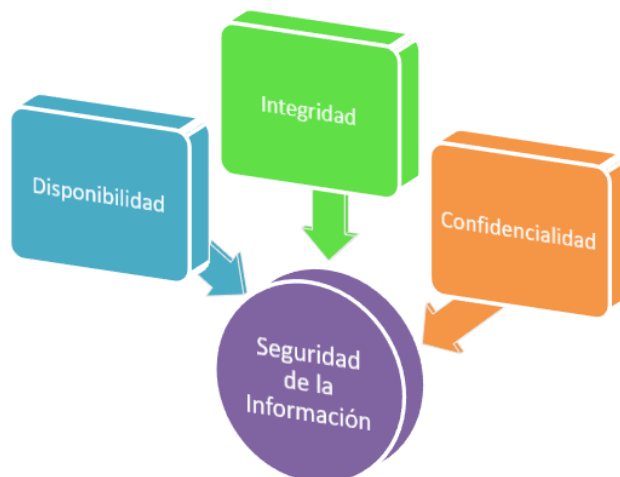


Figura 3: Pilares de la Seguridad Informática

Fuente: Elaboración Propia

Aunque son los principales, existen otros pilares que se detallan a continuación:

d) Autenticidad

Propiedad o característica la cual consiste en que una entidad es quien dice ser, o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

e) Trazabilidad

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Todas estas características pueden ser requeridas o no dependiendo de cada caso.

1.3 Conceptos de Vulnerabilidad, Amenaza, Riesgo

Para poder comprender la seguridad informática es necesario conocer algunos conceptos que son básicos para poder comprender el presente documento.

1.3.1 Vulnerabilidad

Las vulnerabilidades son debilidades que se pueden presentar en los procesos de la información. Los atacantes aprovechan las falencias de los sistemas de información para ingresar de forma no autorizada y robar la información de una organización.

1.3.2 Amenaza

Según el (Instituto Nacional de Ciberseguridad, 2017) Expone que una amenaza es toda acción que aprovecha una vulnerabilidad para atentarse contra la seguridad de un sistema de información. Es decir, las amenazas podrían ocasionar pérdidas dentro de la organización, las amenazas pueden ser ataques, fraudes, de efecto natural (incendios, inundaciones), mal manejo de contraseñas, etc.

1.3.3 Riesgo

Según (Voutssas M., 2010) define el riesgo como la probabilidad de que un evento nocivo ocurra combinando con su impacto en la organización.

En la Figura 4 se puede apreciar la relación de las amenazas, vulnerabilidades y los sistemas de información los cuales se encuentran expuestos y causan riesgos a la organización.



Figura 4: Relación de Vulnerabilidad, Amenazas y Sistemas de Información

Fuente: Elaboración Propia

1.4 Clasificación de las amenazas informáticas

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

- Amenazas Físicas
- Amenazas Lógicas

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

- Personas
- Programas o aplicaciones específicas
- Catástrofes naturales

1.4.1 Tipos de amenazas informáticas.

Hay muchas amenazas informáticas en el mundo, como lo describe. (Tarazona, 2007)

Algunas de estas amenazas son:

- Virus informáticos
- Uso no autorizado de los sistemas informáticos.
- Robo de información
- Suplantación de identidad
- Divulgación de la información
- Desastres naturales

A continuación, se detallan algunas de las principales amenazas:

- **Spyware:** Código malicioso cuyo principal objetivo es recoger información sobre las actividades en cualquier ordenador.
- **Troyanos, virus y gusanos:** Son programas maliciosos, que se posicionan en los ordenadores con el propósito de permitir el acceso no autorizado a un atacante.
- **Phishing:** Es un ataque del tipo de ingeniería social, en la cual cumple con el objetivo de obtener de manera fraudulenta datos confidenciales de un usuario, especialmente financieros.
- **Spam:** Estos llegan a través de correo electrónico, el cuales difundir grandes cantidades de mensajes comerciales o propagandísticos.
- **Botnets:** Es una amenaza que controla los ordenadores de forma remota, quedando incorporadas en redes distribuidas de ordenadores llamadas robot.

- **Trashing:** Este nombre hace referencia al manejo de la basura, estos se manejan también por ingeniería social, el objetivo de ello es recopilar información desechada para robar su identidad.

1.4.2 Ataques informáticos

Los ataques informáticos aprovechan las debilidades en el software, en el hardware, y en el personal humano que son parte de un ambiente informático. Para obtener un beneficio, por lo general de índole económico, afectando a la seguridad del ordenador, que a su vez repercute a los activos de la organización.

Para evadir estos ataques es necesario emplear varios procedimientos, es decir las mejores prácticas que facilitan la lucha contra las actividades delictivas y que reduzcan notablemente el campo de acción de las mismas. (Mieres, 2011)

En la siguiente figura se puede apreciar según el informe de riesgos globales del año 2019 los riesgos globales siendo los principales los riesgos ambientales, aunque estos se desarrollaran a largo plazo (Cecilia Reyes, 2017)

En la figura 5 se puede apreciar los riesgos y el incremento en el 2019.

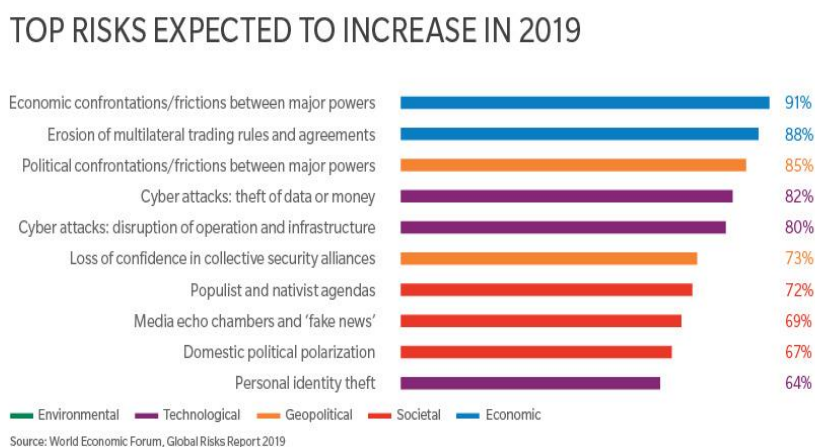


Figura 5: Riesgos globales

Fuente: <https://www.marsh.com/ar/es/insights/research/informe-riesgos-globales-2019.html>

1.5 Estándares ISO 27000

1.5.1 ¿Qué son los Estándares ISO 27000?

Las normas ISO 27000 son un conjunto de estándares desarrollados en fase de desarrollo por ISO (International Organization for Standardization), e IEC (International Electrotechnical Commission). Estas proporcionan un marco de gestión de seguridad de la información utilizando Organización pública, privada, grande y pequeño. (International Organization for Standardization, 2017)

1.5.2 Estándares que conforman la Familia de la ISO 27000

La familia ISO 27000 tiene una serie de estándares certificables de seguridad como se muestra en la Figura 6.

La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Información (SGSI).

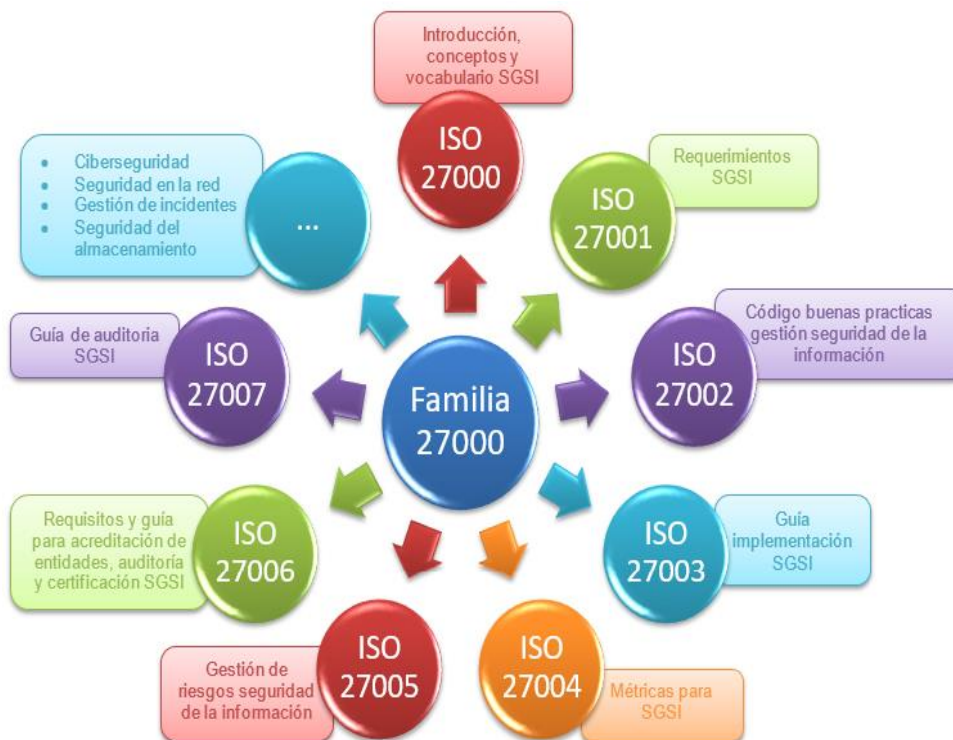


Figura 6: Serie de Estándares de la familia ISO 27000.

Fuente: Elaboración Propia

La Organización Internacional de Estandarización (ISO) contiene una serie de normas que conforman la familia de ISO 27000, la cual contiene una serie de definiciones y términos y que pueden ser usados dependiendo el caso, para mayor explicación se ha resumido cada estándar como se detalla en la tabla 1.

Tabla 1: Normativa ISO 27000

| NORMA | DESCRIPCION |
|-------------------|--|
| ISO/IEC | |
| ISO 27000: | Es una norma internacional que proporciona una visión de los sistemas de gestión de seguridad de la información y los términos de uso en la familia de normas de SGSI. Esta norma se puede aplicar a todo tipo y tamaño de organización. |
| ISO 27001: | Detalla los requisitos para establecer, implementar, monitorear, operar, revisar y mejorar los sistemas de gestión de seguridad, determinando los riesgos globales de negocio, de igual manera especifica los requisitos para la aplicación de controles de seguridad de la información. |
| ISO 27002: | Provee una lista de objetivos de control de las mejores prácticas para ser utilizadas como una guía de implementación en la selección y la aplicación de control para la seguridad de la información. |
| ISO 27003 | Proporciona una guía práctica de implementación y proporciona información para implementar, establecer, operar, revisar y mejorar un SGSI basándose en la ISO/IEC 27001 |
| ISO 27004 | Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA. (International Organization for Standardization, 2017) |
| ISO 27005 | Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. (International Organization for Standardization, 2017) |

ISO 27006: Especifica requisitos y proporciona una guía para los organismos que realizan la auditoría y la certificación del SGSI según IS/IEC 27001. Se basa en apoyar la acreditación de organismos de certificación.

ISO 27007: Es una guía sobre la realización de auditorías de SGSI, así como la orientación sobre la competencia de los auditores de sistemas de gestión de seguridad de la información.

Fuente: Propia

1.6 Estándares ISO/IEC 270001 e ISO/IEC 27002

1.6.1 Estándar ISO/IEC 27001

Es la norma internacional que permite la seguridad, la confidencialidad e integridad de los datos, así como de los sistemas que la procesan, además proporciona la aplicación de los controles necesarios para mitigarlos o eliminarlos. (International Organization for Standardization, 2017)

Esta norma puede ser aplicada por cualquier tipo de organización, con o sin fines de lucro, está redactada por profesionales en el tema y proporciona varios controles para implementar la gestión de la seguridad de la información en una organización. Esta norma es usada a nivel mundial para salvaguardar la información de cualquier entidad ya sea esta pública o privada.

Con la implementación de esta norma se puede obtener una ventaja comercial con menores costos y una mejor organización en las empresas. (International Organization for Standardization, 2017)

Este estándar emplea un ciclo continuo PDCA (Plan-Do-Check-Act) para obtener mejoras en 4 pasos como se puede apreciar en la figura 7 la cual se basa en los sistemas de seguridad de la información.

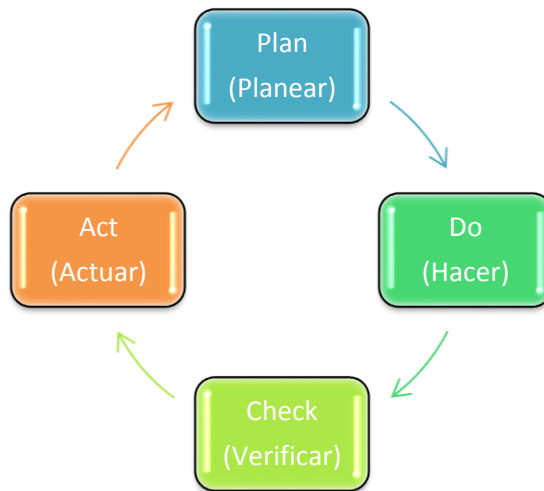


Figura 7: Ciclo de Deming PDCA Sistema de Gestión ISO/IEC 27001

Fuente: Elaboración Propia

1.6.2 Norma ISO 27002

Este es un estándar para la seguridad de la información creada por la organización internacional de normalización y comisión electrotecnia internacional. La versión más reciente de la norma ISO 27002:2017, brinda diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

Esta norma internacional establece directrices para la seguridad de la información en las organizaciones y las prácticas de gestión de seguridad de la información incluyendo la selección, la implantación, y la gestión de los controles. Además, considera el entorno de los riesgos de seguridad de la información de la organización. (INEN, 2017)

El valor de esta información se propaga por palabras escritas, números e imágenes, por ejemplo: el conocimiento, conceptos son formas intangibles de información. La información y sus procesos relacionados, los sistemas, las redes y el personal implicado en la operación y manejo de la información y protección. Estos son los activos que resultan valiosos para el negocio de las organizaciones y en consecuencia requieren protección contra diversos peligros.

La seguridad de la información se consigue mediante la implantación de un conjunto adecuado de controles, lo que incluye políticas, procesos, estructuras organizativas y funciones de hardware y software. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización.

1.6.3 Antecedentes y Contexto del Estándar ISO/IEC 27002:2017

Esta norma está diseñada para que las organizaciones la usen como referencia para seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001. También sirve como documento guía para organizaciones que necesiten implementar controles de seguridad de la información comúnmente aceptados. (INEN, 2017)

Las organizaciones de todo tipo y tamaño (incluyendo sector público y privado, comercial y sin ánimo de lucro) recogen, procesan, almacenan y transmiten información de muchas formas que incluyen medios electrónicos, físicos y verbales (por ejemplo, conversaciones y presentaciones). (INEN, 2017)

Los activos están expuestos ante amenazas deliberadas como accidentales, mientras que los procesos relacionados, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. Los cambios en los procesos y sistemas de negocio u otros cambios externos (por ejemplo, nuevas leyes y reglamentos) pueden crear nuevos riesgos de seguridad de la información. Por lo tanto, debido a las múltiples amenazas que existen en la actualidad, podrían aprovecharse de las vulnerabilidades para dañar a la organización y los riesgos de seguridad de la información siempre están presentes. Un ejemplo de seguridad de la información eficaz reduce estos riesgos protegiendo a la organización frente a amenazas y vulnerabilidades, en consecuencia reduce el impacto en sus activos. (INEN, 2017)

1.6.4 Ciclo de vida de la Norma ISO 27002

La información tiene un ciclo de vida natural, desde la creación y el origen de esta, pasando por el almacenamiento, tratamiento, utilización y transmisión hasta su deterioro. El valor y los riesgos para los activos puede variar durante su tiempo de vida, pero la seguridad de la información continúa siendo importante hasta cierto punto en todas las etapas.

Los sistemas de información tienen ciclos de vida en los cuales son creados, especificados, diseñados, desarrollados, probados, implantados, utilizados y finalmente retirados del servicio y eliminados. Los nuevos desarrollos del sistema y los cambios en los sistemas actuales presentan oportunidades para que las organizaciones actualicen y mejoren los controles de seguridad, teniendo en cuenta tanto los incidentes reales como los riesgos de seguridad asociados a incidentes actuales y futuros. (INEN, 2017)

1.6.5 Estructura de la Norma ISO 27002

La Norma ISO 27002:2017 está compuesta de 14 capítulos de controles de seguridad que en conjunto proporcionan un total de 35 categorías principales y 114 controles.

En la figura 8 se mencionan los 14 capítulos que posee la norma ISO 27002:2017.



Figura 8: Estructura Norma ISO/IEC 27002:2017

Fuente: Elaboración Propia

1.7 Metodologías para el Análisis de Riesgos

1.7.1 ¿Cuáles son las metodologías para el Análisis de Riesgos?

El análisis de riesgos informáticos es una parte fundamental en la administración de la seguridad, tiene algunos beneficios como son: identificar los puntos débiles de la estructura de TI la cual se encarga de dar soporte a los procesos críticos de la organización, es una guía de selección de medidas de protección de costo adecuado, y ayuda a determinar donde es necesario contar con esquemas de desastres y recuperación de desastres y continuidad del negocio mediante la realización de políticas de seguridad que mejor se adapten a las necesidades de la organización (Gutián, 2014).

Las metodologías de análisis de riesgos conforman una disciplina que permite realizar importantes escaneos de vulnerabilidades, mediante el uso de modelos y procesos para proponer una forma segura de cuidar la información y los recursos de TI. (Helena Alemán Novoa, 2015)

Los objetivos de las metodologías de análisis de riesgos tocan puntos importantes como: planificación de la reducción de accidentes, visualización y detección de las debilidades existentes en los sistemas. (Helena Alemán Novoa, 2015)

En la seguridad de la información existen diversas metodologías de análisis de riesgos dentro de las cuales tenemos:

- a) Octave: (Operational Critical Threat, Asset and Vulnerability Evaluation):** Es una Metodología muy usada por las empresas, evalúa los riesgos de seguridad de la información y propone un plan de mitigación dentro de la organización. Esta metodología realiza procesos de evaluación de activos relacionados con la información, analiza y estudia la infraestructura de la información. La metodología Octave tiene como finalidad orientar a la organización para que dirija y gestione sus evaluaciones de riesgo, proteja activos críticos de información, ya que es un método operativo orientado a resultados. (Huerta, 2012)
- b) Magerit:** Es una metodología de gestión de riesgos de la información, la que permite estudiar los riesgos que soporta un sistema de información y el entorno asociado al mismo, la metodología detalla desde tres perspectivas: describir los pasos para realizar un análisis del estado del riesgo y gestionar su mitigación, describe tareas básicas para realizar un proyecto de análisis y gestión de riesgos.

Permite descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos de evaluación y los resultados se expresan en valores económicos (Helena Alemán Novoa, 2015).

- c) **Mehari:** Método Armonizado de Análisis de Riesgos: es la metodología de análisis y gestión de riesgos desarrollada por la CLUSIF (Club de la Sécurité de l'Information Français) en 1995 y deriva de las metodologías previas Melissa y Marion. La metodología ha evolucionado proporcionando una guía de implantación de la seguridad en una entidad a lo largo del ciclo de vida. Del mismo modo, evalúa riesgos en base a los criterios de disponibilidad, integridad y confidencialidad (Helena Alemán Novoa, 2015).
- d) **NIST SP 800-30:** Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la seguridad de la información, necesita el apoyo de la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito. (Universitaria, Castellanos, & Ingeniería, 2018)
- e) **Coras:** la misión de esta metodología, consiste en proporcionar un marco de trabajo encaminado a sistemas en los que la seguridad es crítica, la aplicación de esta metodología permite la detección de fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad mediante las etapas que contempla la metodología. (Universitaria et al., 2018)

1.8 Selección de metodología para análisis de riesgos.

Para elegir una de las metodologías para el análisis de riesgos de la información se basó en un estudio realizado de una comparación entre la metodología CRAMM y MAGERIT que según (Cordero Torres & Crespo, 2016) realizó con la normativa ISO 31000 la cual ofrece directrices y principios para gestionar el riesgo de las organizaciones, esta normativa recomienda que las organizaciones desarrollen, implanten y mejoren continuamente el marco de trabajo teniendo el objetivo de integrar el proceso de gestión de riesgos en cada una de las actividades.

Según (ISOTools, 2016) el proceso técnico de la gestión del riesgo, se encuentra estructurado mediante una secuencia, cuyas fases se ordenan de la siguiente forma:

- **Establecer el contexto estratégico:** Consiste en la definición de parámetros básicos para la gestión del riesgo, alcance y criterios para los procesos, se debe hacer de manera necesaria desde el conocimiento de todos los aspectos que se engloban en la actividad que se lleva a cabo en la organización (ISOTools, 2016).
- **Identificar los riesgos:** la empresa tiene que identificar los riesgos de forma sistémica, las causas y los posibles efectos que tendría su materialización. Se encuentran recogidas las acciones que se relacionan con la clasificación del riesgo, dependiendo de su tipología (ISOTools, 2016).
- **Analizar el riesgo:** en esta fase se establece la probabilidad de que suceda un riesgo y el impacto que generan sus consecuencias, mediante una calificación y evaluación con el fin de establecer el nivel de riesgo y acciones correctoras. El éxito de este proceso depende en gran medida de la calidad de la información que se haya tenido en la fase de identificación y tipo de método que se haya escogido para realizar el análisis (ISOTools, 2016).
- **Valoración de riesgos:** se deberán confrontar los resultados obtenidos a raíz del análisis del riesgo, con las medidas de control que han sido especificadas se establece prioridades en el tratamiento de los riesgos y fijar políticas de gestión adecuadas (ISOTools, 2016).
- **Políticas de administración de riesgos:** constituye la fase final, una vez que se tenga identificado, clasificado y valorado los riesgos es el momento de establecer las políticas de gestión del riesgo, las cuales se encuentran en 4 ejes diferentes que son: transferencia del riesgo, retención del riesgo, reducción del riesgo o evitar el riesgo (ISOTools, 2016).
- **Monitorización y revisión:** teniendo en cuenta que es difícil que los riesgos detectados dejen de suponer una amenaza para la organización es necesario establecer indicadores de seguimiento sobre medidas que se establecen para la gestión de riesgos (ISOTools, 2016).

Una vez que se ha explicado los parámetros que componen la ISO 31000, se procede a realizar comparación de la metodología MAGERIT y CRAMM.

Esta comparativa permitirá verificar porque se escogió MAGERIT como metodología de análisis de riesgos para el presente trabajo.

Tabla 2: Comparación Metodologías MAGERIT y CRAMM

| PARAMETROS | MAGERIT | CRAMM | CUMPLE |
|-------------------------------|--|---|----------------|
| ISO 31000 | | | |
| Comunicación | <p>Permite tener un contacto con:</p> <ul style="list-style-type: none"> • Miembros de gobierno y la toma de decisiones. • Usuarios y técnicos del sistema. | Permite tener contactos con los actores de la organización. | MAGERIT |
| Establecer el contexto | <p>Magerit lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que seguirá para la gestión de riesgos mediante:</p> <ul style="list-style-type: none"> • Alcance del análisis. • Obligaciones propias y contraídas. • Relaciones con otras organizaciones (intercambio de información y servicio) <p>Permite documentar el entorno en el que opera la organización.</p> | CRAMM determina los alcances de la organización. | MAGERIT |

| | | | |
|-------------------------------|---|---|----------------|
| Establecer el contexto | <p>Identifica las obligaciones legales y reglamentos contractuales.</p> <p>Identifica el contexto interno en el que se desenvuelve las actividades de la organización como:</p> <ul style="list-style-type: none"> • Políticas de seguridad y normas. • Requisitos de cumplimiento normativo. • Obligaciones contractuales. • Roles y funciones. • Criterios de valoración de información y servicios. • Criterios de valoración de riesgos. • Criterios de aceptación de riesgos. • Contingencias o riesgos de los activos. <p>Contexto de riesgos:</p> <ul style="list-style-type: none"> • Arboles de ataques: permite modelar las diferentes formas de alcanzar un mismo objetivo dentro de la organización. | <p>CRAMM determina los alcances de la organización.</p> | MAGERIT |
| Identificación | <p>Magerit identifica los activos de acuerdo a la función dentro de la organización por medio de levantamiento de procesos e identificando cada activo relevante a cada</p> | <p>CRAMM identifica los activos: tres tipos de activos que componen la información:</p> <ul style="list-style-type: none"> • Físicos | MAGERIT |

departamento, tomando en cuenta la criticidad y se categorizan de la siguiente manera:

- Activos fundamentales: Información
- Activos secundarios: servicios, aplicaciones informáticas, hardware, redes, instalaciones, personas.

También utiliza métodos de identificación como:

- Modelo de apéndice: activos con código, nombres descriptivos.
- Modelo cuantitativo: cierta dimensión es un número mayor a 0.
- Modelo cualitativo: asigna a cada activo un valor con una dimensión, identifica las dependencias del activo, valor acumulado.

Riesgos:

- Situación: activo – tiempo – amenaza.
- Riesgo acumulado.
- Riesgo repercutido.

- Software (aplicaciones)
- Datos (toda la información obtenida de los sistemas)

Identificación

| | | | |
|--|--|--|-----------------------|
| <p>Análisis</p> | <ul style="list-style-type: none"> • Riesgos cualitativos: permite saber que hay, sin cuantificar con precisión trabajando sobre una escala discreta de valores basada en impacto y probabilidad. • Riesgo cuantitativo: identifica que hay cuantificando con precisión, trabajando en números reales. • Modelo escalonado: determina una serie ordenada de escalones de valoración. <p>Se basa en: impacto, probabilidad y nivel de necesidad de salvaguardas.</p> | <p>CRAMM no realiza este procedimiento</p> | <p>MAGERIT</p> |
| <p>Técnicas específicas para el análisis de riesgos</p> | <p>Dentro de la metodología MAGERIT se aplican las siguientes técnicas:</p> <ul style="list-style-type: none"> • Tablas: no son muy precisas, pero aciertan con la identificación utilizando una escala de valores que permiten calificar a los activos: <p>MB: muy bajo B: bajo M: medio A: alto MA: muy alto.</p> | <p>CRAMM no realiza este procedimiento</p> | <p>MAGERIT</p> |

| | | | |
|---------------------------|--|-------------------------------------|----------------|
| Técnicas generales | <p>La metodología MAGERIT permite varias técnicas como:</p> <ul style="list-style-type: none"> • Técnicas gráficas: se centra en representaciones graficas ara apoyar la toma de decisiones todo depende de la obtención de información. | CRAMM no realiza este procedimiento | MAGERIT |
| Evaluación | <ul style="list-style-type: none"> • Riesgo Intrínseco: medida del daño probable sobre un sistema sin considerar las salvaguardas. • Riesgo residual: media del daño una vez que se hayan considerado las salvaguardas. • Riesgo efectivo: medida del daño probable al que está sometido el activo tras la valoración de las salvaguardas y tomando en cuenta el valor propio de cada activo. • Las salvaguardas son evaluadas según su eficacia, reduciendo el riesgo de cada activo que protege. | CRAMM no realiza este procedimiento | MAGERIT |
| Tratamiento | <ul style="list-style-type: none"> • Eliminación: se pueden eliminar varias cosas siempre y cuando no se altere la esencia de la organización. | CRAM no realiza este procedimiento | MAGERIT |

-
- Mitigación: reducir la degradación causada por una amenaza, reducir la probabilidad de que una amenaza se materialice. CRAM no realiza este procedimiento
 - Compartición del riesgo: riesgo cualitativo mediante la externalización de componentes del sistema, riesgo cualitativo por medio de la contratación de seguros.
 - Financiación: una vez que se hayan aceptado los riesgos la organización destinara un fondo económico en caso de que el riesgo llegue a concretarse.

