REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

EVALUACIÓN TÉCNICA INFORMÁTICA DE LAS VULNERABILIDADES EN CIBERSEGURIDAD EN LOS LABORATORIOS DE COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON BASE EN COBIT 2019.

Trabajo de Investigación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

AUTOR: Martha Cecilia Pantoja Mejía

DIRECTOR: MSc. Cosme MacArthur Ortega Bustamante

IBARRA - ECUADOR

2023

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

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

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:	040133501-3		
APELLIDOS Y NOMBRES:	Pantoja Mejía Martha Cecilia		
DIRECCIÓN:	Av. 17 de Julio y Tulipanes		
E-MAIL:	mcpantoja@utn.edu.ec		
TELÉFONO FIJO:	No dispone	**TELÉFONO MÓVIL:**	0992552633

DATOS DE LA OBRA	
TÍTULO:	Evaluación técnica informática de las vulnerabilidades en ciberseguridad en los laboratorios de computación de la universidad técnica del norte con base en COBIT 2019.
AUTOR (ES):	Pantoja Mejía Martha Cecilia
FECHA: DD/MM/AA	27/11/2023
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ PREGRADO ☒ POSGRADO
TÍTULO POR EL QUE OPTA:	Magister en computación con mención en seguridad informática
ASESOR/DIRECTOR:	Msc. Evelin Enríquez, Msc. Cosme Ortega

CONSTANCIAS

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

Ibarra, a los 27 días del mes de noviembre de 2023

EL AUTOR:

Firma: 

Nombre: Pantoja Mejía Martha Cecilia

CI: 040133501-3

APROBACIÓN DEL TUTOR

Yo MSc. Cosme MacArthur Ortega Bustamante, en calidad de director de la tesis titulada: **"EVALUACIÓN TÉCNICA INFORMÁTICA DE LAS VULNERABILIDADES EN CIBERSEGURIDAD EN LOS LABORATORIOS DE COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON BASE EN COBIT 2019"** de autoría de la Ing. Martha Cecilia Pantoja Mejía, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 27 días del mes de noviembre de 2023

Lo certifico

1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE

Firmado digitalmente por 1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE
Fecha: 2023.11.27 17:51:22 -05'00'

MSc. Cosme MacArthur Ortega Bustamante

CI: 1001580396

DIRECTOR DE TESIS

DEDICATORIA

A mi familia, cuyo amor, confianza y estímulo inquebrantables han sido mi fuerza motriz en la vida. A mi director de tesis, por su guía inestimable, retroalimentación constructiva y estímulo intelectual. Y a mis amigos y colegas, por su apoyo desinteresado, paciencia y comprensión durante este viaje emocionante pero desafiante. Sin ustedes, este logro no habría sido posible, gracias por siempre estar conmigo en cada etapa de mi vida y mantener intacto el cariño manifestando su preocupación por mi bienestar.

Martha Cecilia Pantoja Mejía

AGRADECIMIENTO

A la Gloriosa Universidad Técnica del Norte y a su principal autoridad el Dr. Miguel Naranjo Toro - Rector; ya que sin su valiosa gestión la posibilidad de cursar esta maestría no habría existido. A mis padres, por su amor y apoyo incondicional a lo largo de mi vida y en este proyecto en particular. A mi director Msc. MacArthur Ortega, por su tiempo, paciencia y conocimientos valiosos. A mis amigos, por su respaldo constante. A todas las personas que han influido positivamente en mi vida, gracias por todo el aporte que han hecho para llegar hasta aquí, pequeñas acciones marcan grandes diferencias y sobre todo cada palabra de aliento me motivó a continuar hasta culminar este objetivo, los llevo siempre en mi corazón, cuando los años pasen recordaré mi vida y sabré que tomé la mejor decisión cuando seguí esta maestría, el conocimiento te salva de la ignorancia y te salva de perder el tiempo en cosas inútiles.

Martha Cecilia Pantoja Mejía

ÍNDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENSIÓN EN SEGURIDAD INFORMÁTICA

EVALUACIÓN TÉCNICA INFORMÁTICA DE LAS VULNERABILIDADES EN CIBERSEGURIDAD EN LOS LABORATORIOS DE COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON BASE EN COBIT 2019.

Autor: Martha Cecilia Pantoja Mejía

Director: Msc. Cosme Ortega

Año: 2023

RESUMEN

La ciberseguridad se ha convertido en un tema crítico en la era digital, especialmente en entornos educativos donde los laboratorios de computación son fundamentales para el aprendizaje y la investigación. La presente tesis tiene como objetivo evaluar las vulnerabilidades en ciberseguridad presentes en los laboratorios de computación de la Universidad Técnica del Norte, utilizando como marco de referencia el modelo de gobierno de TI COBIT 2019.

El estudio se basa en una metodología de evaluación técnica informática que abarca diferentes aspectos de seguridad, como la identificación de riesgos, la evaluación de controles de seguridad existentes, la detección de vulnerabilidades y la recomendación de medidas de mitigación. Para llevar a cabo esta evaluación, se realizará un análisis exhaustivo de los

laboratorios de computación, teniendo en cuenta tanto los aspectos técnicos como los procesos y políticas de seguridad implementados.

Se utilizará COBIT 2019 como marco de referencia debido a su enfoque integral y su reconocimiento internacional en el ámbito de gobierno de TI. Este modelo proporciona un conjunto de objetivos y controles específicos para la gestión de la seguridad de la información, permitiendo una evaluación precisa de las vulnerabilidades presentes en los laboratorios de computación.

Los resultados de la evaluación técnica informática se analizarán en función de los estándares y mejores prácticas establecidos en COBIT 2019, lo que permitirá identificar las áreas de mayor riesgo y las deficiencias en los controles de seguridad implementados.

Después de socializar el informe de recomendaciones con los laboratoristas, se concluye que existe una respuesta favorable a las sugerencias planteadas al finalizar esta investigación. La respuesta favorable por parte de los laboratoristas después de la socialización de estas recomendaciones es un testimonio claro de la relevancia y utilidad de este estudio. La aceptación de las sugerencias por parte de los profesionales que trabajan directamente en los laboratorios demuestra que las recomendaciones son prácticas y factibles de implementar en el entorno real. Además, este apoyo refuerza la idea de que la seguridad cibernética es un asunto de interés común y que la comunidad universitaria reconoce la importancia de garantizar un entorno de aprendizaje seguro.

Los resultados y recomendaciones obtenidos servirán como base sólida para fortalecer la seguridad de la información en los laboratorios, garantizando un entorno de aprendizaje seguro y confiable para la comunidad universitaria.

Palabras clave: evaluación técnica informática, vulnerabilidades, ciberseguridad, laboratorios de computación, COBIT 2019.

ABSTRACT

Cybersecurity has become a critical issue in the digital age, particularly in educational settings where computer labs are essential for learning and research. This thesis aims to assess the cybersecurity vulnerabilities in the computer labs of the Technical University of the North, using the COBIT 2019 IT governance framework as a reference model.

The study employs a methodology for technical IT assessment that encompasses various security aspects, including risk identification, evaluation of existing security controls, vulnerability detection, and recommendations for mitigation measures. To carry out this evaluation, a comprehensive analysis of the computer labs will be conducted, considering both technical aspects and the implemented security processes and policies.

COBIT 2019 is chosen as the reference framework due to its comprehensive approach and international recognition in IT governance. This model provides a set of specific objectives and controls for information security management, enabling a precise assessment of vulnerabilities in the computer labs.

The results of the technical IT assessment will be analyzed in line with the standards and best practices established in COBIT 2019, facilitating the identification of high-risk areas and deficiencies in the implemented security controls.

Following the dissemination of the recommendations report to the lab staff, it is concluded that there is a favorable response to the suggestions presented at the conclusion of this research. This positive response from the lab staff serves as clear evidence of the relevance and utility of this study. The acceptance of the recommendations by professionals working directly in the labs demonstrates that the suggestions are practical and feasible to implement in the real-world environment. Additionally, this support reinforces the idea that cybersecurity is a matter of

common interest, and the university community recognizes the importance of ensuring a secure learning environment.

The results and recommendations obtained will serve as a solid foundation to strengthen information security in the labs, ensuring a safe and reliable learning environment for the university community.

Keywords: computer technical evaluation, vulnerabilities, cybersecurity, computer laboratories, COBIT 2019

CAPITULO I

1. EL PROBLEMA

1.1 Planteamiento del problema

La tecnología es extremadamente importante en la actualidad debido a su impacto en casi todos los aspectos de nuestra vida, incluyendo el trabajo, la comunicación, el entretenimiento, la educación, la investigación y el desarrollo. La tecnología ha transformado la forma en que interactuamos con el mundo y entre nosotros mismos, específicamente en el ámbito de la educación, la tecnología ha facilitado el acceso a recursos educativos y ha permitido la educación en línea y la educación a distancia.

La Universidad Técnica del Norte con 37 años de vida institucional ha experimentado cambios cuantitativos y cualitativos en el transcurrir del tiempo, donde el protagonismo de la tecnología ha ido de la mano con el desarrollo de los diferentes ejes estratégicos de la institución como son: gestión, vinculación, investigación y docencia.

Es así que cada una de las Facultades cuenta con laboratorios de computación que son utilizados para impartir clases, realizar investigaciones, ejecutar proyectos entre otras actividades, junto a otras infraestructuras como aulas y talleres se recepta la visita de diferentes usuarios como docentes, estudiantes, personal administrativo y usuarios externos, que hacen uso de estos espacios académicos para ejecutar los objetivos institucionales enfocados en la misión y visión de la Universidad Técnica del Norte.

Dentro del proceso de préstamo de laboratorios de computación de la Universidad Técnica del Norte, las directrices generales son darle un uso responsable a los equipos, ya que son utilizados para impartir clases y para realizar tareas, sin embargo los usuarios (estudiantes, docentes, personal administrativo, usuarios externos) son propensos a ingresar a páginas que

representan un riesgo tanto para los equipos y también para los datos que sin reparar en la importancia ingresan sin ningún cuidado, de aquí que la necesidad de evaluar las vulnerabilidades que se puedan presentar en los laboratorios de computación de la UTN, con el fin de garantizar la seguridad de la información y minimizar los riesgos asociados a la manipulación y procesamiento de datos en dichos espacios, además capacitar y concienciar a los usuarios acerca del uso correcto de equipos y la navegación responsable y consiente en internet sin proporcionar información sensible a páginas no seguras, que es un problema solucionable siempre y cuando se aplique la normativa correcta, basada en los estándares y reglamentos , como las normas ISO, las mismas que se enumeran de manera progresiva y en función de su finalidad, se categorizan en familias para reunir aquellas que aborden temas similares. El propósito de estas directrices y regulaciones radica en la identificación de métodos, políticas, directrices de formación, y más, en relación con su objetivo, que puede ser la seguridad, la continuidad, la calidad entre otros aspectos. El correcto análisis y el basarnos en las normas ISO/EC 27001:2022 y COBIT 2019 específicamente garantizará mejorar el tratamiento de la información que se emite dentro de los Laboratorios de computación de la Universidad Técnica del Norte.

La evaluación técnica informática de las vulnerabilidades en los laboratorios de la UTN es un proceso crítico para identificar las posibles brechas de seguridad, amenazas y riesgos a los que están expuestos los sistemas y equipos informáticos en dichos espacios. Por lo tanto, el objetivo de esta investigación es proponer un enfoque técnico de evaluación informática que posibilite la identificación y reducción de potenciales vulnerabilidades y amenazas de seguridad en los entornos digitales de los laboratorios de la UTN.

Para abordar este problema de investigación, se llevará a cabo una revisión bibliográfica exhaustiva sobre COBIT 2019 y las normas ISO 27001, además, se realizará un estudio de

campo en los laboratorios de la Universidad Técnica del Norte, utilizando técnicas y herramientas de evaluación para identificar las vulnerabilidades existentes y proponer medidas de mitigación. Los resultados de esta investigación serán de utilidad para mejorar la seguridad de la información en los laboratorios de la UTN y garantizar la continuidad del servicio.

1.2. Interrogantes de la investigación

Con este antecedente se generan interrogantes fundamentales para esta investigación: ¿Cuál es el procedimiento ante un potencial ataque cibernético a los laboratorios de computación de la Universidad Técnica del Norte? ¿Cómo podemos reducir los riesgos de seguridad en los laboratorios de computación de la Universidad Técnica del Norte?,¿Qué riesgos son frecuentes en el desarrollo de las actividades de los laboratorios de computación de la Universidad Técnica del Norte?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Evaluar las vulnerabilidades en ciberseguridad presentes en los laboratorios de computación de la Universidad Técnica del Norte mediante el uso de COBIT 2019, con el fin de identificar oportunidades de mejora y fortalecer la seguridad informática.

1.3.2 Objetivos específicos

- Identificar los activos de información críticos de los laboratorios de computación de la Universidad Técnica del Norte, y determinar su nivel de riesgo y asegurar su protección.
- Analizar el proceso de control en ciberseguridad de los laboratorios de computación de la Universidad Técnica del Norte, con base en la fase de riesgos de la norma ISO/IEC 27001:2022

- Elaborar un informe con recomendaciones específicas de controles para mejorar la ciberseguridad de los laboratorios de computación de la Universidad Técnica del Norte, basadas en las buenas prácticas de COBIT 2019.
- Evaluar de manera preliminar las recomendaciones de controles para mejorar la ciberseguridad de los laboratorios de computación de la Universidad Técnica del Norte.

1.4 Justificación

La inseguridad en entornos digitales y sistemas informáticos se debe al gran número de amenazas que circulan en el internet y el amplio acceso que se tiene a esta herramienta, debido a este motivo, es imperativo que los niveles de seguridad de una organización sean extremadamente elevados, dado que podrían experimentar filtraciones de datos críticos para su funcionamiento. La acción de actualizar el antivirus de forma constante no garantiza la seguridad completa del sistema. Es necesario incorporar otros tipos de software que prevenga el acceso no autorizado por parte de individuos o usuarios ajenos a la institución o que no cuenten con los permisos o roles autorizados para los diferentes procesos.

Cuando nos referimos a la protección de la información, se toman en cuenta los tres aspectos fundamentales de la seguridad de la información: las personas, los procedimientos y la tecnología.

Cada uno de estos elementos es de igual relevancia que los otros. Dentro de los componentes tecnológicos, se identifican tres elementos esenciales:

- Confidencialidad hablamos de confidencialidad cuando nos referimos a la característica que asegura que los usuarios no tengan acceso a la información solo mediante autorización y de forma controlada.

- Disponibilidad asegura que los recursos de sistema y los datos estén accesibles exclusivamente para los usuarios en el momento que lo requieran.

- Integridad nos indica que toda modificación de la información solo es realizada por usuarios autorizados, por medio de procesos también autorizados. (Telcel, 2023)

Actualmente, las instituciones educativas enfrentan notables deficiencias en la seguridad de la información en diversas áreas. Por lo tanto, es fundamental analizar las debilidades que afectan la protección de los datos y los principios de seguridad establecidos por la institución. Por lo tanto, resulta necesario iniciar con una evaluación técnica en el ámbito informático para identificar las vulnerabilidades que puedan existir y abordar así los incidentes que se manifiestan en los laboratorios de la Universidad Técnica del Norte. En este contexto, se hace imprescindible la implementación de mecanismos que contribuyan a reducir los riesgos en la seguridad de la información, ya que estos pueden convertirse en puntos críticos que afecten el desenvolvimiento normal y eficiente de las actividades en los laboratorios de la Universidad Técnica del Norte. Si bien el desarrollo de la presente investigación complementa los diferentes procesos de los Laboratorios de Computación de la Universidad Técnica del Norte teniendo como línea base la norma ISO/IEC 27001 2022 y COBIT 2019 las cuales permitirán establecer un marco de referencia para la gestión de la seguridad de la información, lo que ayudará a la UTN a garantizar la confidencialidad, integridad y disponibilidad de la información, lo que es fundamental para el buen funcionamiento de todos los procesos institucionales y así mantener la confianza de nuestros usuarios garantizando la calidad en los servicios para proteger los activos y la reputación institucional, para llegar a este fin es necesario mantener una supervisión constante y continua en este procedimiento, con la finalidad de que se mantenga un control de las seguridades y la certeza de que se aplique normas y reglamentos establecidos para

salvaguardar la integridad de los procesos que se ejecutan dentro de los Laboratorios de Computación de la Universidad Técnica del Norte.

CAPITULO II

2. MARCO REFERENCIAL

2.1 Antecedentes

> La evaluación técnica informática de las vulnerabilidades en los laboratorios de la Universidad Técnica del Norte básicamente se refiere a mantener bajo control los riesgos para la infraestructura de TI en todo momento. Como parte crucial del ciclo de vida de la gestión de vulnerabilidades, una evaluación de vulnerabilidades ayuda a calificar los riesgos de las vulnerabilidades presentes en su ecosistema para que pueda priorizar los problemas que tienen consecuencias graves y que requieren atención inmediata en cualquier momento. (ManageEngine, 2023)

En la actualidad el desempeño de los laboratorios de la UTN se desarrolla dentro de parámetros y procedimientos generales, establecidos desde el Departamento de Desarrollo Tecnológico de la Universidad Técnica del Norte, al cual todas las dependencias referentes a laboratorios pertenecen y están bajo su responsabilidad ya que es competencia de este departamento mantener el buen funcionamiento de equipos y todo lo relacionado a las actividades que en esta área se desarrolla.

La evaluación técnica de las vulnerabilidades en ciberseguridad en laboratorios de computación es un asunto que cobra una relevancia significativa debido al aumento constante de amenazas y ataques cibernéticos que afectan a organizaciones a nivel global. Los laboratorios de computación son entornos donde se lleva a cabo la investigación, el desarrollo

y la experimentación de tecnologías y sistemas informáticos, lo que los convierte en objetivos atractivos para los ciberdelincuentes.

En la actualidad, la evaluación técnica de vulnerabilidades en ciberseguridad en laboratorios de computación se enfrenta a desafíos significativos. Uno de los principales desafíos es la evolución constante de las amenazas y los métodos de ataque. Los ciberdelincuentes están en constante búsqueda de nuevas formas de explotar vulnerabilidades y acceder a sistemas y datos sensibles. Esto requiere que las organizaciones estén al tanto de las últimas tendencias y técnicas de ataque, y sean proactivas en la evaluación y mitigación de vulnerabilidades.

Otro desafío importante es la complejidad de los sistemas y tecnologías utilizados en los laboratorios de computación. Estos entornos suelen contar con una amplia variedad de dispositivos, sistemas operativos, aplicaciones y servicios, lo que aumenta la superficie de ataque y dificulta la identificación y gestión de vulnerabilidades. Además, los laboratorios de computación suelen estar interconectados con otros sistemas y redes, lo que agrega otro nivel de complejidad a la evaluación de vulnerabilidades.

La falta de conciencia y capacitación en ciberseguridad también es un problema común en la evaluación técnica de vulnerabilidades en laboratorios de computación. Muchas organizaciones no cuentan con personal especializado en ciberseguridad o no brindan la capacitación adecuada a su personal técnico. Esto puede llevar a una falta de comprensión de las mejores prácticas de seguridad y a una implementación deficiente de medidas de protección, lo que aumenta el riesgo de vulnerabilidades y ataques.

Además de estos desafíos, también existen algunas tendencias y avances en la evaluación técnica de vulnerabilidades en ciberseguridad en laboratorios de computación. Una de estas tendencias es el uso de herramientas y técnicas de evaluación automatizadas. Estas

herramientas utilizan algoritmos y escaneos automáticos para identificar y evaluar vulnerabilidades en los sistemas de manera rápida y eficiente. Esto permite una evaluación más exhaustiva y frecuente de las vulnerabilidades, lo que a su vez facilita la implementación de medidas de mitigación.

Otra tendencia importante es la adopción de enfoques de evaluación basados en amenazas. En lugar de simplemente evaluar las vulnerabilidades técnicas, estos enfoques consideran los escenarios y las tácticas que los ciberdelincuentes podrían utilizar para explotar las vulnerabilidades. Esto permite una evaluación más realista y centrada en los riesgos más probables, lo que ayuda a las organizaciones a priorizar sus esfuerzos de mitigación.

En términos de estándares y marcos de referencia, COBIT 2019 es un marco de gobernanza y gestión de tecnología de la información que puede ser utilizado como base para la evaluación técnica de vulnerabilidades en ciberseguridad en laboratorios de computación.

COBIT proporciona un enfoque integral para la gestión de riesgos de TI, incluyendo la identificación y evaluación de vulnerabilidades. Al seguir las pautas y mejores prácticas establecidas en COBIT 2019, las organizaciones pueden mejorar la eficacia de sus evaluaciones de vulnerabilidades y la implementación de medidas de mitigación.