Fuente: *Elaboración Propia*

A considerar:

- Magerit es la metodología más usada a nivel de Latinoamérica.
- El beneficio que presenta la metodología MAGERIT es que está en idioma español e inglés.
- Las dos metodologías son de gestión de riesgos en caso de CRAMM tiene dos herramientas que son CRAMM Expert, CRAMM Express son comerciales y están en inglés, el caso de MAGERIT usa la herramienta EAR es comercial pero la herramienta PILAR es gratuita.
- Las metodologías se adaptan para trabajar con estándares internacionales. MAGERIT adopta prácticas de las ISO 27001⁶, 27002⁷, 15408⁸ y 13335⁹. La metodología CRAMM tiene un enfoque práctico en referencia a la ISO 27002, también contempla fundamentos de la ISO 27005 e ISO 31000.
- El ciclo de vida de la metodología CRAMM se basa en identificar primero los riesgos y luego estimar la frecuencia de presentación, mientras que MAGERIT empieza con la identificación de activos, luego identifica amenazas lógicas y de entorno, establece frecuencias e impacto para poder identificar salvaguardas y gestionar el riesgo residual.
- MAGERIT considera activos de información al hardware, software, información electrónica, personas, instalaciones, medios de soporte y elementos de comunicación de datos. La metodología CRAMM considera como activos de información solamente a los datos.
- Para la identificación de activos la metodología CRAMM identifica riesgos y amenazas utilizando solamente métodos cualitativos y cuantitativos, además de valorar los activos en términos de costo de reemplazo y en dimensiones de disponibilidad, integridad y confidencialidad. La metodología MAGERIT además de los dos métodos ya explicados utiliza el método mixto, determina los valores de los activos considerando la dimensión de la disponibilidad, integridad,

⁶ ISO 27001: Sistemas de Gestión.

⁷ ISO 27002: Buenas prácticas para la gestión de la seguridad de la información.

⁸ ISO 15408: Evaluación de los criterios Comunes de la Seguridad en la Tecnología de la Información.

⁹ ISO 13335: Guía para la gestión de seguridad TI.

confidencialidad, trazabilidad y autenticidad, estableciendo escala de valoración en diferentes niveles: muy alto, alto, medio, bajo, muy bajo y despreciable, ésta metodología utiliza el impacto determinando el valor de los activos, el impacto acumulado se calcula mediante el valor acumulado del activo y las amenazas a las que afronta, y el impacto repercutido se considera el valor propio y las amenazas .

- La metodología MAGERIT se desarrollada para organizaciones públicas gubernamentales, mientras de CRAMM puede ser usada en cualquier organización.

Con respecto a lo establecido se escoge a la metodología MAGERIT por ser la más completa y evaluar todos los pilares de la seguridad informática, y tener un software de complemento como lo es el EAR/PILAR.

1.9 Metodología de Análisis y Gestión de Riesgos de Información (Magerit)

1.9.1 Introducción

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, fue elaborada por el Consejo Superior de Administración de España, actualizada en 2012 su versión 3, Brinda un método sistemático para analizar los riesgos del uso de las tecnologías de la información y la comunicación. 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 el uso de tecnologías de la información. (Ministerio de Hacienda y Administraciones Publicas de España, 2012)

En la Figura 9 se puede apreciar cómo se encuentra estructurada la Metodología de análisis y riesgos de los sistemas informáticos.

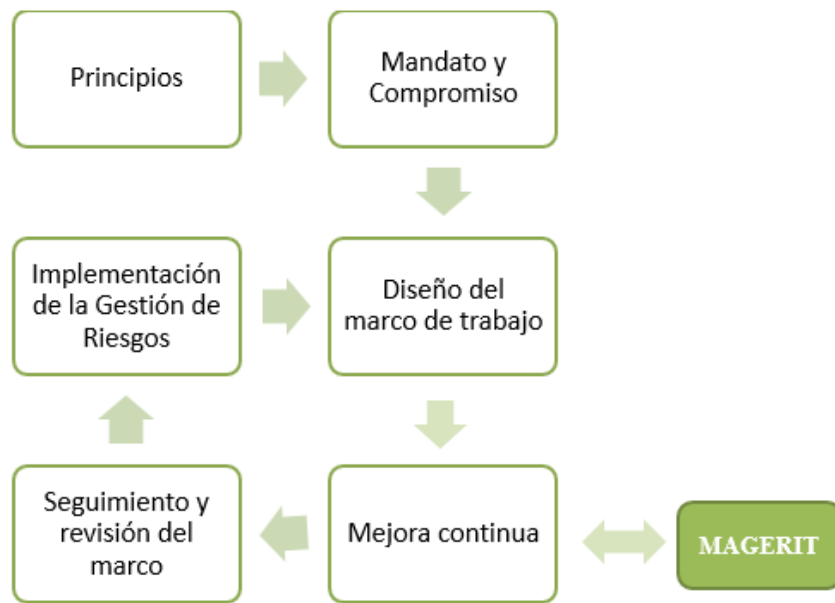


Figura 9: Marco de trabajo para la gestión de riesgos

Fuente: (Ministerio de Hacienda y Administraciones Publicas de España, 2012)

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte.

Todas buscan realizar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por lo que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

1.9.2 Objetivos de Magerit

Magerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones Tics¹⁰
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.9.3 Características de Magerit

Magerit tiene las siguientes características:

- Mantiene en gran medida la estructura de la versión 2
- Actualizada para un mejor alineamiento con la norma ISO
- Integración dentro del marco organizacional de la gestión de riesgos dirigido desde los órganos de gobierno.
- Eliminación de partes poco importantes.
- Mejora la normalización de actividades.

¹⁰ Tics: Tecnologías de la Información y las comunicaciones.

1.9.4 Estructura MAGERIT

La metodología consta de 3 libros: método, catálogo de elementos y guía de técnicas. Estos libros presentan pasos para analizar y tratar los riesgos, ofrecen elementos que ayudan a la organización a realizar los análisis y el conjunto de técnicas para llevar a cabo los proyectos de análisis de riesgos y la gestión de los mismos.

- **Libro I Método:** trata sobre las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos. De igual manera describe opciones y criterios para el tratamiento adecuado de los riesgos.
- **Libro II Catálogo de Elementos:** Presenta una clasificación de los activos, distintas dimensiones y criterios para realizar la valoración. También se plantean las amenazas típicas sobre los sistemas de información y las salvaguardas para proteger.
- **Libro III Guía de Técnicas:** En este libro se describe las técnicas utilizadas en análisis y gestión de riesgos, se explica el objetivo que se persigue al utilizarla, los elementos básicos asociados, los principios fundamentales de la elaboración.

CAPÍTULO 2

Desarrollo

2 Marco Contextual

Para determinar la importancia de estos riesgos es necesario realizar una evaluación de riesgos, mediante el análisis se establecerá si la información está expuesta de forma interna o externa, el éxito será que se apliquen las políticas de seguridad que existan dentro del Departamento de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.

2.1 Descripción del Sistema Informático Integrado Universitario (SIU)

La Universidad Técnica del Norte en la actualidad ofrece servicios en línea a todos los estudiantes y empleados en general, esto aumentó significativamente el volumen de accesos al Sistema Informático Integrado Universitario (SIU), mismo que abarca a los diferentes sistemas que posee la Universidad, por lo que se buscó soluciones tecnológicas asequibles, eficientes y seguras. La Universidad eligió la solución que mejor se adaptaba a las necesidades y preparó el entorno para la implementación de Oracle Cloud Infrastructure, siendo la única Universidad en el país que gestiona sus servicios Tic en plataformas cloud (DATTA BUSINESS INNOVATION, 2019).

Con la implementación de Oracle IaaS y Oracle PaaS se alcanzó un 99.9% de disponibilidad, se redujo la latencia al aumentar el rendimiento de SIU en 500 % ya que Oracle Cloud Infrastructure Compute Classic ofrece procesadores más rápidos y eficientes, resolviendo problemas de baja velocidad debido a cargas de big data, incrementó la capacidad de almacenamiento de forma inmediata y facilitó la futura expansión de la capacidad, pues las funciones elásticas de Oracle Database Cloud Service permiten que se agregue o elimine memoria y capacidad de almacenamiento según sea necesario, Aumentó la seguridad, ya que Oracle Cloud Infrastructure Compute Classic y Oracle Cloud Infrastructure Dedicated Compute Classic – SPARC aseguraron un entorno confiable de respaldo y recuperación de información ante desastres, y un firewall dinámico que controla el tráfico de red entre individuos y entre grupos (DATTA BUSINESS INNOVATION, 2019).

2.1.1 Sistema Académico - Universidad Técnica del Norte

Dentro del Sistema Informático Integrado Universitario (SIIU), consta el sistema académico, mismo que gestiona el proceso de matrículas, calendario académico, gestión de horarios, gestión docente, portafolio estudiantil y docentes, evaluación docente, entre otras, con el fin de brindar información de calidad a la Universidad optimizando tiempos de respuesta en reportes que ayuden en la toma de decisiones a las respectivas autoridades.

Dentro de este sistema académico se encuentra el sistema de evaluación docentes, el cual permite calificar el desempeño de los docentes y a las autoridades de cada carrera y facultad facilitando los procedimientos.

2.1.2 Sistema de Evaluación Docentes – Universidad Técnica del Norte

La evaluación del desempeño docente es importante para todas las instituciones educativas que buscan la calidad, en donde el producto final son los profesionales puestos al servicio de la sociedad. Los cuales deberán responder con solvencia a las necesidades del entorno y de esta manera garantizar los procesos académicos de la institución. ((CEIDPA), 2018)

La ejecución del proceso de evaluación docentes está basada en la aplicación de varios instrumentos como la autoevaluación, coevaluación y heteroevaluación para de esta manera obtener un diagnóstico real de los datos evaluados.

El DDTI es el encargado de recopilar los datos que se obtengan mediante el sistema de evaluación docentes, ya que este proceso consta de 4 fases como se detalla en la siguiente figura 10.



Figura 10: Proceso de evaluación integral

Fuente: ((CEIDPA), 2018)

- En la primera fase la planificación del proyecto consiste en cargar la información de las comisiones de coevaluación, y el departamento de DDTI generará claves y usuarios para poder ingresar se socializará a docentes de la actividad a realizar.
- La segunda fase de ejecución se realizará la evaluación de los docentes y directivos conforme lo registrado en cada distributivo aplicando las 4 evaluaciones correspondientes, estas evidencias serán verificadas en el portafolio docente del SIIU¹¹.
- La tercera Fase de resultados consiste en generar reportes los cuales se extiende al CEIDPA¹² y el comité encargado elaborará el informe correspondiente.
- La última fase consiste en el seguimiento al plan de perfeccionamiento en el periodo académico posterior al periodo evaluado.

¹¹ SIIU: Sistema Informático Integrado Universitario

¹² CEIDPA: Comisión Institucional de Evaluación Interna del Desempeño del Personal Académico

2.2 Estructura Organizacional

La estructura organizacional de la Universidad Técnica del Norte (UTN), está constituida por autoridades, funcionarios y organismos consultivos.

2.2.1 Organigrama Estructural UTN

La Universidad Técnica del Norte se encuentra constituida por los siguientes niveles administrativos como se detalla en la siguiente figura 11.

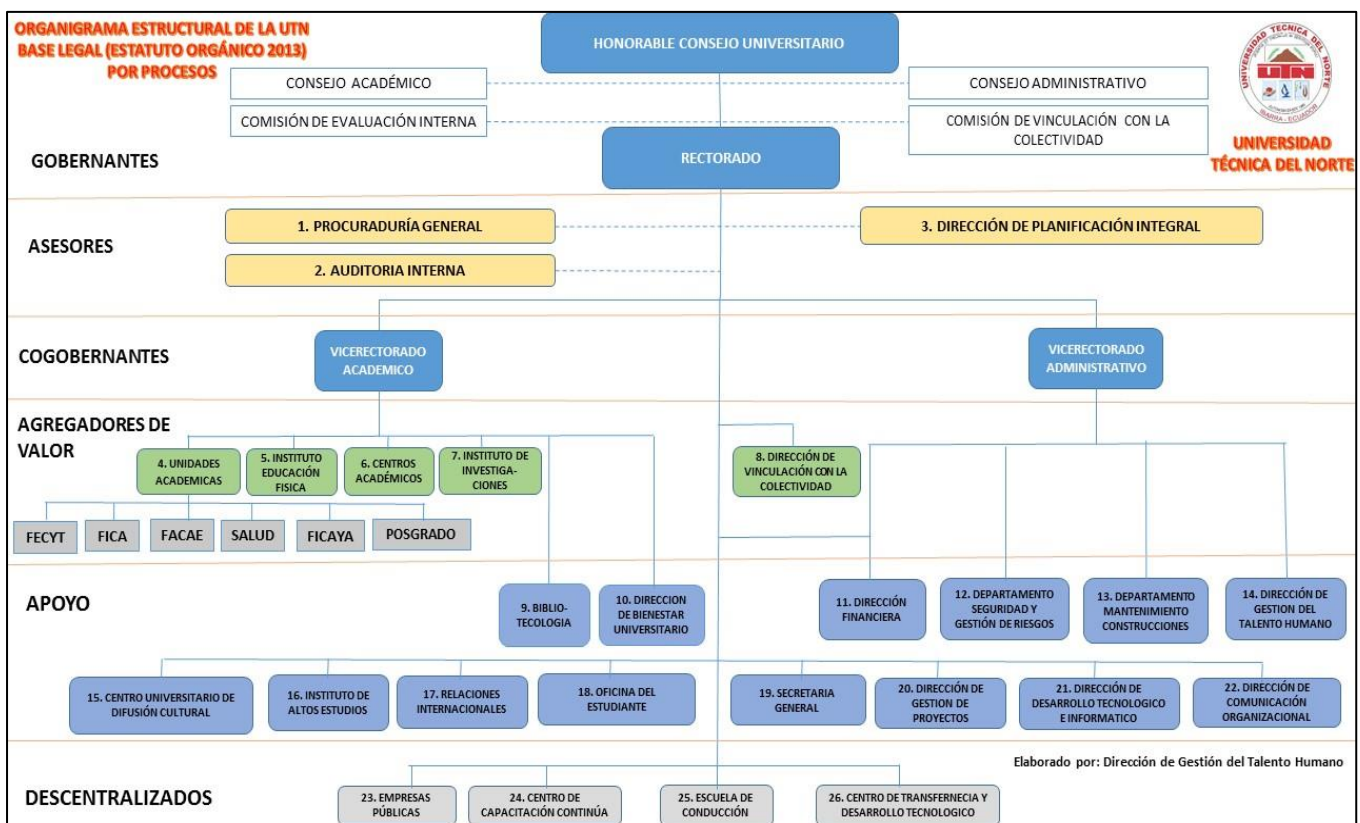


Figura 11: Organigrama Estructural UTN (2013)

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

2.2.2 Organigrama Departamento de Desarrollo Tecnológico e Informático UTN

Dentro del Departamento de Desarrollo Tecnológico e Informático (DDTI) se maneja un nivel administrativo que cumple con un orden jerárquico como se puede apreciar en la figura 12.



Figura 12: Organigrama Dirección Informática UTN

Fuente: (Departamento de Desarrollo Tecnológico e Informático - UTN, 2013)

2.2.3 Misión

“A la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, se encarga de administrar los servicios de informática, computación y comunicaciones; sin afectar a 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”. (Departamento de Desarrollo Tecnológico e Informático - UTN, 2013)

2.2.4 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 comunicaciones” (Departamento de Desarrollo Tecnológico e Informático - UTN, 2013)

2.3 Roles y Responsabilidades, funciones del personal de DDTI

En la siguiente tabla se detalla la función que realiza el personal dentro del DDTI.

Tabla 3: Roles y responsabilidades del personal de DDTI-UTN

| PUESTO | RESPONSABILIDADES Y FUNCIONES |
|------------------------------|---|
| Jefe de Proyecto | Es el encargado de asignar recursos, gestionar prioridades, coordinar las interacciones con los clientes, usuarios. Mantener al equipo del proyecto enfocado en los objetivos institucionales. Debe establecer y coordinar un conjunto de prácticas que aseguran la integridad y calidad del proyecto a efectuarse. Debe impulsar y desarrollar proyectos de tecnologías de información y comunicación que la Universidad requiera. Corroborar el buen funcionamiento y brindar mejores servicios para todos los usuarios. |
| Analista de Sistemas | de Su principal función es capturar, especificar y validar los requisitos, interactuando con el cliente y los usuarios mediante entrevistas, para satisfacer sus necesidades e inquietudes. Colaborar en la elaboración de las pruebas funcionales y modelos de datos mediante un sistema amigable fácil y atractivo al usuario. |
| Programador | Es el encargado de construir prototipos, elaborar las pruebas funcionales, modelos de datos y las validaciones con el usuario. |
| Ingeniero de Software | de Se encarga de la gestión de requisitos, la configuración y elaboración del modelo de datos, prepara las pruebas funcionales y la elaboración de la documentación. |

| | |
|--------------------------------|--|
| Administrador de la Red | <p>Su responsabilidad es realizar la adquisición de paquetes de software, licencias y hardware que permitan dar solución a las necesidades tecnológicas en el momento y situación oportuna.</p> <p>Tener una red monitoreada las 24 horas y operando al 100%.</p> <p>Disponer de equipos para el monitoreo permanente de la red de la Universidad.</p> |
| Web master | <p>Su principal función es la de fortalecer la investigación, implementación de nuevas tecnologías para la administración del Geo portal.</p> <p>Su rol es ser participe en dar soporte y soluciones informáticas de los diferentes planes y proyectos en las áreas de la institución que buscan mejorar las condiciones de procesos.</p> |
| Ingeniero de Hardware | <p>Gestiona y direcciona la adquisición de los insumos de software y hardware necesarios.</p> <p>Establece políticas de operación y control informático.</p> <p>Elabora y establece un plan de contingencia para asegurar la protección del hardware y la información ante algún desastre natural o provocado.</p> <p>Se encarga del manejo adecuado del catálogo electrónico de equipos informáticos del Sistema Nacional de Compras Públicas.</p> <p>Soporte técnico en el sitio y de soporte.</p> |

Fuente: Elaboración Propia

2.4 Técnicas de Investigación

2.4.1 Población y Muestra

Para calcular el tamaño de la muestra se utilizó el método de muestreo, para poder establecer el número de encuestados y determinar los servicios y seguridades del sistema de Evaluación Docentes de la Universidad Técnica del Norte.

El tamaño está determinado por 3 factores:

- Proporción estimada de la variable considerada
- Nivel deseado de fiabilidad
- Margen de error aceptable

El tamaño de la muestra está basado en una muestra aleatoria simple y que puede calcularse con la siguiente formula.

$$n = \frac{z^2 * (p * q)}{e^2 + \left(\frac{z^2(p * q)}{N}\right)}$$

En donde:

n= tamaño de la muestra

z= nivel de confianza deseado

p= proporción de la población con la característica deseada (éxito)

q= proporción de la población sin la característica deseada (fracaso)

e= nivel de erros dispuesto a cometer

N= tamaño de la población

Para este proyecto se dividió la población en: docentes, estudiantes y personal encargado del manejo del sistema de evaluación docentes.

Tabla 4: Usuarios Universidad Técnica del Norte

| Usuarios | Cantidad |
|----------------------|-----------------|
| Estudiantes | 9000 |
| Docentes | 770 |
| Personal DDTI | 17 |
| Total | 9785 |

Fuente: (Departamento de Desarrollo Tecnológico e Informático - UTN, 2013)

Con la fórmula aplicada se obtuvo una muestra de 343 estudiantes, 33 docentes y 3 personas encargadas del manejo del sistema de evaluación docentes a las cuales se aplicó las encuestas que se encuentran en el anexo 1 y anexo 2.

2.5 Fuentes y técnicas para la recolección de información

2.5.1 Tipos de Investigación

Para realizar el proceso de evaluación de amenazas y vulnerabilidades de la seguridad de la información se averiguo sobre la infraestructura tecnológica que posee la Universidad Técnica del Norte mediante dos tipos de investigación que son:

- **Descriptiva:** Se realizó este tipo de investigación para poder trabajar con las actividades, procedimientos y características fundamentales que tiene la universidad; de esta manera evaluar los riesgos relacionados con la seguridad de la información del sistema de evaluación docentes.
- **Mixta:** se aplica este método de investigación para verificar las políticas existentes en la Universidad y el departamento de Informática relacionadas con la seguridad de la información mediante encuestas a los usuarios del sistema de evaluación docente.

2.5.2 Fuentes y técnicas de recolección de información

Para la obtención de la información se tomará en cuenta las siguientes técnicas de recolección de información:

- **Encuestas:** Esta herramienta facilitó la recolección de información para poder identificar el nivel conocimiento que tienen los usuarios acerca del funcionamiento del sistema de evaluación docentes, esta encuesta fue aplicada a docentes, estudiantes y el encargado del manejo del sistema.
- **Revisión de documentación:** se realizó la técnica de revisión de documentación de los siguientes documentos:
 - a) Políticas, estándares, normas y procedimientos dentro del departamento de tecnologías.
 - b) Planes de seguridad y continuidad del departamento.
 - c) Organigrama departamental y manual de funciones de todo el personal.
 - d) Registros de información perteneciente a los módulos.
 - e) Documento de Proyecto CEIDPA

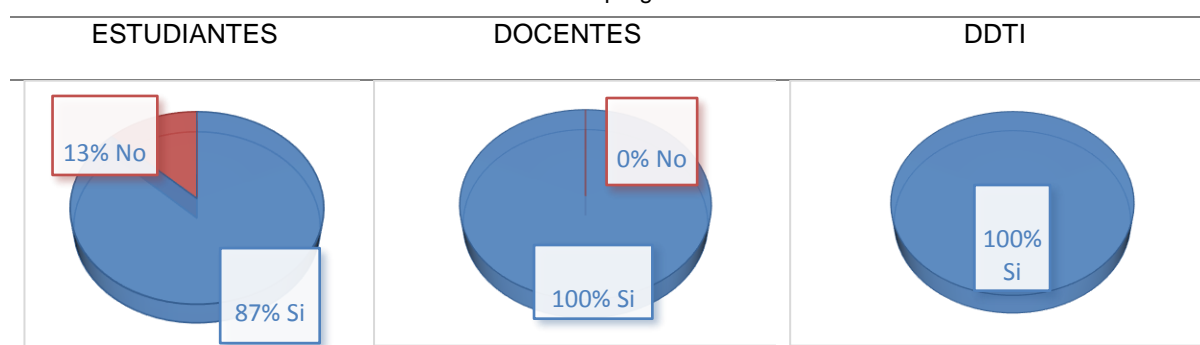
- **Check List:** Se realizó un Check List con los controles de la norma ISO 27002:2017 después de haber usado la Metodología y ver qué resultados arroja para poder hacer una correcta recomendación al DDTI.

2.5.3 Análisis de encuestas

Para el desarrollo de la evaluación del sistema de docentes, se recopiló información de los usuarios que usan el sistema de evaluación docente de la Universidad Técnica del Norte. Con la finalidad de evaluar la seguridad que brinda el sistema al momento de realizar la evaluación docente. A continuación, se detallan las preguntas realizadas al número de usuarios resultantes de la muestra calculada.

1) ¿Usted conoce el funcionamiento del sistema de evaluación docente de la Universidad Técnica del Norte?

Tabla 5: Primera pregunta encuesta



Fuente: *Elaboración Propia*

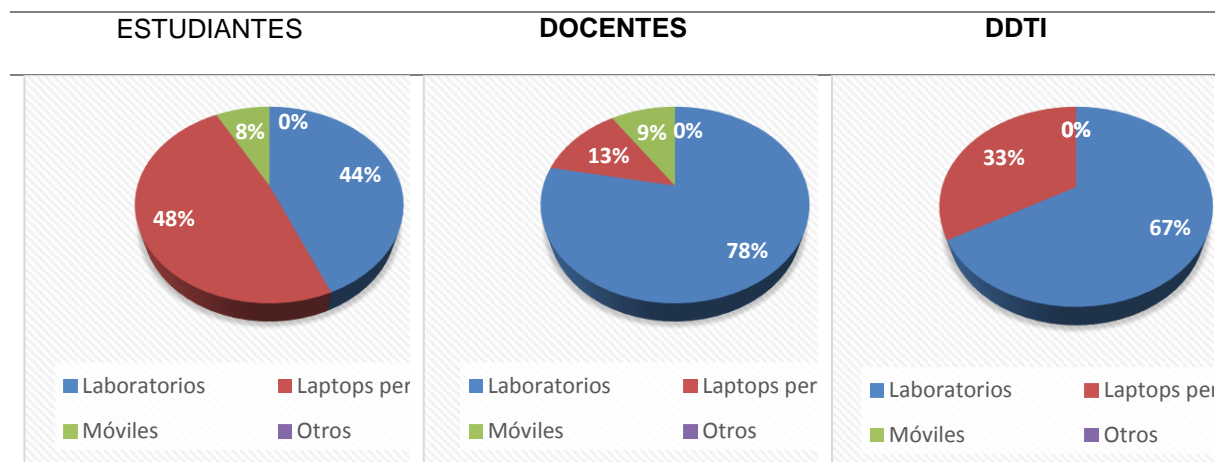
Análisis de resultados

En la tabla 5 se puede apreciar los resultados obtenidos de la primera pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. Se observa que todos los docentes y los miembros del DDTI conocen el funcionamiento del sistema de evaluación docente. Por otro lado, el 87% de los estudiantes encuestados conoce el funcionamiento del sistema, mientras que el 13 % no tiene conocimiento sobre el funcionamiento de este. En base a los resultados obtenidos es posible concluir que la mayoría de los usuarios conocen el funcionamiento del sistema de evaluación docente.

2) ¿Desde qué dispositivos se puede acceder al sistema de evaluación docente?

Tabla 6: Segunda pregunta encuesta

| Dispositivo | Estudiantes | Docentes | DDTI |
|--------------------|-------------|----------|------|
| Laboratorios | 150 | 20 | 2 |
| Laptops personales | 166 | 10 | 1 |
| Móviles | 27 | 3 | 0 |
| Otros | 0 | 0 | 0 |



Fuente: *Elaboración Propia*

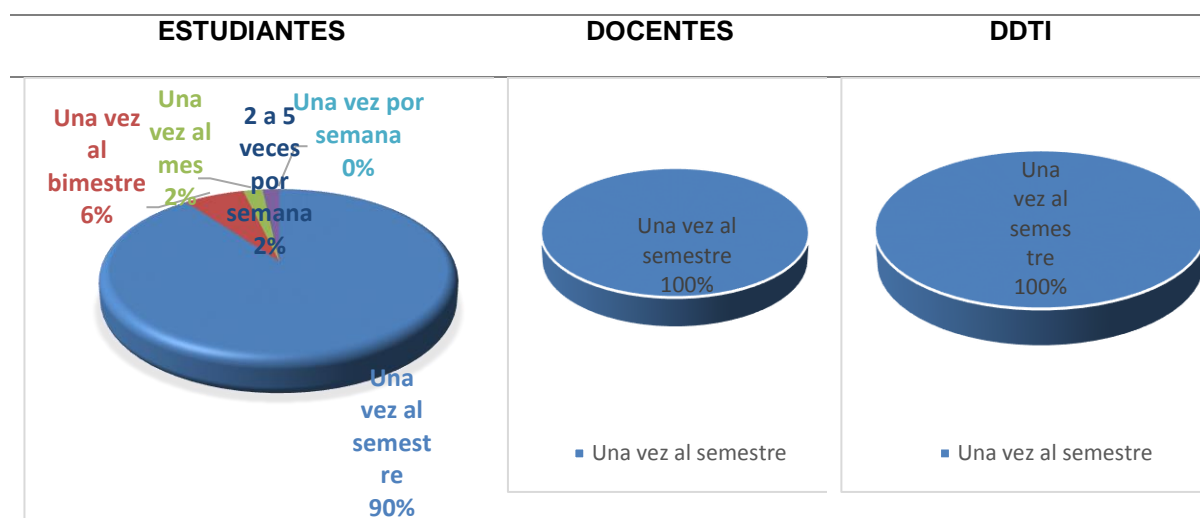
Análisis de resultados

En la tabla 6 se puede apreciar los resultados obtenidos de la segunda pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. Se observa que la mayor parte de usuarios ingresa al sistema de evaluación docente mediante los laboratorios, es decir accede desde las computadoras que se encuentra en los laboratorios de la Universidad, las respuestas se encuentran distribuidas de la siguiente forma: 44% estudiantes, 78% docentes y 67% miembros DTI. También es posible afirmar que un 48% de estudiantes ingresa desde laptops personales, al igual que un 13% de docentes y 33% de los miembros de DDTI. Además, existe un 8% de estudiantes, 9% de docentes y 0% de miembros del DTI que ingresan al sistema de evaluación docente mediante móviles. Por otro lado, no existe evidencia que los usuarios usen otro tipo de dispositivos además de los ya mencionados para ingresar al sistema de evaluación docente.

3) ¿Con que frecuencia usted utiliza el sistema de evaluación docente?

Tabla 7: Tercera pregunta encuesta

| Frecuencia | Estudiantes | Docentes | DDTI |
|------------------------|-------------|----------|------|
| Una vez al semestre | 308 | 33 | 3 |
| Una vez al bimestre | 22 | 0 | 0 |
| Una vez al mes | 7 | 0 | 0 |
| 2 a 5 veces por semana | 6 | 0 | 0 |
| Una vez por semana | 0 | 0 | 0 |



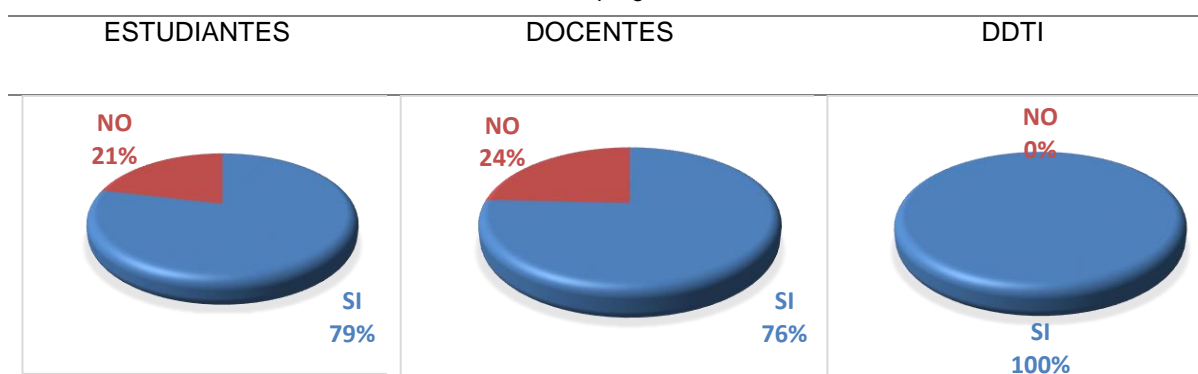
Fuente: Elaboración Propia

Análisis de resultados

En la tabla 7 se puede apreciar los resultados obtenidos de la tercera pregunta realizada tanto a estudiantes, docentes y a miembros del DDTI. Los docentes como los miembros del DDTI ingresan al sistema una sola vez al semestre, lo cual es una cantidad muy baja. Por otro lado, el 90 % de los estudiantes ingresan una vez al semestre, el 6% ingresan una vez al bimestre, el 2% ingresa una sola vez al mes y un 2% ingresa de 2 a 5 veces a la semana, cabe recalcar que este último porcentaje es de estudiantes que no tenían el conocimiento del sistema. Es posible decir que los usuarios que ingresan con mayor frecuencia al sistema de evaluación docentes son los estudiantes.

4) ¿Cree usted que existe algún control de acceso al sistema de evaluación docente?

Tabla 8: Cuarta pregunta encuesta



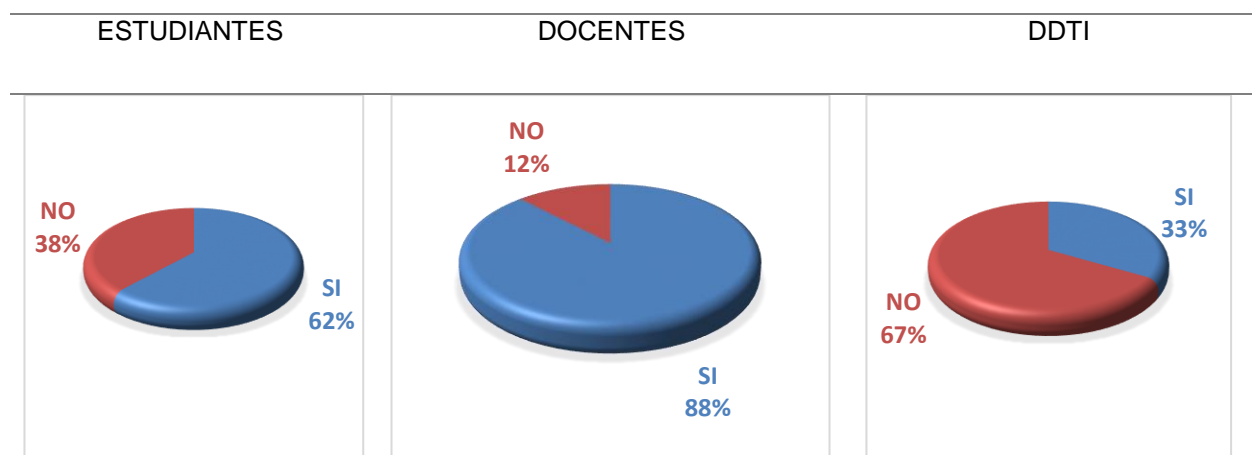
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 8 se puede apreciar los resultados obtenidos de la cuarta pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI respondió que existe un control en el sistema de evaluación docente. Por otra parte, el 76% de los docentes creen que, si existe un control del sistema de evaluación, mientras que el 24% restante piensa que no. Por último, el 79% de los estudiantes creen que existe algún tipo de control para el ingreso al sistema de evaluación docente, mientras que el 21% cree que no. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente creen que existe control en el acceso al sistema de evaluación docente.

5) ¿La contraseña que usted emplea para acceder al sistema de evaluación docente cuenta con requerimientos de seguridad?

Tabla 9: Quinta pregunta encuesta



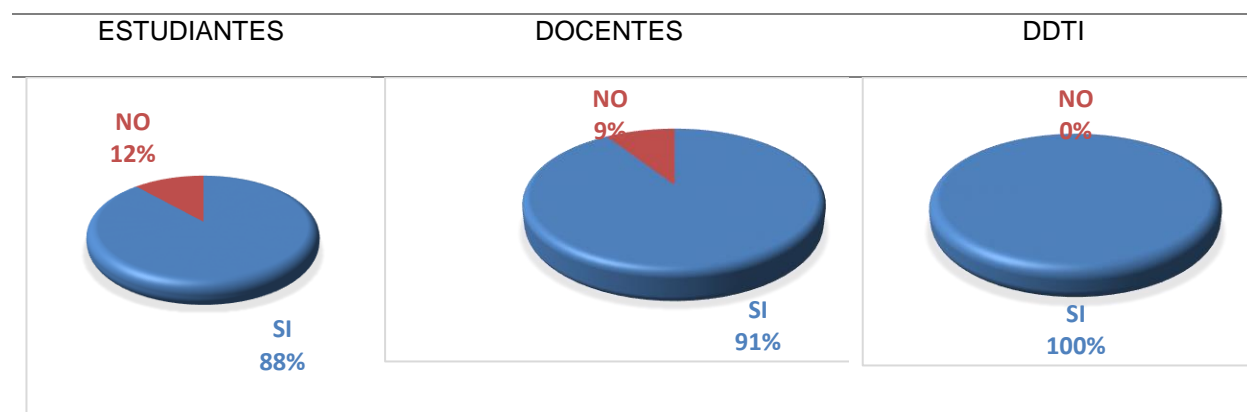
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 9 se puede observar los resultados obtenidos de la quinta pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 67% de los miembros del DDTI cree que no tiene una contraseña segura para acceder al sistema de evaluación de docente, mientras que el 33% cree que la contraseña es segura. Por otra parte, el 88% de los docentes creen que tiene una contraseña segura para acceder al sistema de evaluación de docente, mientras que el 12% restante piensa que no. Por último, el 62% de los estudiantes creen que tiene una contraseña segura para acceder al sistema de evaluación de docente, mientras que el 38% cree que no, la razón es que siguen conservando la contraseña que se les fue asignada. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente creen que tiene una contraseña segura para acceder al sistema de evaluación de docente.

6) ¿El sistema de evaluación docente tiene una política de bloqueo sesiones o de computadores después de un tiempo determinado?

Tabla 10: Sexta pregunta encuesta



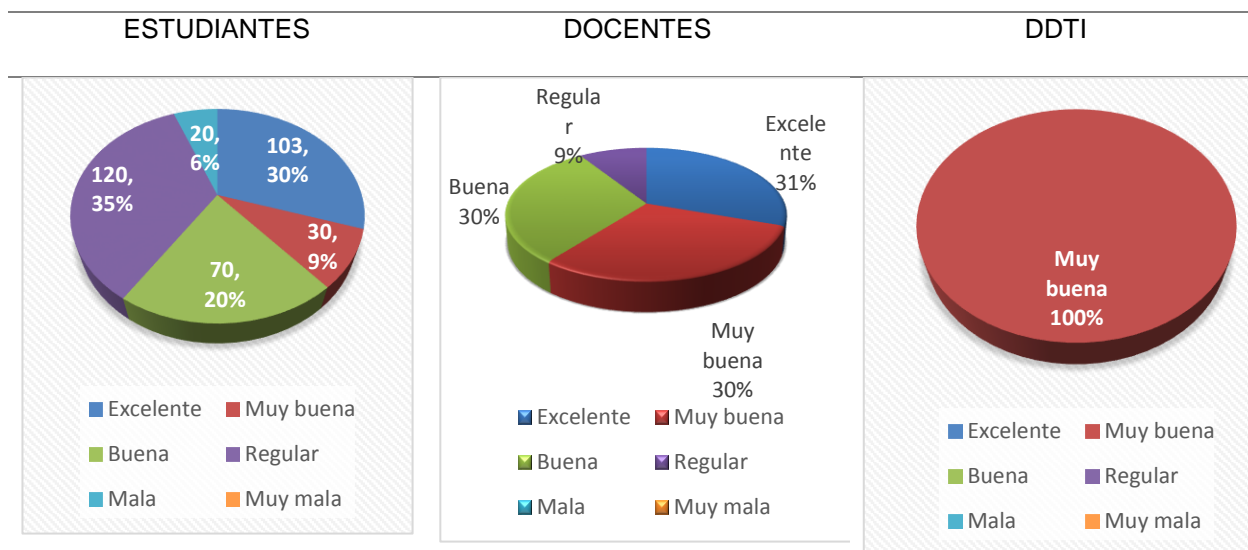
Fuente: Elaboración Propia

Análisis de resultados

En la tabla 10 se puede apreciar los resultados obtenidos de la sexta pregunta realizada tanto a estudiantes, docentes y a miembros del DDTI. El 100% de los miembros del DDTI cree que tiene el sistema de evaluación docente tiene una política de bloqueo sesiones o de computadores después de un tiempo determinado. Por otra parte, el 91% de los docentes cree que el sistema de evaluación docente tiene una política de bloqueo sesiones o de computadores después de un tiempo determinado, mientras que el 9% restante piensa que no. Por último, el 88% de los estudiantes cree que el sistema de evaluación docente tiene una política de bloqueo sesiones o de computadores después de un tiempo determinado, mientras que el 12% cree que no. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente cree que tiene una política de bloqueo sesiones o de computadores después de un tiempo determinado.

7) ¿Cuál es el nivel de facilidad de uso del sistema de evaluación docente?

Tabla 11: Séptima pregunta encuesta



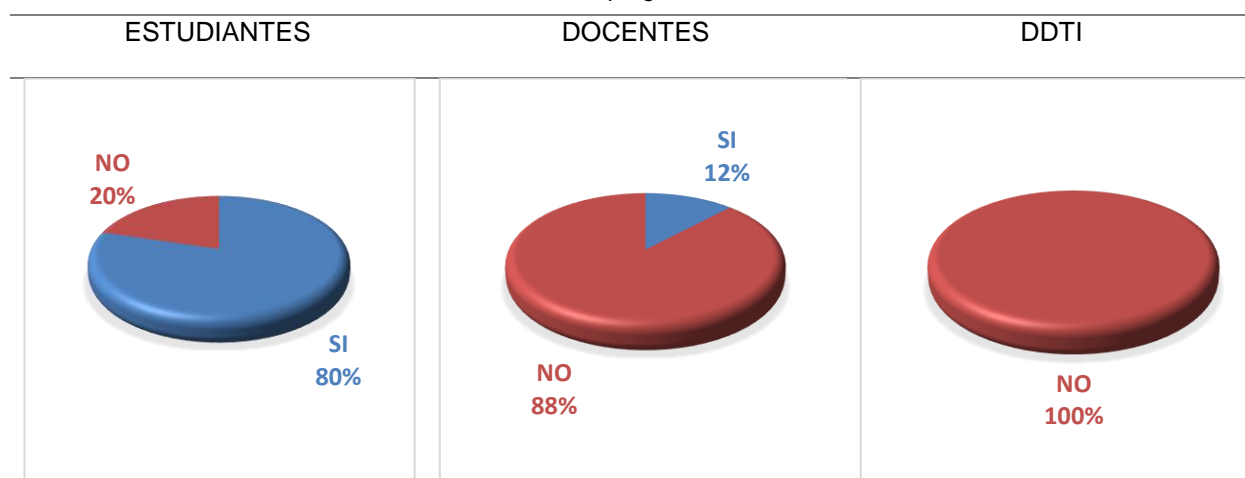
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 11 se puede apreciar los resultados obtenidos de la séptima pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI cree que el sistema de evaluación docente tiene un nivel de facilidad de uso muy bueno. Por otra parte, el 31% de los docentes cree que el sistema de evaluación docente tiene un nivel de facilidad de uso excelente, el 30% cree que tiene un nivel de facilidad de uso muy bueno, mientras que el 9% restante piensa que la facilidad de uso es regular. Por último, el 30% de los estudiantes cree que el sistema de evaluación docente tiene un nivel de facilidad de uso excelente, el 9% cree que tiene un nivel de facilidad de uso muy bueno, el 20% cree que tiene un nivel de facilidad de uso bueno, 35% cree que tiene un nivel de facilidad de uso regular, mientras que el 6% cree que el nivel de facilidad de uso es malo. Es posible decir que el promedio de opiniones sobre la facilidad de uso del sistema de evaluación docente es intermedio.

8) ¿Usted ha tenido inconvenientes con el servicio de evaluación docente?

Tabla 12: Octava pregunta encuesta



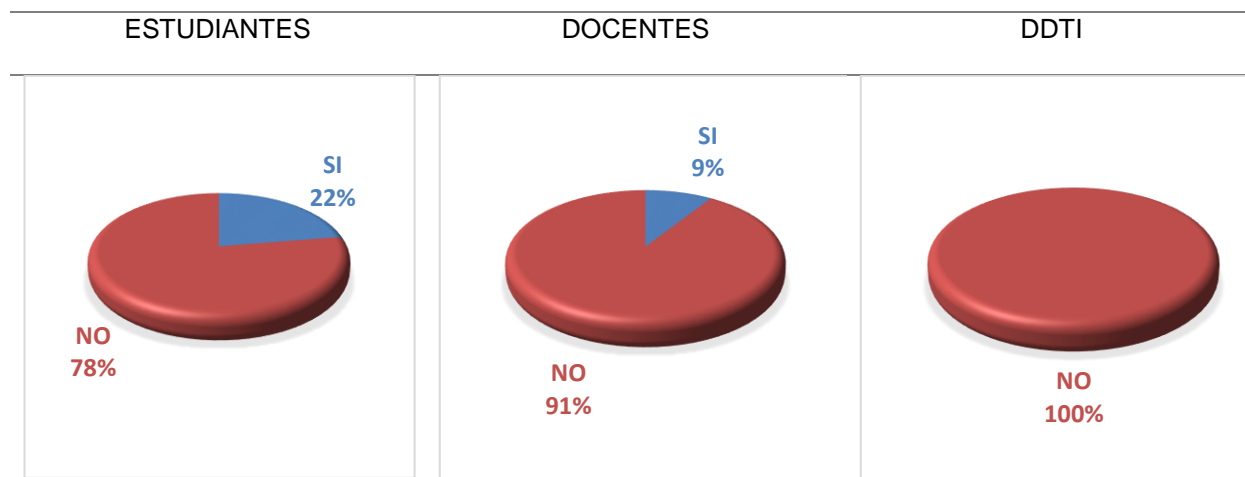
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 12 se puede apreciar los resultados obtenidos de la octava pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI afirma que no ha tenido inconvenientes con el servicio de evaluación docente. Por otra parte, el 88% de los docentes afirma que no ha tenido inconvenientes con el servicio de evaluación docente, mientras que el 12% restante afirma que sí. Por último, el 80% de los estudiantes afirma que ha tenido inconvenientes con el servicio de evaluación docente, mientras que el 20% afirma que no. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente afirman que han tenido inconvenientes con el servicio de evaluación docente.

9) ¿Usted ha tenido inconvenientes con la información ingresada en el sistema de evaluación docente?

Tabla 13: Novena pregunta encuesta



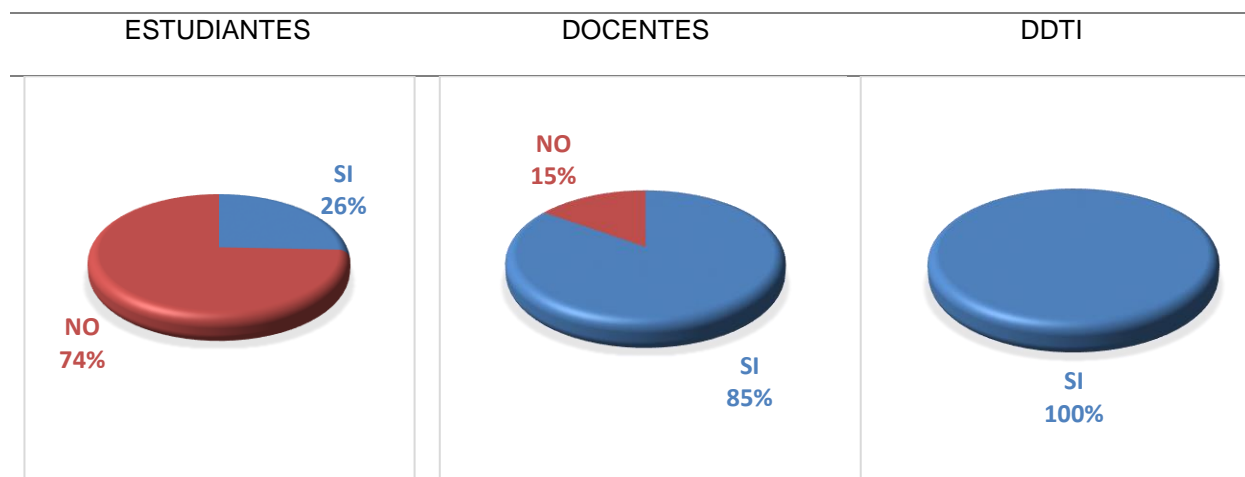
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 13 se puede apreciar los resultados obtenidos de la novena pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI afirman que han tenido inconvenientes con la información ingresada en el sistema de evaluación docente. Por otra parte, el 91% de los docentes afirman que han tenido inconvenientes con la información ingresada en el sistema de evaluación docente, mientras que el 9% restante afirma que no. Por último, el 78% de los estudiantes afirman que han tenido inconvenientes con la información ingresada en el sistema de evaluación docente, mientras que el 22% afirman que no. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente afirman que ha tenido inconvenientes con la información ingresada en el sistema de evaluación docente, esto se debería a una falta de socialización hacia los usuarios, sobre el manejo del mismo.

10) ¿Existe algún responsable del sistema de evaluación docente que brinde atención cuando sea necesario?

Tabla 14: Décima pregunta encuesta



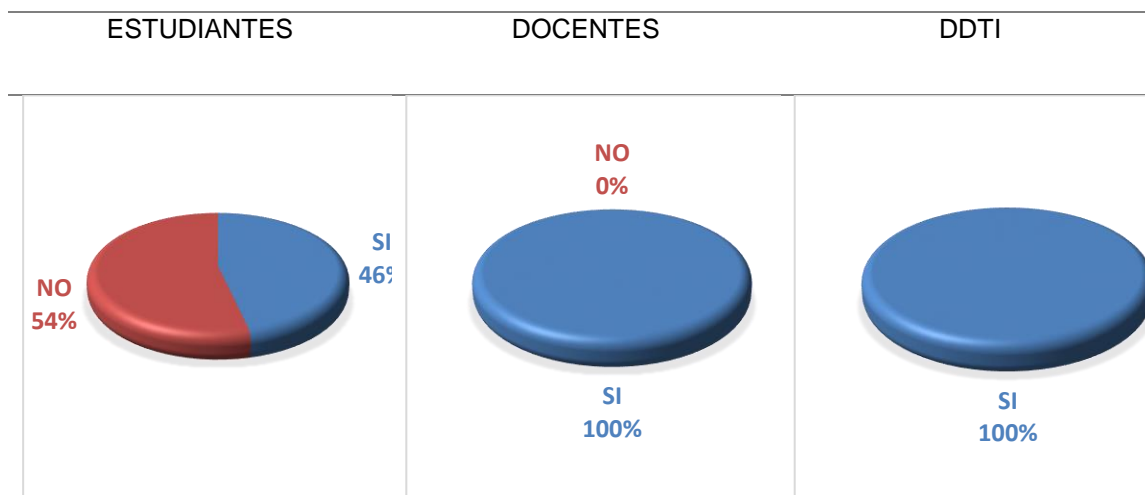
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 14 se puede apreciar los resultados obtenidos de la décima pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI piensan que existe algún responsable del sistema de evaluación docente que brinde atención cuando sea necesario. Por otra parte, el 85% de los docentes piensan que existe algún responsable del sistema de evaluación docente que brinde atención cuando sea necesario, mientras que el 15% restante piensa que no. Por último, el 74% de los estudiantes piensan que no existe algún responsable del sistema de evaluación docente que brinde atención cuando sea necesario, mientras que el 26% piensa que sí. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente piensa que existe algún responsable del sistema de evaluación docente que brinde atención cuando sea necesario.

11) ¿Usted cree que la información que ingresa al sistema de evaluación docente es confidencial?

Tabla 15: Onceava pregunta encuesta



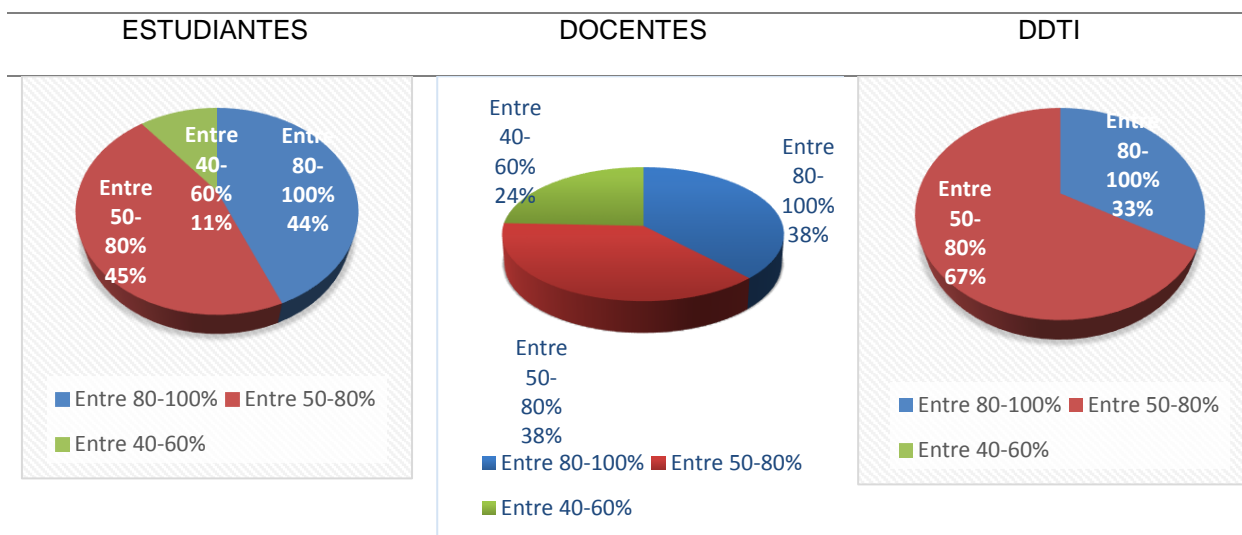
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 15 se puede apreciar los resultados obtenidos de la décimo primera pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI cree que la información que ingresa al sistema de evaluación docente es confidencial. Por otra parte, el 100% de los docentes cree que la información que ingresa al sistema de evaluación docente es confidencial. Por último, el 54% de los estudiantes cree que la información que ingresa al sistema de evaluación docente no es confidencial, mientras que el 46% cree que sí. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente creen que la información que ingresa al sistema de evaluación docente es confidencial.