La evaluación técnica de vulnerabilidades en ciberseguridad en laboratorios de computación enfrenta desafíos significativos debido a la evolución constante de las amenazas, la complejidad de los sistemas y la falta de conciencia y capacitación en ciberseguridad. Sin embargo, también existen tendencias y avances que pueden mejorar la eficacia de estas evaluaciones, como el uso de herramientas automatizadas y enfoques basados en amenazas. Además, COBIT 2019 proporciona un marco de referencia sólido para la gestión de riesgos de TI en laboratorios de computación. Es fundamental que las organizaciones reconozcan la

importancia de la evaluación técnica de vulnerabilidades en ciberseguridad y asignen los recursos necesarios para llevar a cabo evaluaciones regulares y efectivas.

Una de las necesidades que se ha evidenciado es generar un informe con recomendaciones específicas de controles para mejorar la ciberseguridad de los laboratorios de computación de la Universidad Técnica del Norte basado en las buenas prácticas de COBIT que es la norma internacional que proporciona un marco de trabajo que ayuda a garantizar el Gobierno Corporativo de la Información y la Tecnología (GEIT). Al igual que la certificación ISO/IEC 27001:2022 resulta crucial salvaguardar los activos más críticos, que incluyen los datos de clientes y empleados, la reputación corporativa y otra información confidencial. La normativa ISO abarca un enfoque que se basa en procesos para implementar, operar y mantener un SGSI.

> La implantación de la ISO 27001 es la respuesta ideal a los requisitos legislativos y de los clientes, incluyendo amenazas potenciales, como: Crimen cibernético, violación de los datos personales, vandalismo / terrorismo, fuego / daños, uso malintencionado, robo y ataque de virus. (Organismo de certificación global, 2023)

> Las normas de la serie 27000 nacen en 1995 con la BS 7799, redactada por el Departamento de Comercio e Industria (DTI) del Reino Unido. Las normas se denominan correctamente "ISO / IEC" porque son desarrolladas y mantenidas conjuntamente por dos organismos internacionales de normas: ISO (la Organización Internacional de Normalización) y la IEC (la Comisión Electrotécnica Internacional). Sin embargo, en el uso diario, la parte "IEC" a menudo se descarta. Actualmente hay 45 normas publicados en la serie ISO 27000. La ISO 27001 es la única norma destinada a la certificación. (NQA, 2023)

Cuando hablamos de COBIT empezamos por evidenciar que es una herramienta que nos permite implementar si el caso lo amerita directrices de funciones, estructura organizativa adecuada al entorno de trabajo, con el fin de mantener un control más minucioso y también evaluar el tipo de riesgo que se puede admitir dentro de los procesos en este caso del manejo adecuado de las actividades de los laboratorios de la UTN, relacionados a la seguridad de la información e infraestructura.

> COBIT aumenta la gestión de control al ofrecer un conjunto de principios directrices que pueden ser empleados en todos los aspectos del control de los sistemas de tecnología de la información con el propósito de optimizar su utilidad y disminuir los riesgos asociados.
>
> COBIT es un conjunto de estándares desarrollado por el IT Governance Institute (ITGI). Este marco puede ayudar a las organizaciones a comprender los rápidos cambios en la tecnología y la complejidad de administrar todos los aspectos de TI. (Dictsolutions, 2019)

2.2 Marco teórico

Entre los conceptos que se consideran en el desarrollo de este proyecto se definirán y citarán en este apartado los más importantes y que son un eje transversal dentro de la seguridad de la información y como base de la investigación que se plantea, refiriéndonos a conceptos que nos permiten comprobar la importancia de estudios previos y la manera en la que pueden ser aplicados a nuestro proyecto propuesto contemplando todos los detalles que nos permitan ejecutar un trabajo minucioso con el fin de cumplir los objetivos propuestos.

2.3 Tecnologías de la Información y Comunicación (TC)

Actualmente las Tecnologías de la Información y Comunicación se han convertido en un medio de enseñanza ya que en la última década toda la información que reposa en internet ha servido de incentivo para mejorar la educación en las aulas debido al acceso ilimitado a la información; en la actualidad se ha vuelto normal evidenciar en toda institución el uso de dispositivos con el fin de transmitir de mejor manera la información lo que permite el aumento de producción, reducción de tiempo de espera, contribuyen de manera efectiva en el aprendizaje interactivo para despertar capacidades que muchas veces en un entorno sin tecnología no serían evidentes.

En síntesis, las tecnologías de la Información y Comunicación (TIC) se refieren a las herramientas computacionales e informáticas que gestionan, almacenan, sintetizan, recuperan y presentan información en diversas formas. Es un conjunto de herramientas, soportes y canales para el tratamiento y acceso a la información (Suarez, 2023). Constituyen nuevas plataformas y medios para la creación, registro, conservación y distribución de contenidos informativos. Ejemplos de estas tecnologías incluyen la pizarra digital (combinando una computadora personal y un proyector multimedia), los blogs, los podcasts y, por supuesto la web. En el ámbito educativo, las TIC funcionan como herramienta y recursos auxiliares, es decir sirven como instrumentos y materiales de apoyo que facilitan el proceso de aprendizaje, el desarrollo de habilidades y diversas modalidades de enseñanza, adaptándose a los estilos y ritmo de aprendizaje de los estudiantes.

2.4 Buenas y mejores prácticas en el manejo de Tecnologías de la información y comunicación.

En la actualidad se experimenta un rápido progreso en el campo de las Tecnologías de la Información y Comunicación, esto implica que, a medida que se utilizan estas tecnologías,

es esencial mantener al día todas las herramientas utilizadas para este fin como se puede mencionar marcos de referencias, metodologías específicas, porque se ha evidenciado que el principal problema en las buenas prácticas es no mantener la coherencia entre la documentación y la ejecución o puesta en marcha por la diversidad de versiones o actualizaciones de herramientas que se pueden desfasar en la aplicación generando de esta manera brechas importantes en lo referente al proceso en sí de la institución .

A continuación, en la Figura 1, los 5 fundamentos de la gestión de TI, los mismos son importantes para la definición posterior de la planificación y los recursos necesarios para mantener y controlar aspectos como el financiero, necesidades futuras y transparencia de los procesos.

Figura 1 *Fundamentos de la Gestión TI*

Nota. Fuente: Tomado de (Erráez, 2011)

La gestión de Tecnologías de la Información (TI) se refiere a la planificación, implementación, organización y control de los recursos y procesos relacionados con la

tecnología de la información en una organización. Los fundamentos de la gestión de TI se basan en una serie de principios clave que ayudan a las organizaciones a aprovechar al máximo sus inversiones en TI y a alinear sus objetivos de negocio con las capacidades tecnológicas. A continuación, se presentan algunos de los fundamentos más importantes de la gestión de TI según Erráez (2011):

- Alcance y objetivos claros: La gestión de TI debe comenzar por definir claramente el alcance y los objetivos de las iniciativas tecnológicas. Esto implica comprender las necesidades y prioridades del negocio y establecer metas realistas para el uso de la tecnología. Al tener un alcance y objetivos claros, las organizaciones pueden enfocar sus esfuerzos y recursos de manera efectiva.

- Alineación con el negocio: La gestión de TI debe estar alineada con los objetivos y estrategias del negocio. Esto implica entender cómo la tecnología puede contribuir al logro de los objetivos empresariales y cómo los cambios en el negocio pueden afectar las decisiones y la implementación de la tecnología. La alineación con el negocio asegura que las inversiones en TI sean relevantes y generen valor para la organización.

- Gestión de riesgos: La gestión de TI implica la identificación, evaluación y mitigación de los riesgos asociados con el uso de la tecnología. Esto implica comprender las amenazas y vulnerabilidades de seguridad, así como los riesgos operativos y estratégicos relacionados con la tecnología. La gestión de riesgos permite a las organizaciones tomar decisiones informadas y establecer medidas de seguridad y continuidad del negocio adecuadas.

- Gobierno de TI: El gobierno de TI se refiere al establecimiento de estructuras y procesos que aseguren la toma de decisiones efectiva, la rendición de cuentas y la

supervisión de las iniciativas de tecnología en una organización. Esto incluye la definición de roles y responsabilidades claras, la implementación de políticas y procedimientos, y la supervisión de los resultados y el cumplimiento de los objetivos. El gobierno de TI asegura una gestión efectiva y responsable de los recursos y procesos de TI.

- Gestión de proyectos y servicios de TI: La gestión de TI implica la implementación efectiva de proyectos y servicios relacionados con la tecnología. Esto implica la planificación, ejecución y control de proyectos de TI, así como la gestión de los servicios de TI proporcionados a los usuarios internos y externos. La gestión de proyectos y servicios de TI garantiza la entrega oportuna y efectiva de soluciones tecnológicas y la satisfacción de los usuarios.

Estos son solo algunos de los fundamentos clave de la gestión de TI. Es importante tener en cuenta que la gestión de TI es un proceso continuo y evolutivo que requiere adaptabilidad y actualización constante para mantenerse al día con los cambios tecnológicos y los requisitos del negocio. Al seguir estos fundamentos, las organizaciones pueden maximizar el valor de sus inversiones en TI y garantizar un uso efectivo y eficiente de la tecnología en apoyo de sus objetivos empresariales.

Dentro de estos aspectos es fundamental mantener una comunicación clara con el equipo de trabajo lo que permite que haya fluidez al compartir la información y consolidar las relaciones laborales para una empresa exitosa.

En la Figura 2, se muestra 5 estrategias para la mejora en la comunicación empresarial, estas estrategias son viables de aplicación en varios contextos, ya que ofrece nuevas herramientas de receptividad y sitios con los que se puede compartir información segura y confiable para mejorar el flujo de procesos y actividades.

Figura 2 *Estrategias para mejorar la comunicación empresarial*

Nota. Fuente: Tomado de (Estrada, 2011)

Para poder ejecutar las buenas prácticas en el manejo de TI es importante implementar procedimientos probados, aplicados y aceptados en la industria, como consecuencia de estos procedimientos el resultado será el aporte de valor a la institución o empresa donde se apliquen.

Las estrategias de comunicación empresarial desempeñan un papel fundamental en el manejo de Tecnologías de la Información (TI). La comunicación efectiva es esencial para garantizar que los equipos de TI y el resto de la organización estén alineados, comprendan los objetivos y las iniciativas de TI, y trabajen juntos de manera colaborativa para lograr el éxito.

Las estrategias de comunicación empresarial pueden ayudar a transmitir de manera clara y concisa los objetivos y la visión de TI a toda la organización (Estrada, 2011). Esto implica comunicar los beneficios y el impacto que las iniciativas de TI pueden tener en el negocio, así

como las metas a largo plazo que se desean alcanzar. Una comunicación clara y efectiva ayuda a alinear a todos los miembros de la organización en torno a los objetivos de TI y a generar un mayor compromiso y motivación.

También pueden facilitar la colaboración y el trabajo en equipo entre los equipos de TI y los demás departamentos de la organización. Esto implica fomentar la comunicación abierta y transparente, proporcionar canales de comunicación efectivos y promover la participación y el intercambio de ideas (Uría, 2013). La comunicación efectiva entre los equipos de TI y los demás departamentos ayuda a resolver problemas de manera más rápida y eficiente, mejora la toma de decisiones y promueve la innovación y la creatividad.

Los proyectos de TI a menudo implican cambios en los procesos, las herramientas y la forma de trabajar de los empleados (Torres, 2020). Una comunicación efectiva puede ayudar a preparar a los empleados para estos cambios, explicar los beneficios y proporcionar apoyo y recursos para facilitar la transición. Además, la comunicación continua y abierta durante todo el proceso de implementación de TI puede ayudar a identificar y abordar cualquier problema o resistencia que pueda surgir.

Las estrategias de comunicación empresarial también pueden proporcionar una vía para recopilar retroalimentación y opiniones de los empleados sobre las iniciativas de TI. Esto puede ayudar a identificar áreas de mejora, resolver problemas y adaptar las estrategias de TI de acuerdo con las necesidades y preferencias de los usuarios. La comunicación bidireccional y la participación activa de los empleados en el proceso de toma de decisiones de TI pueden generar un mayor compromiso y una mayor aceptación de los cambios.

En resumen, las estrategias de comunicación empresarial desempeñan un papel crítico en el manejo de TI al facilitar la comunicación clara de los objetivos y la visión de TI, fomentar la colaboración y el trabajo en equipo, gestionar las expectativas y los cambios, y permitir la

retroalimentación y la mejora continua. Al implementar estrategias de comunicación efectivas, las organizaciones pueden maximizar el valor de sus inversiones en TI y lograr una implementación exitosa de las iniciativas de TI.

En el ámbito de la gestión de servicios de TI las buenas prácticas pueden provenir de muchas fuentes, marcos públicos de trabajo como ITIL, COBIT y CMMI, normas como la ISO/IEC 20000.

2.5 Beneficios del uso de buenas prácticas en la gestión de servicios de TI

- Se garantiza la congruencia entre los propósitos de Tecnologías de la información (TI) y los propósitos empresariales, generando un valor añadido.
- Se disminuyen los gastos relacionados con TI y se aumenta la excelencia en la prestación de los servicios de TI.
- Se administra con eficacia los riesgos vinculados al uso de servicios de TI.
- Se permite evaluar de manera precisa el valor real de los servicios de TI.
- Hace posible la gobernabilidad de TI, es decir la responsabilidad que tiene la dirección y los niveles superiores de la gerencia para asegurar que el sistema de Tecnologías de la Información (TI) de su organización apoyan en forma efectiva los objetivos y estrategia de la organización.
- Se mejora la comunicación entre el departamento de Tecnologías de la Información (TI) y otros sectores de la empresa.
- Se asegura que se cumplan las normativas vigentes en el campo de Tecnologías de la Información (TI).

- Se obtiene una mayor adaptabilidad, lo que posibilita la implementación de modificaciones en la empresa a la velocidad requerida por el cliente.

- Se reduce el efecto que experimenta la empresa y sus clientes en el caso de situaciones fortuitas o interrupciones no planificadas en el servicio.

- Las decisiones se fundamentan en métricas que abarcan tanto el aspecto empresarial como el tecnológico.

- Mediante la mejora de la eficiencia de los servicios de TI, se incrementa el grado de satisfacción del cliente.

2.6 Seguridad de la Información

La Seguridad de la Información puede ser descrita como el conjunto de acciones técnicas, administrativas y legales que habilitan a la entidad a garantizar la confidencialidad, integridad y accesibilidad de su sistema de información. Con el fin de aplicar la seguridad de la información cualquier organización debe implementar un Sistema de Gestión de la Información o más conocido como SGSI para poder proteger la información el primer paso es catalogar o identificar el tipo de activos que posee la institución con el fin de aplicar el plan PDCA.

Luego debe aplicarse el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

Se concibe a la seguridad como un procedimiento continuo, dado que los riesgos son persistentes y, aunque no pueden ser eliminados por completo, pueden ser gestionados. De estos riesgos se deriva que los asuntos relacionados con la seguridad no se limitan exclusivamente a lo tecnológico, y, por lo tanto, nunca son completamente erradicados.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos, procesos y controles diseñados para gestionar y proteger la información sensible y los activos relacionados en una organización. El objetivo principal de un SGSI es establecer un marco de trabajo para identificar, evaluar y gestionar los riesgos de seguridad de la información de manera sistemática y efectiva.

Un SGSI se basa en la norma ISO 27001, que es un estándar internacional para la gestión de la seguridad de la información (Guano & Jaramillo, 2021). La norma ISO 27001 proporciona una guía detallada sobre cómo establecer, implementar, mantener y mejorar un SGSI. No obstante, es fundamental considerar que un Sistema de Gestión de Seguridad de la Información (SGSI) puede ser ajustado para satisfacer las particularidades y requisitos específicos de cada entidad.

Establecer políticas y procedimientos claros y documentados es fundamental para garantizar una gestión eficaz de la seguridad de la información (Orellana, 2022). Estas políticas y procedimientos deben abordar aspectos como el acceso y la autorización, la protección de datos, la gestión de incidentes y la continuidad del negocio.

Un SGSI debe incluir un proceso para identificar y evaluar los riesgos de seguridad de la información. Esto implica analizar las amenazas potenciales, evaluar la vulnerabilidad de los activos de información y determinar el impacto potencial de un incidente de seguridad (Chicaiza & Muñoz, 2020). A partir de esta evaluación, es necesario aplicar medidas de control apropiadas para reducir los riesgos detectados.

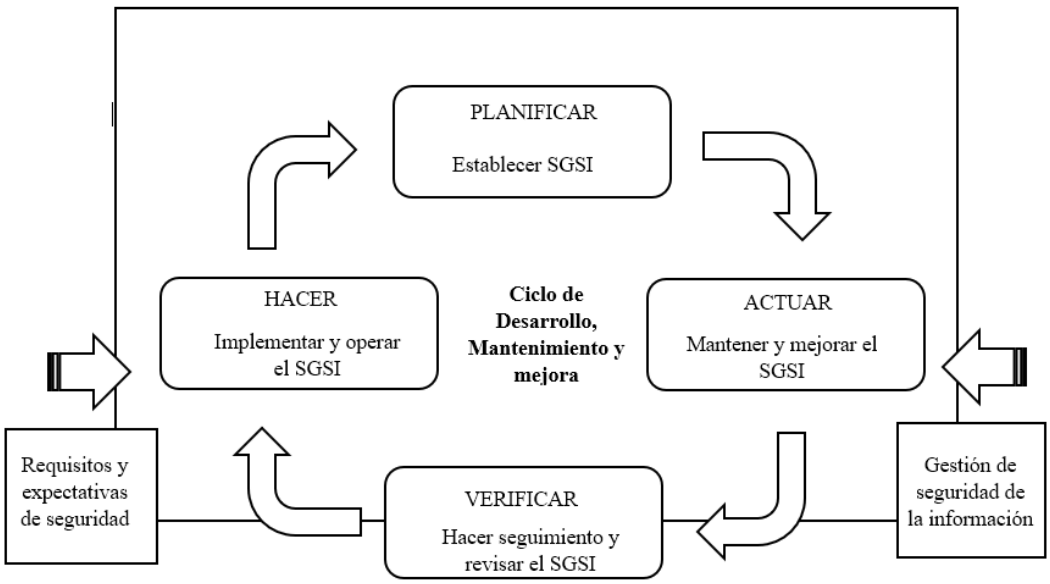
También debe incluir una variedad de controles de seguridad de la información para proteger los activos de información de la organización. Estos controles pueden incluir medidas técnicas, como firewalls y sistemas de detección de intrusos, así como medidas organizativas, como la segregación de funciones y la conciencia de seguridad de los empleados.

Además, es necesario un proceso de auditoría y revisión periódica para evaluar la efectividad del sistema y garantizar su mejora continua (Hidalgo, 2022). Esto implica realizar auditorías internas para evaluar el cumplimiento de los controles de seguridad de la información y llevar a cabo revisiones periódicas de la efectividad del SGSI en su conjunto.

Por último, contar con programas de capacitación y conciencia de seguridad para garantizar que los empleados estén informados y sean conscientes de las políticas y procedimientos de seguridad de la información. Esto ayuda a promover una cultura de seguridad y a reducir el riesgo de errores o comportamientos inseguros.

Un SGSI como se muestra en la Figura 3, siempre sigue un ciclo constante de cuatro etapas, que inicia con la planificación y culmina con la acción, logrando de esta manera un incremento en la seguridad.

Figura 3 SGSI planificación



Nota. Fuente: Elaborado por el autor

Según Guano & Jaramillo (2021) un SGSI siempre consta de:

- PLANIFICAR (Plan): implica definir el entorno en el que se desarrollan las políticas de la seguridad, llevar a cabo el análisis de riesgos, seleccionar controles y determinar su aplicabilidad.

- HACER (Do): implica poner en práctica el sistema de gestión de la seguridad de la información, ejecutar el plan de riesgos y aplicar los controles correspondientes.

- VERIFICAR (Check): involucra la supervisión de las actividades y ejecutar auditorías internas.

- ACTUAR (Act): implica llevar a cabo labores de mantenimiento, propuestas para mejorar, medidas preventivas y correctivas.

La tarea principal de la seguridad informática radica en la minimización de riesgos que pueden surgir de diversas fuentes, incluyendo la entrada de datos, el medio de transmisión de información el hardware utilizado para la transmisión, los usuarios y los protocolos implementados. Lo que debe contemplar la seguridad se puede clasificar en tres partes como son los siguientes según (Hidalgo (2022):

- Los usuarios

- La información, y

- La infraestructura

Los usuarios se consideran el punto más vulnerable de la cadena, ya que es difícil ejercer un control absoluto sobre sus acciones. Un simple error o accidente por parte de un usuario puede comprometer el trabajo acumulado durante mucho tiempo. En muchos casos, es necesario proteger el sistema y la información de las acciones involuntarias de los propios usuarios. La información se considera el activo más valioso en el ámbito de la seguridad

informática, ya que es el elemento que se busca proteger a toda costa. Por último, se encuentra la infraestructura, que puede ser más controlable en ciertos aspectos, pero no está exenta de riesgos, dependiendo en última instancia de los procesos que se implementen. Deben considerarse desafíos complejos, que abarcan desde accesos no autorizados y robo de identidad hasta problemas más cotidianos, como el hurto de equipos, inundaciones, incendios u otros desastres naturales que pueden afectar la integridad del hardware de la organización

2.7 Principios y modelos de seguridad

Los principios de seguridad nos permiten evidenciar cuando un sistema es seguro y confiable, solo si se puede garantizar los tres pilares fundamentales que son:

2.8 Confidencialidad de la información

Este principio, que se denomina también privacidad, establece que la información debe estar restringida únicamente a las personas que tienen la necesidad y la autorización para acceder a ella. Su finalidad es garantizar que la información no se comparta de forma accidental o deliberada.