12) ¿En qué porcentaje usted considera que el sistema de evaluación docente satisface sus necesidades?

Tabla 16: Doceava pregunta encuesta



Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 16 se puede apreciar los resultados obtenidos de la décima segunda pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 67% de los miembros del DTI creen que el sistema de evaluación docente satisface sus necesidades, mientras que, el 33% cree que no. Por otra parte, el 38% de los docentes creen que el sistema de evaluación docente satisface sus necesidades, mientras que, el 24% cree que no. Por último, el 45% de los estudiantes creen que el sistema de evaluación docente satisface sus necesidades, mientras que, el 33% cree que no. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente cree que este satisface sus necesidades.

13) Si el porcentaje escogido en la pregunta anterior es entre 40-60% indique el motivo de su respuesta.

Tabla 17: Treceava pregunta encuesta



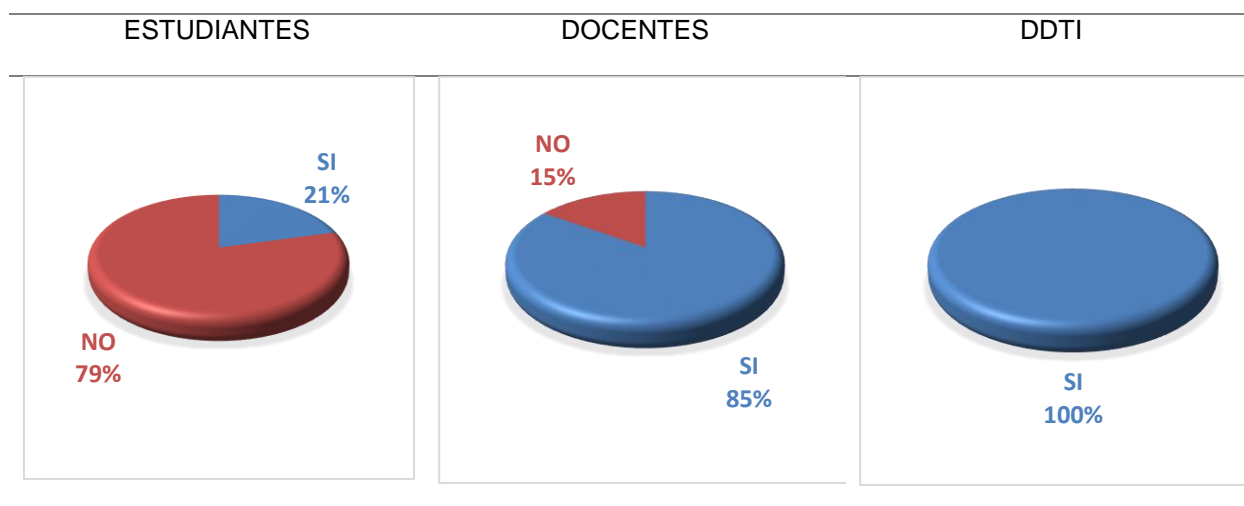
Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 17 se puede apreciar los resultados obtenidos de la décima tercera pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 40 % de los usuarios afirma que no existe disponibilidad al sistema de evaluación docente. El 33% de los usuarios afirma que no existe retroalimentación de las evaluaciones realizadas en el sistema. Por último, el 20 % afirma que existen fugas de información en el sistema de evaluación docente mientras que el 7% dio otra razón diferente a las expuestas. Se concluye que la mayor parte de usuarios afirman que el sistema de evaluación docente no satisface sus necesidades debido a que no existe retroalimentación de las evaluaciones realizadas.

14) ¿Tiene la confianza suficiente para presentar quejas sobre las fallas del sistema de evaluación docente?

Tabla 18: Catorceava pregunta encuesta



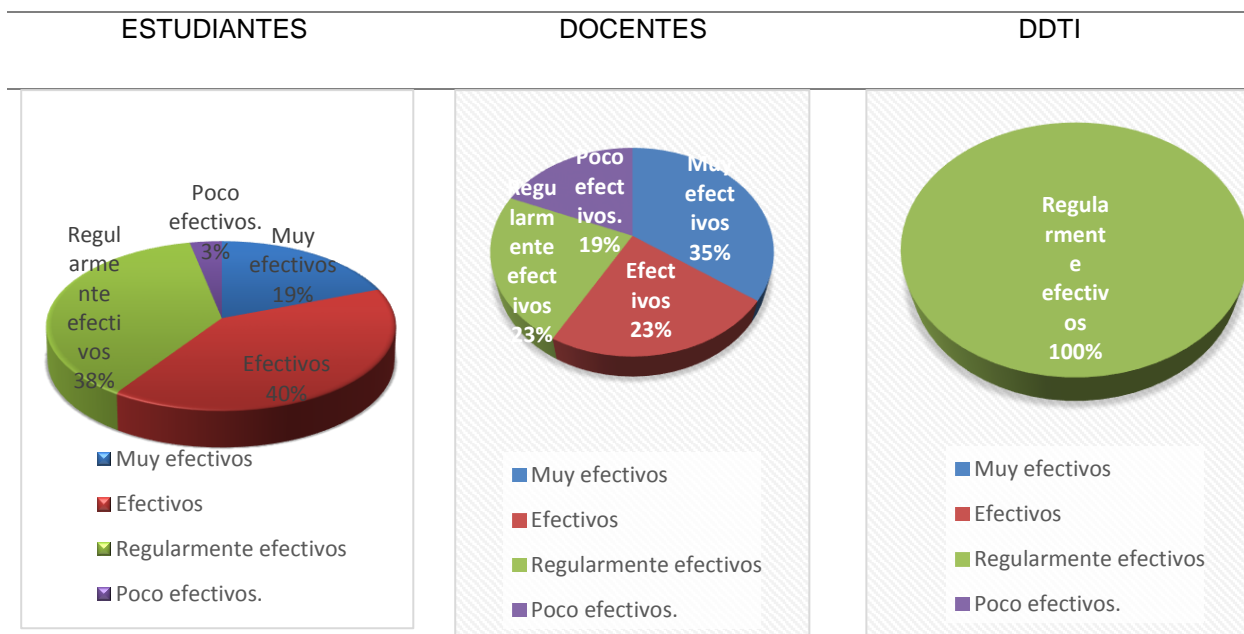
Fuente: *Elaboración Propia*

Análisis de Resultados

En la tabla 18 se puede apreciar los resultados obtenidos de la décimo cuarta pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI tienen la confianza suficiente para presentar quejas sobre fallas del sistema de evaluación docente. Por otra parte, el 85% de los docentes tienen la confianza suficiente para presentar quejas sobre fallas del sistema de evaluación docente, mientras que el 15% restante no tiene confianza para reportar fallas en el sistema. Por último, el 79% de los estudiantes no tienen la confianza suficiente para presentar quejas sobre las fallas del sistema de evaluación docente, mientras que el 21% afirman tener confianza para reportar fallos del sistema de evaluación docente. Es posible decir que la mayoría de los usuarios docentes y DDTI tienen la confianza suficiente para presentar quejas sobre las fallas del sistema de evaluación docente, mientras que los estudiantes no tienen la confianza suficiente para presentar quejas sobre fallas al sistema.

15) ¿Qué tan efectivos son los técnicos para resolver problemas del sistema de evaluación docente?

Tabla 19: Quinceava pregunta encuesta



Fuente: *Elaboración Propia*

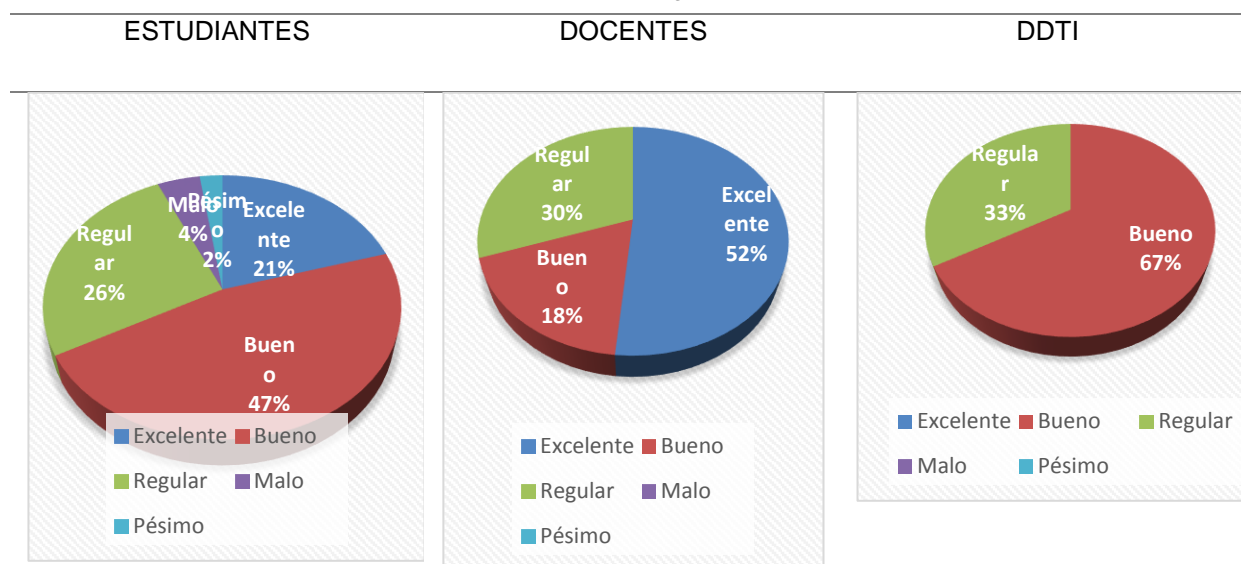
Análisis de resultados

En la tabla 19 se puede apreciar los resultados obtenidos de la décima quinta pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 100% de los miembros del DDTI considera que son regularmente efectivos los técnicos para resolver problemas del sistema de evaluación docente. Por otra parte, el 35% de los docentes considera que los técnicos son muy efectivos para resolver problemas del sistema de evaluación docente, el 23% restante piensa que los técnicos son efectivos para resolver problemas del sistema de evaluación docente, el 23% considera los técnicos son regularmente efectivos para resolver problemas del sistema de evaluación docente y el 19% considera que los técnicos son poco efectivos para resolver problemas del sistema de evaluación docente. Por último, el 40% de los estudiantes considera que los técnicos son efectivos para resolver problemas del sistema de evaluación docente, el 38% considera que los técnicos son regularmente efectivos para resolver problemas del sistema de evaluación

docente, el 19% considera que los técnicos son muy efectivos para resolver problemas del sistema de evaluación docente y el 3% considera que los técnicos son poco efectivos para resolver problemas del sistema de evaluación docente. Es posible concluir que la mayoría de los usuarios del sistema de evaluación docente creen los técnicos son regularmente efectivos para resolver problemas del sistema de evaluación docente.

16) ¿Cómo califica el sistema de evaluación docente de la Universidad Técnica del Norte?

Tabla 20: Dieciséisava pregunta encuesta



Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 20 se puede apreciar los resultados obtenidos de la décima sexta pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 67% de los miembros del DDTI califica como bueno el sistema de evaluación docente de la UTN., mientras que, el 33% cree que es regular. Por otra parte, el 52% de los docentes considera que el sistema de evaluación docente de la UTN es excelente, el 30% piensa que es regular y el 18% considera que es bueno. Por último, el 47% de los estudiantes cree el sistema de

evaluación docente es bueno, el 26% considera que es regular, el 21% considera que es excelente, el 4% considera que es malo y el 2% opina que es pésimo. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente considera que el sistema de evaluación docente de la UTN es bueno.

17) ¿Usted considera que el servicio de evaluación docente debe estar disponible a cualquier hora y para cualquier usuario?

Tabla 21: Diecisieteava pregunta encuesta



Fuente: *Elaboración Propia*

Análisis de resultados

En la tabla 21 se puede apreciar los resultados obtenidos de la décimo séptima pregunta realizada tanto a estudiantes como a docentes y a miembros del DDTI. El 67% de los miembros del DDTI piensa que el servicio de evaluación docente no debe estar disponible a cualquier hora y para cualquier usuario, mientras que el 33% piensa que sí. Por otra parte, el 91% de los docentes piensan que el servicio de evaluación docente debe estar disponible a cualquier hora y para cualquier usuario, mientras que el 9% restante piensa que no. Por último, el 79% de los estudiantes piensan que el servicio de evaluación docente debe estar disponible a cualquier hora y para cualquier usuario, mientras que el 21% cree que no. Es posible decir que la mayoría de los usuarios del sistema de evaluación docente creen que el

servicio de evaluación docente debe estar disponible a cualquier hora y para cualquier usuario, pero la realidad es que como el sistema se encuentra solo habilitado al final del semestre para que cada usuario pueda evaluar no puede estar disponible a cualquier hora, porque no se podría obtener datos reales de la evaluación.

PREGUNTAS ADICIONALES PARA LOS TÉCNICOS DEL DDTI

Para poder responder a estas preguntas se realizó el análisis que dicta la metodología Magerit la cual es determinación de activos críticos, teniendo en cuenta las dimensiones establecidas según (Ministerio de Hacienda y Administraciones Publicas de España, 2012), como “las características o atributos que hacen valioso un activo”. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión, se encuentran propuestas en el libro II de Magerit, en el cual se establecen las dimensiones de disponibilidad, integridad de datos, confidencialidad de la información, autenticidad y trazabilidad para poder determinar el valor que representa cada activo para la Universidad.

Mediante las dimensiones de valoración que establece la metodología MAGERIT se realizó las siguientes preguntas que se detallan en la siguiente tabla:

Tabla 22: Dimensiones de Valoración

| DIMENSIONES DE VALORACIÓN | DESCRIPCIÓN | VALORACION |
|----------------------------------|---|-------------------|
| Disponibilidad | ¿Qué Nivel de daño representaría para la Universidad si el servicio no estuviera disponible? | |
| Integridad | ¿Qué nivel de daño representaría para la universidad que los datos del sistema de evaluación docente fueran total o parcialmente falsos, modificados, o faltaran datos? | |
| Confidencialidad | ¿Qué nivel de daño representaría para la universidad que los datos que se obtienen en el sistema de evaluación docentes fuera conocido por personas no autorizadas? | |

| | |
|---------------------|---|
| Autenticidad | ¿Qué nivel de daño representaría para la Universidad que la persona que acceda a la información no sea realmente quien se cree? |
| Trazabilidad | ¿Qué nivel de daño representaría para la universidad que no quedara constancia del uso del servicio o el acceso a los datos? |

Fuente: *Elaboración Propia*

Para poder evaluar estas preguntas se estableció una escala de valoración en la cual 1 representa un daño muy bajo a presentarse al sistema de evaluación docente y 5 un daño muy alto, estos valores fueron representados en la siguiente tabla.

Tabla 23: Escala de Valoración

| ÍTEM | DESCRIPCIÓN |
|-------------|--------------------|
| 1 | Daño muy bajo |
| 2 | Daño bajo |
| 3 | Daño medio |
| 4 | Daño alto |
| 5 | Daño muy alto |

Fuente: *Elaboración Propia*

Aplicando la encuesta al personal encargado del manejo del sistema de evaluación docente se determinó que el daño que ocasionaría a la Universidad sería un daño muy alto ya que no se cumpliría con los parámetros de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, la encuesta realizada se encuentra en el anexo 3.

2.6 Procedimiento Informático Lógico para el Análisis de Riesgos (PILAR)

PILAR, es un acrónimo de “Procedimiento Informático Lógico para el Análisis de Riesgos” es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit (Ministerio de Hacienda y Administraciones Publicas de España, 2012).

La herramienta soporta todas las fases del método Magerit:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración

- Caracterización de las amenazas
- Evaluación de las salvaguardas

La herramienta incorpora los inventarios del "Catálogo de Elementos" permitiendo una homogeneidad en los resultados del análisis:

- tipos de activos
- dimensiones de valoración
- criterios de valoración
- catálogo de amenazas

Una vez realizado el análisis con MAGERIT, se procedió a ingresar los datos en la herramienta PILAR, la misma que ayudó a evaluar la situación actual y de esta manera poder proponer soluciones eventuales en el Departamento de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte de la Universidad Técnica del Norte.

Para aplicar la metodología MAGERIT, se tiene que llevar a cabo el proceso que se describe en la Figura 13.

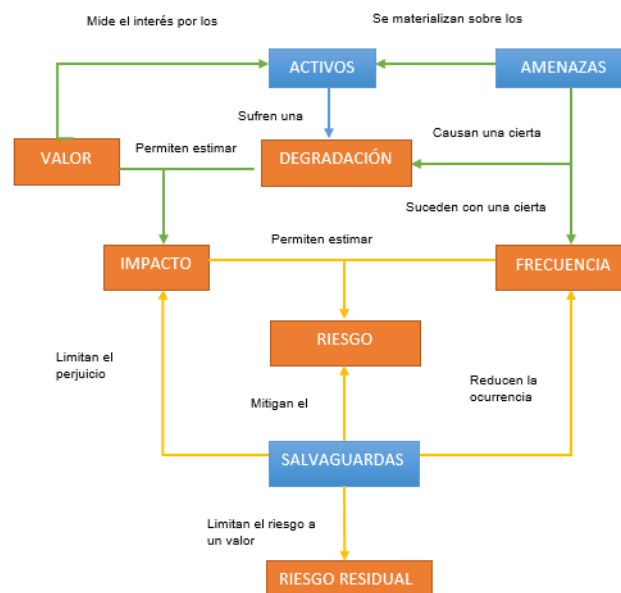


Figura 13: Procesos para aplicar MAGERIT

Fuente: *Elaboración Propia*

Para aplicar la metodología MAGERIT se deben seguir los siguientes pasos:

- a) **Identificación de Activos:** Son todos los activos que posee la organización, clasificados de acuerdo a su función.
- b) **Valoración de Activos:** Esta valoración asignada al activo de acuerdo a la criticidad.
- c) **Identificación de amenazas:** Son eventos que degradarían el valor que tiene los activos.
- d) **Frecuencia:** Se refiere a los eventos que suceden en un tiempo determinado.
- e) **Degradación:** Es cuan perjudicado resultaría el activo al materializarse las amenazas.
- f) **Impacto:** Consecuencia que sobre un activo tiene la materialización de una amenaza.
- g) **Riesgo:** Es la probabilidad de materialización de amenazas sobre el activo.
- h) **Identificación y Valoración de Salvaguardas:** Son las medidas precisas a tomar para reducir el riesgo.
- i) **Riesgo Residual:** Es el riesgo permanente después de aplicar las salvaguardas.

Para complementar el análisis de gestión de riesgos fue necesario usar PILAR es un software que utiliza la metodología MAGERIT, y posee una biblioteca que permite evaluar con puntajes a la seguridad informática.

El software EAR/PILAR permite realizar un análisis de riesgo sobre varias dimensiones importantes para la seguridad de la información, estas son:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- Trazabilidad

A partir de los parámetros establecidos, es posible calcular el impacto y el riesgo acumulado, potencial, y residual.

En la situación actual y lo establecido en la norma ISO 27002:2017 el software establece posibles salvaguardas. Las salvaguardas se califican por fases, además es posibles implementarlas en cualquier fase del proyecto. Pilar permite realizar un análisis cuantitativo y cualitativo.

En la figura 14 se observa la pantalla principal de EAR/PILAR donde vamos a escoger la opción de análisis cualitativo

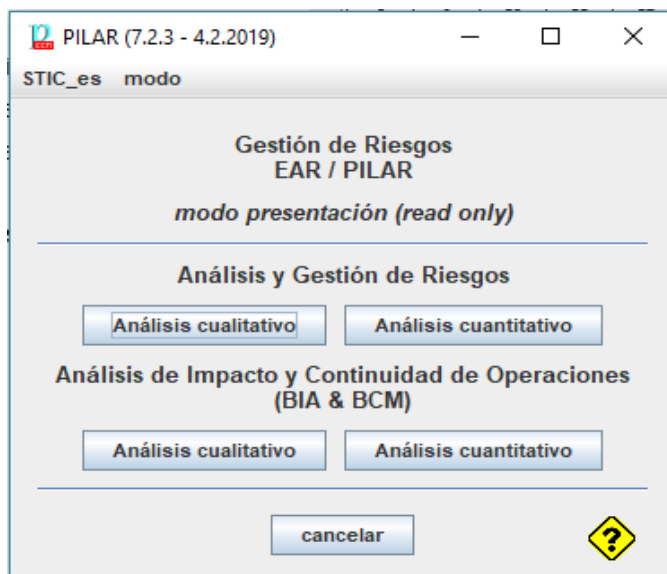


Figura 14: Pantalla principal PILAR- MAGERIT

Fuente: Elaboración Propia

Completando los datos del proyecto figura 15 describiendo que se va a realizar en el departamento de tecnologías informáticas.

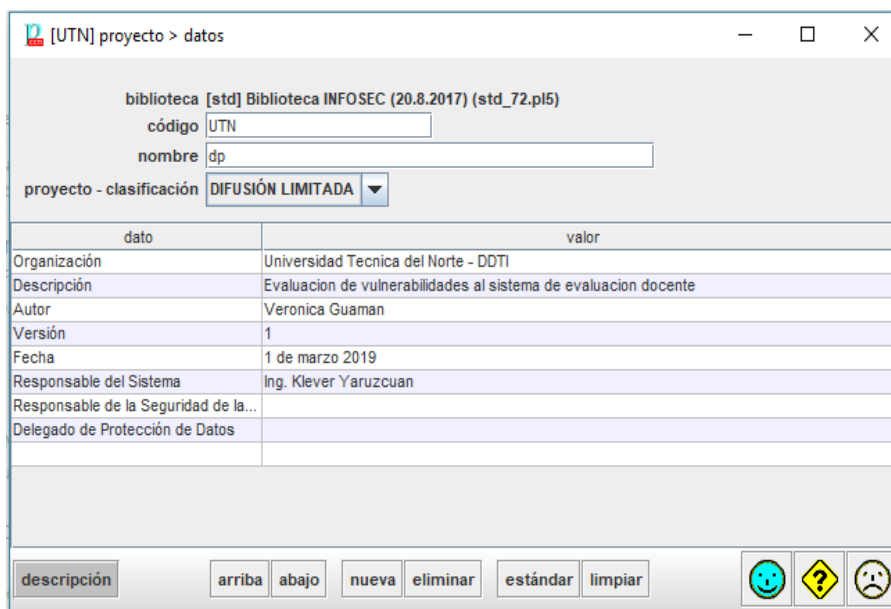


Figura 15: Información del proyecto.

Fuente: Elaboración Propia

2.6.1 Determinación de activos

Un activo es algo que es valioso o de utilidad para la organización. La finalidad de los activos es brindar protección para asegurar de alguna forma la operación del negocio y la continuidad.

Los activos según la norma ISO 17799:2005 se clasifican en:

- **Activos de información:** dentro de este grupo se encuentran bases de datos, documentación del sistema, manuales de usuario, procedimientos operativos, procedimientos de apoyo, planes de continuidad y manuales de entrenamiento.
- **Documentos impresos:** dentro de este grupo se encuentran documentos impresos, lineamientos, contratos de la compañía, documentos con información importante del negocio y contratos.
- **Activos de software:** dentro de este grupo se encuentran los softwares de aplicación, herramientas de desarrollo y software de sistemas.
- **Activos físicos:** dentro de este grupo se encuentran equipos informáticos, dispositivos de comunicación y diversos equipos tecnológicos.
- **Activo humano:** dentro de este grupo se encuentran los clientes, suscriptores y personal afín al negocio.
- **Imagen y reputación de la compañía.**
- **Servicios:** en este grupo se encuentran los servicios técnicos, tales como servicios de computación entre otros.

Dentro de la organización a evaluar, cada trabajador que forma parte de la organización es designado para manejar uno o varios activos de la institución según el cargo que ocupe. Pero todos los activos no tienen la misma importancia dentro de la organización; por lo tanto, los mecanismos de seguridad que se empleen dependen de las amenazas existentes para cada activo.

Tabla 24: Clasificación de Activos

| TIPO DE ACTIVO | ACTIVO |
|-----------------------|--|
| Datos y/o información | Bases de Datos de estudiantes y personal académico. |
| Software | Licencia GNU Oracle Linux 6 Licenciamiento Campus Agreement Microsoft Licencia perpetua Oracle 11g Database and Applications |

| | |
|--|---|
| | Licenciamiento Adobe Creative Cloud MLP Ed Subscription Multi Latin American Languages Licenciamiento Eset NOd 32 Antivirus Licencia ToolBook Licencia GNU Linux Centus Software libre licencia GNU para el Geoportal Licencia de ESRI Arcgis 10.1 Licencia GNU Dspace para Repositorio Digital Licencia GNU Moodle para aula virtual |
| Equipamiento Informático (Hardware) | Servidores HP Blade System Equipos Informáticos PC Laptop's Call Manager Gateway de voz IVR (contestadora automática) Tape Backup Switchs Core Switchs de acceso Cisco ASA Firewall Ipx Router Antenas y radio enlaces Access point Torres Racks Cableado estructurado |
| Redes de Comunicaciones | Red telefónica Red de datos Red inalámbrica Internet |
| Soportes de Información | Nube Oracle Apex |
| Equipamiento Auxiliar | Ups Fibra Óptica |
| Instalaciones | Departamento de DDTI - UTN |
| Personal | Miembros del Área de DDTI |

Fuente: (Departamento de Desarrollo Tecnológico e Informático - UTN, 2013)

A continuación, se clasifican los activos por función en el sistema de evaluación docente.

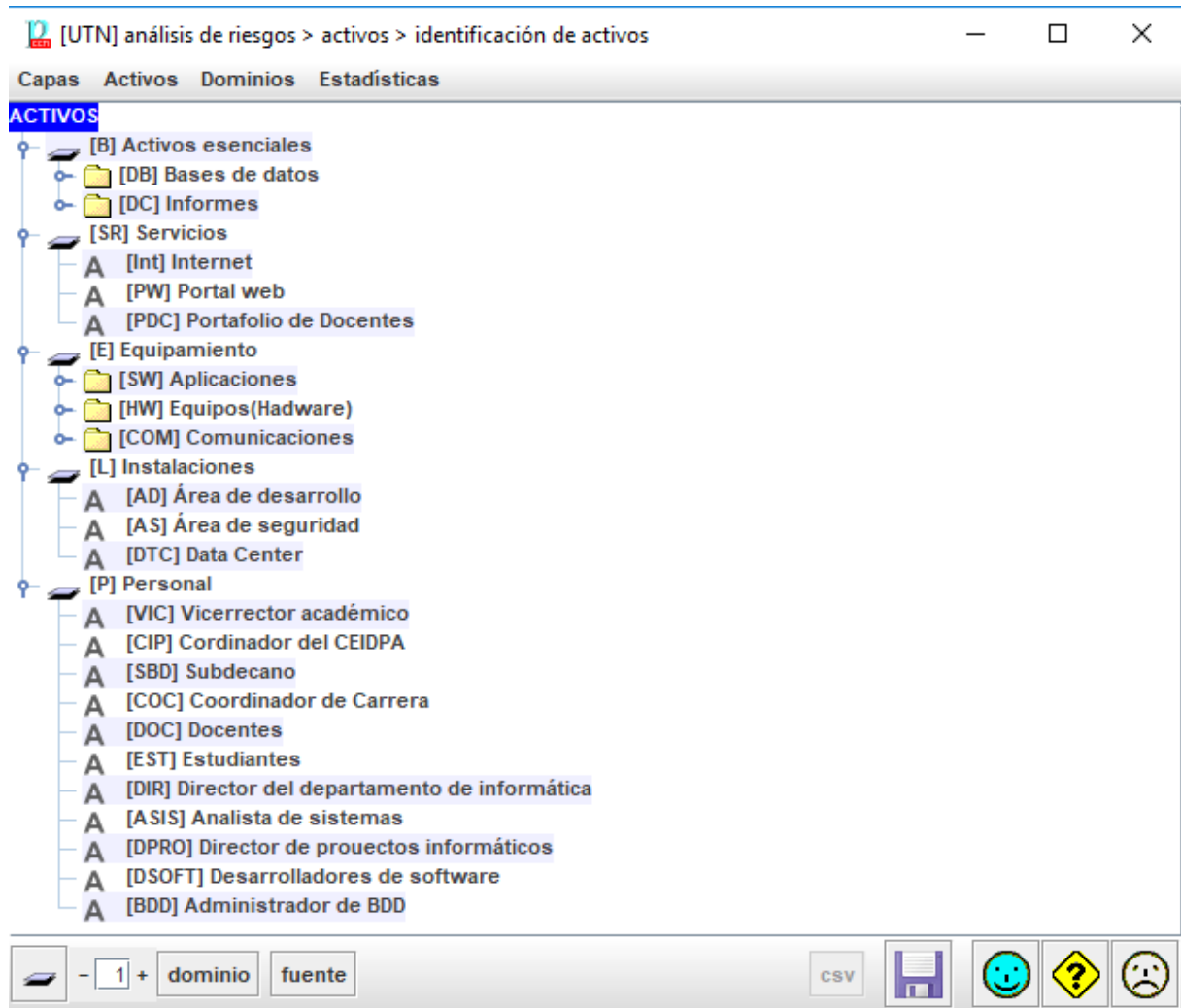


Figura 16: Activos del sistema de evaluación docente.

Fuente: Elaboración Propia

2.6.2 Dependencia entre activos

En una organización existen activos que dependen de otros más significativos, entre ellos puede estar involucrados equipos, comunicaciones, personal entre otros. Es importante identificar si existe dependencia entre activos, puesto que tal vez exista un activo importante que se vea afectado materializarse una amenaza en un activo de inferior importancia. Si existe dependencia entre los activos se formaría un árbol de dependencias.

Es posible decir que los activos de inferior grado son la base para los activos de un grado mayor, pero si la dependencia entre activos se vuelve muy fuerte es necesario diseñar prevenciones más efectivas, de lo contrario al ocurrir un fallo en un activo de menor grado y este a su vez ser dependiente de un activo mayor y este a su vez ser dependiente de otro, el fallo puede resultar muy perjudicial para toda la organización.

a) Capa 1: El entorno: son activos esenciales para precisar las siguientes capas.

Dentro de esta capa se encuentra:

- Equipamiento y suministros de energía, sistemas de comunicación y climatización.
- Personal de desarrollo, operación, directivo, entre otros.
- Edificios, mobiliario, entre otros.

b) Capa 2 Sistema de información.

Dentro de esta capa se encuentran elementos como:

- Equipos informáticos en cuanto a hardware.
- Software
- Comunicaciones.
- RespalDOS de información.

c) Capa 3 Información.

Dentro de esta capa se encuentran todos los datos relacionados a la organización.

d) Capa 4 Funciones de la organización.

Dentro de esta capa se describen el objetivo y la misión, además de los servicios producidos.

e) Capa 5 Otros activos.

Dentro de esta capa se encuentran activos como la credibilidad y solvencia.

2.6.3 Valoración de activos

La valoración del activo se lo puede hacer de forma cuantitativa, es decir asignando una cantidad numérica, también es posible valorar el activo de forma cualitativa, es decir asignado niveles.

Para que la valoración de activos sea lo más precisa posible es necesario conocer con gran profundidad el proceso a evaluar, para lograrlo es necesario revisar toda la documentación de relevancia a la organización, además de establecer contacto con las personas que están dentro del proceso o sistema a evaluar.

A continuación, en la figura 17 se muestra la valoración entre activos del sistema de evaluación docente con su respectiva valoración en parámetros de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

| activo | [D] | [I] | [C] | [A] | [T] | [V] | [DP] |
|--|------|------|------|------|--------|--------|--------|
| ACTIVOS | | | | | | | |
| [B] Activos esenciales | | | | | | | |
| [DB] Bases de datos | | | | | | | |
| [DB] [BDC] Base de datos del Sistema de evaluación Docente | [7] | [8] | [6] | [7] | [9] | [n.a.] | [n.a.] |
| [DC] Informes | | | | | | | |
| [RP] Reportes | [10] | [10] | [10] | [10] | [9] | [n.a.] | [n.a.] |
| [SR] Servicios | | | | | | | |
| [Int] Internet | [9] | [7] | [7] | [6] | [9] | [n.a.] | [n.a.] |
| [PW] Portal web | [10] | [9] | [8] | [9] | [n.a.] | [n.a.] | [n.a.] |
| [PDC] Portafolio de Docentes | [10] | [9] | [8] | [6] | [10] | | |
| [E] Equipamiento | | | | | | | |
| [SW] Aplicaciones | | | | | | | |
| [GH] Gestion de horarios | [9] | [9] | [6] | [8] | [7] | [n.a.] | [n.a.] |
| [HD] Ayuda | [10] | [5] | [5] | [9] | [2] | [n.a.] | [n.a.] |
| [PWB] Portal Web | [9] | [6] | [5] | [9] | [6] | [n.a.] | [n.a.] |
| [EVAL] Evaluación Docente | [7] | [8] | [7] | [6] | [8] | [n.a.] | [n.a.] |
| [SEc] Seguridad Firewall | [10] | [9] | [9] | [9] | [10] | [n.a.] | [n.a.] |
| [HW] Equipos(Hardware) | | | | | | | |
| [SBDD] Servidor de BDD | [9] | [9] | [9] | [9] | [9] | [n.a.] | [n.a.] |
| [PTR] Puestos de trabajo | [7] | [7] | [7] | [8] | [7] | [n.a.] | [n.a.] |
| [SPW] Servidor de portal web | [9] | [8] | [8] | [8] | [8] | [n.a.] | [n.a.] |
| [SRP] Servidor de reportes | [9] | [8] | [8] | [7] | [7] | [n.a.] | [n.a.] |
| [SAPL] Servidor de aplicaciones | [6] | [7] | [7] | [7] | [6] | [n.a.] | [n.a.] |
| [Fir] Firewall | [10] | [9] | [9] | [9] | [9] | [n.a.] | [n.a.] |
| [COM] Comunicaciones | | | | | | | |
| [RITN] Red interna UTN | [9] | [9] | [9] | [9] | [9] | [n.a.] | [n.a.] |
| [L] Instalaciones | | | | | | | |
| [AD] Área de desarrollo | [8] | [8] | [7] | [7] | [10] | [n.a.] | [n.a.] |
| [AS] Área de seguridad | [8] | [8] | [8] | [8] | [7] | [n.a.] | [n.a.] |
| [DTC] Data Center | [10] | [9] | [9] | [9] | [9] | [n.a.] | [n.a.] |
| [P] Personal | | | | | | | |
| [VIC] Vicerrector académico | [10] | [9] | [9] | [9] | [9] | [n.a.] | [n.a.] |
| [CIP] Cordinador del CEIDPA | [7] | [7] | [7] | [7] | [7] | [n.a.] | [n.a.] |
| [SBD] Subdecano | [9] | [9] | [9] | [9] | [9] | [n.a.] | [n.a.] |
| [COC] Coordinador de Carrera | [8] | [8] | [7] | [7] | [8] | [n.a.] | [n.a.] |
| [DOC] Docentes | [9] | [9] | [9] | [9] | [9] | [n.a.] | [n.a.] |
| [EST] Estudiantes | [6] | [6] | [6] | [6] | [6] | [n.a.] | [n.a.] |
| [DIR] Director del departamento de informática | [9] | [8] | [8] | [8] | [8] | [n.a.] | [n.a.] |
| [ASISI] Analista de sistemas | [7] | [7] | [5] | [5] | [7] | [n.a.] | [n.a.] |

Figura 17: Valoración de activos del sistema de evaluación docente.

Fuente: *Elaboración Propia*

En esta gráfica se puede apreciar el valor del dominio de seguridad del sistema de evaluación docente.

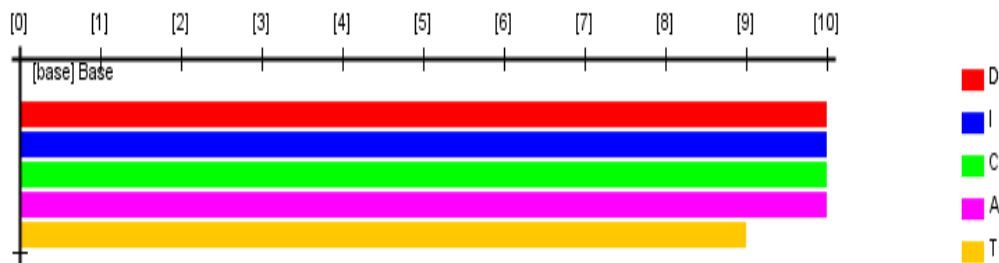


Figura 18: Valoración del dominio de seguridad UTN

Fuente: *Elaboración Propia*

La siguiente figura 19 se realizó con la información ingresada de los activos que posee el Departamento de Desarrollo Tecnológico e Informático (DDTI – UTN) con los diferentes niveles de valor asignado a cada activo.

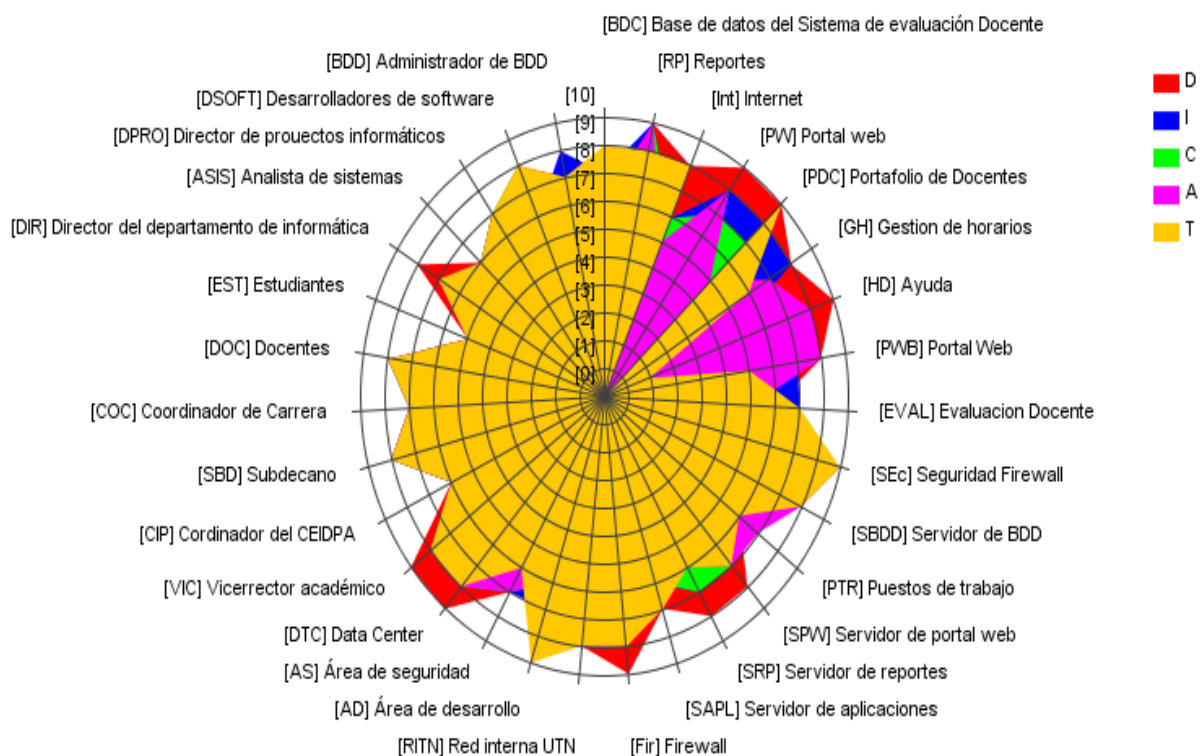


Figura 19: Gráfica de valor/activos

Fuente: *Elaboración Propia*

2.6.4 Identificación de amenazas

La identificación de amenazas consiste en identificar posibles amenazas que pueden afectar a cada uno de los activos. Para ello fue necesario revisar documentación acerca de políticas de seguridad del sistema a evaluar, por ejemplo, verificar si existe políticas para el acceso al sistema de evaluación docente.

Es posible identificar dos tipos de amenazas.

- **Deliberadas:** Este tipo de amenazas con las que están previamente planificadas para causar daño a la organización.
- **Accidentales:** Este tipo de amenazas son las que no están planificadas por ningún actor, sin embargo, generan daños a la organización.

Una vez valorados los activos Pilar asocia a cada uno de los activos del sistema de evaluación docente, amenazas posibles para dicho activo. A continuación, en la figura 20 se presentan las amenazas asociadas a los activos del sistema de evaluación docente.

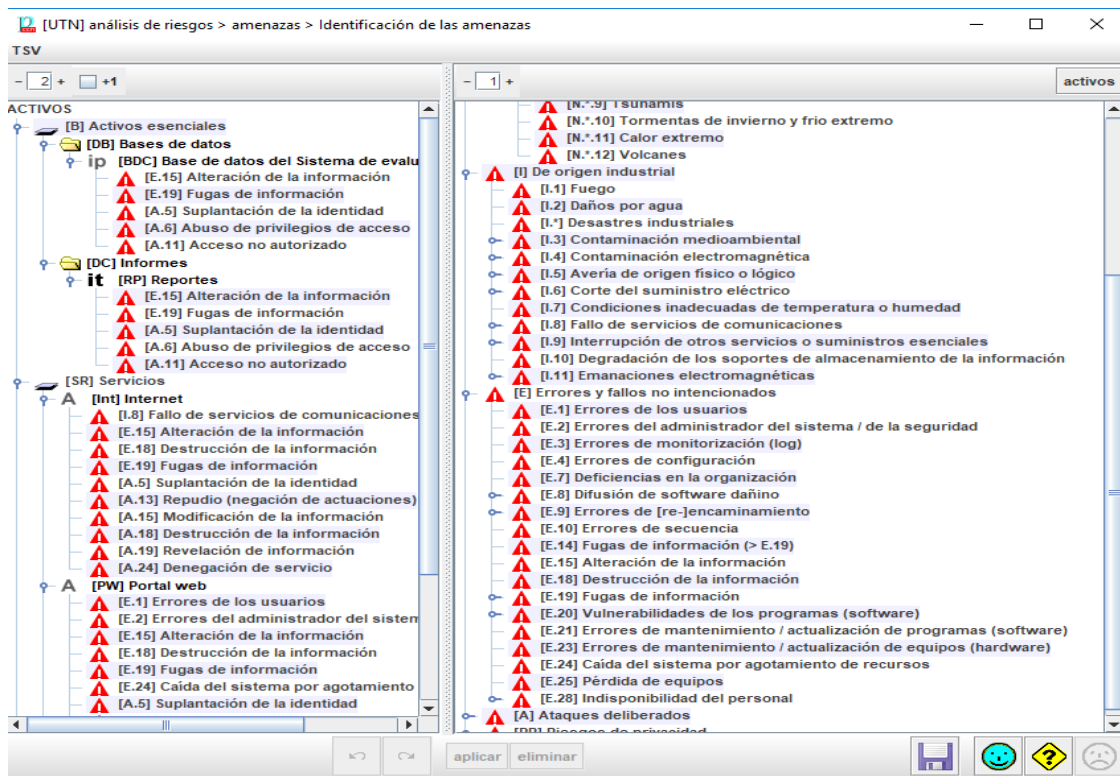


Figura 20: Amenazas del sistema de evaluación docente.

Fuente: Elaboración Propia

2.6.5 Valoración de amenazas

Para la valoración de amenazas se toma en cuenta dos factores importantes:

- **Probabilidad de ocurrencia:** es el registro de ocurrencia de una amenaza cuando se materializa una amenaza.
- **Porcentaje de degradación:** es el daño que causo el incidente ocurrido.

Para evaluar la ocurrencia se lo hace mediante los parámetros presentados en la tabla 26.

Tabla 25: Probabilidad 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: *Elaboración Propia*

Para valorar de forma adecuada las amenazas es necesario diferenciar entre amenazas accidentales e intencionadas. El porcentaje de degradación es la relación entre la amenaza y dimensión, esta se mide entre 0% y 100%.

A continuación, en la figura 21 se presentan los porcentajes recomendados por Pilar para el sistema de evaluación docente.

| activo | co. | frecuencia | [D] | [I] | [C] | [A] | [T] | [V] | [DP] |
|---|-----|------------|------|------|------|------|------|-----|------|
| [BDC] Base de datos del Sistema de evaluación Docente | | | 100% | 100% | 100% | 100% | | | |
| [DC] Informes | | | 0 | 10% | 50% | 100% | | | |
| [SR] Servicios | | | | | | | | | |
| [Int] Internet | | | 100% | 100% | 100% | 100% | 100% | | |
| [PW] Portal web | | | 50% | 50% | 50% | 100% | | | |
| [PDC] Portafolio de Docentes | | | 50% | 50% | 50% | 100% | 100% | | |
| [E] Equipamiento | | | | | | | | | |
| [SW] Aplicaciones | | | | | | | | | |
| [G] Gestion de horarios | | | 100% | 100% | 100% | | | | |
| [HD] Ayuda | | | 100% | 100% | 100% | | | | |
| [PWS] Portal Web | | | 100% | 100% | 100% | | | | |
| [EVAL] Evaluación Docente | | | 100% | 100% | 100% | | | | |
| [SEC] Seguridad Firewall | | | 100% | 100% | 100% | | | | |
| [HW] Equipos(Hardware) | | | | | | | | | |
| [SBDD] Servidor de BDD | | | 100% | 100% | 100% | | | | |
| [PTR] Puestos de trabajo | | | 100% | 10% | 50% | | | | |
| [SPW] Servidor de portal web | | | 100% | 100% | 100% | | | | |
| [SRP] Servidor de reportes | | | 100% | 100% | 100% | | | | |
| [SAPL] Servidor de aplicaciones | | | 100% | 100% | 100% | | | | |
| [Fw] Firewall | | | 100% | 10% | 100% | | | | |
| [COM] Comunicaciones | | | | | | | | | |
| [RTN] Red interna UTN | | | 50% | 20% | 50% | 100% | | | |
| [I] Instalaciones | | | | | | | | | |
| [AD] Area de desarrollo | | | 100% | | | | | | |
| [AS] Area de seguridad | | | 100% | | | | | | |
| [DTC] Data Center | | | 100% | | | | | | |
| [P] Persona | | | | | | | | | |
| [VIC] Vicerrector académico | | | 50% | 50% | 20% | | | | |
| [CIP] Coordinador del CEIOPA | | | 50% | 50% | 50% | | | | |
| [SBO] Subdecano | | | 50% | 50% | 20% | | | | |
| [COC] Coordinador de Carrera | | | 50% | 50% | 20% | | | | |
| [DDC] Docentes | | | 100% | 100% | 20% | | | | |
| [EST] Estudiantes | | | 50% | 50% | 20% | | | | |
| [DIR] Director del departamento de informática | | | 50% | 100% | 100% | | | | |
| [ASIS] Analista de sistemas | | | 50% | 100% | 100% | | | | |
| [DPRO] Director de proyecciones informáticas | | | 50% | 50% | 50% | | | | |
| [DSOFT] Desarrolladores de software | | | 20% | 100% | 100% | | | | |
| [BDD] Administrador de BDD | | | 50% | 100% | 100% | | | | |

Figura 21: Amenazas del sistema de evaluación docente.

Fuente: Elaboración Propia

En la figura 22 de acuerdo a la tabla 26 la probabilidad de ocurrencia en el sistema podemos evidenciar en la columna de frecuencia.

| activo | co. | frecuencia | [D] | [I] | [C] | [A] | [T] | [V] | [DP] |
|---|-----|------------|------|------|------|------|------|------|------|
| [B] Activos esenciales | | | | | | | | | |
| [DB] Bases de datos | | | | | | | | | |
| [BDC] Base de datos del Sistema de evaluación Docente | | | 1% | 10% | 50% | 100% | | | |
| [E.15] Alteración de la información | 1 | 1 | | 1% | | | | | |
| [E.18] Destrucción de la información | 1 | 1 | 1% | | | | | | |
| [E.19] Fugas de información | 1 | 1 | | | 10% | | | | |
| [A.5] Suplantación de la identidad | 10 | 10 | | | 10% | 100% | | | |
| [A.6] Abuso de privilegios de acceso | 10 | 10 | 1% | | 10% | 50% | | | |
| [A.11] Acceso no autorizado | 10 | 10 | | | 10% | 50% | | | |
| [DC] Informes | | | | | | | | | |
| [RP] Reportes | | | 0 | 10% | 50% | 100% | | | |
| [SR] Servicios | | | | | | | | | |
| [Int] Internet | | | 100% | 100% | 100% | 100% | 100% | | |
| [I.8] Fallo de servicios de comunicaciones | 1 | 1 | 100% | | | | | | |
| [E.15] Alteración de la información | 1 | 1 | | 10% | | | | | |
| [E.18] Destrucción de la información | 1 | 1 | 10% | | | | | | |
| [E.19] Fugas de información | 1 | 1 | | | 10% | | | | |
| [A.5] Suplantación de la identidad | 0.2 | 0.2 | | | 100% | 100% | 100% | 100% | |
| [A.13] Repudio (negación de actuaciones) | 1 | 1 | | | | | | | |
| [A.15] Modificación de la información | 1 | 1 | | 50% | | | | | |
| [A.18] Destrucción de la información | 1 | 1 | 50% | | | | | | |
| [A.19] Revelación de información | 1 | 1 | | | 50% | | | | |
| [A.24] Denegación de servicio | 1 | 1 | 50% | | | | | | |
| [PW] Portal web | | | 50% | 50% | 50% | 100% | | | |
| [E.1] Errores de los usuarios | 1 | 1 | 10% | 10% | 10% | | | | |
| [E.2] Errores del administrador del sistema / de la seguridad | 1 | 1 | 20% | 20% | 20% | | | | |
| [E.15] Alteración de la información | 1 | 1 | | 1% | | | | | |
| [E.18] Destrucción de la información | 1 | 1 | 10% | | | | | | |
| [E.19] Fugas de información | 1 | 1 | | | 10% | | | | |
| [E.24] Caída del sistema por agotamiento de recursos | 10 | 10 | 50% | | | | | | |
| [A.5] Suplantación de la identidad | 1 | 1 | | 50% | 50% | 100% | | | |
| [A.6] Abuso de privilegios de acceso | 1 | 1 | 1% | 10% | 10% | 100% | | | |
| [A.7] Uso no previsto | 1 | 1 | 1% | 10% | 10% | 100% | | | |
| [A.11] Acceso no autorizado | 1 | 1 | | 10% | 50% | 100% | | | |
| [A.15] Modificación de la información | 10 | 10 | | 50% | | | | | |
| [A.18] Destrucción de la información | 1 | 1 | 50% | | | | | | |
| [A.24] Denegación de servicio | 10 | 10 | 50% | | | | | | |
| [PDC] Portafolio de Docentes | | | 50% | 50% | 50% | 100% | 100% | | |

Figura 22: Tabla de amenazas y porcentaje de probabilidad de ocurrencia

Fuente: Elaboración Propia

2.6.6 Estimación de impacto

El impacto es el daño que se originó en los activos una vez que las amenazas se materializaron. Para la estimación de impacto se lo hace mediante los siguientes factores:

- La materialización de una amenaza puede afectar a todo un recurso informático o solo a una parte de este.
- La materialización de una amenaza puede afectar a partes claves de información o a partes independientes.
- Una vez materializada la amenaza es temporal o permanente.

Los impactos pueden traer consigo impactos cualitativos o cuantitativos, por ejemplo, pérdidas económicas, mala imagen de los clientes hacia la empresa entre muchas otras.

Es posible establecer una relación entre la consecuencia de los riesgos materializados y las salvaguardas necesarias. También se debe tomar en cuenta la frecuencia de ocurrencia de las amenazas, debido muchas amenazas materializándose al mismo tiempo puede causar considerables pérdidas y daños a la organización.

2.6.7 Impacto acumulado

Es posible conocer el impacto acumulado, su cálculo es para cada activo, cada amenaza y la dimensión de valoración, el resultado está descrito en función de la degradación y el valor acumulado; por lo tanto, mientras más grande sea la degradación, mayor será el impacto acumulado.

El impacto acumulado es de mucha utilidad para saber que salvaguardas se deben aplicar en la organización para mitigar los riesgos.