2.9 Integridad de la información

Se refiere al hecho de que la información, ya sea almacenada en dispositivos o transmitida a través de cualquier medio de comunicación no ha sufrido ninguna alteración intencionada por parte de terceros. Esto asegura que la información permanecerá sin modificaciones por personas no autorizadas.

2.10 Disponibilidad de la información

Este principio establece que la información debe encontrarse accesible en todo momento para las personas con la debida autorización y que pueda recuperarse en caso de que se presente

un evento de seguridad que resulte en su pérdida o daño. En otras palabras, garantiza que la información esté disponible cuando sea requerida.

Cuando nos referimos al concepto de un modelo de seguridad, podemos explicar que este brinda una representación que describe las características funcionales y estructurales relacionadas con la seguridad de nuestro sistema. Facilita a los desarrolladores trabajar con una definición de alto nivel acerca de los requisitos de protección y las políticas de seguridad, permitiendo, al mismo tiempo, la creación de una descripción concisa y precisa del comportamiento esperado del sistema.

Una organización define un modelo de seguridad para cubrir sus necesidades de negocio. El modelo sirve como una base para definir los requisitos y la implementación real de un sistema de seguridad.

Un modelo de seguridad tiene ciertos objetivos distintivos, que incluyen verificar la identidad de los usuarios mediante sistemas de autenticación que abarcan factores como la robustez de las contraseñas. Asimismo, permite el acceso a recursos por parte de usuarios autorizados, gracias a sistemas de autorización que establecen procesos basados en solicitudes o roles, junto con el suministro correspondiente. Estos recursos comprenden cuentas, servicios, información de usuarios y funciones del IBM Security Identity Manager, por ejemplo. Además, un modelo de seguridad requiere de procesos adicionales para determinar los recursos a los que un usuario tiene permiso de acceso. También implica supervisar que operaciones y servicios son permitidos para cuentas y usuarios, así como delegar ciertas actividades de un usuario a otros, ya sea por solicitud o asignación. Otro aspecto importante es salvaguardar información confidencial, como lista de usuarios o atributos de cuentas, y garantizar la integridad de las comunicaciones y los datos

En la presente época, se encuentran disponibles varios modelos de seguridad, y cada uno aborda diversas demandas y requerimientos de los usuarios. Existen esquemas que se basan en la integridad de la información, otros esquemas se basan en la autenticación de los usuarios del sistema y otros tantos se basan en la privacidad de la información, (C. Arellano et al, s.f.).

- Modelos basados en el control de acceso por role (RBAC Role Based Access Control).
- Modelo basado en la separación de tareas (SoD Separation of Duties).

La separación física y lógica de tareas puede mejorar la prevención de actividades no autorizadas. Los principales modelos existentes contemplan, como principal preocupación, el control de acceso y la integridad; modelos como los utilizados por los productos de Microsoft, implementan una seguridad y control de cambios para sus documentos basados en autentificación de usuario, este puede proteger sus documentos y conocer la identidad de los usuarios que realizan cambios sobre un documento, pero no le asegura que el 19 documento no sufrió modificaciones en el transcurso del proceso de colaboración, (C. Arellano et al, s.f.). En contextos de seguridad en general, los modelos deben incluir los siguientes elementos:

- Resguardar la información de manera que no sea accesible ni alterable por individuos no autorizados.
- Evitar que individuos no autorizados añadan o eliminen información.
- Comprobar la identidad tanto del remitente como del destinatario de la información.
- Facilitar a los usuarios la transición de documentos con firmas electrónicas a través de medios electrónicos.

2.11 Amenazas y ataques comunes en entornos universitarios

2.11.1 Ciberseguridad

La ciberseguridad abarca el conjunto de enfoques, tecnologías y procedimientos concebidos con el fin de salvaguardar sistemas informáticos, redes, software y datos frente a eventuales amenazas, ataques, fraudes, la sustracción de información y diversas modalidades de delitos informáticos. La ciberseguridad busca garantizar la privacidad, la integridad y la disponibilidad de la información y de los sistemas informáticos, y se enfoca en la prevención, detección y respuesta a incidentes de seguridad. La ciberseguridad es esencial en el mundo digital actual para proteger los activos y recursos digitales y garantizar la confidencialidad, la integridad y la disponibilidad de la información crítica y sensible.

Hoy en día, se encuentran disponibles diversas categorías de seguridad cibernética que se centran en la protección de las diferentes partes el sistema. De manera que se pude hacer referencia a:

- Seguridad de hardware. En todas las operaciones informáticas, se emplea un dispositivo, que puede ser físico, virtual o basado en la nube. Por lo tanto, es esencial salvaguardar estos componentes contra posibles ataques. Con este fin, los diseñadores de hardware incorporan tecnologías de seguridad integradas que defienden estos componentes de las principales amenazas cibernéticas. Un ejemplo de esto son los módulos de seguridad de hardware, que son dispositivos fortificados y resistentes a manipulaciones diseñados para proteger las operaciones criptográficas.

- Seguridad de software. Estas estrategias de seguridad cibernética están orientadas a prevenir posibles vulnerabilidades en los sistemas informáticos, incluyendo el sistema operativo, aplicaciones y programas, con el fin de evitar intrusiones no autorizadas. Ejemplos de estas medidas incluyen la instalación de programas antivirus en

computadoras y dispositivos móviles, así como la aplicación de actualizaciones en programas para proteger contra nuevas amenazas como virus y malware.

- Seguridad de redes. Este enfoque de seguridad cibernética se orienta en establecer filtros y mecanismos de protección para resguardar tanto el hardware como los datos que transitan a través de la red. Se asegura la integridad de la información durante su emisión, tránsito y recepción, de modo que no sea susceptible de interceptación o desciframiento no autorizado. Para alcanzar este propósito, se pueden emplear tecnologías como firewalls, redes privadas virtuales VPN y filtros contra correo no deseado anti-spam. (Qué es la ciberseguridad, 2022)

2.11.2 Activos de Información

Los activos de información son todos los recursos y elementos de la información que son importantes para el funcionamiento y éxito de una organización. Estos activos pueden incluir la información de los clientes, los planes estratégicos, los secretos comerciales, la propiedad intelectual, la información financiera, los recursos humanos y cualquier otro tipo de información que sea vital para la operación de la organización. Los activos de información pueden ser almacenados en diferentes formas y medios, como documentos físicos, archivos electrónicos, bases de datos, sistemas de gestión de contenidos, servidores, redes y cualquier otro medio en el que se recopile, procese o transmita la información. Es fundamental garantizar la adecuada salvaguardia de los activos de información para garantizar la continuidad del negocio, la privacidad de la información y la conformidad con las leyes y regulaciones aplicables.

La seguridad de la información es un conjunto de medidas que tienen como objetivo proteger a los activos de información de una organización, evitando vulneraciones o

incidentes sin importar la forma en que están almacenados. Así mismo, involucra a las medidas de reacción y respuesta ante eventuales incidentes.

La seguridad de la información contempla a todos los mecanismos para proteger a los activos de información en una organización, siendo un concepto amplio que deja debajo de su "paraguas" a otras sub-disciplinas tales como la seguridad informática, seguridad digital o ciberseguridad. (Redvoiss, 2021)

2.11.3 Vulnerabilidades

En el contexto de la seguridad informática, una vulnerabilidad se refiere a una debilidad o fallo en un sistema, aplicación o dispositivo que puede ser explotado por un atacante para comprometer la seguridad de la información o el sistema mismo. Las vulnerabilidades pueden ser causadas por errores en el diseño o la implementación de un sistema, configuraciones incorrectas, falta de actualizaciones de seguridad, entre otras razones. Una vez que un atacante descubre una vulnerabilidad, puede utilizar técnicas de explotación para aprovecharla y acceder a información confidencial, instalar malware, modificar configuraciones o tomar control del sistema afectado. Es importante identificar y remediar las vulnerabilidades en los sistemas y aplicaciones para evitar posibles ataques y mantener la integridad y confidencialidad de la información.

En este contexto un análisis de vulnerabilidades nos proporcionará un panorama claro de lo que está sucediendo en nuestro entorno, para lo cual es importante tener en consideración diferentes recomendaciones que nos pueden ayudar:

- Mantener al día las aplicaciones implica garantizar que todos los sistemas, componentes y sus respectivas actualizaciones y versiones recientes estén ejecutadas a la fecha. Esto se hace con el objetivo de mejorar tanto la seguridad, el

funcionamiento y la visibilidad de estos sistemas, ya que dichas actualizaciones están diseñadas con ese propósito.

- Adherirse a regulaciones como la norma ISO 27001, la cual fue creada con el propósito de resguardar la información de las empresas, ya sea en términos de reputación, datos personales, información de clientes, entre otros aspectos. Bien sea a nivel de imagen, datos personales, información de clientes, etc.

- Conducir evaluaciones de vulnerabilidades lo que implica realizar escaneos para identificar posibles debilidades y, a partir de eso tomar medidas correctivas. Es crucial destacar que las evaluaciones de vulnerabilidades no deben ser confundidas con las pruebas de penetración o pentesting. Las evaluaciones de vulnerabilidades son procesos completamente automatizados, en contraste, el pentesting implica una ejecución manual

- La realización de pruebas de penetración en los sistemas posibilita la obtención de resultados relacionados con las debilidades presentes en aplicaciones e infraestructura, además de su nivel de riesgo asociado. Esta prueba, junto al análisis de vulnerabilidades, evitarán brechas de seguridad informática al arrojar toda la información necesaria para detectar y mitigar las fallas en sistemas. (Delta protect, 2023)

2.11.4 Evaluación Técnica

La evaluación técnica es un proceso sistemático de análisis y revisión de las características técnicas de un sistema, dispositivo o aplicación. El objetivo de la evaluación técnica es identificar y evaluar el desempeño, la seguridad, la calidad y la eficiencia del sistema o dispositivo en cuestión. La evaluación técnica puede involucrar la revisión de los aspectos técnicos de los sistemas, incluyendo su diseño, arquitectura, funcionamiento, configuración,

rendimiento, seguridad y compatibilidad con otros sistemas. Los resultados de la evaluación técnica pueden utilizarse para mejorar la calidad y la seguridad de los sistemas y aplicaciones, optimizar su rendimiento, identificar y corregir posibles vulnerabilidades de seguridad, y garantizar la conformidad con las normas y regulaciones aplicables. La evaluación técnica se puede realizar mediante pruebas, análisis y revisiones exhaustivas de los componentes técnicos de un sistema o aplicación, y puede ser llevada a cabo por profesionales especializados en diferentes áreas técnicas, tales como ingenieros, programadores, analistas de sistemas, entre otros.

2.11.5 Administración de Riesgos

La administración de riesgos en ciberseguridad se refiere a un proceso sistemático y continuo de identificación, análisis, evaluación y mitigación de los riesgos asociados a la seguridad de la información en un entorno digital. El objetivo de la administración de riesgos en ciberseguridad es identificar y valorar los riesgos para la información y los sistemas digitales, y tomar medidas para minimizar su impacto en caso de que ocurran. La administración de riesgos en ciberseguridad implica la evaluación de los riesgos de seguridad informática y la selección de medidas adecuadas para prevenir, mitigar o transferir esos riesgos, con el fin de proteger los activos digitales y garantizar la continuidad del negocio.

El proceso de administración de riesgos en ciberseguridad implica la identificación de los activos digitales, la evaluación de las amenazas potenciales, la determinación de la probabilidad e impacto de los riesgos, y la selección de medidas adecuadas de mitigación de riesgos. La administración de riesgos en ciberseguridad también incluye la monitorización continua de los sistemas y la implementación de medidas para adaptarse a los cambios en las amenazas y riesgos de seguridad informática. La administración de riesgos en ciberseguridad es un proceso integral que abarca la implementación de políticas, procedimientos, tecnologías

y controles para garantizar la seguridad de la información y la continuidad del negocio en un entorno digital.

2.12 COBIT 2019

COBIT 2019 es un marco de gobierno y gestión de TI que se enfoca en la gestión efectiva y eficiente de los recursos de tecnología de la información (TI) de una organización. COBIT significa Control Objectives for Information and Related Technology (Objetivos de Control para la Tecnología de la Información y Relacionados) y fue desarrollado por la ISACA (Asociación de Auditoría y Control de Sistemas de Información).

El marco COBIT 2019 se centra en la gobernanza y la gestión de TI para ayudar a las organizaciones a cumplir sus objetivos empresariales y garantizar la entrega de valor a través de la tecnología. COBIT 2019 proporciona un conjunto completo de herramientas y recursos para ayudar a las organizaciones a establecer políticas y procedimientos de TI efectivos, y para monitorear y mejorar continuamente su rendimiento en la gestión de TI. COBIT 2019 cubre áreas como la planificación estratégica de TI, la gestión de la seguridad de la información, la gestión de riesgos de TI, la gestión de proyectos de TI y la gestión de servicios de TI, entre otros temas relacionados con la gestión de TI.

Es un marco de trabajo (framework) para el gobierno y la gestión de las tecnologías de la información (TI) empresariales y dirigido a toda la empresa. (GlobalSuite, 2022)

Este marco de referencia establece las mejores prácticas para la gestión de la seguridad informática en las organizaciones, incluyendo la evaluación de riesgos, la identificación de vulnerabilidades y la implementación de medidas de seguridad adecuadas.

COBIT 2019 (Control Objectives for Information and Related Technologies) es un marco de gobierno y gestión de TI desarrollado por ISACA (Information Systems Audit and

Control Association). COBIT proporciona un enfoque estructurado y completo para ayudar a las organizaciones a gestionar y controlar sus sistemas de información de manera efectiva.

El objetivo principal de COBIT 2019 es ayudar a las organizaciones a lograr sus objetivos empresariales a través de la implementación de controles y procesos de TI efectivos. El marco se basa en un conjunto de principios y prácticas que se pueden aplicar a cualquier tipo de organización, independientemente de su tamaño, sector o ubicación geográfica.

Se centra en identificar y satisfacer las necesidades de las partes interesadas clave, como los accionistas, los clientes y los reguladores. Esto implica establecer y mantener una relación clara entre los objetivos empresariales y los objetivos de TI.

COBIT 2019 abarca todos los aspectos de la empresa de TI, incluyendo personas, procesos, información y tecnología. Esto garantiza que todos los componentes de TI estén adecuadamente alineados y contribuyan a los objetivos empresariales, se basa en un enfoque holístico que considera todos los aspectos de la gestión de TI, desde la estrategia hasta la implementación y el monitoreo (Cynthus, 2022). Esto ayuda a las organizaciones a comprender cómo los diferentes componentes de TI interactúan entre sí y cómo pueden afectar el logro de los objetivos empresariales.

Esta metodología distingue claramente entre la gobernanza de TI y la gestión de TI. La gobernanza se refiere al establecimiento de políticas y directrices, mientras que la gestión se refiere a la implementación de estas políticas y directrices (Mora, Leon, Huilcapi, & Escobar, 2017). Esta separación ayuda a garantizar una clara responsabilidad y rendición de cuentas en todos los niveles de la organización, además se basa en un enfoque basado en procesos que ayuda a las organizaciones a identificar, diseñar, implementar, monitorear y mejorar continuamente los procesos de TI. Esto garantiza una gestión eficiente y efectiva de los recursos de TI.

COBIT 2019 proporciona un conjunto de cinco principios de gobernanza y gestión de TI, junto con una serie de objetivos de control y prácticas recomendadas (Chicaiza & Muñoz, 2020). Estos objetivos de control se agrupan en dominios y procesos, que cubren áreas clave como la planificación y organización de TI, la adquisición e implementación de sistemas, la entrega y soporte de servicios, y el monitoreo y evaluación de TI.

COBIT 2019 brinda una estructura para la evaluación del nivel de madurez en la gestión de Tecnologías de la Información de una entidad. Esto conduce a las empresas a detectar áreas susceptibles de mejora y a establecer metas para el progreso constante en la administración de TI. COBIT 2019 es utilizado por muchas organizaciones en todo el mundo como un marco de referencia para la gestión de TI, y es ampliamente reconocido como un estándar líder en la industria para la gestión de TI empresarial.

La implementación de COBIT desde una perspectiva centrada en el control de TI también se guía por el criterio de calidad. Para alcanzar este objetivo, se aplican otros principios tales como:

- Efectividad, se traduce en la relevancia de la información para los procesos y requisitos del negocio, asegurando que sea entregada de manera oportuna, precisa y concisa

- Eficiencia, ejecutar los procesos de manera productiva y efectiva.

- Integridad, para que la información utilizada sea precisa, abarque la totalidad de los datos y sea válida.

- Confidencialidad, se asegura que la información esté resguardada y no será revelada sin el debido permiso.

El modelo COBIT es un apoyo para establecer metas realizables a través de los componentes de Tecnologías de la Información, lo que resulta en una variedad de ventajas al aplicar este enfoque. A continuación, se mencionan los beneficios clave:

- Ofrece visión clara de TI: Proporciona una comprensión precisa de las Tecnologías de la Información al establecer objetivos empresariales que se alinean con los procesos de acuerdo a las necesidades del negocio.

- Define propiedades y responsabilidades claras: Establece roles y responsabilidades bien definidos al fundamentar sus procesos en la utilización de las capacidades individuales y la infraestructura.

- Perfecciona la gestión del desempeño: Mejora la administración del rendimiento al posibilitar la evaluación de cada una de las tareas dentro de la organización o empresa. Esto permite identificar áreas de mejora, eliminar procesos redundantes, optimizar recursos y realizar las actividades que generan un valor significativo para el negocio.

- Aumenta la confianza en el sistema de información empresarial: Incrementa la confianza en la infraestructura de la información empresarial al establecer y administrar planes realistas y equilibrados. Cada uno de los principios y procesos contribuye a potenciar la eficiencia de las redes de información, evitando así comprometer la seguridad de los datos, lo que fomenta la confiabilidad de las empresas

- Provee un modelo abierto y flexible: Ofrece un modelo de naturaleza abierta y adaptable. Esta cualidad destaca como una de sus características principales,

permitiendo una actualización constante y una rápida adaptación a las modificaciones y requisitos de los usuarios.

La gestión eficiente de las Tecnologías de la información es un componente esencial para el triunfo de la empresa, y el modelo COBIT, en particular, proporciona recursos apropiados para evaluar de manera ágil y uniforme el logro de los objetivos establecidos en este ámbito. Por ello, es una de las mejores opciones para controlar los sistemas de información. (Cynthus, 2022)

El propósito de COBIT es brindar a la Alta Dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan (Mora, Leon, Huilcapi, & Escobar, 2017). COBIT proporciona orientación sobre cómo administrar la utilización de sistemas, al mismo tiempo que establece un conjunto de estándares de calidad que los proveedores de sistemas deben seguir. Asimismo, COBIT provee las herramientas necesarias para supervisar todas las actividades vinculadas a TI.

Herramienta OCTAVE en base a COBIT 2019

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología de evaluación de riesgos desarrollada por el CERT Coordination Center de la Universidad Carnegie Mellon (Hurtado, 2023). Esta metodología se centra en la identificación y gestión de riesgos de seguridad de la información, especialmente en el ámbito de los riesgos operativos.

El objetivo principal de OCTAVE es ayudar a las organizaciones a comprender sus operaciones, identificar los activos críticos de información, evaluar las amenazas y vulnerabilidades asociadas, y desarrollar estrategias de mitigación de riesgos adecuadas. OCTAVE proporciona un enfoque sistemático y estructurado para la evaluación de riesgos,

centrándose en la comprensión del contexto operativo y en la identificación de riesgos específicos.

Para aplicar OCTAVE en la evaluación técnica de vulnerabilidades en ciberseguridad en laboratorios de computación, se puede seguir el siguiente proceso según Alvarez & Silva (2019):

- Preparación:

Familiarización con OCTAVE y sus principios fundamentales.

Identificación y asignación de un equipo de evaluación que incluya a expertos en seguridad de la información y personal técnico del laboratorio.

Definición del alcance de la evaluación, identificando los activos críticos de información y los sistemas específicos a evaluar.

- **Análisis de la situación:**

Realización de encuestas y talleres con el personal del laboratorio para comprender las operaciones y los procesos clave.

Identificación de los activos críticos de información y su importancia para las operaciones del laboratorio.

Identificación de las amenazas y vulnerabilidades potenciales asociadas a los activos críticos de información.

- **Evaluación de riesgos:**

Identificación de los riesgos más significativos y su impacto potencial en el laboratorio.

Evaluación de la probabilidad de ocurrencia de cada riesgo identificado.

Evaluación del impacto potencial de cada riesgo en términos de pérdida financiera, daño a la reputación, interrupción de las operaciones, entre otros factores relevantes.