A continuación, en la figura 23 se presenta el impacto acumulado en los activos del sistema de Evaluación docente.

| potencial | current | target | PILAR | | [D] | [I] | [C] | [A] | [T] | [V] | [DP] |
|-----------|---------|--------|-------|---|------|------|------|------|------|------|------|
| | | | | activo | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | [B] Activos esenciales | [10] | [7] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [DB] Bases de datos | [10] | [7] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [BDC] Base de datos del Sistema de evaluación Docente | [10] | [7] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [DC] Informes | [10] | [7] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [RP] Reportes | [10] | [7] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SR] Servicios | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [Int] Internet | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [PW] Portal web | [9] | [9] | [9] | [10] | [10] | [9] | [10] |
| | | | | ↳ [PDC] Portafolio de Docentes | [9] | [9] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [E] Equipamiento | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SW] Aplicaciones | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [GH] Gestion de horarios | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [HD] Ayuda | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [PW] Portal Web | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [EVAL] Evaluación Docente | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SEc] Seguridad Firewall | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [HW] Equipos(Hardware) | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SBDD] Servidor de BDD | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [PTR] Puestos de trabajo | [10] | [7] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SPW] Servidor de portal web | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SRP] Servidor de reportes | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SAPL] Servidor de aplicaciones | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [Fir] Firewall | [10] | [7] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [COM] Comunicaciones | [9] | [8] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [RITN] Red interna UTN | [9] | [9] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [I] Instalaciones | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [AD] Área de desarrollo | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [AS] Área de seguridad | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [DTC] Data Center | [10] | [10] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [PI] Personal | [9] | [9] | [10] | [10] | [10] | [10] | [10] |
| | | | | ↳ [VIC] Vicerrector académico | [9] | [9] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [CIP] Coordinador del CEIDPA | [9] | [9] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [SBD] Subdecano | [9] | [9] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [COC] Coordinador de Carrera | [9] | [9] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [DOC] Docentes | [9] | [9] | [9] | [10] | [10] | [10] | [10] |
| | | | | ↳ [EST] Estudiantes | [9] | [9] | [9] | [10] | [10] | [10] | [10] |

Figura 23: Impacto acumulado del sistema de evaluación docente.

Fuente: Elaboración Propia

En la figura 24 se muestra un gráfico en que se detalla el riesgo acumulado del sistema de evaluación docente.

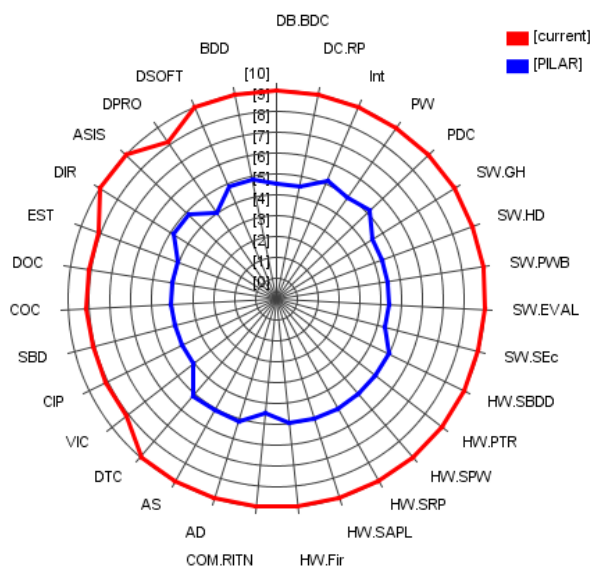


Figura 24: Situación actual del impacto acumulado del sistema de evaluación docentes.

Fuente: Elaboración Propia

En la figura 24 se evidencia el gráfico del impacto acumulado al sistema de evaluación docente, el gráfico en rojo es el porcentaje en el que se encuentra la Universidad, mientras que lo azul es lo recomendable por Pilar.

2.6.8 Riesgo acumulado

A continuación, en la figura 26 se presenta el riesgo acumulado en los activos del sistema de Evaluación docente.

| activo | [D] | [I] | [C] | [A] | [T] | [V] | [DP] |
|---|-------|-------|-------|-------|-------|-----|------|
| ACTIVOS | (7,2) | (7,2) | (8,1) | (7,7) | (7,4) | | |
| [B] Activos esenciales | | (6,8) | (8,1) | (7,7) | | | |
| [DB] Bases de datos | | (6,8) | (8,1) | (7,7) | | | |
| [BDC] Base de datos del Sistema de evaluación Docente | | (6,8) | (8,1) | (7,7) | | | |
| [DC] Informes | | (6,8) | (8,1) | (7,7) | | | |
| [RP] Reportes | | (6,8) | (8,1) | (7,7) | | | |
| [SR] Servicios | (7,2) | (7,2) | (6,3) | (6,8) | (7,4) | | |
| [Int] Internet | (6,8) | (6,3) | (6,3) | (6,2) | (6,2) | | |
| [PW] Portal web | (7,2) | (7,2) | (6,3) | (6,8) | | | |
| [PDC] Portafolio de Docentes | (7,2) | (7,2) | (6,3) | (6,8) | (7,4) | | |
| [E] Equipamiento | (7,2) | (6,8) | (6,8) | (6,8) | | | |
| [SW] Aplicaciones | (6,8) | (6,8) | (6,8) | | | | |
| [GH] Gestion de horarios | (6,8) | (6,8) | (6,8) | | | | |
| [HD] Ayuda | (6,8) | (6,8) | (6,8) | | | | |
| [PWB] Portal Web | (6,8) | (6,8) | (6,8) | | | | |
| [EVAL] Evaluación Docente | (6,8) | (6,8) | (6,8) | | | | |
| [SEC] Seguridad Firewall | (6,8) | (6,8) | (6,8) | | | | |
| [HW] Equipos(Hardware) | (7,2) | (6,8) | (6,8) | | | | |
| [SBD] Servidor de BDD | (7,2) | (6,8) | (6,8) | | | | |
| [PTR] Puestos de trabajo | (7,2) | (6,3) | (6,3) | | | | |
| [SPW] Servidor de portal web | (7,2) | (6,8) | (6,8) | | | | |
| [SRP] Servidor de reportes | (7,2) | (6,8) | (6,8) | | | | |
| [SAPL] Servidor de aplicaciones | (7,2) | (6,8) | (6,8) | | | | |
| [Fir] Firewall | (7,2) | (6,3) | (6,3) | | | | |
| [COM] Comunicaciones | (7,2) | (6,3) | (6,3) | (6,8) | | | |
| [RIT] Red interna UTN | (7,2) | (6,3) | (6,3) | (6,8) | | | |
| [L] Instalaciones | (6,8) | | | | | | |
| [AD] Área de desarrollo | (6,8) | | | | | | |
| [AS] Área de seguridad | (6,8) | | | | | | |
| [DTC] Data Center | (6,8) | | | | | | |
| [P] Personal | (6,3) | (6,8) | (7,2) | | | | |
| [VIC] Vicerrector académico | (6,0) | (6,3) | (6,5) | | | | |
| [CIP] Cordinador del CEIDPA | (6,0) | (6,3) | (7,2) | | | | |
| [SBD] Subdecano | (6,0) | (6,3) | (6,5) | | | | |
| [COC] Coordinador de Carrera | (6,0) | (6,3) | (6,5) | | | | |
| [DOC] Docentes | (6,0) | (6,3) | (6,5) | | | | |
| [EST] Estudiantes | (6,0) | (6,3) | (6,5) | | | | |

Figura 25: Riesgo acumulado del sistema de evaluación docente.

Fuente: Elaboración Propia

2.6.9 Impacto repercutido

El valor repercutido se calcula en base al valor del activo, permite conocer las consecuencias que tendría la ocurrencia de accidentes técnicos en el sistema de información.

Calculo de nivel de riesgo

Para calcular en nivel de riesgo es necesario identificar los riesgos. Para la identificación de riesgos existen varios métodos entre los cuales destacan:

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

Valoración de riesgos.

La valoración de riesgos es un proceso secuencia, es decir se tiene que seguir la siguiente secuencia, identificación de activos, identificación de amenazas y la estimación de vulnerabilidades de amenazas sobre cada activo.

Para la valoración de riesgos existe cuatro zonas:

- Bajo: Indica que el riesgo es bajo; por lo tanto, no es necesario emplear salvaguardas adicionales.
- Medio: Indica que el riesgo es medio; por lo tanto, se debe considerar la implementación de salvaguardas.
- Alto: Indica que el riesgo es alto; por lo tanto; es obligatorio emplear salvaguardas para mitigar riesgos.
- Crítico: Indica que el riesgo es crítico; por lo tanto, es obligatorio emplear salvaguardas adicionales para minimizar el riesgo.

La moderación para el riesgo se presenta en la tabla 26

Tabla 26: Nivel de riesgo

| | | | | |
|---|---|--------------------------------|---|----|
| 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: *Elaboración Propia*

Los datos presentados en la figura 27 son el resultado del producto entre la probabilidad de ocurrencia y la importancia del riesgo.

| <i>Probabilidad De Ocurrencia</i> | <i>Importancia del riesgo</i> | <i>Nivel de riesgo</i> |
|---------------------------------------|-----------------------------------|------------------------|
| <i>Bajo</i> 1 | <i>Bajo</i> 1 | <i>Bajo</i> 1 |
| <i>Medio</i> 2 | <i>Normal</i> 2 | <i>Bajo</i> 2 |
| <i>Alto</i> 3 | <i>Alto</i> 3 | <i>Bajo</i> 3 |
| | <i>Critico</i> 4 | <i>Medio</i> 4 |
| | | <i>Medio</i> 5 |
| | | <i>Medio</i> 6 |
| | | <i>Alto</i> 7 |
| | | <i>Alto</i> 8 |
| | | <i>Alto</i> 9 |
| | | <i>Critico</i> 10 |
| | | <i>Critico</i> 11 |
| | | <i>Critico</i> 12 |

Figura 26: Tabla de Nivel de Riesgo

Fuente: *Elaboración Propia*

Para determinar el nivel de riesgo se aplica la siguiente expresión.

$$\text{Nivel de riesgo} = \frac{\sum_{i=1}^n \text{Probabilidad de ocurrencia del riesgo (i)} * \text{importancia del riesgo (i)}}{n}$$

Donde

N es la cantidad total de riesgos.

Independiente de la metodología que se emplee es muy importante determinar una lista de riesgos para cada activo, así como también el impacto que implicaría que dicho riesgo se materialice.

Es importante mencionar que el riesgo más peligroso será aquel que no se ha previsto y para el cual no se ha preparado, por ello no independientemente de la prioridad no se debe omitir la existencia de ningún riesgo.

2.6.10 Situación actual del riesgo acumulado

En la figura 28 se muestra un gráfico en que se detalla el riesgo acumulado del sistema de evaluación docente, la gráfica en verde es el riesgo que actualmente posee el sistema de evaluación docentes, el rosa es lo recomendado por Pilar.

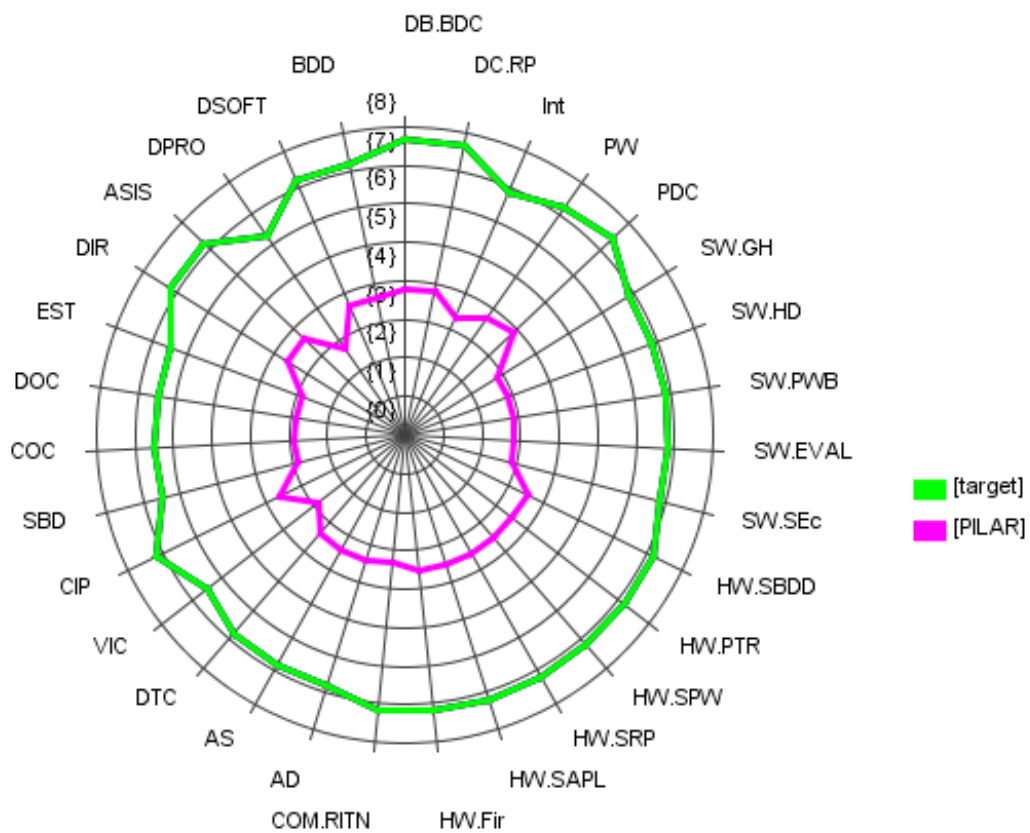


Figura 27: Situación actual del riesgo acumulado del sistema de evaluación docente.

Fuente: Elaboración Propia

En la figura 29 se puede apreciar el riesgo acumulado/ dimensión cabe mencionar que lo recomendado por la metodología es más bajo a lo que actualmente se encuentra.

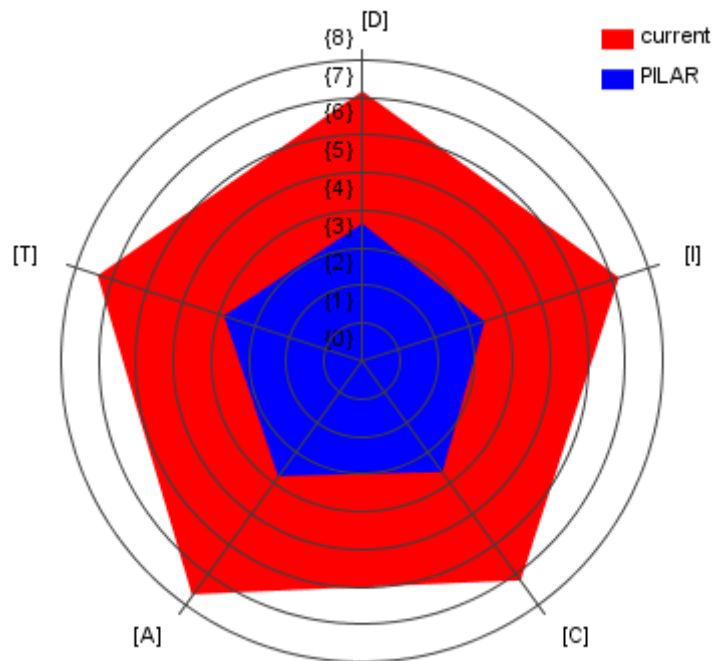


Figura 28: Riesgo Acumulado/dimensión

Fuente: Elaboración Propia

Con los resultados que se obtenidos mediante el análisis es necesario amenorar los riesgos existentes ya que le valor que se encontró es muy alto a diferencia de lo recomendado por la metodología, de esta manera se estaría preservando la seguridad de la información.

Capítulo 3

Resultados

3.1 Informe de Resultados

En esta sección se evalúa el cumplimiento del sistema de evaluación docente en cuanto a seguridad de la información de la Universidad Técnica del Norte, como base para la evaluación se toma en cuenta la norma ISO/IEC 27002:2017, misma que establece un estándar de control de seguridad de la información.

Se ha revisado la documentación existente acerca del sistema de Evaluación docente, para conocer la situación actual del mismo, lo que contribuye a la identificación de vulnerabilidades y amenazas.

El sistema de Evaluación docente es parte de un sistema más grande que abarca todos los servicios de la plataforma virtual de la UTN.

El sistema de Evaluación docente posee varios niveles, en cada nivel existe un actor para la evaluación docente.

Los actores por niveles son los siguientes:

- 1) Vicerrector académico
- 2) CEIDPA
- 3) Subdecano
- 4) Coordinador de carrera
- 5) Docentes
- 6) Estudiantes

3.2 Evaluación del cumplimiento

Para evaluar el cumplimiento de los controles del sistema de Evaluación docente, se tomó como referencia los controles de la norma ISO/IEC 27002:2017.

Se elaboró un Check List de los controles más relevantes para el sistema, mismos que se presentan en la tabla 27.

Tabla 27: Evaluación de cumplimiento de controles ISO 27002:2017

| Aspecto general | Objetivo de control | Control | Observación | Cumplimiento |
|---|--|---|---|--------------|
| Políticas de seguridad de la información | Dirección de gestión de la seguridad de la información | Políticas de seguridad de la información | Existe un plan de desarrollo informático de la UTN 2018-2022 en donde establece políticas para la seguridad de la información. Este se basa en el plan de desarrollo informático de la UTN 2013-2017. | SI |
| | | Revisión de las políticas para la seguridad de la información | No existe procedimientos para la revisión de políticas de seguridad de la información del sistema de evaluación docente. | NO |
| Organización de la seguridad informática | Organización interna | Roles y responsabilidades de seguridad de la información | El personal del área de informática da la UTN desarrolla varias actividades de manera esporádica. No sigue las instrucciones del manual de funciones definido en el plan de desarrollo. | NO |

| | | | | |
|---|------------------------------------|---|--|----|
| Organización de la seguridad informática | | Separación de funciones | Los miembros del departamento de informática tienen funciones específicas de acuerdo a la planificación de desarrollo de la UTN. | SI |
| | | Contacto con las autoridades | En caso de algún inconveniente es posible el contacto con las autoridades mediante la plataforma QUIPUX. | SI |
| | | Contacto con los grupos de interés especial | La UTN mantiene relaciones con proveedores nacionales y extranjeros, de los cuales ninguno es representativo en cuanto a seguridad de la información. | NO |
| | Dispositivos móviles y teletrabajo | Política de dispositivos móviles | No existe una política de soporte para la gestión de riesgos por el uso de dispositivos móvil para ingresar al sistema de evaluación docente. | NO |
| Seguridad en recursos humanos | Antes del empleo | Investigación de antecedentes | LA UTN para integrar un nuevo miembro a su equipo de trabajo solicita las hojas de vida con sus respectivos documentos habilitantes. | SI |
| | | Términos y condiciones de empleo | La UTN no dispone de documentos en donde se describe las funciones y responsabilidades para la seguridad de la información. Debido a que existe un llamamiento a concurso. | NO |

| | | | | |
|--------------------------------------|---------------------------------|---|--|----|
| Seguridad en recursos humanos | Durante el empleo | Responsabilidades de dirección | Existe un manual de funciones, en donde se define las responsabilidades referentes a la seguridad de la información, así como la confidencialidad. | SI |
| | | Conciencia, educación y formación en seguridad de la información. | No existe una capacitación planificada relacionado con la seguridad de la información | NO |
| | | Proceso disciplinario | La UTN no dispone de un proceso disciplinario definido, para sancionar a empleados que hayan violado la seguridad de la información. | NO |
| Seguridad en recursos humanos | Finalización o cambio de empleo | Responsabilidades ante la finalización o cambio de empleo | La UTN no posee documentación oficial acerca de la confidencialidad de la información, una vez terminado el contrato de un empleado. | NO |
| Gestión de activos | Responsabilidad de los activos | Inventario de activos | En el plan estratégico informático existe un inventario de los equipos, servidores y todos los dispositivos empleados en los diferentes módulos. | SI |

| | | | | |
|---------------------------|--|-----------------------------------|--|----|
| Gestión de activos | | Propiedad de activos | Existe responsables de los activos del sistema de evaluación docente, pero no existe un propietario específico. | SI |
| | | Uso adaptable de activos | Existen encargados y responsables del manejo información exclusiva | SI |
| | | Devolución de activos | No existe un procedimiento definido para el registro de activos devueltos por parte de los empleados que terminan su contrato. Pero los activos son registrados de forma directa en la lista de activos fijos. | SI |
| Control de acceso | Requisito de negocio para el control de acceso | Política de control de acceso | La UTN no dispone de políticas para el acceso al sistema de evaluación docente, | NO |
| | | Acceso a redes y servicios de red | La UTN no dispone de políticas para el acceso de redes, pero existe un monitoreo continuo. | NO |
| | Gestión de acceso de los usuarios | Registro y retiro de usuario | La UTN emplea el módulo de personal involucrado para la revisión permanente de usuarios. | SI |
| | | Provisión de acceso a usuarios | No existe un procedimiento definido para asignar o revocar los derechos de acceso a usuarios. Es gestionado por el módulo de seguridad | NO |

| | | | | |
|--------------------------|---|--|---|----|
| | | Gestión de la información secreta de autenticación de los usuarios | No existe políticas de confidencialidad de las claves de acceso de los usuarios | NO |
| Control de acceso | | Revisión de los derechos de acceso de usuario | Existe un seguimiento del acceso de los miembros que ya no son parte de la UTN. También se verifica el usuario cuando se identifica una anomalía. | NO |
| | | Retiro y ajuste de los derechos de acceso | No existe una eliminación de acceso cuando un estudiante ya no es parte de la UTN | NO |
| | Responsabilidades del usuario | Uso de la información secreta de autenticación | No existe un procedimiento definido para el acceso a la plataforma y las debidas seguridades. Las claves son administradas por la base de datos. | NO |
| Control de acceso | Control de acceso a sistemas y aplicaciones | Procedimientos seguros de inicio de sesión | No existe una política de acceso seguro. Únicamente se trabaja con el bloque por contraseña | NO |
| Control de acceso | | Sistema de gestión de contraseñas | No existe políticas para la asignación de contraseñas. Las contraseñas son asignadas por la base de datos | NO |

| | | | | |
|---------------------------------------|--------------------------|--|--|----|
| Control de acceso | | Control de acceso al código fuente del programa | No existe documentación acerca del acceso al código fuente. Solo los usuarios autorizados ingresan al código fuente dependiendo de rango | SI |
| | Controles criptográficos | Política de uso de los controles criptográficos | Existe documentado en el sistema de gestión de procesos | SI |
| Criptografía | | Gestión de llaves | No existe políticas para la gestión de llaves. Las llaves se gestionan directamente desde la base de datos en base a su configuración. | NO |
| | Áreas seguras | Perímetro de seguridad física | La UTN cuenta con un área exclusiva para el área de desarrollo debidamente señalizada. | SI |
| Seguridad física y del entorno | | Controles físicos de entrada | El ingreso es mediante un biométrico | SI |
| | | Protección contra amenazas externas y ambientales. | No existe procedimientos definidos contra eventualidades externas. | NO |
| | Equipos | Ubicación y protección de equipos | No existe políticas para el consumo de alimentos o cualquier líquido que dañe los equipos o documentos. | NO |

| | | | | |
|---------------------------------------|--|--|--|----|
| Seguridad física y del entorno | | Instalaciones de suministro | No existe suministro redundante que garantice la continuidad operativa. | NO |
| | | Seguridad del cableado | El cableado de voz, datos y eléctrico está protegido contra daños | SI |
| | | Mantenimiento de los equipos | Existe un plan de mantenimiento adecuado para el Data Center, lo cual garantiza la continuidad del servicio de la plataforma. Además, existe contratos con proveedores externos para la reparación en caso de posibles fallas. | SI |
| Seguridad de las operaciones | Procedimientos y responsabilidades operacionales | Documentación de procedimientos de operación | En base a trabajos de pregrado, la universidad posee procesos que son contradictorios. | SI |
| | | Gestión de cambios | Los cambios son posibles mediante la plataforma Quipux | SI |
| | | Gestión de capacidades | Las funciones del departamento de informática son designadas de tal forma que se evitan modificaciones significativas. | SI |

| | | | | |
|-------------------------------------|--------------------------------------|---|---|----|
| Seguridad de las operaciones | | Separación de ambientes de desarrollo, pruebas y producción | Existe áreas de desarrollo y de producción debidamente separadas, además el ambiente de prueba es el mismo entorno de desarrollo de cada programador. | SI |
| | Protección contra un malware | Controles contra un malware | Todos los terminales del DDTI cuenta con Eset-EndPoint corporativo. Además, se cuenta con un firewall para el acceso a internet, | SI |
| | Copias de seguridad | Copias de seguridad de la información | Existen copias de seguridad realizadas a diario. La documentación física es respaldada cada semestre | SI |
| Seguridad de las operaciones | Registro y monitoreo | Registro de eventos | No existe procesos de registro de eventos. | NO |
| | | Protección de la información de registro | Los registros se encuentran protegidos de los accesos no autorizados. | SI |
| | Control del software operacional | Instalación del software en los sistemas operativos | Todo software implementado en los dispositivos cuenta con licencias. | SI |
| | Gestión de la vulnerabilidad técnica | Gestión de las vulnerabilidades técnicas | No existe procedimientos definidos para las vulnerabilidades técnicas. En caso de algún fallo no existe herramientas de backup, | NO |

| | | | | |
|---|---|---|---|----|
| | | Restricciones en la instalación del software | No existe normas para la sanción del personal que instale software no adecuado. | NO |
| Seguridad de las operaciones | Consideraciones sobre la auditoria de sistemas de información | Controles de auditoria de sistemas de información | El control de la auditoria del sistema de evaluación docente está gestionado por el sistema de auditoria. Toda la documentación del proceso se encuentra en una tesis, la cual la describe como una aplicación del módulo de gestión académica. | SI |
| | Gestión de la seguridad de redes | Controles de red | Existe control mediante el portal cautivo para estudiantes, docentes y administrativos mediante filtrado MAC | SI |
| Seguridad en las telecomunicaciones. | | Seguridad de los servicios de red | La UTN cuenta con mecanismos de seguridad Cisco ASA. | SI |
| | | Separación en las redes | La red de la UTN se encuentra segmentada en varias VLAN. Existe documentación de ello. | SI |
| | Requisitos de seguridad de los sistemas de información | Análisis de requisitos y especificaciones de seguridad de la información. | Los requisitos de seguridad de la información se encuentran documentados en los manuales de procedimiento en el área de desarrollo. | SI |

| | | | | |
|--|---|--|---|----|
| Adquisición. Desarrollo y mantenimiento del sistema | Seguridad en el desarrollo y en los procesos de soporte | Política de desarrollo seguro | Para el desarrollo del sistema de evaluación docente la UTN hace empleo de una metodología RUP. | SI |
| | | Procedimientos de control de cambios en el sistema | El control de cambios se realiza mediante el módulo de Planificación del Sistema Integra Informático. | SI |
| | Datos de prueba | Protección de datos de prueba | Las pruebas de software se realizan en el puesto de trabajo de los programadores. No existe directrices para el uso de datos reales para pruebas. | NO |
| Relaciones con proveedores | Gestión de la provisión de servicios del proveedor | Monitoreo y revisión de los servicios de proveedores | La UTN mantiene relaciones con proveedores externos, pero no existe procesos de seguimiento. | NO |
| | | Gestión de cambios en los servicios de proveedores. | Los contratos con proveedores externos se encuentran en proveeduría. | SI |

| | | | | |
|---|--|--|---|----|
| Gestión de incidentes de seguridad de la información | Gestión de los incidentes de seguridad de la información y mejoras | Responsabilidades y procedimientos | La UTN no cuenta con un software Help Desk, pero no lo tiene implementado. | NO |
| | | Informe de los eventos de seguridad de la información | No existe un proceso definido para la recopilación de errores del sistema de evaluación docente. | NO |
| | | Informe de debilidades de seguridad de la información | no existe un procedimiento definido, para la recopilación de errores por parte de proveedores. | NO |
| | | Respuesta a incidentes de seguridad de la información | La respuesta ante incidentes de seguridad se realiza mediante registros de Quipux, los registros son autorizados por la dirección de informática. | SI |
| | Gestión de incidentes de | Aprendizaje de los incidentes de seguridad de la información | No existe un manual de evaluación de incidentes que permita mejorar los errores cometidos en cuanto a la seguridad de la información. | NO |

| | | | | |
|---|--|---|---|----|
| seguridad de la información | | Recopilación de evidencias | La recopilación de incidentes se lo realiza mediante la plataforma Quipux. | SI |
| Aspectos de seguridad de la información para la gestión de la continuidad del negocio. | Continuidad de seguridad de la información | Planificación de la continuidad de seguridad de la información | El departamento de informática cuenta con un plan de continuidad a baja escala, el plan no toma en cuenta daños ni catástrofes y no incluyen en la seguridad de la información. | NO |
| | Redundancias | Disponibilidad de las instalaciones de procesamiento de la información | El departamento de informática no dispone de la infraestructura necesaria para brindar un servicio de alta disponibilidad. | NO |
| Cumplimiento | Cumplimiento de los requisitos legales contractuales | Identificación de la legislación aplicable de los requisitos contractuales. | Se aplica la Ley de Educación Superior y el Reglamento Interno de la UTN | SI |
| | | Derechos de propiedad intelectual | Cada trabajo de titulación y desarrollo de software cuenta con derechos de autor. | SI |

| | | | |
|---------------------|--|---|----|
| Cumplimiento | Protección de los registros | La información proporcionada de la evaluación docente es almacenada en una base de datos específica | SI |
| | Protección y privacidad de la información de carácter personal | El DDTI no cuenta con algún documento sobre confidencialidad de la información | NO |