- **Desarrollo de estrategias de mitigación:**

Identificación de medidas de mitigación adecuadas para reducir la probabilidad e impacto de los riesgos identificados.

Priorización de las medidas de mitigación en función de su efectividad y costo.

Desarrollo de un plan de acción detallado que incluya la implementación de las medidas de mitigación y los responsables de cada acción.

- **Implementación y seguimiento:**

Implementación de las medidas de mitigación definidas en el plan de acción.

Monitoreo continuo de las medidas implementadas para asegurar su efectividad.

Realización de revisiones periódicas para evaluar la eficacia de las medidas de mitigación y realizar ajustes si es necesario.

Al aplicar OCTAVE en la evaluación técnica de vulnerabilidades en ciberseguridad en laboratorios de computación, es importante tener en cuenta los principios y directrices establecidos en COBIT 2019 (Campos & León, 2020). COBIT proporciona un marco de referencia para la gestión y gobernanza de los sistemas de información, y se puede utilizar en conjunto con OCTAVE para asegurar una gestión integral de los riesgos de seguridad de la información.

OCTAVE es una metodología de evaluación de riesgos que se centra en los riesgos operativos y la gestión de riesgos de seguridad de la información (Andocilla & Fuentes, 2019). Al aplicar OCTAVE en la evaluación técnica de vulnerabilidades en ciberseguridad en laboratorios de computación, se puede identificar y evaluar los riesgos específicos asociados a los activos críticos de información y desarrollar estrategias de mitigación adecuadas. COBIT 2019 puede ser utilizado en conjunto con OCTAVE para garantizar una gestión integral de los riesgos de seguridad de la información, asegurando la alineación con los objetivos de negocio y las mejores prácticas de gestión de TI.

OCTAVE se centra en la identificación y evaluación de amenazas, activos y vulnerabilidades dentro de una organización, permitiendo a las empresas comprender mejor los riesgos asociados con sus sistemas de información y tomar medidas adecuadas para mitigarlos.

Una de las principales fortalezas de OCTAVE es su enfoque basado en riesgos. La metodología ayuda a las entidades a evidenciar y priorizar los riesgos de seguridad de una manera sistemática y estructurada. Esto permite a las empresas enfocar sus esfuerzos y recursos en las áreas más críticas y vulnerables, maximizando así el impacto de las medidas de seguridad implementadas.

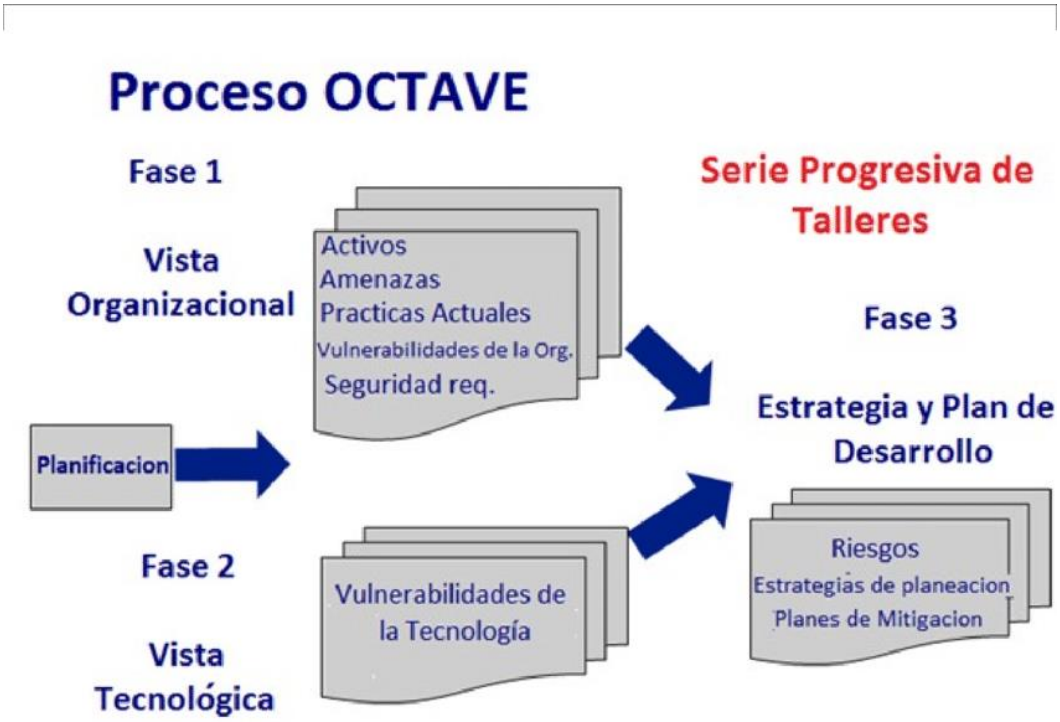
OCTAVE también se destaca por su enfoque en la gestión de riesgos operativos. La metodología no solo se centra en las amenazas externas, sino que también aborda los riesgos internos y los desafíos operativos que pueden afectar la seguridad de la información. Esto ayuda a las organizaciones a comprender los aspectos más amplios de la ciberseguridad y a tomar medidas para abordar los problemas en todas las áreas relevantes.

Además, OCTAVE promueve la colaboración y el enfoque participativo en el proceso de evaluación y gestión de riesgos. Involucra a diferentes partes interesadas dentro de la organización, como el personal de TI, los usuarios finales y los líderes empresariales,

fomentando así una comprensión compartida de los riesgos y la responsabilidad colectiva en la seguridad de la información.

En la Figura 4, se muestra un flujo normal de procesos en la metodología OCTAVE, las diferentes fases se muestran como una serie progresiva de talleres en los que se identifica las practicas actuales, riesgos y vulnerabilidades en las tecnologías e información en un objeto de evaluación técnica de ciberseguridad.

Figura 4 *Proceso OCTAVE*



Nota. Fuente: Tomado de (Dominguez, 2015)

OCTAVE ayuda a combatir los problemas de ciberseguridad al proporcionar un enfoque estructurado y sistemático para identificar, evaluar y gestionar los riesgos de seguridad de la información. Al enfocarse en los riesgos operativos, involucrar a las partes interesadas y priorizar las acciones basadas en riesgos, OCTAVE permite a las organizaciones tomar medidas

efectivas para proteger sus activos de información y mitigar los riesgos asociados con la ciberseguridad.

2.13 Marco legal

Para el desarrollo de este proyecto el Marco Legal se basa en leyes y normativas específicas, así como en marcos de referencia reconocidos a nivel internacional, para garantizar la seguridad de la información y la protección de datos personales en la universidad, entre estas podemos mencionar las siguientes:

2.13.1 Ley de Protección de Datos Personales

Esta ley establece las obligaciones de las organizaciones para proteger los datos personales de sus usuarios, incluyendo medidas de seguridad informática adecuadas para prevenir vulnerabilidades y ataques cibernéticos.

Con la Ley de Protección de Datos Personales, se busca cuidar a las personas titulares de los datos, para que ellas puedan decidir a quién entregar su información personal porque confían en los proveedores de servicios digitales. (Registrospublicos, 2021)

2.13.2 Ley Orgánica de Telecomunicaciones

Esta ley regula el uso de las tecnologías de la información y comunicación (TIC) en el país, incluyendo las medidas de seguridad informática que deben implementar las organizaciones que utilizan TIC.

Esta Ley constituye una herramienta de política pública, que promueve el desarrollo adecuado de las telecomunicaciones, bajo una visión orientada a fomentar el acceso universal a las Tecnologías de la Información y Comunicación (TIC). (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2023)

2.13.3 Normativa interna de la Universidad Técnica del Norte

La universidad cuenta con políticas, procedimientos y normas específicas para la gestión de procesos. (UTN, 2021)

2.13.4 Reglamento General a la Ley Orgánica de Telecomunicaciones

Este reglamento establece las disposiciones específicas para la aplicación de la Ley Orgánica de Telecomunicaciones en Ecuador. Incluye disposiciones relacionadas con la seguridad de la información, la protección de datos personales y la prevención de incidentes de seguridad.

2.13.5 Reglamento Especial General a la Ley Orgánica de Telecomunicaciones Para Protección de los Usuarios de Servicios de Telecomunicaciones

Este reglamento establece las disposiciones específicas para la protección de los usuarios de servicios de telecomunicaciones en Ecuador. Incluye disposiciones relacionadas con la seguridad de la información y la protección de datos personales de los usuarios.

Además de estas leyes y normativas, existen otras disposiciones y regulaciones específicas que abordan aspectos más técnicos de la ciberseguridad, como el Reglamento Técnico Ecuatoriano RTE INEN 2 (ISO/IEC 27001:2013) sobre sistemas de gestión de seguridad de la información.

CAPITULO III

3. Metodología

La metodología de investigación cuantitativa es un enfoque científico que se utiliza para recopilar, analizar e interpretar datos numéricos y estadísticos. Este método se centra en la medición objetiva y el análisis estadístico para responder preguntas de investigación.

4. Instrumentos de recopilación de información

Descripción del área de estudio

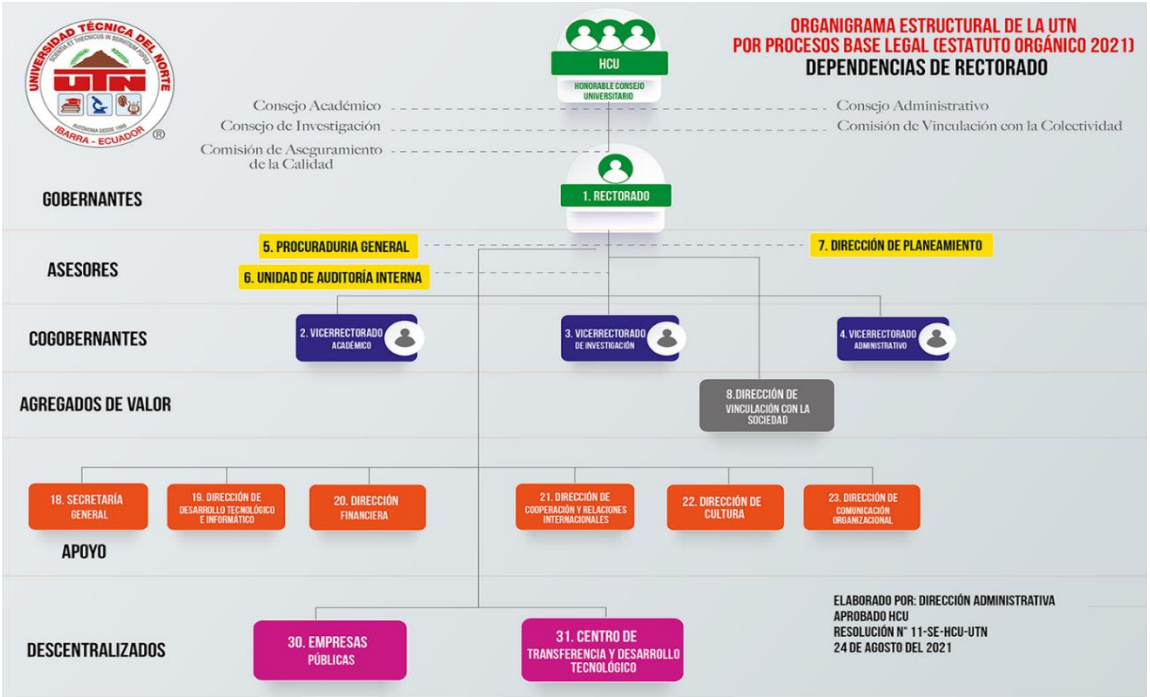
La Universidad Técnica del Norte está situada en Ibarra, la capital de la provincia de Imbabura en el Norte del Ecuador, a una altitud de aproximadamente 2.200 metros sobre el nivel del mar. La universidad cuenta con varios campus distribuidos en diferentes lugares de la ciudad, donde se imparten las diversas carreras y programas académicos. Ibarra es una ciudad de tamaño medio, con una población de alrededor de 200.000 habitantes, y cuenta con una gran infraestructura educativa, cultural y comercial. La ubicación de la Universidad Técnica del Norte en Ibarra permite a los estudiantes disfrutar de un entorno tranquilo y seguro, rodeado de hermosos paisajes naturales y con fácil acceso a servicios y comodidades.

Figura 5 *Campus principal UTN*

Nota. Fuente: Tomado de (UTN, 2023)

A continuación, en la Figura 6 se muestra la estructura organizacional de la Universidad Técnica del Norte

Figura 6 *Organigrama estructural de la UTN*



Nota. Fuente: Tomado de (UTN, 2023)

Características biofísicas y demográficas

Se encuentra ubicado en la Av. 17 de julio 5-21 y General José María Córdova, área Urbana, provincia de Imbabura, cantón de Ibarra, parroquia Sagrario, cuenta con una extensión de 91332.62. m2, 16 edificios con modernas instalaciones, equipadas con tecnología de vanguardia, cuentan con auditorios, biblioteca, centro de copias e impresión, salas de exposición, salas de cómputo, laboratorios de investigación, talleres de diseño, salas de clase, complejo acuático, canchas deportivas, cubiertos de amplias áreas verdes, acoge a más de 12.000 personas entre docentes, estudiantes y funcionarios en jornada diurna y nocturna (UTN, 2023).

Población

La población total designada para el estudio corresponde a un total de estudiantes de 306 personas que conforman la comunidad educativa de la Universidad Técnica del Norte específicamente la FACAE.

Muestra

Para la discriminación de la muestra significativa de estudio se ha utilizado un muestreo probabilístico aplicando la fórmula de muestreo se obtiene que:

$$n = \frac{NZ^2pq}{e^2(N-1) + Z^2pq}$$

Donde:

$n = Tamaño\ de\ la\ muestra$

$N = Total\ de\ la\ población$

$Z^2 = Nivel\ de\ confianza\ del\ 95\% = 1.96\ tabla\ Z$

$p = Proporción\ de\ la\ población\ con\ la\ característica\ deseada\ (éxito)$

$q = Proporción\ de\ la\ población\ \text{sin}\ la\ característica\ deseada\ (fracaso)$

$e = Nivel\ de\ error\ dispuesto\ a\ cometer$

$N = 3106$

$Z = 1{,}96$

$p = 0{,}5$

Aplicando la formula a la población obtenida para la investigación se tiene que la muestra de análisis es:

$$n = \frac{(3106) \times (1{,}96)^2 \times (0{,}5 \times 0{,}5)}{(0{,}05)^2 \times (3106 - 1) + [(1{,}96)^2 \times (0{,}5 \times 0{,}5)]}$$

$$n = 342$$

En este caso se ha determinado como 342 el número de individuos de análisis para aplicar el instrumento tipo encuesta.

Diseño y tipo de investigación

Enfoque de investigación mixto

Según Gallardo (2017) el enfoque de investigación mixto, también conocido como investigación combinada o integrada, es un enfoque metodológico que combina tanto métodos cuantitativos como cualitativos en un estudio de investigación (pág. 20). En lugar de utilizar solo uno de estos enfoques, se busca complementarlos y aprovechar sus fortalezas para obtener una comprensión más completa y profunda del fenómeno investigado.

En un enfoque de investigación mixto, se recopilan y analizan datos cuantitativos y cualitativos de manera simultánea o secuencial. Esto permite abordar preguntas de investigación complejas y explorar diferentes aspectos de un fenómeno desde múltiples perspectivas.

Los métodos cuantitativos se utilizan para recopilar datos numéricos y realizar análisis estadísticos. Estos datos se obtienen a través de encuestas, cuestionarios, mediciones objetivas u otros instrumentos estandarizados. Los métodos cualitativos, por otro lado, se utilizan para recopilar datos descriptivos y explorar las experiencias, percepciones y significados de los participantes (Chávez, 2016). Estos datos se obtienen a través de entrevistas, observaciones, análisis de documentos u otros métodos de recolección de datos cualitativos.

Después de recopilar los datos, se lleva a cabo un análisis integrado, donde se combinan los hallazgos cuantitativos y cualitativos para obtener una comprensión más completa del fenómeno investigado. Esto puede implicar la triangulación de datos, la comparación de resultados, la explicación de los hallazgos cualitativos con base en los cuantitativos, entre otros enfoques.

El enfoque de investigación mixto es especialmente útil cuando se busca profundizar en la comprensión de un fenómeno, explorar las razones detrás de una evaluación a las vulnerabilidades de ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte y sus resultados cuantitativos y cualitativos enriquecer los hallazgos obtenidos en una fase de la investigación con la otra. Además, permite abordar cuestiones de investigación más complejas y capturar la complejidad y diversidad de los fenómenos estudiados.

Investigación de tipo descriptiva

La investigación de tipo descriptiva es un enfoque utilizado en el campo de la investigación científica para describir y analizar fenómenos, eventos o situaciones tal como se presentan en la realidad (Hernández, y otros, 2018). Su objetivo principal es recopilar información detallada y precisa sobre un tema o problema específico, sin manipularlo o modificarlo.

La investigación descriptiva se centra en la recopilación de datos objetivos y verificables a través de métodos y técnicas como encuestas y observación directa para análisis de datos secundarios. Estos datos se analizan y se presentan de manera clara y concisa, utilizando herramientas estadísticas u otros métodos de análisis.

A diferencia de otros tipos de investigación, como la investigación experimental o la investigación correlacional, la investigación descriptiva no busca establecer relaciones de causa y efecto o probar hipótesis. En cambio, su objetivo es brindar una descripción completa y detallada de un fenómeno o situación, identificando características, comportamientos, opiniones o actitudes de una población o muestra específica en este caso en los laboratorios de computación de la Universidad Técnica del Norte.

Investigación de tipo explicativa

Para Cabezas, Andrade y Torres (2018) en contraste con la investigación descriptiva que se concentra en la descripción y análisis de fenómenos en su estado actual, la investigación explicativa tiene como objetivo indagar más profundamente y proporcionar respuestas a interrogantes como "¿por qué?" o "¿cómo?" se produce un fenómeno. Se basa en la identificación y análisis de variables independientes y dependientes, y busca establecer relaciones de causa y efecto entre ellas.

Para llevar a cabo una investigación explicativa, se utilizan diferentes métodos y técnicas, como experimentos controlados, estudios de caso, análisis de datos secundarios, entre otros. Estos métodos permiten manipular y controlar variables, establecer grupos de comparación y realizar análisis estadísticos o cualitativos para identificar las relaciones causales.

A través de esta investigación, se logrará obtener conocimiento más profundo y fundamentado acerca de las vulneraciones que pudieran existir en los laboratorios de computación de la Universidad Técnica del Norte, lo que puede ayudar a desarrollar intervenciones o soluciones más efectivas.

En resumen, la investigación de tipo explicativa busca comprender las causas o razones que subyacen a un fenómeno o problema específico. Su objetivo es establecer relaciones causales entre variables, y se basa en métodos y técnicas que permiten manipular y controlar variables, realizar análisis estadísticos o cualitativos y obtener un conocimiento más profundo y fundamentado.

Procedimiento de investigación

Para el desarrollo de la investigación se utilizara un desarrollo progresivo de análisis de información en fases de procesos OCTAVE, como se explicó en la fundamentación teórica la manera más recomendable de esto es utilizar la información técnicamente recolectada como un flujo que termina en una estrategia de planeación de riesgos tras la evaluación de vulnerabilidades de ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte, para ello se han implementado las siguientes fases

FASE 1 o de recopilación de información

- Vista organizacional

- Planificación de recolección de datos
- Identificación de activos críticos
- Identificación de amenazas
- Seguridad requerida
- Vulnerabilidades de la organización

FASE 2 o Vista tecnológica

- Vulnerabilidades evaluadas
- Evaluación del impacto operativos y reputacional
- Identificación de controles de seguridad

FASE 3 o Desarrollo de estrategia

- Plan de mitigación
- Estrategia de planeación

Operacionalización Variables

Figura 7 *Operacionalización de variables*

Variable cuantitativa discreta	**Definición**	**Dimensiones**	**Indicadores**	**Técnicas e instrumentos**
Vulnerabilidades en ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte	debilidades o fallos en los sistemas, aplicaciones, configuraciones de red, políticas de seguridad u otros componentes relacionados con la seguridad de la información en los laboratorios de computación. Estas vulnerabilidades representan puntos de	Evaluación de calidad Procesamiento de datos Análisis Divulgación de resultados	Tiempo Resultados Recursos	Observación directa Encuestas

	entrada o explotación para posibles amenazas o ataques cibernéticos.			
Variable cualitativa nominal	**Definición**	**Dimensiones**	**Indicadores**	**Técnicas e instrumentos**
Fenómenos detectados con metodología OCTAVE que influyen en las vulneraciones de ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte	Eventos y situaciones identificados con OCTAVE que influyen en vulneraciones de ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte. Incluyen amenazas internas y externas, debilidades en activos, brechas en controles y posibles impactos.	Procedimientos lineales Eficiencia Oportunidad de la intervención	Tiempo Resultados Recursos	Observación directa Encuestas

Nota. Fuente: Elaborado por el autor

Técnicas

4.1 Encuesta de evaluación de riesgos

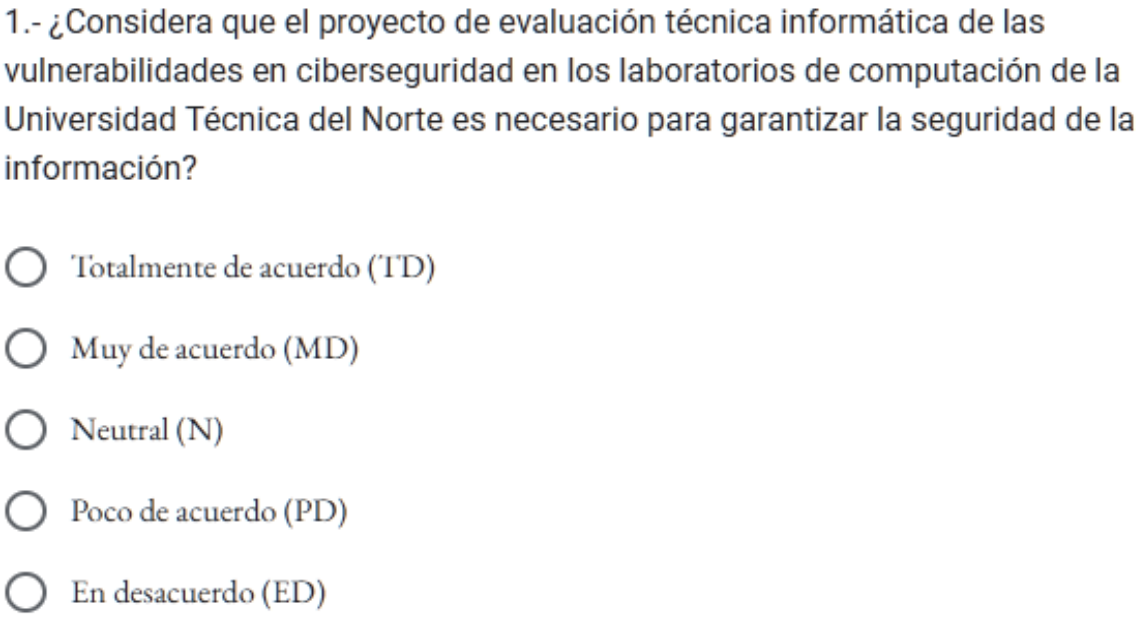
Una encuesta de evaluación de riesgos es un instrumento utilizado para recopilar información y opiniones sobre los riesgos asociados a una determinada actividad, proyecto o situación. Su objetivo principal es identificar y evaluar los riesgos, así como recopilar datos relevantes para tomar decisiones informadas y aplicar medidas de control adecuadas.

En este tipo de encuestas generalmente se incluyen una serie de preguntas relacionadas con diferentes aspectos, como los posibles riesgos identificados, su probabilidad de ocurrencia, su impacto potencial, las medidas de control existentes y la percepción de los participantes sobre la gestión de riesgos en general.

Se utilizará esta herramienta para obtener una visión general de los riesgos existentes en el laboratorio de computación de la Universidad Técnica del Norte, identificar áreas de mejora y priorizar las acciones necesarias para minimizar o mitigar los riesgos identificados. Los resultados de la encuesta pueden ayudar a desarrollar planes de acción, asignar recursos adecuados y mejorar la gestión de riesgos en general.

Es importante destacar que una encuesta de evaluación de riesgos debe ser diseñada de manera adecuada, con preguntas claras y relevantes, y debe ser aplicada a una muestra representativa de personas involucradas en el proceso o actividad evaluada en este caso la población designada corresponde al personal que opera directamente como trabajador dentro de los laboratorios.

Figura 8 *Modelo de encuesta*



2.- ¿Cree que el enfoque basado en COBIT 2019 es adecuado para abordar las vulnerabilidades en ciberseguridad en los laboratorios de computación de la universidad?

- ◯ Totalmente de acuerdo (TD)
- ◯ Muy de acuerdo (MD)
- ◯ Neutral (N)
- ◯ Poco de acuerdo (PD)
- ◯ En desacuerdo (ED)

3.- ¿Siente que el proyecto lograra identificar de manera efectiva las principales vulnerabilidades en ciberseguridad en los laboratorios de computación?

- ◯ Totalmente de acuerdo (TD)
- ◯ Muy de acuerdo (MD)
- ◯ Neutral (N)
- ◯ Poco de acuerdo (PD)
- ◯ En desacuerdo (ED)

4.- ¿Considera que las acciones propuestas en el proyecto son adecuadas para mitigar las vulnerabilidades en los principales activos críticos de información?

- ◯ Totalmente de acuerdo (TD)
- ◯ Muy de acuerdo (MD)
- ◯ Neutral (N)
- ◯ Poco de acuerdo (PD)
- ◯ En desacuerdo (ED)

5.- ¿Está de acuerdo en que que el proyecto considera como activo critico de información a los servidores y sistemas de almacenamiento de datos?

- ◯ Totalmente de acuerdo (TD)
- ◯ Muy de acuerdo (MD)
- ◯ Neutral (N)
- ◯ Poco de acuerdo (PD)
- ◯ En desacuerdo (ED)

6.- ¿Está de acuerdo en que el proyecto considera como activo critico de información a la red de comunicación y conectividad entre equipos?

- ◯ Totalmente de acuerdo (TD)
- ◯ Muy de acuerdo (MD)
- ◯ Neutral (N)
- ◯ Poco de acuerdo (PD)
- ◯ En desacuerdo (ED)

7.- ¿Está de acuerdo en que el proyecto considera como activo critico de información a los equipos informáticos y su uso dentro del laboratorio?

- ◯ Totalmente de acuerdo (TD)
- ◯ Muy de acuerdo (MD)
- ◯ Neutral (N)
- ◯ Poco de acuerdo (PD)
- ◯ En desacuerdo (ED)

8.- ¿Considera que el proyecto debe definir los requerimientos y ejecutar los procedimientos correspondientes e indicados por la institución para obtener los recursos necesarios a fin de llevar a cabo la evaluación técnica informática de las vulnerabilidades en ciberseguridad?

- ◯ Totalmente de acuerdo (TD)
- ◯ Muy de acuerdo (MD)
- ◯ Neutral (N)
- ◯ Poco de acuerdo (PD)
- ◯ En desacuerdo (ED)

Nota. Fuente: Elaborado por el autor

4.2 Ficha de observación de procesos clave y activos críticos de información

Una ficha de observación de procesos clave y activos críticos de información en un laboratorio de computación es una herramienta útil para documentar y analizar la situación actual de la seguridad de la información en el laboratorio, y para guiar la implementación de mejoras y medidas de protección adicionales.

En este caso la ficha de observación se utilizará como herramienta de descripción de trabajo de campo, teniendo un acercamiento directo del investigador con el objeto de estudio siendo este los laboratorios de computación de la Universidad Técnica del Norte.

4.3 Modelo de la ficha de observación

Criterio de observación 1: Cumplimiento de políticas y procedimientos de seguridad de la información.

Bueno ( )
Regular ( )
Malo ( )

OBSERVACIONES:

Criterio de observación 2: Existencia de controles de acceso físico y lógico en el laboratorio.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 3: Actualización de los sistemas operativos y aplicaciones en los equipos.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 4: Implementación de medidas de protección contra malware y virus

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 5: Existencia de copias de seguridad periódicas y su almacenamiento seguro.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 6: Adopción de medidas de prevención y detección de intrusos.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 7: Existencia de políticas y procedimientos para la gestión de contraseñas seguras.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 8: Uso de certificados digitales y cifrado de datos sensibles.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 9: Control y monitoreo de los registros de actividad y eventos del sistema.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 10: Implementación de medidas de prevención y respuesta ante incidentes de seguridad.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 11: Existencia de un plan de continuidad de negocio en caso de interrupciones.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 12: Uso de software y aplicaciones legítimas y licenciadas.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 13: Control y gestión de los permisos de acceso a los sistemas y recursos.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 14: Existencia de políticas y procedimientos para el manejo adecuado de la información confidencial.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 15: Implementación de medidas de seguridad física, como cámaras de seguridad y cerraduras en las instalaciones.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 16: Aplicación de políticas de uso aceptable de los recursos informáticos.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 17: Existencia de medidas de protección para la privacidad de los usuarios.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 18: Control y gestión de los dispositivos de almacenamiento externo, como unidades USB.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 19: Mantenimiento regular de los equipos informáticos y su correcto funcionamiento.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Criterio de observación 20: Existencia de un programa de concienciación y capacitación en seguridad de la información para el personal y los usuarios del laboratorio.

Bueno ( )
Regular ( )
Malo ( )
OBSERVACIONES:

Tabla 1 *Propuesta en base a ficha de observación*

<table>
<tr><th colspan="2">ACTITUDES MEJORABLES/ PROPUESTAS DE MEJORA</th></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Proponente/ Observante:
Martha Cecilia Pantoja Mejía
Aspirante a título de:
Magister en computación con mención en seguridad informática</td><td>Mando Directo autorizante:
……
Cargo:
……</td></tr>
<tr><td>Firma:

……</td><td>Firma:

……</td></tr>
</table>

Nota. Fuente: Elaborado por el autor

CAPITULO IV

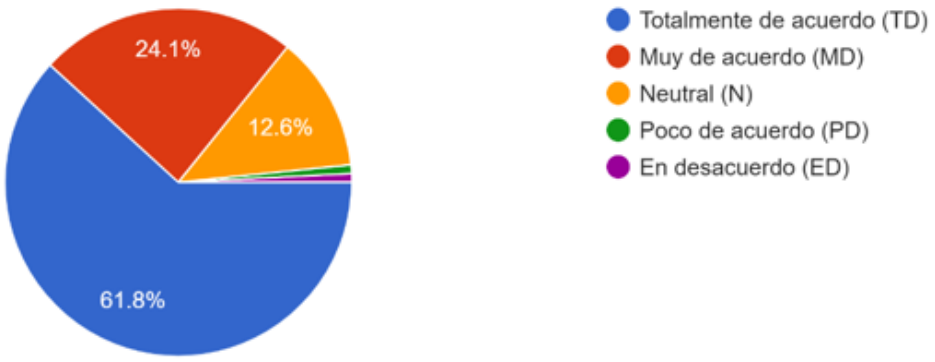
5. RESULTADOS

En este capítulo, se presentarán detalladamente los resultados obtenidos durante el curso de esta investigación, los cuales constituyen la culminación de un riguroso proceso de recopilación, análisis y síntesis de datos. Estos resultados son el producto de un extenso trabajo de campo y de laboratorio, así como de una exhaustiva revisión bibliográfica, que han permitido arrojar luz sobre las interrogantes planteadas al inicio de este estudio. A lo largo de las siguientes secciones, se analizarán en profundidad los hallazgos obtenidos, desglosando cada aspecto relevante para responder a los objetivos de la investigación. Estos resultados no solo contribuyen al avance del conocimiento en el área de estudio, sino que también ofrecen valiosas perspectivas para futuras investigaciones y aplicaciones prácticas en el campo.

5.1 Aplicación de la encuesta

Pregunta 1. ¿Considera que el proyecto de evaluación técnica informática de las vulnerabilidades en ciberseguridad en los laboratorios de c computación en la Universidad Técnica del Norte es necesario para garantizar la seguridad de la información?

Figura 9 *Resultados pregunta 1*



Elaborado por el autor

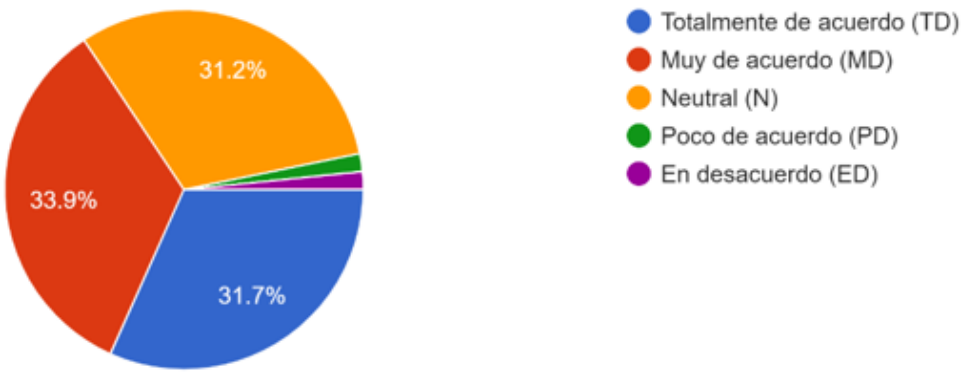
Análisis

Estos resultados indican que hay un alto nivel de conciencia entre los participantes sobre la necesidad de proteger la información en el entorno informático de la universidad. La alta tasa de acuerdo también implica que existe un entendimiento generalizado sobre la presencia de vulnerabilidades en los sistemas informáticos universitarios que necesitan ser evaluadas y corregidas, la aceptación general del proyecto indica que los participantes confían en que el enfoque propuesto para la evaluación técnica informática es sólido y efectivo. La seguridad de la información es crucial en el mundo digital actual. El acuerdo generalizado sugiere que la comunidad universitaria está preparada para hacer frente a las amenazas cibernéticas, mostrando una mentalidad proactiva hacia la seguridad.

También sugiere que el proyecto está alineado con los objetivos generales de la Universidad Técnica del Norte en cuanto a la seguridad de la información y el uso adecuado de la tecnología, y además es un fuerte apoyo y comprensión entre los participantes sobre la importancia de evaluar y abordar las vulnerabilidades en ciberseguridad en los laboratorios de computación universitarios.

Pregunta 2. ¿Cree que el enfoque basado en COBIT 2019 es adecuado para abordar las vulnerabilidades en ciberseguridad en los laboratorios de computación de la universidad?

Figura 10 *Resultados pregunta 2*



Elaborado por el autor

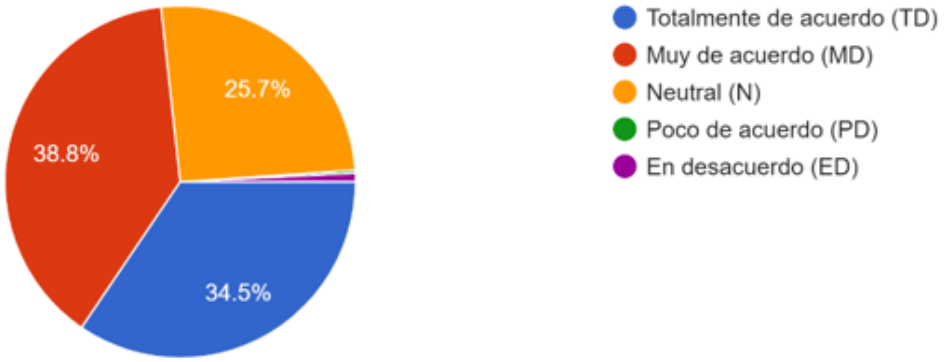
Análisis

El 31.2% de los participantes que respondieron como "neutral" señalan una falta de convicción o tal vez una falta de experiencia directa con el enfoque COBIT 2019. Esta neutralidad podría deberse a una falta de comprensión completa de COBIT 2019 o a la necesidad de más información sobre cómo se aplicaría en el contexto específico de los laboratorios de computación universitarios. La diversidad en las respuestas sugiere que existe una necesidad de mayor claridad y comunicación sobre cómo se implementará COBIT 2019 en los laboratorios de computación. Aquellos que se sienten neutrales podrían cambiar de opinión con información adicional y una comprensión más profunda de cómo este enfoque específico se traducirá en acciones concretas.

Este tipo de respuestas mixtas también podrían señalar una falta de comunicación institucional efectiva sobre la elección del enfoque COBIT 2019. Aclarar los beneficios y proporcionar orientación adicional podría ayudar a alinear las percepciones y crear un consenso más fuerte.

Pregunta 3. ¿Siente que el proyecto lograra identificar de manera efectiva las principales vulnerabilidades en ciberseguridad en los laboratorios de computación?

Figura 11 *Resultados pregunta 3*



Elaborado por el autor

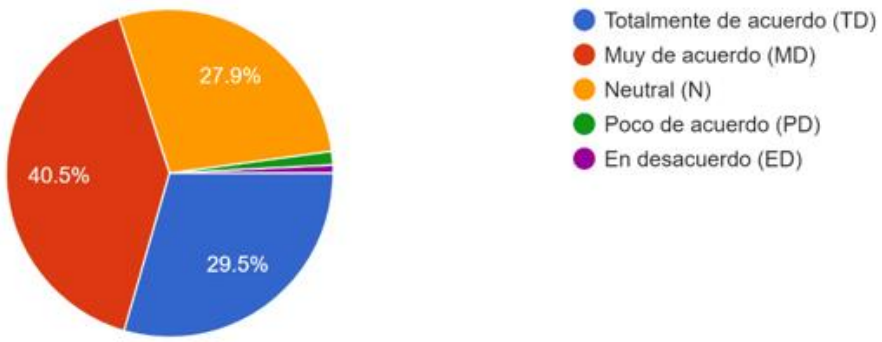
Análisis

La mayoría de los participantes 73.3%, cifra que toma en cuenta las respuestas afirmativas sugiere que están confiados en que el proyecto será efectivo para identificar las principales vulnerabilidades en ciberseguridad. Esta percepción positiva es crucial, ya que indica un alto nivel de confianza en la metodología y en el equipo que está llevando a cabo el proyecto. Además, que confían en la capacidad del proyecto para llevar a cabo una identificación exhaustiva y precisa de las vulnerabilidades. Esto implica que los métodos y herramientas utilizados son considerados adecuados y robustos.

Existe ciertas reservas o incertidumbres entre un grupo significativo de participantes. Estas reservas podrían ser el resultado de una falta de información detallada sobre el enfoque del proyecto, la metodología utilizada o las capacidades del equipo encargado. La presencia de respuestas neutrales subraya la importancia de la transparencia en el proceso y la necesidad de una comunicación clara y efectiva. Proporcionar información adicional sobre el enfoque del proyecto y los métodos utilizados podría abordar las inquietudes y aumentar la confianza de aquellos que se sienten neutrales.

Pregunta 4. ¿Considera que las acciones propuestas en el proyecto son adecuadas para mitigar las vulnerabilidades en los principales activos críticos de información?

Figura 12 *Resultados pregunta 4*



Elaborado por el autor

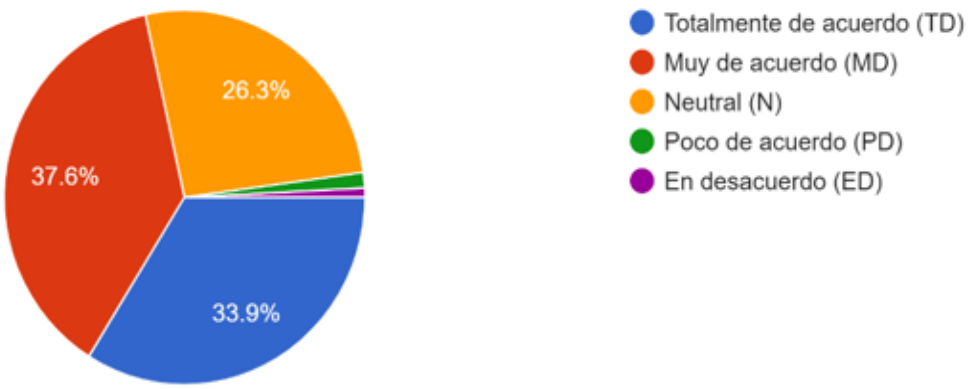
Análisis

La pregunta se enfoca específicamente en los "principales activos críticos de información", lo que implica una comprensión compartida de la importancia de estos activos para la institución. La alta aprobación de las acciones propuestas destaca la seriedad con la que se toma la protección de estos recursos vitales. el análisis revela un fuerte consenso entre los participantes sobre la idoneidad de las acciones propuestas en el proyecto para mitigar las vulnerabilidades en los activos críticos de información. Esta alta aceptación sugiere una base sólida para la implementación y un alto grado de confianza en el éxito futuro del proyecto en la protección de los valiosos recursos de información de la institución.

Esta confianza puede derivar de la creencia en la idoneidad de las soluciones propuestas, la experiencia del equipo encargado del proyecto o una combinación de ambos.

Pregunta 5. ¿Está de acuerdo en que el proyecto considera como activo critico de información a los servidores y sistemas de almacenamiento de datos?