Fuente: *Elaboración Propia*

Después de haber realizado el Check List de la norma ISO 27002 se observó que dentro del Departamento de Desarrollo Tecnológico e Informático (DDTI) no se cumple con ciertos controles y este resultado se ve reflejado en la figura 30 el porcentaje de cumplimiento mediante la norma ISO 27002:2017

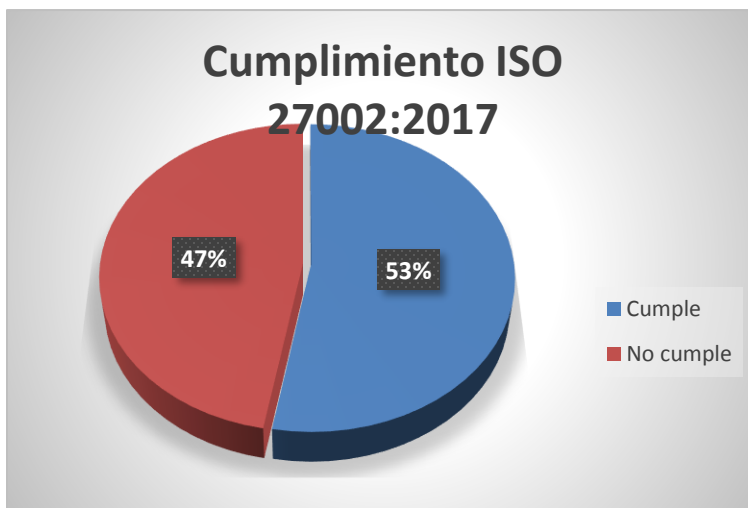


Figura 29: Cumplimiento de controles ISO 27002:2017

Fuente: *Elaboración Propia*

Mediante este resultado es necesario elaborar un listado de observaciones y recomendaciones en base a la normativa para que esta pueda ser puesta en marcha dentro del Departamento de Desarrollo Tecnológico e Informático (DDTI).

3.3 Informe de No Conformidades ISO 27002:2017

La siguiente tabla es un resumen de los controles que no se cumplen según recomendación de la Norma ISO 27002:2017 dentro del Departamento de Desarrollo Tecnológico e Informático (DDTI), ante esta situación se realiza las recomendaciones necesarias para que dicho control pueda ser aplicado y lograr un cumplimiento a un mediano plazo de la Normativa. La siguiente información se detalla en la Tabla 30.

Figura 30: Observaciones y recomendaciones de los controles ISO 27002:2017

| Aspecto general | Objetivo de control | Control | Observación | Cumplimiento | Recomendación |
|---|--|---|---|---------------------|--|
| Políticas de seguridad de la información | Dirección de gestión de la seguridad de la información | Revisión de las políticas para la seguridad de la información | No existe procedimientos para la revisión de políticas de seguridad de la información del sistema de evaluación docente. | NO | Asignar a un analista la tarea de crear políticas de seguridad de la información y sus respectivos procedimientos. Además, el analista será el encargado dar seguimiento al cumplimiento de las políticas creadas. |
| Organización de la seguridad informática | Organización interna | Roles y responsabilidades de seguridad de la información | El personal del área de informática da la UTN desarrolla varias actividades de manera esporádica. No sigue las instrucciones del manual de funciones definido en el plan de desarrollo. | NO | Revisar el manual de funciones, para comprobar si es necesario hacer modificaciones a los procedimientos y posterior a ello hacer cumplir procedimientos. |

| | | | | | |
|---|------------------------------------|---|--|----|--|
| | Organización interna | Contacto con los grupos de interés especial | La UTN mantiene relaciones con proveedores nacionales y extranjeros, de los cuales ninguno es representativo en cuanto a seguridad de la información. | NO | Establecer contactos con grupos de la seguridad de la información. |
| Organización de la seguridad informática | Dispositivos móviles y teletrabajo | Política de dispositivos móviles | No existe una política de soporte para la gestión de riesgos por el uso de dispositivos móvil para ingresar al sistema de evaluación docente. | NO | Establecer políticas de seguridad para el ingreso desde dispositivos móviles. Las medidas de seguridad deberán ser difundidas para el conocimiento de todas las partes implicadas. |
| Seguridad en recursos humanos | Antes del empleo | Términos y condiciones de empleo | La UTN no dispone de documentos en donde se describe las funciones y responsabilidades para la seguridad de la información. Debido a que existe un llamamiento a concurso. | NO | Definir de forma clara y concisa los términos y condiciones de contrato, para las diferentes actividades del DDTI. |

| | | | | | |
|--------------------------------------|--|---|--|----|---|
| | Durante el empleo | Conciencia, educación y formación en seguridad de la información. | No existe una capacitación planificada relacionado con la seguridad de la información | NO | Crear un plan de capacitación, para dar a conocer los puntos importantes sobre la seguridad de la información. |
| Seguridad en recursos humanos | Durante el empleo | Proceso disciplinario | La UTN no dispone de un proceso disciplinario definido, para sancionar a empleados que hayan violado la seguridad de la información. | NO | Crear un proceso disciplinario bien definido, para la sanción de actores que violen la seguridad de la información. |
| | Finalización o cambio de empleo | Responsabilidades ante la finalización o cambio de empleo | La UTN no posee documentación oficial acerca de la confidencialidad de la información, una vez terminado el contrato de un empleado. | NO | Elabora un plan para el cese de cambios de personal. Para retirar el acceso a los estudiantes y docentes que no pertenezcan a la UTN. |
| Control de acceso | Requisito de negocio para el control de acceso | Política de control de acceso | La UTN no dispone de políticas para el acceso al sistema de evaluación docente. | NO | Crear políticas de para el acceso y control del sistema de evaluación docente. |
| | Requisito de negocio para el control de acceso | Acceso a redes y servicios de red | La UTN no dispone de políticas para el acceso de redes, pero existe un monitoreo continuo. | NO | Crear un plan de monitores del sistema de evaluación docente. |

| | | | | | |
|--------------------------|-----------------------------------|--|---|----|---|
| | Gestión de acceso de los usuarios | Provisión de acceso a usuarios | No existe un procedimiento definido para asignar o revocar los derechos de acceso a usuarios. Es gestionado por el módulo de seguridad | NO | Crear un proceso para la creación de nuevos usuarios y revocar a usuarios. |
| Control de acceso | Gestión de acceso de los usuarios | Gestión de la información secreta de autenticación de los usuarios | No existe políticas de confidencialidad de las claves de acceso de los usuarios | NO | Crear medidas de seguridad para el acceso al sistema de evaluación docente y difundirlas. |
| | Gestión de acceso de los usuarios | Revisión de los derechos de acceso de usuario | Existe un seguimiento del acceso de los miembros que ya no son parte de la UTN. También se verifica el usuario cuando se identifica una anomalía. | NO | Crear un proceso para revisar los derechos de acceso al sistema de evaluación docente. |
| Control de acceso | Gestión de acceso de los usuarios | Retiro y ajuste de los derechos de acceso | No existe una eliminación de acceso cuando un estudiante ya no es parte de la UTN | NO | Crear un proceso para la eliminación de acceso a los estudiantes y docentes que ya no pertenecen a la UTN |

| | | | | | |
|--------------------------|---|--|--|----|---|
| Control de acceso | Responsabilidades del usuario | Uso de la información secreta de autenticación | No existe un procedimiento definido para el acceso a la plataforma y las debidas seguridades. Las claves son manejadas por la base de datos. | NO | Crear una guía de seguridad para el acceso al sistema de evaluación docente y difundirla. |
| Control de acceso | Control de acceso a sistemas y aplicaciones | Procedimientos seguros de inicio de sesión | No existe una política de acceso seguro. Únicamente se trabaja con el bloque por contraseña | NO | Crear un proceso para inicios de sesión y desbloqueo para el sistema de evaluación docente. |
| | Control de acceso a sistemas y aplicaciones | Sistema de gestión de contraseñas | No existe políticas para la asignación de contraseñas. Las contraseñas son asignadas por la base de datos | NO | Crear una política para la gestión de contraseñas y políticas de confidencialidad |
| Criptografía | Controles criptográficos | Gestión de llaves | No existe políticas para la gestión de llaves. Las llaves se gestionan directamente desde la base de datos en base a su configuración. | NO | Crear políticas para la gestión de llaves del sistema de evaluación docente. |
| | Áreas seguras | Protección contra amenazas externas y ambientales. | No existe procedimientos definidos contra eventualidades externas. | NO | Establecer procedimientos contra eventualidades externas. |

| | | | | | |
|---------------------------------------|--------------------------------------|--|---|----|--|
| Seguridad física y del entorno | Equipos | Ubicación y protección de equipos | No existe políticas para el consumo de alimentos o cualquier líquido que dañe los equipos o documentos. | NO | Establecer políticas contra consumo de alimentos en sitios de procesamiento de datos físicos. |
| | Equipos | Instalaciones de suministro | No existe suministro redundante que garantice la continuidad operativa. | NO | Proponer un plan de redundancia eléctrica. |
| Seguridad de las operaciones | Registro y monitoreo | Registro de eventos | No existe procesos de registro de eventos. | NO | Proponer un procedimiento para la recopilación de evidencia de incidentes del sistema de evaluación docente. |
| Seguridad de las operaciones | Gestión de la vulnerabilidad técnica | Gestión de las vulnerabilidades técnicas | No existe procedimientos definidos para las vulnerabilidades técnicas. En caso de algún fallo no existe herramientas de backup. | NO | Proponer procedimientos ante vulnerabilidades técnicas para el sistema de evaluación docente |
| Seguridad de las operaciones | Gestión de la vulnerabilidad técnica | Restricciones en la instalación del software | No existe normas para la sanción del personal que instale software no adecuado. | NO | Establecer un reglamento para la instalación de nuevo software en los equipos del DDTI |

| | | | | | |
|---|--|--|---|----|---|
| Adquisición Desarrollo y mantenimiento del sistema | Datos de prueba | Protección de datos de prueba | Las pruebas de software se realizan en el puesto de trabajo de los programadores. No existe directrices para el uso de datos reales para pruebas. | NO | Establecer procedimientos para la realización de prueba con datos reales de software nuevo. |
| Relaciones con proveedores | Gestión de la provisión de servicios del proveedor | Monitoreo y revisión de los servicios de proveedores | La UTN mantiene relaciones con proveedores externos, pero no existe procesos de seguimiento. | NO | Establecer un políticas para la seguridad de la información por parte de proveedores. |
| Gestión de incidentes de seguridad de la información | Gestión de los incidentes de seguridad de la información y mejoras | Responsabilidades y procedimientos | La UTN cuenta con un software Help Desk, pero no lo tiene implementado. | NO | Realizar las pruebas necesarias de Help Desk con la finalidad de ponerlo en operación. |
| | Gestión de los incidentes de seguridad de la información y mejoras | Informe de los eventos de seguridad de la información | No existe un proceso definido para la recopilación de errores del sistema de evaluación docente. | NO | Establecer un procedimiento oficial para la documentación de errores del sistema de evaluación docente. |

| | | | | | |
|--|--|--|---|----|---|
| Gestión de incidentes de seguridad de la información | Gestión de los incidentes de seguridad de la información y mejoras | Informe de debilidades de seguridad de la información | no existe un procedimiento definido, para la recopilación de errores por parte de proveedores. | NO | Establecer un procedimiento para la recopilación de errores en el sistema de información del sistema de evaluación docente. |
| seguridad de la información | Gestión de los incidentes de seguridad de la información y mejoras | Aprendizaje de los incidentes de seguridad de la información | No existe un manual de evaluación de incidentes que permita mejorar los errores cometidos en cuanto a la seguridad de la información. | NO | Establecer un plan de mejoras del sistema de seguridad de la información, la misma que tendrá como base la recopilación de errores registrados del sistema. |
| Aspectos de seguridad de la información para la gestión de la | Continuidad de seguridad de la información | Planificación de la continuidad de seguridad de la información | El departamento de informática cuenta con un plan de continuidad a baja escala, el plan no toma en cuenta daños ni catástrofes y no incluyen en la seguridad de la información. | NO | Agregar al plan de continuidad la seguridad de la información del sistema de evaluación docente. |

| | | | | | |
|---------------------------------|--|--|--|----|---|
| continuidad del negocio. | Redundancias | Disponibilidad de las instalaciones de procesamiento de la información | El departamento de informática no dispone de la infraestructura necesaria para brindar un servicio de alta disponibilidad. | NO | Establecer un plan de redundancia para el sistema de evaluación docente. |
| Cumplimiento | Cumplimiento de los requisitos legales contractuales | Protección y privacidad de la información de carácter personal | El DTI no cuenta con algún documento sobre confidencialidad de la información | NO | Elaborar procedimientos para el manejo de información confidencial del sistema de evaluación docente. |

Fuente: *Elaboración Propia*

3.4 Identificación de Vulnerabilidades

La explotación de vulnerabilidades se ha convertido en la mayor preocupación para las organizaciones en materia de seguridad, le siguen otros incidentes como infección de malware, fraudes, phishing o ataques de denegación de servicio.

Para poder realizar las identificaciones de vulnerabilidades existen varias herramientas que para este estudio se utilizados las siguientes herramientas que se detallan a continuación.

a) SiteVerify

Es una herramienta gratuita para la plataforma de Windows para escanear enlaces e imágenes para averiguar si están rotas o funcionan correctamente. La aplicación es compatible con todas las versiones de Microsoft Windows a partir de Windows XP. Es compatible con versiones de cliente servidor (Brinkmann, 2017).

Los enlaces son una de las principales piedras angulares de Internet. Pueden apuntar a recursos o contenidos locales o remotos, y tienen diferentes estatus asociados con ellos (Brinkmann, 2017).

Los webmasters pueden querer asegurarse de que los enlaces funcionan correctamente en sus páginas. Esto es importante ya que los enlaces rotos se ven generalmente como una señal de baja calidad. Los usuarios de Internet también pueden necesitar herramientas de verificación de enlace, por ejemplo, cuando analizan sus marcadores para los enlaces que ya no funcionan (Brinkmann, 2017).

Se utilizó SiteVerify para verificar si los enlaces son válidos los cuales se extraen y se puede diferenciar con los siguientes colores:

- Azul: Urls que están activas y han sido visitadas.
- Rojo: Urls que no fueron encontradas.
- Verde: Imágenes Validas.
- Negro entradas que no han sido visitadas.

Para realizar la verificación de esta vulnerabilidad se usó el enlace del portafolio estudiantil:
<http://cloud2.utm.edu.ec/ords/f?p=109:LOGIN:.....>

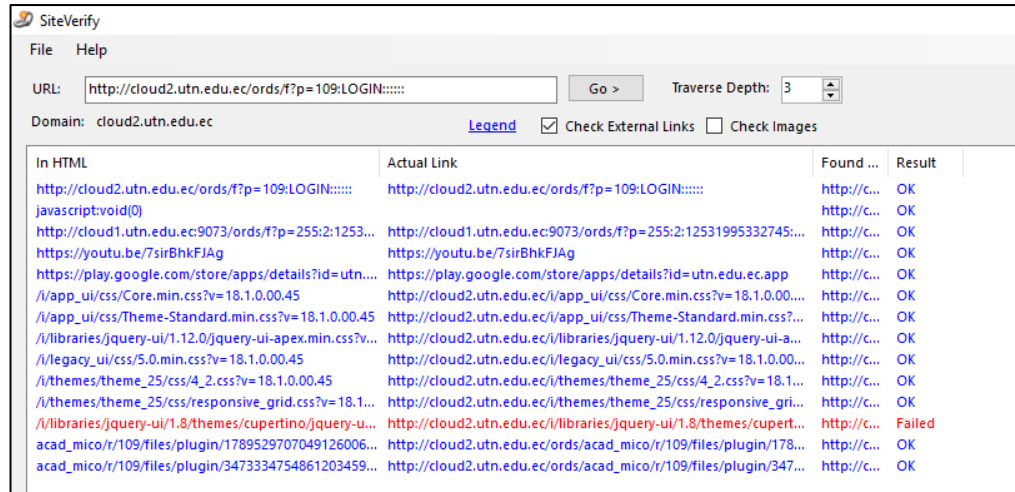


Figura 31: Utilización de la herramienta SiteVerify

Fuente: Elaboración Propia

En la figura 31 se observa que los enlaces están activos y han sido visitados (color azul)
 Y un solo enlace no se encuentra disponible (rojo)

b) Nmap

Nmap es una aplicación multiplataforma usada para explorar redes y obtener información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la conjunción de éstos (Seguinfo, 2007).

Esta aplicación es muy usada, las técnicas de escaneo han sido implementadas en sistemas de detección de intrusos y firewall (Seguinfo, 2007).

Se escogió esta herramienta Nmap para verificación de puertos debido a que es un sistema robusto y el mejor en su área, permitiendo el escaneo en IPv4 e IPv6, el escaneo de host, denegación de servicios, se puede obtener uniforme detallado de los resultados, posee interfaz gráfica para el usuario, es de software gratuito, se puede usar en diferentes plataformas, es de alta velocidad de exploración, comprueba la configuración de elementos de seguridad (cortafuegos, sistemas de detección de intrusos entre otros)

Se procede a realizar un escaneo de puertos habilitados usando a la dirección IP 129.144.x.x esta prueba fue efectuada con herramienta Nmap en Windows se detalla en la figura 32.

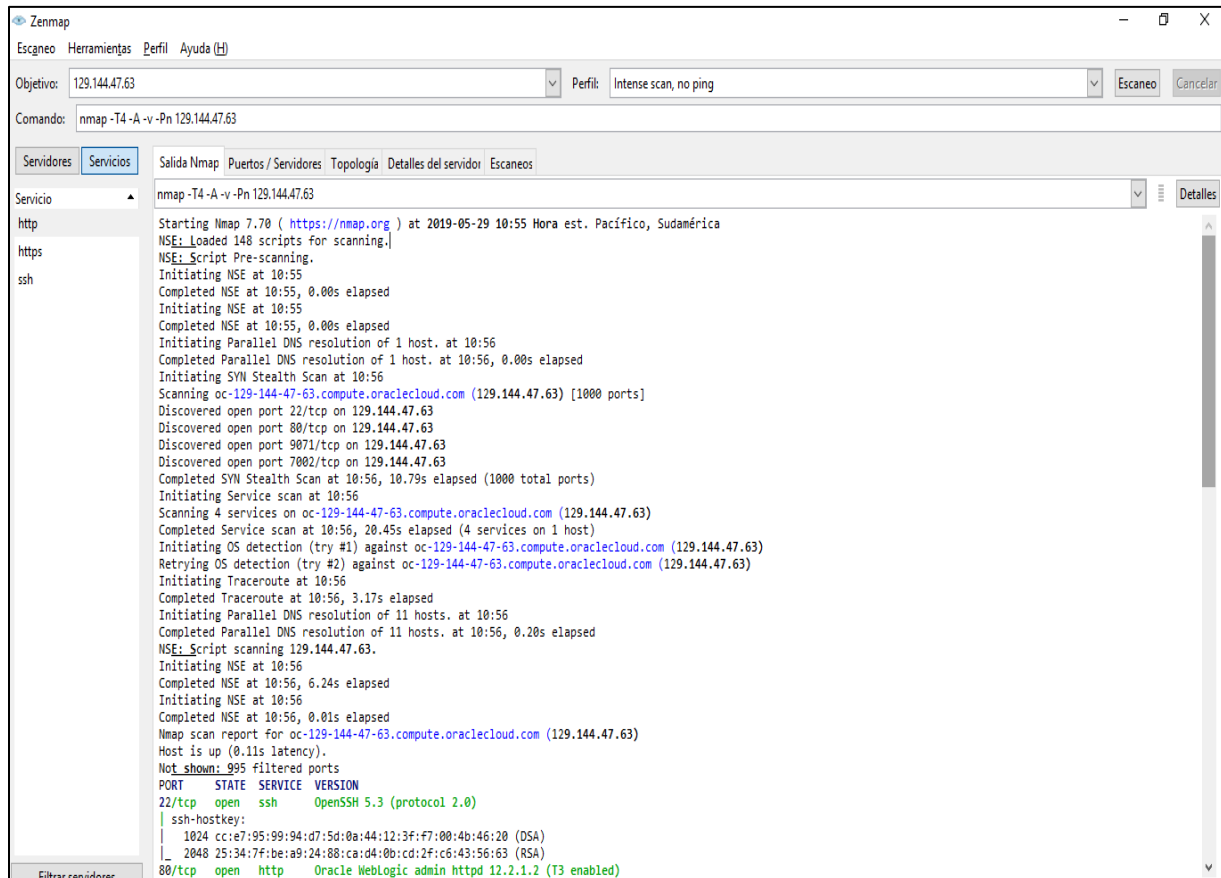


Figura 32 Escaneo con Nmap

Fuente: Propia

Se encontró que existen 4 puertos que están habilitados y uno solo se encuentra seguro el puerto 443 de la página de la Universidad es el único que cuenta con seguridad https.


```

Salida Nmap  Puertos / Servidores  Topología  Detalles del servidor  Escaneos
nmap -T4 -A -v -Pn 129.144.47.63
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 cc:e7:95:99:94:d7:5d:0a:44:12:3f:f7:00:4b:46:20 (DSA)
|_ 2048 25:34:7f:be:a9:24:88:ca:d4:0b:cd:2f:c6:43:56:63 (RSA)
80/tcp    open  http     Oracle WebLogic admin httpd 12.2.1.2 (T3 enabled)
|_ http-title: Error 404--Not Found
|_ weblogic-t3-info: T3 protocol in use (WebLogic version: 12.2.1.2)
443/tcp   closed https
7002/tcp  open  ssl/http Oracle WebLogic admin httpd
|_ http-title: Error 404--Not Found
|_ ssl-cert: Subject: commonName=DemoCertFor_UTNAPEX3_domain
|_ Issuer: commonName=CertGenCA/organizationName=MyOrganization/stateOrProvinceName=MyState/countryName=US
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2019-01-05T05:00:37
|_ Not valid after: 2024-01-04T05:00:37
|_ MD5: 72d3 6acc ea59 3139 dad7 93be 3c9d cf6f
|_ SHA-1: 8c1d 29e1 c5c9 244e 3875 d63f aa74 2b1d b6fe f257
|_ ssl-date: 2019-05-29T15:56:43+00:00; +1s from scanner time.
9071/tcp  open  http     Oracle WebLogic admin httpd
|_ http-title: Error 404--Not Found
|_ weblogic-t3-info: T3 protocol in use (WebLogic version: 12.2.1.2)
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (94%), Synology DiskStation Manager 5.X (86%), WatchGuard Firewall 11.X (86%), FreeBSD 6.X (85%)
OS_CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4.4 cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:firewall:11.8 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 4.0 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (90%), Linux 2.6.32 - 3.0 (89%), Linux 3.11 - 4.1 (88%), Linux 3.2 - 3.8 (88%), Linux 2.6.18 (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 25.107 days (since Sat May 04 08:22:11 2019)
Network Distance: 17 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)

```

Figura 33: Puertos habilitados Nmap

Fuente: *Elaboración Propia*

Como conclusión se pudo obtener que el firewall implementado es muy restrictivo a nivel de direccionamiento público y es por esta razón que se encontró 4 puertos abiertos los cuales son:

Tabla 28: Identificación de puertos

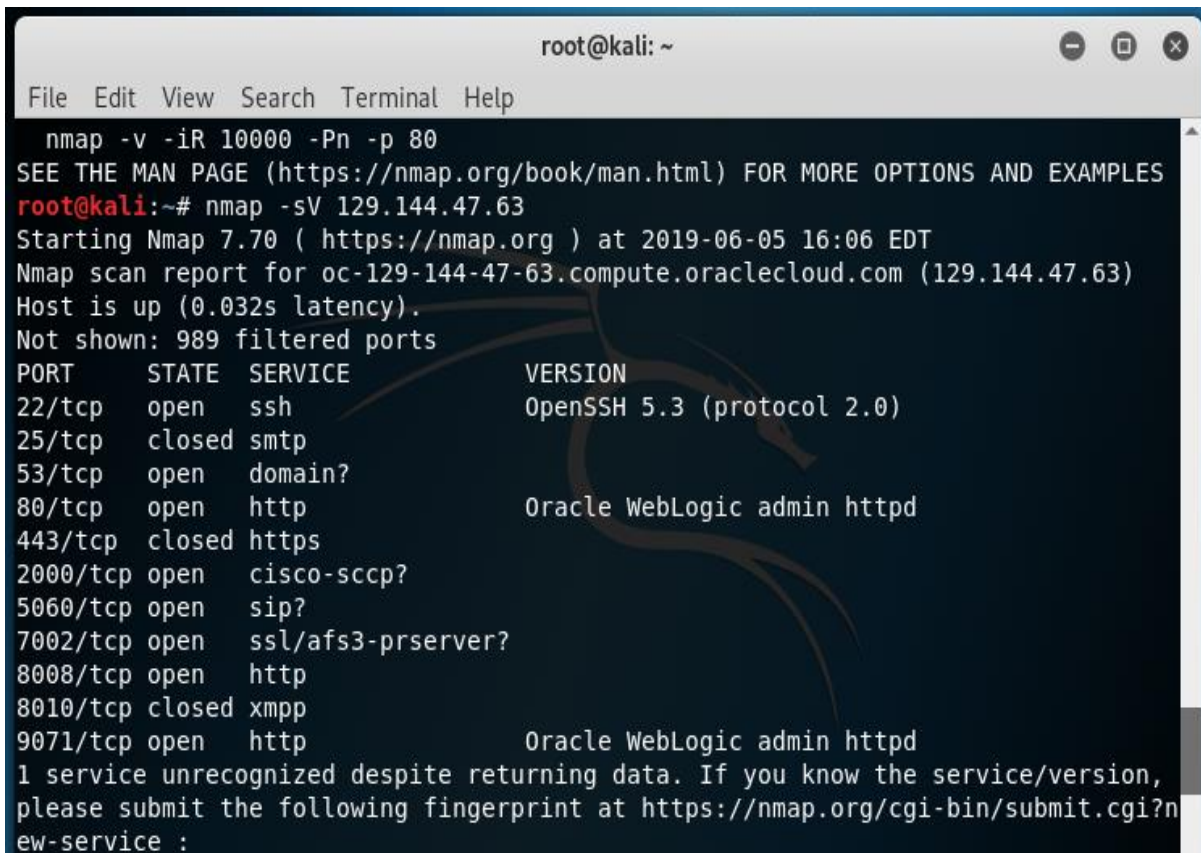
| Puerto | Versión de Vulnerabilidad |
|--------|---------------------------------|
| 22 | ssh: OpenSSH 5.3 (Protocol 2.0) |
| 7002 | ssl/http |
| 80 | Oracle WebLogic admin httpd |
| 9071 | Oracle WebLogic admin httpd |

Fuente: *Elaboración Propia*

Utilizando la herramienta nmap en Kali Linux mediante el comando **-Sv** el cual se usa para identificar servicios y versiones se precede a verificar si es posible realizar ataques intermedios al sistema usando los puertos abiertos.