Figura 13 *Resultados pregunta 5*



Elaborado por el autor

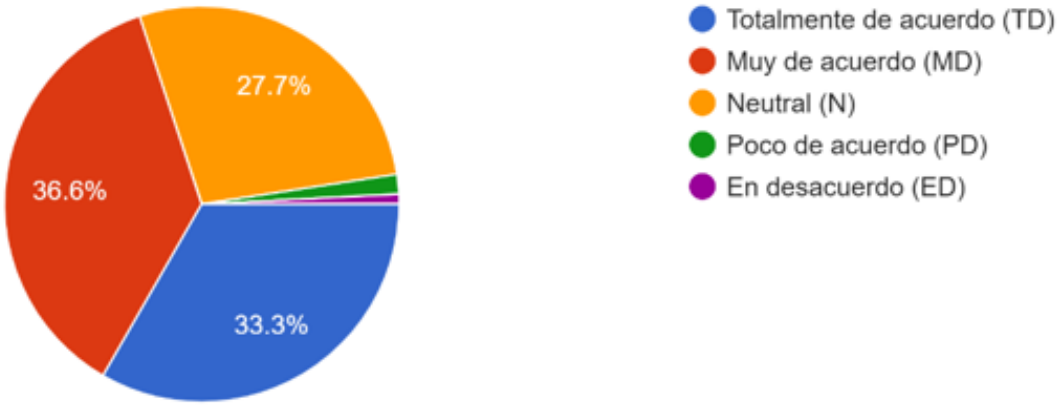
Análisis

La tasa de respuestas repartidas entre TD y MD indica que los participantes reconocen de manera generalizada que los servidores y sistemas de almacenamiento de datos son activos críticos de información. Este reconocimiento es fundamental, ya que estos sistemas son esenciales para el funcionamiento y la integridad de los datos en cualquier organización. Además de un consenso generalizado sobre la clasificación de los servidores y sistemas de almacenamiento como activos críticos. Este acuerdo puede ayudar a establecer una base sólida para las decisiones y medidas relacionadas con la seguridad de estos sistemas.

El 26.3% de respuestas neutrales podría indicar cierta falta de conocimiento o comprensión sobre cómo se clasifican los activos críticos en el contexto del proyecto. Esto subraya la importancia de la educación y la comunicación claras para asegurar que todos los participantes comprendan completamente las clasificaciones y los criterios utilizados en el proyecto.

Pregunta 6. ¿Está de acuerdo en que el proyecto considera como activo critico de información a la red de comunicación y conectividad entre equipos?

Figura 14 *Resultados pregunta 6*



Elaborado por el autor

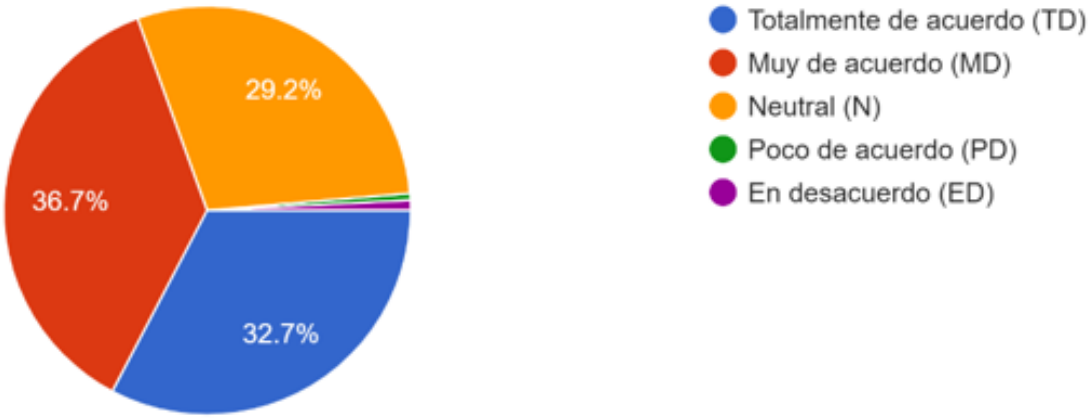
Análisis

Se puede evidenciar en estas respuestas claramente el reconocimiento la centralidad de la infraestructura de red para el funcionamiento efectivo de los sistemas informáticos y la comunicación dentro de la organización, resalta la comprensión de los participantes sobre la interconectividad de los sistemas en un entorno tecnológico moderno. Los participantes parecen entender que la seguridad de la red es fundamental para garantizar la integridad, confidencialidad y disponibilidad de la información que se transmite a través de ella.

Considerar la red de comunicación y conectividad como un activo crítico de información implica que se comprenden las implicaciones significativas que tiene la seguridad de la red en la seguridad global de la información. Los participantes reconocen que la seguridad de los datos no puede considerarse de manera aislada, sino que debe integrarse con la seguridad de la red para ser verdaderamente efectiva. Esta comprensión compartida proporciona una base sólida para las estrategias y medidas de seguridad específicas dirigidas a la red, lo que es esencial para garantizar la integridad y confidencialidad de la información en el entorno digital de la organización.

Pregunta 7. ¿Está de acuerdo en que el proyecto considera como activo critico de información a los equipos informáticos y su uso dentro del laboratorio?

Figura 15 *Resultados de la pregunta 7*



Elaborado por el autor

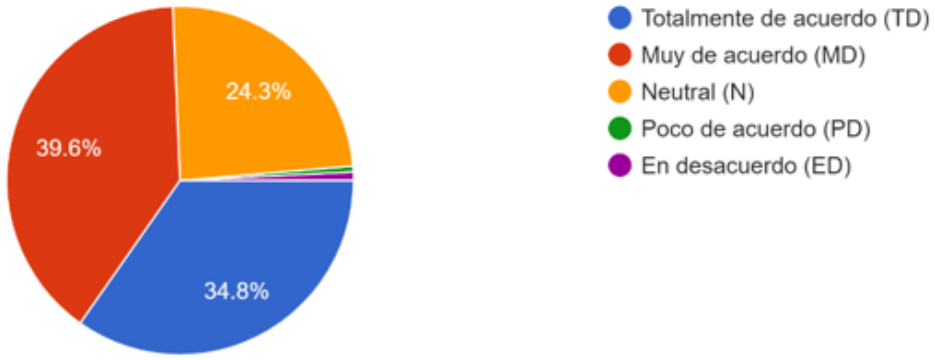
Análisis

La clasificación de los equipos informáticos como activos críticos sugiere un reconocimiento de la vulnerabilidad potencial de estos dispositivos, que son propensos a amenazas como malware, intrusiones y pérdida de datos. Este reconocimiento es esencial para tomar medidas proactivas de seguridad. A pesar de la mayoría positiva, el 29.2% de respuestas neutrales indican ciertas reservas o falta de convicción entre un grupo significativo de participantes. Estas reservas podrían deberse a una falta de información detallada sobre cómo se consideran los equipos informáticos como activos críticos o a la necesidad de más claridad sobre los criterios de clasificación utilizados en el proyecto.

Pregunta 8. ¿Considera que el proyecto debe definir los requerimientos y ejecutar los procedimientos correspondientes e indicados por la institución para obtener los recursos

necesarios a fin de llevar a cabo la evaluación técnica informática de las vulnerabilidades en ciberseguridad?

Figura 16 *Resultados pregunta 8*



Elaborado por el autor

Análisis

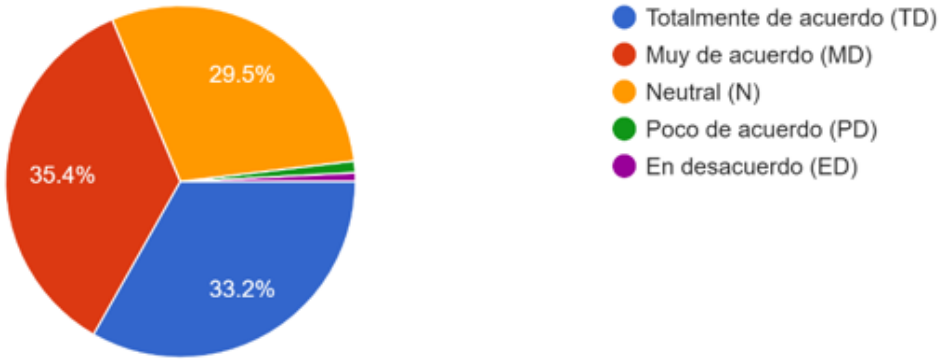
La mayoría de los participantes están de acuerdo en que los equipos informáticos y su uso en el laboratorio son activos críticos de información. Esta conciencia es esencial, ya que los equipos informáticos son herramientas fundamentales para el procesamiento, almacenamiento y transmisión seguros de información en un laboratorio. Los bajos, pero existentes porcentajes de desacuerdo podrían deberse a una falta de información detallada sobre cómo se consideran los equipos informáticos como activos críticos o a la necesidad de más claridad sobre los criterios de clasificación utilizados en el proyecto.

Aunque la mayoría de los participantes está de acuerdo en que los equipos informáticos y su uso en el laboratorio son activos críticos de información, las respuestas neutrales indican la necesidad de una comunicación más clara y una definición más precisa de lo que constituye un "activo crítico". La transparencia y la claridad en la comunicación podrían aumentar la confianza y la comprensión entre los participantes, asegurando así un entendimiento común y

un respaldo sólido para las medidas de seguridad relacionadas con los equipos informáticos en el laboratorio.

Pregunta 9. ¿Puede afirmar que el proyecto tendrá un impacto positivo en la seguridad de la información en los laboratorios de computación de la Universidad Técnica del Norte?

Figura 17 *Resultados pregunta 9*



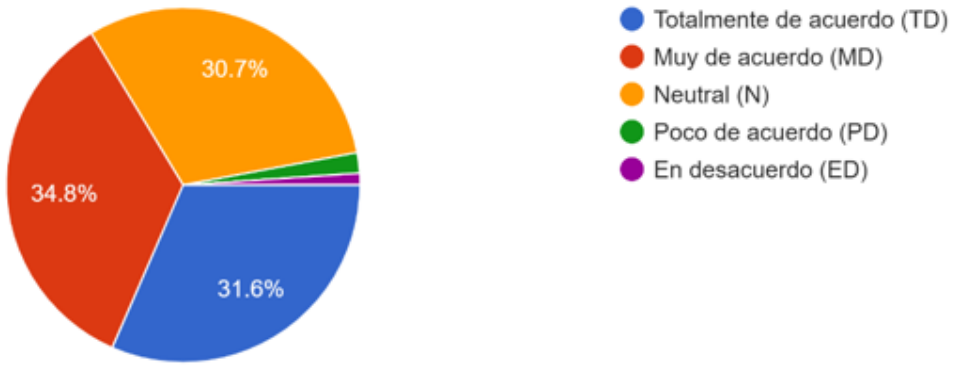
Elaborado por el autor

Análisis

Aunque la mayoría de los participantes muestra cierto grado de confianza en que el proyecto tendrá un impacto positivo en la seguridad de la información en los laboratorios de computación, las respuestas neutrales indican la necesidad de proporcionar información adicional y una comunicación transparente para abordar las preocupaciones y asegurar el respaldo completo del proyecto. Es crucial brindar detalles claros sobre las estrategias y los métodos de evaluación del impacto para aumentar la confianza y el apoyo de todos los participantes.

Pregunta 10. ¿Estaría dispuesto a recomendar las evaluaciones técnicas informáticas de vulnerabilidades en ciberseguridad en los laboratorios de computación de la universidad en el futuro basadas en COBIT 2019?

Figura 18 *Resultados de la pregunta 10*



Elaborado por el autor

Análisis

Estas respuestas pueden ser el resultado de la falta de familiaridad con COBIT 2019 o la necesidad de más información sobre cómo se aplicará en el contexto específico de los laboratorios de computación. Sin embargo, indica que una parte significativa de los participantes estaría dispuesta a recomendar las evaluaciones técnicas informáticas de vulnerabilidades basadas en COBIT 2019 en el futuro. Esto sugiere una confianza considerable en la eficacia y utilidad de COBIT 2019 como marco de referencia para las evaluaciones de ciberseguridad.

Aplicación de la ficha de observación

Esta ficha de observación se elaboró en contacto directo con los laboratoristas intentando ser lo más objetivo posible en la identificación de activos críticos de información y características que pueden ser mejorables en las dinámicas de comportamiento del uso y resguardo de información en los laboratorios de computación.

Criterio de observación 1: Cumplimiento de políticas y procedimientos de seguridad de la información.

Bueno (X)
Regular ( )
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 2: Existencia de controles de acceso físico y lógico en el laboratorio.

Bueno ( )
Regular (X)
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 3: Actualización de los sistemas operativos y aplicaciones en los equipos.

Bueno (X)
Regular ( )
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 4: Implementación de medidas de protección contra malware y virus

Bueno ( )
Regular (X)
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 5: Existencia de copias de seguridad periódicas y su almacenamiento seguro.

Bueno ( )
Regular ( )
Malo (X)
OBSERVACIONES: Se recomienda urgentemente implementar un sistema de copias de seguridad regular y seguro para garantizar la integridad y disponibilidad de los datos en caso de cualquier eventualidad.

Criterio de observación 6: Adopción de medidas de prevención y detección de intrusos.

Bueno ( )
Regular ( )
Malo (X)
OBSERVACIONES: La falta de una sólida infraestructura para prevenir y detectar intrusos pone en peligro la integridad, confidencialidad y disponibilidad de los datos críticos. Además, aumenta significativamente el riesgo de robo de información sensible, interrupción de riesgo de robo de información sensible, interrupción de servicios y daño a la reputación institucional.

Criterio de observación 7: Existencia de políticas y procedimientos para la gestión de contraseñas seguras.

Bueno ( )
Regular (X)
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 8: Uso de certificados digitales y cifrado de datos sensibles.

Bueno ( )
Regular (X)
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 9: Control y monitoreo de los registros de actividad y eventos del sistema.

Bueno (X)
Regular ( )
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 10: Implementación de medidas de prevención y respuesta ante incidentes de seguridad.

Bueno ( )
Regular (X)
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 11: Existencia de un plan de continuidad de negocio en caso de interrupciones.

Bueno ( )
Regular ( )
Malo (X)
OBSERVACIONES: Se recomienda desarrollar e implementar un plan de continuidad de negocio sólido que incluya estrategias para mantener operaciones esenciales, proteger datos críticos, y minimizar el tiempo de inactividad en caso de interrupciones.

Criterio de observación 12: Uso de software y aplicaciones legítimas y licenciadas.

Bueno ( )
Regular (X)
Malo ( )
OBSERVACIONES: Sin observaciones

Criterio de observación 13: Control y gestión de los permisos de acceso a los sistemas y recursos.

Bueno ( )
Regular (X)
Malo ( )
OBSERVACIONES:

Criterio de observación 14: Existencia de políticas y procedimientos para el manejo adecuado de la información confidencial.

Bueno (X)
Regular ( )
Malo ( )

OBSERVACIONES: Sin observaciones

Criterio de observación 15: Implementación de medidas de seguridad física, como cámaras de seguridad y cerraduras en las instalaciones.

Bueno ( )
Regular (X)
Malo ( )

OBSERVACIONES: Sin observaciones

Criterio de observación 16: Aplicación de políticas de uso aceptable de los recursos informáticos.

Bueno ( )
Regular (X)
Malo ( )

OBSERVACIONES: Sin observaciones

Criterio de observación 17: Existencia de medidas de protección para la privacidad de los usuarios.

Bueno ( )
Regular (X)
Malo ( )

OBSERVACIONES: Sin observaciones

Criterio de observación 18: Control y gestión de los dispositivos de almacenamiento externo, como unidades USB.

Bueno (X)
Regular ( )
Malo ( )

OBSERVACIONES: Sin observaciones

Criterio de observación 19: Mantenimiento regular de los equipos informáticos y su correcto funcionamiento.

Bueno (X)
Regular ( )
Malo ( )

OBSERVACIONES: Sin observaciones

Criterio de observación 20: Existencia de un programa de concienciación y capacitación en seguridad de la información para el personal y los usuarios del laboratorio.

Bueno ( )
Regular ( )
Malo (X)

OBSERVACIONES: La implementación efectiva no solo fortalecerá la postura de seguridad del laboratorio, sino que también fomentará una cultura de seguridad cibernética entre el personal y los usuarios, reduciendo así el riesgo de violaciones y pérdidas de datos.

Tabla 2 *Actividades propuestas para la ficha de observación aplicada*

<table>
<tr><th colspan="2">ACTITUDES MEJORABLES/ PROPUESTAS DE MEJORA</th></tr>
<tr><td colspan="2">Se recomienda desarrollar e implementar un programa de concienciación y capacitación en seguridad de la información que eduque a los empleados y usuarios sobre las mejores prácticas de seguridad, las amenazas comunes y cómo reconocer y evitar situaciones de riesgo. Además, este programa debería ser continuo y estar alineado con las últimas tendencias en ciberseguridad para mantener a todos los involucrados actualizados y alerta frente a las amenazas emergentes.

Se recomienda llevar a cabo una revisión exhaustiva de las políticas y prácticas de privacidad existentes. Esto debería incluir una evaluación de la conformidad con las regulaciones y leyes de privacidad pertinentes, así como la identificación y mitigación de posibles vulnerabilidades en la protección de datos. Además, es crucial proporcionar una formación continua al personal para garantizar que estén completamente informados sobre las mejores prácticas de privacidad y que estén al tanto de las amenazas y tácticas de ingeniería social que podrían comprometer la privacidad de los usuarios.</td></tr>
<tr><td>Proponente/ Observante:

Martha Cecilia Pantoja Mejía

Aspirante a título de:

Magister en computación con mención en seguridad informática</td><td>Mando Directo autorizante:

…….

Cargo:

…….</td></tr>
<tr><td>Firma:

……</td><td>Firma:

…….</td></tr>
</table>

5.2 Plan de gestión de seguridad informática

5.2.1 Informe de recomendaciones

Este informe presenta una serie de recomendaciones destinadas a mejorar la seguridad de la información en el laboratorio. Las recomendaciones se basan en la revisión exhaustiva de

las prácticas actuales y están diseñadas para fortalecer la postura de seguridad del laboratorio y mitigar los riesgos asociados con la gestión de datos críticos.

Programa de Concienciación y Capacitación en Seguridad Informática

Se recomienda desarrollar e implementar un programa de concienciación y capacitación en seguridad de la información. Este programa debe educar a los empleados y usuarios sobre las mejores prácticas de seguridad, las amenazas comunes y cómo reconocer y evitar situaciones de riesgo. Además, el programa debe ser continuo y estar alineado con las últimas tendencias en ciberseguridad para mantener a todos actualizados y alerta frente a las amenazas emergentes.

Revisión Exhaustiva de Políticas y Prácticas de Privacidad

Es esencial llevar a cabo una revisión completa de las políticas y prácticas de privacidad existentes. Esta revisión debe incluir una evaluación de la conformidad con las regulaciones y leyes de privacidad pertinentes, así como la identificación y mitigación de posibles vulnerabilidades en la protección de datos. Además, se debe proporcionar una formación continua al personal para garantizar que estén completamente informados sobre las mejores prácticas de privacidad y estén al tanto de las amenazas y tácticas de ingeniería social que podrían comprometer la privacidad de los usuarios.

Desarrollo e Implementación de un Plan de Continuidad de Negocio

Se recomienda desarrollar e implementar un plan de continuidad de negocio sólido que incluya estrategias para mantener operaciones esenciales, proteger datos críticos y minimizar el tiempo de inactividad en caso de interrupciones. Este plan debe ser detallado, incluyendo un cronograma, responsabilidades claras y recursos necesarios para garantizar una respuesta efectiva ante cualquier eventualidad.

Mejora en la Prevención y Detección de Intrusos

Es crucial implementar medidas de prevención y detección de intrusos efectivas. La falta de una sólida infraestructura para prevenir y detectar intrusos pone en peligro la integridad, confidencialidad y disponibilidad de los datos críticos. Además, aumenta significativamente el riesgo de robo de información sensible, interrupción de servicios y daño a la reputación institucional. Se recomienda invertir en tecnologías y herramientas de seguridad avanzadas para proteger el sistema contra amenazas cibernéticas.

Implementación de Copias de Seguridad Regulares y Seguras

Se urge la implementación de un sistema de copias de seguridad regular y seguro para garantizar la integridad y disponibilidad de los datos en caso de cualquier eventualidad. Las copias de seguridad deben ser periódicas y almacenadas en ubicaciones seguras, preferiblemente fuera del sitio, para proteger los datos contra pérdidas debidas a desastres naturales o ataques cibernéticos.

5.3 Política de seguridad

La Universidad Técnica del Norte reconoce la importancia de la seguridad informática para garantizar la confidencialidad, integridad y disponibilidad de la información en el laboratorio de computación. Esta política establece las directrices y los procedimientos para proteger los sistemas, datos y recursos del laboratorio contra amenazas cibernéticas y garantizar un entorno seguro para todos los usuarios.

5.3.1 Objetivos

- Proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos del laboratorio.
- Prevenir y mitigar las amenazas cibernéticas, incluyendo ataques de malware, phishing y acceso no autorizado.

- Garantizar el cumplimiento de las leyes y regulaciones de privacidad de datos aplicables.
- Fomentar una cultura de seguridad cibernética entre los empleados y usuarios del laboratorio.

5.3.2 Responsabilidades

Autenticación y Autorización: Se utilizarán prácticas de autenticación fuerte para el acceso a sistemas y datos sensibles. Los usuarios tendrán autorizaciones basadas en sus roles y responsabilidades.

Actualizaciones y Parches: Todos los sistemas y software se mantendrán actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.

Copia de Seguridad: Se realizarán copias de seguridad periódicas de los datos, y estas copias se almacenarán de forma segura fuera del sitio para garantizar la recuperación en caso de pérdida de datos.

Firewalls y Antivirus: Se implementarán firewalls y software antivirus actualizado en todos los sistemas para proteger contra amenazas externas e internas.

Monitoreo y Detección de Intrusos: Se establecerán sistemas de monitoreo continuo para detectar y responder a actividades inusuales en la red o en los sistemas del laboratorio.

5.3.3 Educación y concientización

- Se llevarán a cabo programas regulares de formación y concientización sobre seguridad informática para empleados y usuarios.
- Se proporcionará información sobre las últimas amenazas y técnicas de seguridad para mantener a todos informados y alerta.

5.3.4 Cumplimiento y auditoria

- Se realizarán auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad.
- Se tomarán medidas correctivas inmediatas en caso de violaciones de seguridad o incumplimiento de las políticas.

5.3.5 Revisión y actualización

Esta política será revisada anualmente y actualizada según sea necesario para adaptarse a las nuevas amenazas y tecnologías emergentes.

Esta política de seguridad informática tiene como objetivo proporcionar un entorno de laboratorio de computación seguro y protegido para todos los usuarios. El cumplimiento de estas directrices es obligatorio y cualquier violación será tratada con seriedad, sujeta a las acciones disciplinarias correspondientes.

Tabla 3 *Diseño de aplicabilidad de objetivos y ocurrencia de amenazas para PLAN DE SEGURIDAD*

Tipo de Activo	**Amenaza**	**Probabilidad de ocurrencia**	**Objetivos de Control en base ISO 27001**
Hardware	Robo o pérdida física del hardware Ataque de ingeniería social Ataques físicos Fallo del Hardware Dispositivos USB maliciosos	Alta Baja Baja Alta Alta	Garantizar que el hardware de la organización se mantenga seguro contra el robo o pérdida física, reduciendo así el riesgo de acceso no autorizado a la información almacenada en estos dispositivos. Proteger al personal contra los engaños de ingeniería social, educándolos y promoviendo la conciencia sobre las tácticas y técnicas utilizadas por los atacantes. Garantizar que el hardware esté protegido contra daños físicos intencionados o accidentales, asegurando la continuidad operativa. Establecer procedimientos para identificar, mitigar y recuperarse de fallos de hardware para minimizar la interrupción de servicios y la pérdida de datos. Prevenir la introducción de malware a través de dispositivos USB, protegiendo así los sistemas y la información contra amenazas externas.

Software	Malware y Virus Ataques de Denegación de Servicio (DoS) y Distribuidos (DDoS) Inyección de Código Fugas de Información (Data Leakage) Errores y Vulnerabilidades de Desarrollo	Alta Baja Media Baja Baja	Garantizar que el software esté protegido contra malware y virus, minimizando el riesgo de infección y los impactos asociados. Minimizar la interrupción del servicio causada por ataques DoS y DDoS, manteniendo la disponibilidad de los servicios y sistemas. Evitar la inyección de código malicioso en aplicaciones y bases de datos, asegurando la integridad y la confidencialidad del software. Evitar la fuga de información confidencial fuera de la organización, asegurando que los datos estén protegidos adecuadamente. Identificar, mitigar y gestionar errores y vulnerabilidades en el desarrollo del software para prevenir el acceso no autorizado y proteger la integridad del sistema.
Redes de comunicación	Ataques de Intercepción de Datos Suplantación de Identidad (Spoofing) Ataques de Ransomware	Alta Alta Baja	Garantizar la confidencialidad de los datos en tránsito al prevenir y detectar ataques de intercepción de datos en la red de comunicación del laboratorio de computación. Prevenir la suplantación de identidad para garantizar la autenticidad de los dispositivos y usuarios en la red de comunicación. Prevenir la infección por ransomware y minimizar el impacto en caso de un ataque para proteger los sistemas y datos.

Nota. Fuente: Elaborado por el autor

Tabla 4 *Modelo de control y seguimiento Plan de Seguridad Informática*

Objetivo de control	**Nombre del indicador**	**Métrica de medición**	**Frecuencia de medición**
Garantizar que el hardware de la organización se mantenga seguro contra el robo o pérdida física, reduciendo así el riesgo de acceso no autorizado a la información almacenada en estos dispositivos.	Seguridad Física del Hardware	(Número de dispositivos de hardware seguros / Total de dispositivos de hardware) * 100	Mensual
Proteger al personal contra los engaños de ingeniería social, educándolos y promoviendo la conciencia sobre las tácticas y técnicas utilizadas por los atacantes.	Concienciación sobre Ingeniería Social	(Número de empleados que participaron en programas de concienciación / Total de empleados) * 100	Mensual

Garantizar que el hardware esté protegido contra daños físicos intencionados o accidentales, asegurando la continuidad operativa.	Continuidad operativa del Hardware	Suma del tiempo de recuperación de cada fallo de hardware / Número de fallos de hardware	Semanal
Establecer procedimientos para identificar, mitigar y recuperarse de fallos de hardware para minimizar la interrupción de servicios y la pérdida de datos.	Continuidad operativa del Hardware	Suma del tiempo de recuperación de cada fallo de hardware / Número de fallos de hardware	Diario
Prevenir la introducción de malware a través de dispositivos USB, protegiendo así los sistemas y la información contra amenazas externas.	Prevención de introducción de Malware a través de Dispositivos USB	Número total de incidentes de malware desde dispositivos USB	Diario

Garantizar que el software esté protegido contra malware y virus, minimizando el riesgo de infección y los impactos asociados.	Protección contra Malware y Virus	(Número de sistemas escaneados con malware detectado / Total de sistemas escaneados) * 100	Semanal
Minimizar la interrupción del servicio causada por ataques DoS y DDoS, manteniendo la disponibilidad de los servicios y sistemas.	Disponibilidad del Servicio frente a ataques DoS y DDoS	((Tiempo de disponibilidad del servicio durante ataques / Duración total del ataque) * 100	Semanal
Evitar la inyección de código malicioso en aplicaciones y bases de datos, asegurando la integridad y la confidencialidad del software.	Integridad del Código de Software	Número total de vulnerabilidades de inyección de código reportadas	Mensual
Evitar la fuga de información confidencial fuera de la organización, asegurando que los datos estén protegidos adecuadamente.	Prevención de Fugas de Información	Número total de incidentes de fuga de información	Mensual

Identificar, mitigar y gestionar errores y vulnerabilidades en el desarrollo del software para prevenir el acceso no autorizado y proteger la integridad del sistema.	Gestión de Vulnerabilidades en el Desarrollo de Software	(Suma del tiempo tomado para resolver cada vulnerabilidad / Número total de vulnerabilidades)	Diario
Garantizar la confidencialidad de los datos en tránsito al prevenir y detectar ataques de intercepción de datos en la red de comunicación del laboratorio de computación.	Confidencialidad de los datos en transito	(Tráfico de red cifrado / Total de tráfico de red) * 100	Diario
Prevenir la suplantación de identidad para garantizar la autenticidad de los dispositivos y usuarios en la red de comunicación.	Autenticidad en la red de comunicación	(Número de autenticaciones exitosas / Total de intentos de autenticación) * 100	Mensual
Prevenir la infección por ransomware y minimizar el impacto en caso de un ataque para proteger los sistemas y datos.	Prevención y Mitigación del Ransomware	Tiempo necesario para recuperar los sistemas después de un ataque de ransomware	Semanal

Nota. Fuente: Elaborado por el autor

5.4 Mecanismos de control

Seguridad Física del Hardware

Control de Acceso Físico: Implementar sistemas de control de acceso, como tarjetas de proximidad o biometría, para restringir el acceso a áreas donde se encuentran los dispositivos de hardware.

Inventario de Hardware: Mantener un inventario actualizado de todo el hardware de la organización para facilitar la monitorización y la gestión.

Cerraduras y Cámaras de Seguridad: Utilizar cerraduras en gabinetes y salas de servidores, además de cámaras de seguridad para supervisar áreas de acceso restringido.

Concienciación sobre ingeniería social

Programas de Formación: Implementar programas de formación y concienciación regulares para educar a los empleados sobre las tácticas de ingeniería social y cómo reconocer y evitar posibles amenazas.

Simulacros de Phishing: Realizar simulacros de ataques de phishing para evaluar la capacidad de los empleados para identificar correos electrónicos y mensajes sospechosos.

Continuidad operativa del Hardware

Backup y Recuperación: Establecer procedimientos de backup regulares y realizar pruebas periódicas para asegurar la integridad de los datos y la capacidad de recuperación.

Plan de Contingencia: Desarrollar un plan de contingencia que incluya procesos claros para la sustitución rápida de hardware en caso de fallos inesperados.

Prevención de la Introducción de Malware a través de Dispositivos USB

Restricciones de Uso: Limitar el uso de dispositivos USB y aplicar políticas que permitan únicamente dispositivos autorizados y seguros.

Escaneo Automático: Implementar sistemas de escaneo automático para dispositivos USB cuando se conectan a cualquier computadora en la red.

Protección contra Malware y Virus

Antivirus y Antimalware: Utilizar soluciones antivirus y antimalware actualizadas en todos los sistemas y dispositivos.

Firewalls: Configurar firewalls para bloquear tráfico sospechoso y prevenir intrusiones de malware.

Disponibilidad del servicio frente a ataques DoS y DDoS

Filtrado de Tráfico: Implementar soluciones de filtrado de tráfico para identificar y bloquear patrones de tráfico maliciosos asociados con ataques DoS y DDoS.

Servicios de Mitigación: Contratar servicios de mitigación de DDoS proporcionados por proveedores especializados.

Integridad del código de software

Pruebas de Seguridad del Software: Realizar pruebas de seguridad del software para identificar y corregir vulnerabilidades de código.

Control de Versiones Seguro: Implementar sistemas de control de versiones seguros para evitar modificaciones no autorizadas del código fuente.

Prevención de fugas de información

Políticas de Privacidad: Establecer políticas de privacidad claras y educar a los empleados sobre cómo manejar y proteger la información confidencial.

Prevención de Copia y Pegado: Implementar medidas para prevenir la copia y pegado de datos sensibles fuera de aplicaciones seguras.

Gestión de vulnerabilidades en el desarrollo de software

Revisión de Código: Implementar revisiones de código regulares por pares para identificar posibles vulnerabilidades.

Parches y Actualizaciones: Establecer un proceso para aplicar parches y actualizaciones de seguridad tan pronto como estén disponibles.

Confidencialidad de los datos en tránsito:

Cifrado de Datos: Utilizar protocolos de cifrados seguros, como SSL/TLS, para proteger los datos en tránsito durante la comunicación en redes públicas o internas.

Autenticidad de la red

Autenticación Fuerte: Implementar autenticación de dos factores (2FA) para asegurar la autenticidad de los usuarios y dispositivos que acceden a la red.

Prevención y mitigación

Filtrado de Correos Electrónicos: Configurar filtros de correo electrónico para bloquear correos electrónicos de phishing y mensajes con enlaces o archivos adjuntos.

5.5 Monitorización e implementación de mejoras

Para garantizar un entorno seguro, se ha implementado un riguroso plan de seguridad informática que incluye la monitorización constante de las redes, sistemas y dispositivos. Mediante herramientas avanzadas de detección y análisis, se supervisan activamente las actividades de la red para identificar posibles amenazas y vulnerabilidades en tiempo real. Además, se ha establecido un proceso continuo de evaluación y mejora, donde se analizan regularmente los incidentes de seguridad, se realizan auditorías de sistemas y se evalúan las políticas de seguridad existentes. Las mejoras se implementan de manera proactiva en respuesta a las lecciones aprendidas de los incidentes anteriores y las últimas tendencias en ciberseguridad. Esta estrategia integral no solo asegura la integridad, confidencialidad y disponibilidad de los datos, sino que también promueve una cultura de concienciación y responsabilidad en toda la comunidad del laboratorio, preparándolos para enfrentar los desafíos cambiantes del ciberespacio con resiliencia y determinación.

5.6 Flujo de control de plan de seguridad informática

Concienciación sobre Ingeniería Social

Este paso implica educar a los usuarios y empleados sobre las tácticas de ingeniería social utilizadas por los ciberdelincuentes para manipular a las personas y obtener información confidencial. Se pueden organizar sesiones de capacitación y talleres para empleados, destacando ejemplos de ataques de ingeniería social, enseñando cómo identificarlos y fomentando un ambiente en el que los empleados se sientan seguros al informar posibles intentos de ingeniería social.

Continuidad Operativa del Hardware

Implementar redundancia en los sistemas críticos, utilizar tecnologías RAID para la redundancia de datos, realizar mantenimientos regulares para prevenir fallos inesperados y tener un plan de recuperación ante desastres para restaurar los sistemas rápidamente en caso de fallas graves.

Prevención de la Introducción de Malware a través de Dispositivos USB

Implementar políticas que restrinjan el uso de dispositivos USB no autorizados, utilizar software de seguridad que escanee dispositivos USB en busca de malware automáticamente al conectarse y educar a los empleados sobre los riesgos asociados con el uso de dispositivos USB no seguros.

Protección contra Malware y Virus

Utilizar software antivirus y antimalware actualizado, realizar análisis regulares en todos los dispositivos, configurar firewalls para bloquear conexiones maliciosas y mantener el sistema operativo y las aplicaciones actualizadas para cerrar posibles vulnerabilidades.

Disponibilidad del Servicio Frente a Ataques DoS y DDoS

Utilizar servicios anti-DDoS, configurar firewalls para bloquear tráfico malicioso, utilizar servicios de mitigación DDoS proporcionados por proveedores de servicios y mantener una red de respaldo para redirigir el tráfico durante un ataque.

Integridad del Código del Software

Reconocer firmas digitales para verificar la autenticidad del código, utilizar control de versiones para rastrear cambios en el código y realizar auditorías regulares de código para identificar posibles vulnerabilidades.

Prevención de Fugas de Información

Políticas de control de acceso, utilizar tecnologías de cifrado para proteger datos confidenciales, establecer políticas claras sobre el intercambio de información y monitorizar el tráfico de red en busca de posibles fugas de datos.

Confidencialidad de los Datos en Tránsito

En base a decisión de protocolos de cifrados seguros como SSL/TLS para las comunicaciones en línea, implementar VPNs (Redes Privadas Virtuales) para conexiones seguras y utilizar firewalls para bloquear tráfico no deseado.

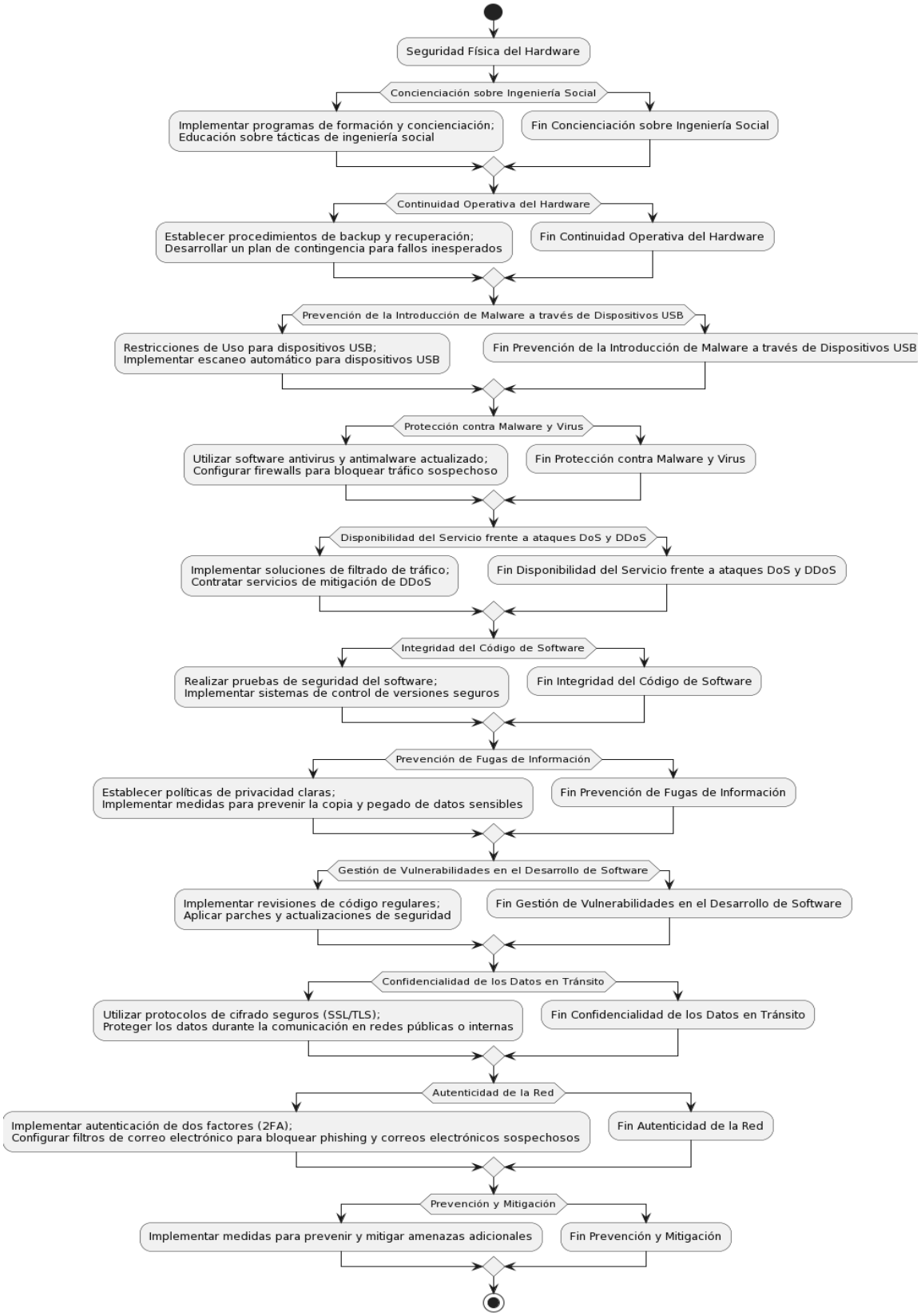
Autenticidad de la Red

Decidir sobre uso de tecnologías de autenticación para redes cableadas e inalámbricas, utilizar certificados digitales para autenticar servidores y dispositivos de red, y configurar firewalls para bloquear conexiones no autorizadas.

Prevención y Mitigación

Realizar pruebas de penetración y evaluaciones de vulnerabilidad regularmente, tener un plan de respuesta a incidentes para actuar rápidamente en caso de un ataque y colaborar con organismos de seguridad

Figura 19 *Flujo de control de Plan de Seguridad Informática*



Nota. Fuente: Elaborado por el autor

CAPITULO V

6. CONCLUSIONES

Se logra concluir que, se llevó a cabo una evaluación exhaustiva de las vulnerabilidades presentes en los laboratorios de computación de la Universidad Técnica del Norte. Utilizando el marco COBIT 2019, se identificaron áreas de mejora y se implementaron estrategias para fortalecer la seguridad informática. Este proceso no solo nos permitió detectar posibles brechas de seguridad, sino que también sentó las bases para un entorno más seguro y resistente a las amenazas cibernéticas. La identificación de activos de información críticos fue fundamental para entender el panorama de riesgos. Al categorizar y evaluar estos activos, pudimos asignar medidas de protección adecuadas. Implementamos protocolos de seguridad robustos para asegurar que estos activos estén resguardados de manera efectiva, garantizando así la confidencialidad, integridad y disponibilidad de la información sensible.

La fase de análisis se centró en evaluar los controles de ciberseguridad en los laboratorios. Siguiendo la norma ISO/IEC 27001:2022, examinamos en detalle los procesos de control, identificando áreas de eficacia y posibles lagunas. Las auditorías internas permitieron ajustar los controles existentes y establecer nuevos protocolos para mejorar la gestión de riesgos y garantizar un ambiente más seguro.

Se generó un informe detallado que proporciona recomendaciones específicas basadas en las buenas prácticas de COBIT 2019. Estas recomendaciones son acciones concretas y realistas que apuntan a fortalecer la ciberseguridad en los laboratorios. Cada recomendación se respalda con análisis detallados y se presenta con un plan de implementación, asegurando así su viabilidad y relevancia para el contexto. Las recomendaciones de controles fueron sometidas a una evaluación preliminar para medir su efectividad y aplicabilidad. A través de pruebas piloto y simulaciones, pudimos validar la eficacia de las medidas propuestas. Este proceso nos

permitió realizar ajustes finos, asegurando que las recomendaciones sean prácticas y estén preparadas para su implementación en toda la infraestructura de los laboratorios de computación.

Los resultados de la encuesta de satisfacción revelan un panorama mayoritariamente positivo en relación con las iniciativas implementadas en nuestro programa de seguridad informática. Los datos recopilados destacan una comprensión generalizada por parte de los usuarios sobre las prácticas de seguridad, así como un reconocimiento de los esfuerzos dedicados a mantener un entorno digital seguro y protegido. La percepción positiva sobre la gestión de activos críticos y las auditorías internas siguiendo estándares como ISO/IEC 27001:2022 es indicativa de la efectividad de las políticas y controles planteados, no obstante no se debe pasar por alto las áreas donde hay margen para mejorar, y las sugerencias proporcionadas por los encuestados serán invaluablemente consideradas para fortalecer aún más la postura de seguridad.