Comando **-Sv 129.144.x.x**

Como se puede observar en la figura 34 de la herramienta nmap de Kali Linux.



```
root@kali: ~
File Edit View Search Terminal Help
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -sV 129.144.47.63
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 16:06 EDT
Nmap scan report for oc-129-144-47-63.compute.oraclecloud.com (129.144.47.63)
Host is up (0.032s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 5.3 (protocol 2.0)
25/tcp    closed smtp
53/tcp    open  domain?
80/tcp    open  http              Oracle WebLogic admin httpd
443/tcp   closed https
2000/tcp  open  cisco-sccp?
5060/tcp  open  sip?
7002/tcp  open  ssl/afs3-prserver?
8008/tcp  open  http
8010/tcp  closed xmpp
9071/tcp  open  http              Oracle WebLogic admin httpd
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
```

Figura 34: Utilización de comando **-Sv** para identificar servicios y versiones

Fuente: *Elaboración Propia*

En el puerto 22 la versión de OpenSSH fue revisada en CVE Details y Openbsd existen vulnerabilidades reportadas, pero no existen herramientas para iniciar los ataques las paginas publicadas en internet para detectar vulnerabilidades (CVE details) y Rapid7 (Rapid7), lo recomendable seria mantener el puerto cerrado.

En la Figura 35 de (CVE details) se encontró que existe un reporte de la vulnerabilidad de la versión de OpenSSH.

OpenSSH Vulnerability: CVE-2016-0778

| Severity | CVSS | Published | Created | Added | Modified |
|----------|--------------------------------------|------------|------------|------------|------------|
| 5 | (AV:N/AC:H /Au:S/C:P /I:P/A:P) | 01/14/2016 | 07/25/2018 | 01/25/2016 | 10/30/2017 |

Description

The (1) `roaming_read` and (2) `roaming_write` functions in `roaming_common.c` in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

Solution(s)

`openbsd-openssh-upgrade-latest`

Related Vulnerabilities

APPLE-SA-2016-03-21-5

80698

[CVE - 2016-0778](#)

DSA-3446

<http://www.openssh.com/txt/release-7.1p2>

Figura 35: Reporte de Vulnerabilidad de OpenSSH en CVE Details

Fuente: (CVE details)

Para los puertos 80 y 9071 existe un código malicioso en reportados en la página Exploit Database que puede ser utilizado y la efectividad dependerá de la seguridad implementada en el servidor.

En la figura 36 se observa que la versión de WebLogic si existe un código que puede ser utilizado para atacar a la información por ese puerto, el firewall implementado es restrictivo, pero aun así se identificó el puerto 80 abierto.

The screenshot displays the Exploit Database interface for a specific vulnerability. The title is "Oracle Application Testing Suite - WebLogic Server Administration Console War Deployment (Metasploit)". The report is organized into several key-value pairs:

- EDB-ID:** 46942
- CVE:** N/A
- Author:** METASPLOIT
- Type:** REMOTE
- Platform:** JAVA
- Published:** 2019-05-29

Additional indicators include "EDB VERIFIED: ✓", "EXPLOIT: 📄 / 📄", and "VULNERABLE APP:". Below these fields is a code block containing the following text:

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient
  include Msf::Auxiliary::Report

  def initialize(info={})
```

Figura 36: Reporte de Vulnerabilidad puerto 80 y 9071 en Exploit Database

Fuente: (EXPLOIT DATABASE, s.f.)

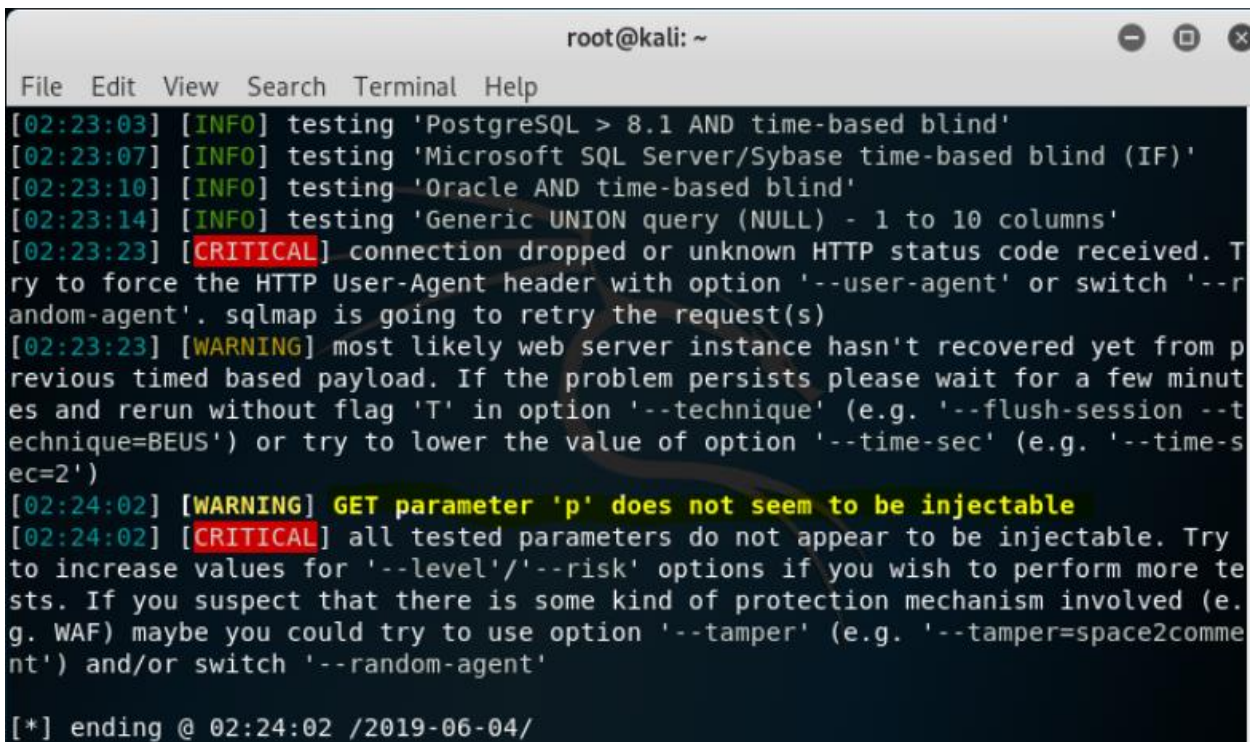
c) SqlMap

SqlMap es una herramienta desarrollada en Python para realizar inyección de código sql automáticamente. Su objetivo es detectar y aprovechar las vulnerabilidades de inyección SQL en aplicaciones web. Una vez que se detecta una o más inyecciones SQL en el host de destino, el usuario puede elegir entre una variedad de opciones entre ellas, enumerar los usuarios, los hashes de contraseñas, los privilegios, las bases de datos o todo el volcado de tablas / columnas

específicas del DBMS, ejecutar su propio SQL SELECT, leer archivos específicos en el sistema de archivos y mucho más (SqlMap).

Mediante la herramienta de SqlMap en Kali Linux se intentó hacer inyección SQL ya que como estudiantes para acceder a la evaluación docentes es por el portfolio estudiantil y se constató que al ser desarrollado en Oracle el lenguaje de desarrollo es elevado y para poder atacar a este tipo de lenguaje sería a través de SQL Plus el cual está incorporado en el paquete de programas de Oracle.

En la figura 37 se puede observar el resultado de la prueba de vulnerabilidad realizada con SqlMap en Kali Linux.



```
root@kali: ~
File Edit View Search Terminal Help
[02:23:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[02:23:07] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[02:23:10] [INFO] testing 'Oracle AND time-based blind'
[02:23:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[02:23:23] [CRITICAL] connection dropped or unknown HTTP status code received. Try to force the HTTP User-Agent header with option '--user-agent' or switch '--random-agent'. sqlmap is going to retry the request(s)
[02:23:23] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag 'T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[02:24:02] [WARNING] GET parameter 'p' does not seem to be injectable
[02:24:02] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[*] ending @ 02:24:02 /2019-06-04/
```

Figura 37: SqlMap en Kali Linux

Fuente: *Elaboración Propia*

3.5 Informe de Auditoría

Nombre de la Entidad: Universidad Técnica del Norte

Fecha del Informe: 01/07/19

AUDITORIA AL SISTEMA DE EVALUACIÓN DOCENTE

OBJETIVO

Evaluar políticas y controles de la seguridad de la información para el funcionamiento del sistema de evaluación docente, utilizando la metodología Magerit en conjunto con la normativa ISO 27002:2017 para determinar el estado actual del sistema y proponer recomendaciones necesarias para proteger la información.

Lugar de la Auditoria: Departamento de Desarrollo Tecnológico e Informático.

Grupo de Trabajo de Auditoria: Verónica Lizeth Guamán Guamán.

HERRAMIENTAS UTILIZADAS

- Metodología Magerit V3.
- Pilar
- ISO 27002:2017.

ALCANCE

El trabajo de tesis denominado **“EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA MAGERIT V3”**, tiene como finalidad evaluar la seguridad de la información, mismo que se inició con la recopilación de datos para evaluar los controles más importantes de la norma ISO/IEC 27002:2017, que contribuyeron con la elaboración del análisis de la situación actual del sistema, basándose en los controles de seguridad que se rigen en dicha norma.

Además, se toma en cuenta los parámetros descritos en ella, para establecer soluciones adecuadas a las falencias encontradas, cumpliendo con los requerimientos de la Norma ISO 27002:2017.

CONCLUSIONES

La evaluación de riesgos realizada al sistema de evaluación docente identifico como una vulnerabilidad critica, el no contar con políticas de seguridad interna que permita establecer lineamientos y pautas para preservar la seguridad de los datos y la infraestructura tecnológica de la institución.

La metodología utilizada para esta investigación fue MAGERIT, permite un análisis de riesgos profundo, valorando cada uno de los activos mediante dimensiones de seguridad como: disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.

La normativa ISO 27002:2017 desempeña un rol importante en este estudio, permite verificar el cumplimiento de controles que garanticen la seguridad de la información del sistema de evaluación docente de la Universidad Técnica del Norte.

La situación actual del sistema de evaluación docente evidencia un nivel considerable de cumplimiento de las políticas de seguridad de la información, tanto física como de gestión (53%), por lo que requiere de un compromiso de autoridades y docentes para un cumplimiento total de la normativa.

Como evidencia del trabajo realizado al sistema de evaluación docente de la Universidad Técnica del Norte se elaboró un documento de los riesgos encontrados con los resultados obtenidos de la aplicación de la metodología MAGERIT en el software PILAR, el mismo que consta en el Departamento de Tecnología Informática – UTN.

RECOMENDACIONES

Concientizar y educar a la comunidad universitaria sobre distintos riesgos informáticos a los que se encuentra expuesta la información de la academia.

Planificar una capacitación adecuada para que los usuarios no atenten contra la confidencialidad, integridad y disponibilidad de los datos de los sistemas informáticos.

Actualizar las políticas de seguridad de la información y procedimientos que se emplean en el sistema de Evaluación docente de la Universidad Técnica del Norte, para garantizar la confiabilidad, integridad y disponibilidad de la información.

Documentar procedimientos del sistema de evaluación docente, así como errores presentados en una bitácora, para crear un plan de optimización del sistema.

Elaborar manuales del sistema de evaluación docente, que sirva como guía para el personal encargado del control y seguridad de la información.

Se recomienda que se realice una revisión periódica de las amenazas y riesgos ya que la tecnología está en constante cambio y estos problemas deben ser controlados para evitar futuros inconvenientes en los sistemas.

Como un trabajo a futuro se podría ejecutar con la presencia de un auditor el análisis de riesgos sobre ERP's académicos, y obtener información detallada sobre el funcionamiento de los mismos, para tener resultados precisos sobre el estado actual, y con el libre acceso al sistema se podría identificar vulnerabilidades con herramientas de detección, así se estaría teniendo un trabajo completo de evaluación de vulnerabilidades y amenazas.

BIBLIOGRAFÍA

- (CEIDPA), C. I. (2018). *Evaluación integral del desempeño del personal académico de la UTN para el período septiembre 2018 - agosto 2019*. Ibarra.
- Aguirre, B. J. (2011). *Auditoría Informática*. MEXICO: UNAM.
- Brinkmann, M. (22 de septiembre de 2017). Obtenido de Ghacks:
<https://www.ghacks.net/2017/09/22/use-siteverify-to-verify-links/>
- Cecilia Reyes. (11 de Junio de 2017). Obtenido de World Economic Forum:
<https://www.weforum.org/agenda/2017/01/global-risks-in-2017/>
- Chilán, S. E., & Williams, P. P. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. *Revista Científica Dominio de las Ciencias*, 284-295.
- Cordero Torres, G., & Crespo, E. (2016). *ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES*. Cuenca, Ecuador.
- Curiel, G. (2006). *Auditoría de Estados Financieros*. Naucalpan de Juárez: PEARSON.
- CVE details. (s.f.). <https://www.cvedetails.com>. Obtenido de https://www.cvedetails.com/vulnerability-list.php?vendor_id=97&product_id=585&version_id=121223&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdir=0&opmemc=0&ophtpr=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=3&cvssscoremax
- DATTA BUSINESS INNOVATION. (2019). UNIVERSIDAD TÉCNICA DEL NORTE, EFICIENCIA EN LA NUBE. *DATTA BUSINESS INNOVATION*, 60-63.
- Departamento de Desarrollo Tecnológico e Informático - UTN. (2013). *Plan de Desarrollo Tecnológico e Informático 2013 - 2017*. Ibarra.
- EXPLOIT DATABASE. (s.f.). Obtenido de <https://www.exploit-db.com/exploits/46942>

- Gabriel Baca Urbina. (2016). *Introducción a la Seguridad Informática* (Vol. 1). Mexico: Grupo Editorial Patria, S.A. de C.V.
- Gonzales, E. F. (2018). *Auditoría Operativa*. Quito: Universidad Central del Ecuador.
- Gutián, G. (2014). Metodologías y modelos para auditar la información. Análisis reflexivo. *Revistas Científicas Complutenses*, 234-235.
- Helena Alemán Novoa, C. R. (2015). Metodologías Para el Análisis de Riesgos en los SGSi. *UNAD Revista Especializada en Ingeniería*, 15-18.
- Hidalguese, U. T. (2011). *Auditoría*. Mexico: UTHH.
- INEN. (2017). *ECUATORIANA Nte INEN-ISO / IEC 27002*. QUITO: INEN.
- International Organization for Standardization. (13 de 12 de 2017). ISO 27000. *International Organization for Standardization*, 1-3-4. Obtenido de INTERNATIONAL ORGANIZATION FOR STANDARDIZATION.
- ISOTools. (19 de Julio de 2016). ISO 31000 Gestión de Riesgos: ¿Cuáles son sus directrices? Recuperado el 12 de Mayo de 2019, de <https://www.isotools.org/2016/07/19/iso-31000-gestion-riesgos-cuales-directrices/>
- Jácome León, J. G., Pusedá Chulde, M. R., & Imbaquingo Esparza, D. E. (2017). *Fundamentos de Auditoría Informática basada en riesgos*. Ibarra-Ecuador: UTN. Obtenido de <http://repositorio.utn.edu.ec/handle/123456789/6794>
- Mieres, J. (2011). *Ataques linformáticos*. Bogota.
- Ministerio de Energía, T. y. (2017). *Proteccion de la Información*. Madrid: Ministerio de Energía, Turismo y Agenda Digital España.
- Ministerio de Hacienda y Administraciones Publicas de España. (2012). *Magerit - versión 3.0. Metodología de Análisis y Gestion de Riesgos de los Sistemas de Información*. MADRID: Ministerio de Hacienda y Administraciones Públicas de Españ.

Miramegias. (11 de 11 de 2018). *Miramegias*. Obtenido de Miramegias:

<http://www.miramegias.com/auditoria/files/apuntes/ut12.pdf>

Poveda, J. M. (27 de Abril de 2011). *www.isaca.org*. Recuperado el 28 de Enero de 2019, de

www.isaca.org:

<http://www.isaca.org/Blogs/282270/archive/2011/04/27/Protecci%C3%B3ndeActivosdeInformaci%C3%B3n.aspx>

Rapid7. (s.f.). *www.rapid7.com*. Obtenido de <https://www.rapid7.com/db/vulnerabilities/openbsd-openssh-cve-2016-0778>

Real Academia de la Lengua Española. (13 de 11 de 2018). *RAE*. Obtenido de RAE:

<http://dle.rae.es/?id=4NVvRTc>

Recursos TIC. (11 de 11 de 2018). *RECURSOS TIC*. Obtenido de RECURSOS TIC:

<http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1>

Seguinfo. (27 de Junio de 2007). *Seguridad Informática - Noticias de Seguridad Informática*. Obtenido de

<https://seguinfo.wordpress.com/2007/06/27/%C2%BFque-es-nmap/>

SqlMap. (s.f.). *sqlmap.org*. Obtenido de <http://sqlmap.org/>

Tarazona, T Cesar H. (2011). *Amenazas Informáticas y Seguridad de la Información*. ETEK Internacional.

Tarazona, T. C. (2007). *Amenazas Informáticas y Seguridad de la Información*. SURVEY.

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

ANEXOS

Anexo 1: Encuesta aplicada a Docentes y Estudiantes



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

Encuesta dirigida para estudiantes y docentes sobre el uso del sistema de evaluación docentes.

Objetivo: Conocer la opinión sobre el funcionamiento del sistema de evaluación docente, verificar los niveles de riesgo que ocasionaría a la Universidad Técnica del Norte

Encuesta sobre el sistema de evaluación docente

Marque con una x la respuesta elegida.

1. ¿Usted conoce el funcionamiento del sistema de evaluación docente de la Universidad Técnica del norte?

SI

NO

2. ¿Desde qué dispositivos se puede acceder al sistema de evaluación docente?

Laboratorios

Laptops personales

Móviles

Otros

3. ¿Con que frecuencia usted utiliza el sistema de evaluación docente?

Una vez al semestre

Una vez al bimestre

Una vez al mes

Una vez por semana

2 a 5 veces por semana

4. ¿Cree usted que existe algún control de acceso al sistema de evaluación docente?

SI

NO

5. ¿La contraseña que usted emplea para acceder al sistema de evaluación docente cuenta con requerimientos de seguridad?

SI

NO

6. ¿El sistema de evaluación docente tiene una política de bloqueo sesiones o de computadores después de un tiempo determinado?

SI

NO

7. ¿Cuál es el nivel de facilidad de uso del sistema de evaluación docente?

Excelente

Muy buena

Buena

Regular

Mala

Muy mala

8. ¿Usted ha tenido inconvenientes con el servicio de evaluación docente?

SI

NO

9. ¿Usted ha tenido inconvenientes con la información ingresada en el sistema de evaluación docente?

SI

NO

10. ¿Existe algún responsable del sistema de evaluación docente que brinde atención cuando sea necesario?

SI

NO

11. ¿Usted cree que la información que ingresa al sistema de evaluación docente es confidencial?

SI

NO

12. ¿En qué porcentaje usted considera que el sistema de evaluación docente satisface sus necesidades?

Entre 80-100%

Entre 50-80%

Entre 40-60%

13. Si el porcentaje escogido en la pregunta anterior es entre 40-60% indique el motivo de su respuesta.

No existe disponibilidad al sistema de evaluación docente.

Al parecer no hay retroalimentación de las evaluaciones a los docentes.

Existe fugas de la información ingresada en el sistema de evaluación docente

Otro

14. ¿Tiene la confianza suficiente para presentar quejas sobre las fallas del sistema de evaluación docente?

SI

NO

15. ¿Qué tan efectivos son los técnicos para resolver problemas del sistema de evaluación docente?

Muy efectivos

Efectivos

Regularmente efectivos

Poco efectivos.

16. ¿Cómo califica el sistema de evaluación docente de la Universidad Técnica del Norte?

Excelente

Bueno

Regular

Malo

Pésimo

17. ¿Usted considera que el servicio de evaluación docente debe estar disponible a cualquier hora y para cualquier usuario?

SI

NO

Anexo 2: Preguntas dirigidas al personal encargado del manejo del sistema.

1. ¿Qué Nivel de daño representaría para la Universidad si el servicio de evaluación docente no estuviera disponible?
2. ¿Qué nivel de daño representaría para la universidad que los datos del sistema de evaluación docente fueran total o parcialmente falsos, modificados, o faltaran datos?
3. ¿Qué nivel de daño representaría para la universidad que los datos que se obtienen en el sistema de evaluación docentes fueran conocidos por personas no autorizadas?
4. ¿Qué nivel de daño representaría para la Universidad que la persona que acceda a la información del sistema de evaluación docente no sea realmente quien se cree?
5. ¿Qué nivel de daño representaría para la universidad que no quedara constancia del uso del servicio de evaluación docente o el acceso a los datos?

Anexo 3: Encuesta de Valoración de Dimensiones



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

Encuesta dirigida a la persona encargada del manejo del sistema de evaluación docentes.

Objetivo: Conocer los niveles de riesgo que ocasionaría al sistema de Evaluación Docente en base a los siguientes interrogantes por medio de la siguiente escala de Valoración.

Escala de Valoración:

| | |
|---|---------------|
| 1 | Daño muy bajo |
| 2 | Daño bajo |
| 3 | Daño medio |
| 4 | Daño alto |
| 5 | Daño muy alto |

Encuesta de Nivel de Riesgo del sistema de evaluación docente

| DIMENSIONES DE VALORACIÓN | DESCRIPCIÓN | NIVEL DE DAÑO |
|---------------------------|---|---------------|
| Disponibilidad | ¿Qué Nivel de daño representaría para la Universidad si el servicio no estuviera disponible? | 5 |
| Integridad | ¿Qué nivel de daño representaría para la universidad que los datos del sistema de evaluación docente fueran total o parcialmente falsos, modificados, o faltaran datos? | 5 |
| Confidencialidad | ¿Qué nivel de daño representaría para la universidad que los datos que se obtienen en el sistema de evaluación docentes fuera conocido por personas no autorizadas? | 5 |
| Autenticidad | ¿Qué nivel de daño representaría para la Universidad que la persona que acceda a la información no sea realmente quien se cree? | 5 |
| Trazabilidad | ¿Qué nivel de daño representaría para la universidad que no quedara constancia del uso del servicio o el acceso a los datos? | 4 |

[Firma manuscrita]

GLOSARIO

Activo: es un procedimiento, sistema u otra cosa que tenga un valor para una organización y por lo tanto deba de ser protegida.

Spyware: Código malicioso cuyo principal objetivo es recoger información sobre las actividades en cualquier ordenador.

Troyanos, virus y gusanos: Son programas maliciosos, que se posicionan en los ordenadores con el propósito de permitir el acceso no autorizado a un atacante.

Phishing: Es un ataque del tipo de ingeniería social, en la cual cumple con el objetivo de obtener de manera fraudulenta datos confidenciales de un usuario, especialmente financieros.

Spam: Estos llegan a través de correo electrónico, el cuales difundir grandes cantidades de mensajes comerciales o propagandísticos.

Botnets: Es una amenaza que controla los ordenadores de forma remota, quedando incorporadas en redes distribuidas de ordenadores llamadas robot.

Trashing: Este nombre hace referencia al manejo de la basura, estos se manejan también por ingeniería social, el objetivo de ello es recopilar información desechada para robar su identidad.

Identificación de Activos: es la identificación de los activos físicos y de otra índole de una organización.

Valoración de Activos: Esta valoración asignada al activo de acuerdo a la criticidad.

Identificación de amenazas: Son eventos que degradarían el valor que tiene los activos.

Frecuencia: son eventos que suceden en un tiempo determinado.

Degradación: nivel de afección de un activo ante una amenaza.

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza.

Riesgo: Es la probabilidad de materialización de amenazas sobre el activo.

Salvaguardas: Son las medidas precisas a tomar para reducir el riesgo.

Riesgo Residual: Es el riesgo permanente después de aplicar las salvaguardas.

Confidencialidad: es la que impide que la información se divulgue a sistemas o personas no autorizadas; por lo tanto, la confidencialidad es la que asegura que solo las personas con la autorización debida, tengan acceso a la información.

Integridad: es la que mantiene los datos libres de modificaciones no autorizadas; por lo tanto, la integridad es la que busca mantener la información tal cual fue generada, libre de manipulaciones o cambios por personas no autorizadas.

Disponibilidad: es la que presenta la información a las personas que deben tener accesos a ella; por lo tanto, la disponibilidad se encarga de colocar la información a disposición a personas o sistemas autorizados para acceder a ella al momento que lo requieran.