En conclusión, es fundamental destacar que cada fase de este proyecto no solo ha mejorado significativamente el marco de ciberseguridad en los laboratorios universitarios, sino que también ha sentado las bases para una cultura duradera y adaptable de seguridad de la información en la Universidad Técnica del Norte. La importancia de este logro no puede ser subestimada, especialmente en una era de evolución digital constante.

La necesidad de una vigilancia continua y de una mejora constante en las prácticas de ciberseguridad es fundamental en nuestro siempre cambiante panorama digital. Es este enfoque de pensamiento proactivo el que permitirá a la universidad mantenerse resiliente ante las amenazas emergentes y los cambios tecnológicos. Al adoptar esta cultura de adaptabilidad y mantener un compromiso sólido con la mejora de la ciberseguridad, la universidad está mejor

preparada para proteger la información sensible, facilitar la investigación y crear un entorno de aprendizaje seguro para su comunidad académica.

Además, la respuesta positiva por parte del personal de laboratorio después de compartir las recomendaciones subraya la practicidad y relevancia de los hallazgos de la investigación. Este respaldo no solo valida el esfuerzo invertido en este estudio, sino que también subraya el compromiso colectivo dentro de la universidad para priorizar y mantener una postura sólida en ciberseguridad.

7. RECOMENDACIONES

Es vital continuar realizando evaluaciones técnicas de forma regular y exhaustiva utilizando marcos de trabajo como COBIT 2019. Recomendamos establecer un calendario periódico para estas evaluaciones, lo que garantizará que cualquier nueva vulnerabilidad sea detectada y mitigada de manera oportuna.

Se sugiere implementar una política de gestión de activos robusta que incluya actualizaciones regulares del inventario de activos críticos. Además, se deben establecer protocolos de seguridad específicos para estos activos, incluyendo medidas físicas y tecnológicas, asegurando así su protección continua. Es esencial realizar auditorías internas periódicas siguiendo estándares como ISO/IEC 27001:2022. Recomendamos mantener un equipo dedicado para estas auditorías, asegurando que los controles existentes sean eficaces y estén alineados con las últimas amenazas y regulaciones.

Se sugiere realizar evaluaciones regulares de las recomendaciones propuestas. Las pruebas piloto y simulaciones deben llevarse a cabo en un entorno controlado para medir la efectividad y relevancia de las recomendaciones. Los ajustes necesarios deben realizarse según los resultados de estas pruebas. Fomentar una cultura de seguridad informática en toda la

universidad es fundamental. Esto implica no solo la implementación de medidas técnicas, sino también la concientización continua del personal y los estudiantes. Se deben llevar a cabo sesiones de capacitación y concientización regulares para mantener a todos actualizados sobre las últimas amenazas y mejores prácticas de seguridad.

La naturaleza del ciberespacio implica que las amenazas evolucionan constantemente. Por lo tanto, es imperativo mantenerse actualizado con las últimas tendencias y tecnologías de seguridad. Recomendamos la participación activa en comunidades de ciberseguridad, la colaboración con expertos externos y la investigación constante para estar preparados para enfrentar cualquier desafío futuro.

REFERENCIAS

Alvarez, E., & Silva, O. (2019). *Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo.* Obtenido de Repositorio Universidad Tecnica de Ambato: https://repositorio.uta.edu.ec/bitstream/123456789/30111/1/Tesis_t1639si.pdf

Andocilla, I., & Fuentes, M. (2019). *PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGO TECNOLÓGICOS PARA LA EMPRESA PÚBLICA METROPOLITANA DE TRANSPORTE DE PASAJEROS DE QUITO*. Obtenido de Repositorio Universidad Israel: http://repositorio.uisrael.edu.ec/bitstream/47000/2182/1/UISRAEL-EC-SIS-378.242-2019-064.pdf

Cabezas, E., Andrade, D., & Torres, J. (2018). *Introducción a la metodología de la investigación científica.* Obtenido de Repositorio Universidad de Las Fuerzas Armadas ESPE: https://repositorio.espe.edu.ec/bitstream/21000/15424/1/Introduccion%20a%20la%20Metodologia%20de%20la%20investigacion%20cientifica.pdf

Campos, C., & León, D. (2020). *Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada en la gestión de riesgos de tecnologías de información en la Unidad de Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.* Obtenido de Repositorio institucional Universidad Nacional Pedro Ruiz Gallo: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/8244/BC-4644%20CAMPOS%20CRUZ-LEON%20TESEN.pdf?sequence=1&isAllowed=y

Chávez, R. (2016). *ntroducción a la metodología de la investigación.* Obtenido de Repositorio Universidad Técnica de Machala:

http://repositorio.utmachala.edu.ec/bitstream/48000/6785/1/63%20INTRODUCCION%20A%20LA%20METODOLOGIA%20DE%20LA%20INVESTIGACION.pdf

Chicaiza, D., & Muñoz, O. (2020). *Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indigena SAC.* Obtenido de Repositorio Universidad Técnica de Ambato: https://repositorio.uta.edu.ec/bitstream/123456789/31305/1/t1709si.pdf

Cynthus. (2022). *COBIT 2019.* Obtenido de CUÁLES SON LAS PRINCIPALES CARACTERÍSTICAS QUE TIENE ESTE MODELO: https://www.cynthus.com.mx/que-es-cobit-beneficios/

Delta protect. (08 de 03 de 2023). *Vulnerabilidad informática: Qué es y cómo protegerse*. Obtenido de https://www.deltaprotect.com/blog/vulnerabilidad-informatica

Dictsolutions. (2019). *Lo que necesita saber sobre el marco COBIT 2019.* Obtenido de https://dictsolutions.com/es/marco-cobit-2019/

Dominguez, J. (2015). *Seguridad Informática Personal y Corporativa (Segunda parte).* Obtenido de Researchgate: https://www.researchgate.net/publication/286371326_Seguridad_Informatica_Personal_y_Corporativa_Segunda_parte/figures?lo=1

Erráez, F. (2011). *Modelo de gestión de procesos de TI para el Departamento de Producción y el Area de Redes y Comunicaciones del I.E.S.S.* Obtenido de Repositorio EPN: https://bibdigital.epn.edu.ec/handle/15000/7706

Estrada, J. (2011). *Estrategias de Comunicación y su incidencia en el Posicionamiento del producto de la empresa Texpaz en la ciudad de Ambato.* Obtenido de Repositorio Universidad Tecnica de Ambato: https://repositorio.uta.edu.ec/handle/123456789/1138

Gallardo, E. (2017). *Metodología de la Investigación.* Obtenido de UNIVERSIDAD CONTINENTAL DEL PERU: https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

GlobalSuite. (22 de 5 de 2022). *Qué es COBIT y para qué sirve*. Obtenido de COBIT (Control Objetives for Information and Related Technology): Qué es COBIT y para qué sirve

Guano, M., & Jaramillo, M. (2021). *Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio.* Obtenido de Repositorio EPN: https://bibdigital.epn.edu.ec/bitstream/15000/21472/1/CD%2010962.pdf

Hernández, A., Ramos, M., Placencia, B., Ganchozo, B., Quimis, A., & Moreno, L. (2018). *METODOLOGIA DE LA INVESTIGACION CIENTIFICA.* Obtenido de Universidad Estatal del Sur de Manabi: http://repositorio.unesum.edu.ec/bitstream/53000/2094/1/METODOLOG%c3%8dA%20DE%20LA.pdf

Hidalgo, M. (2022). *Influencia de un modelo del SGSI (norma ISO/IEC 27001:2013) en la eficacia de la administración de los recursos públicos. registro de la propiedad y mercantil del Cantón Pedro Moncayo, períodos 2019, 2020 y 2021.* Obtenido de Repositorio Instituto de Altos Estudios Nacionales Universidad de Posgrado del Estado: https://repositorio.iaen.edu.ec/handle/24000/6049

Hurtado, M. (2023). *GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT*. Obtenido de Repositorio Universidad Piloto de Colombia: http://polux.unipiloto.edu.co:8080/00004420.pdf

ManageEngine. (2023). Obtenido de https://www.manageengine.com/latam/vulnerability-management/proceso-evaluacion-vulnerabilidades.html

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2023). *Ley organica de telecomunicaciones, en beneficio de los ciudadanos*. Obtenido de ey Orgánica de Telecomunicaciones establece un régimen completo de protección y defensa de los usuarios: https://www.telecomunicaciones.gob.ec/entro-en-vigencia-la-ley-organica-de-telecomunicaciones-en-beneficio-de-los-ciudadanos/

Mora, J., Leon, J., Huilcapi, M., & Escobar, D. (2017). *EL MODELO COBIT 5 PARA AUDITORÍA Y EL CONTROL DE LOS SISTEMAS DE INFORMACIÓN.* Obtenido de Repositorio Pontificia Universidad Catolica del Ecuador Sede Ambato: https://repositorio.pucesa.edu.ec/handle/123456789/2355

NQA. (2023). *NQA-ISO-27001-Guia-de-implantacion.* Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Orellana, M. (2022). *Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia - CEDIA.* Obtenido de Repositorio Universidad Politecnica Salesiana: https://dspace.ups.edu.ec/bitstream/123456789/22091/1/UPS-CT009625.pdf

Organismo de certificación global. (2023). Obtenido de https://www.nqa.com/es-mx/certification/standards/iso-27001#:~:text=%C2%BFQu%C3%A9%20es%20la%20ISO%2027001,informaci%C3%B3n%2C%20as%C3%AD%20como%20cumplimiento%20legal

Qué es la ciberseguridad. (19 de 04 de 2022). Obtenido de Tipos de ciberseguridad: https://universidadeuropea.com/blog/que-es-ciberseguridad/

Redvoiss. (2 de 10 de 2021). *Qué son los activos de información en una empresa*. Obtenido de https://blog.redvoiss.net/que-son-los-activos-de-informacion-en-una-empresa

Registrospublicos. (9 de 11 de 2021). *Lo que necesita saber sobre el marco COBIT 20.* Obtenido de https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/#:~:text=Con%20la%20Ley%20de%20Protecci%C3%B3n,los%20proveedores%20de%20servicios%20digitales

Suarez, J. (2023). *APLICACIÓN DE TÉCNICAS DE MINERÍA DE DATOS PARA LA PREDICCIÓN DEL CRECIMIENTO DEL PORTAFOLIO DE CLIENTES DE LA EMPRESA "CUSTOM PLACE.* Obtenido de Repositorio Universidad Estatal Peninsula de Santa Elena : https://repositorio.upse.edu.ec/xmlui/bitstream/handle/46000/9413/UPSE-TTI-2023-0030.pdf?sequence=1&isAllowed=y

Telcel. (2023). *Todo negocio debe tomar en cuenta estos tres pilares para lograr una protección adecuada de la información*. Obtenido de https://www.telcel.com/empresas/tendencias/notas/pilares-seguridad-de-informacion#:~:text=Los%20tres%20pilares%20principales%20de,de%20seguridad%20de%20la%20informaci%C3%B3n

Torres, T. (2020). *Diseño de una estrategia de comunicación para posicionar el Centro de Capacitación Corazonando Líderes, empresa de preparación para postulantes a las Fuerzas de Seguridad Nacional con presencia en 12 ciudades del Ecuador.* Obtenido de Repositrio Universidad Andina Simón Bolívar: https://repositorio.uasb.edu.ec/bitstream/10644/7264/1/T3148-MCE-Torres-Dise%c3%b1o.pdf

Uría, M. (2013). *Estrategias de comunicación internas y externas para una empresa privada.* Obtenido de Repositorio USFQ: https://repositorio.usfq.edu.ec/bitstream/23000/2460/1/107080.pdf

UTN. (2021). *Gestión Académica*. Obtenido de Normativa de la Gestión Académica de la UTN: https://legislacion.utn.edu.ec/

UTN. (2023). *Uninversidad Técnica del Norte - Ibarra Ecuador.* Obtenido de https://www.utn.edu.ec/campus-universitarios/

ANEXOS

8. Guía de validación de instrumentos N°1

Por favor, marque con una X la respuesta escogida de entre las opciones que se presentan:

	sí	no
El instrumento contiene instrucciones claras y precisas para que los encuestados puedan responderlo adecuadamente (ver Anexo 1)	x	
El número de preguntas del cuestionario es excesivo		x
Las preguntas constituyen un riesgo para el encuestado (en el supuesto de contestar SÍ, por favor, indique inmediatamente abajo cuáles)		x

Preguntas que el experto considera que pudieran ser un riesgo para el encuestado:	
N.º de la(s) pregunta(s)	
Motivos por los que se considera que pudiera ser un riesgo	
Propuestas de mejora (modificación, sustitución o supresión)	

	Evaluación general del cuestionario			
	Excelente	**Buena**	**Regular**	**Deficiente**
Validez de contenido del cuestionario	x			

Observaciones y recomendaciones en general del cuestionario:

Motivos por los que se considera no adecuada	
Motivos por los que se considera no pertinente	
Propuestas de mejora (modificación, sustitución o supresión)	

Identificación del experto

Nombre y apellidos	Sandra Karina Narváez Pupiales
Filiación (ocupación, grado académico y lugar de trabajo)**:**	Gerente SEGURIDAD TECNOLÓGICA Y SERVCIOS SEYTON CIA LTDA Magister en Redes de Comunicación Ibarra, Miguel Endara 2-70
e-mail	snarvaez@seyton.ec
Teléfono o celular	062651452/ 0989964195
Fecha de la validación (día, mes y año)**:**	21/08/2023

Firma	Firmado electrónicamente por: SANDRA KARINA NARVAEZ PUPIALES

Muchas gracias por su valiosa contribución a la validación de este cuestionario.

9. Guía de validación de instrumentos N°2

Por favor, marque con una X la respuesta escogida de entre las opciones que se presentan:

	sí	no
El instrumento contiene instrucciones claras y precisas para que los encuestados puedan responderlo adecuadamente (ver Anexo 1)	x	
El número de preguntas del cuestionario es excesivo		x
Las preguntas constituyen un riesgo para el encuestado (en el supuesto de contestar SÍ, por favor, indique inmediatamente abajo cuáles)	x	
Preguntas que el experto considera que pudieran ser un riesgo para el encuestado:		
N.º de la(s) pregunta(s)	8	

Motivos por los que se considera que pudiera ser un riesgo	Porque considero que el encuestado no puede garantizar totalmente la disponibilidad y acceso a los recursos requeridos para llevar a cabo la evaluación técnica informática de las vulnerabilidades en ciberseguridad. Normalmente dichas actividades dependen de cierto personal jerárquico y procedimientos correspondientes, que no dependen total y exclusivamente del encuestado.
Propuestas de mejora (modificación, sustitución o supresión)	¿Considera que el proyecto debe definir los requerimientos y ejecutar los procedimientos correspondientes e indicados por la institución para obtener los recursos necesarios a fin de llevar a cabo la evaluación técnica informática de las vulnerabilidades en ciberseguridad?

	Evaluación general del cuestionario			
	Excelente	**Buena**	**Regular**	**Deficiente**
Validez de contenido del cuestionario		x		

Observaciones y recomendaciones en general del cuestionario:	
Motivos por los que se considera no adecuada	N/A
Motivos por los que se considera no pertinente	N/A
Propuestas de mejora (modificación,	Solo el replanteo de la pregunta 8
sustitución o supresión)	

Identificación del experto

Nombre y apellidos	Mercy Denisse Anchundia Ruiz
Filiación (ocupación, grado académico y lugar de trabajo)**:**	Especialista de TICS, Master Scientist en Ciberseguridad, EPN
e-mail	marseaplage@gmail.com
Teléfono o celular	0960058067
Fecha de la validación (día, mes y año)**:**	19/08/2023
Firma	 Firmado electrónicamente por: **MERCY DENISSE ANCHUNDIA RUIZ**

Muchas gracias por su valiosa contribución a la validación de este cuestionario.

10. Captura de encuesta aplicada digitalmente

EVALUACIÓN DE RIESGOS INFORMÁTICOS

Lea detenidamente las preguntas y escoja la alternativa que usted considere conveniente

Consentimiento informado

- Acepta participar en la investigación descrita de forma libre y voluntaria. Su participación puede ser suspendida en cualquier momento, sin que esto traiga ningún tipo de consecuencias negativas para usted o a la institución. Este estudio no presenta riesgos identificables para su integridad física o psicológica.
- Los datos solicitados para la aplicación de este cuestionario son anónimos y serán manejados bajo absoluta confidencialidad.

AGRADECEMOS SU VALIOSA COLABORACIÓN

1.- ¿Considera que el proyecto de evaluación técnica informática de las vulnerabilidades en ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte es necesario para garantizar la seguridad de la información? *

- ○ Totalmente de acuerdo (TD)
- ○ Muy de acuerdo (MD)
- ○ Neutral (N)
- ○ Poco de acuerdo (PD)
- ○ En desacuerdo (ED)

2.- ¿Cree que el enfoque basado en COBIT 2019 es adecuado para abordar las vulnerabilidades en ciberseguridad en los laboratorios de computación de la universidad?

- ○ Totalmente de acuerdo (TD)
- ○ Muy de acuerdo (MD)
- ○ Neutral (N)
- ○ Poco de acuerdo (PD)
- ○ En desacuerdo (ED)

3.- ¿Siente que el proyecto lograra identificar de manera efectiva las principales vulnerabilidades en ciberseguridad en los laboratorios de computación?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

4.- ¿Considera que las acciones propuestas en el proyecto son adecuadas para mitigar las vulnerabilidades en los principales activos críticos de información?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

5.- ¿Está de acuerdo en que que el proyecto considera como activo critico de información a los servidores y sistemas de almacenamiento de datos?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

6.- ¿Está de acuerdo en que el proyecto considera como activo critico de información a la red de comunicación y conectividad entre equipos?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

7.- ¿Está de acuerdo en que el proyecto considera como activo critico de información a los equipos informáticos y su uso dentro del laboratorio?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

8.- ¿Considera que el proyecto debe definir los requerimientos y ejecutar los procedimientos correspondientes e indicados por la institución para obtener los recursos necesarios a fin de llevar a cabo la evaluación técnica informática de las vulnerabilidades en ciberseguridad?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

8.- ¿Considera que el proyecto debe definir los requerimientos y ejecutar los procedimientos correspondientes e indicados por la institución para obtener los recursos necesarios a fin de llevar a cabo la evaluación técnica informática de las vulnerabilidades en ciberseguridad?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

9.- ¿Puede afirmar que el proyecto tendrá un impacto positivo en la seguridad de la información en los laboratorios de computación de la Universidad Técnica del Norte?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

10.- ¿Estaría dispuesto a recomendar las evaluaciones técnicas informáticas de vulnerabilidades en ciberseguridad en los laboratorios de computación de la universidad en el futuro, basadas en COBIT 2019?

- Totalmente de acuerdo (TD)
- Muy de acuerdo (MD)
- Neutral (N)
- Poco de acuerdo (PD)
- En desacuerdo (ED)

11. Socialización informe de recomendaciones con laboratoristas.

12. Captura encuesta de satisfacción, aplicada digitalmente en la socialización de informe de recomendaciones.

ENCUESTA DE SATISFACCIÓN

Lea detenidamente las preguntas y escoja la alternativa que usted considere conveniente

Consentimiento informado

- Acepta participar en la investigación descrita de forma libre y voluntaria. Su participación puede ser suspendida en cualquier momento, sin que esto traiga ningún tipo de consecuencias negativas para usted o a la institución. Este estudio no presenta riesgos identificables para su integridad física o psicológica.
- Los datos solicitados para la aplicación de este cuestionario son anónimos y serán manejados bajo absoluta confidencialidad.

AGRADECEMOS SU VALIOSA COLABORACIÓN

martypmx@gmail.com Cambiar cuenta

No compartido

* Indica que la pregunta es obligatoria

1.¿Está al tanto de las evaluaciones técnicas regulares realizadas en nuestra universidad utilizando marcos de trabajo como COBIT 2019? *

- SI
- NO

2. ¿Considera que después de estas evaluaciones técnicas regulares se puede lograr evidenciar a corto plazo una mejora en los sistemas?

- SI
- NO

2. ¿Considera que después de estas evaluaciones técnicas regulares se puede lograr evidenciar a corto plazo una mejora en los sistemas?

- ◯ SI
- ◯ NO

3. ¿Considera que la política de gestión de activos, incluyendo actualizaciones regulares del inventario de activos críticos, contribuirá de manera efectiva a la protección de los activos de información de la universidad?

- ◯ SI
- ◯ NO

4. ¿Ha participado en alguna auditoría interna llevada a cabo siguiendo estándares como ISO/IEC 27001:2022 en los últimos 12 meses?

- ◯ SI
- ◯ NO

5. ¿Tras su experiencia con este informe de resultados podría afirmar que las iniciativas de seguridad informática planteadas lograrían garantizar protección más efectiva contra las amenazas cibernéticas ahora y en el futuro?

- ◯ SI
- ◯ NO