UNIVERSIDAD NACIONAL DE CAAGUAZÚ
FACULTAD DE CIENCIAS Y TECNOLOGÍAS
CARRERA DE INGENIERÍA EN INFORMATICA

PROYECTO FINAL DE GRADO

PROPUESTA DE UN LABORATORIO DE PRACTICAS DE SEGURIDAD EN REDES VIRTUALIZADO BASADO EN LA NORMA ISO 27001 PARA LA FACULTAD DE CIENCIAS Y TECNOLOGIAS

Luis Enrique Portillo Viana

TUTOR: ING. Héctor Estigarribia

COTUTOR: Juan Vicente Bogado Machuca

CORONEL OVIEDO, NOVIEMBRE DE 2024.

DERECHO DE AUTOR

Quien suscribe, Luis Enrique Portillo Viana autor del trabajo de investigación titulado **"Propuesta de un laboratorio de Seguridad en Redes Virtualizado basado en la norma ISO 27001 para la Facultad de Ciencias y Tecnologías"**, declara que voluntariamente cede a título gratuito en forma pura y simple ilimitada e irrevocablemente a favor de la Facultad de Ciencias y Tecnologías – UNCA, el derecho de autor de contenido patrimonial, que le corresponde sobre el trabajo de referencia. Conforme a lo anteriormente expresado, esta sesión le otorga a la FCyT la Facultad de comunicar la obra divulgarla, publicarla y reproducirla en soportes analógicos o digitales en la oportunidad que así lo estime conveniente. La FCyT deberá indicar qué autoría o creación del trabajo corresponde a mi persona y hará referencia al autor y a las personas que hayan colaborado en la realización del presente trabajo de investigación.

En la ciudad de Coronel Oviedo a los …. , del mes de …….. del 2024

…….

Firma/s

PÁGINA DE APROBACIÓN

Trabajo de fin de grado para la obtención del Título de Ingeniero en Sistemas Informáticos, aprobado en representación de la Facultad Ciencias y Tecnología de la Universidad Nacional de Caaguazú, por el Tribunal Examinador constituido por los siguientes profesores y con la siguiente nota final:

CALIFICACIÓN FINAL: _____

ACTA N°:_____

FECHA :_____

Prof. Ing.

Prof. Ing.

Prof. Ing.

DEDICATORIA

A toda mi familia, quienes fueron, son y serán mi apoyo incondicional y mi fuente de inspiración y fuerza en todo mi camino de vida. Gracias por el amor incondicional, la paciencia y por enseñarme el valor de la perseverancia y que todo esfuerzo tendrá tarde o temprano su fruto.

Esta meta no hubiese sido posible sin la confianza, fe y apoyo incondicional hacia mí. Este logro es tanto mío como de ustedes.

AGRADECIMIENTOS

Quiero expresar mi eterno agradecimiento a todas las personas que hacen posible la realización de esta tesis. En primer lugar, a toda mi familia, por todo el apoyo que siempre me brindaron, y por siempre estar a mi lado, dándome ánimos y fuerzas para poder superar todos los desafíos que se interpusieran en mi camino.

A todos los docentes, quienes me extendieron la mano cuando los necesitaba, y me brindaron su conocimiento, guía y paciencia para el desarrollo tanto individual, como también profesional.

A todas mi amistades y compañeros de estudio, los cuales me acompañaron en toda esta etapa, y quienes fueron mi respaldo y aliento en todo momento.

RESUMEN

En la actualidad contar con un laboratorio de prácticas se ha convertido en una herramienta más que esencial y necesaria para la educación de los futuros profesionales, más aún en el área de la ciberseguridad, ya que, contando con este apoyo, se puede proporcionar un entorno de aprendizaje no solo teórico, sino que practico a la par que seguro. Teniendo en cuenta lo anterior, este proyecto tiene como objetivo proponer un laboratorio de prácticas de seguridad en redes virtualizado, la cual esté alineada con los estándares de la norma ISO 27001, con lo que se podrá dar paso a que los estudiantes puedan desarrollar competencias prácticas en un entorno el cual esté controlado, seguro, accesible y estandarizado.

Este proyecto aborda primeramente la identificación de cuáles son los requisitos de seguridad a tener en cuenta según la norma ISO 27001 y la selección de las herramientas las cuales serán necesarias para la implementación del laboratorio, Además, también se realizará un análisis de las características tanto físicas como lógicas que este tipo de laboratorio requiere, pudiendo así evaluar los beneficios y limitaciones, desde la perspectiva del docente encargado.

Con este trabajo se busca ofrecer una posible solución educativa que contribuirá al desarrollo de las habilidades de los futuros profesionales de nuestra institución en el área de la seguridad en redes, en un entorno seguro y accesible, manteniendo el enfoque y los estándares necesarios para la seguridad de la información basados en la ISO 270001.

Palabras Claves:

Tecnologías para la Información y la Comunicación
ODS 4- Educación de Calidad
ODS 9 - Industria, Innovación e Infraestructura
ODS 16 - Paz, Justicia e Instituciones Sólidas

ABSTRACT

Nowadays, having a practical laboratory has become an essential and necessary tool for the education of future professionals, especially in the field of cybersecurity, as it provides a learning environment that is not only theoretical but also practical and secure. With this in mind, the aim of this project is to propose a virtualized network security practical laboratory, aligned with the ISO 27001 standards, allowing students to develop practical skills in a controlled, secure, accessible, and standardized environment.

This project first addresses the identification of the security requirements to be considered according to the ISO 27001 standard and the selection of the tools necessary for the implementation of the laboratory. Additionally, an analysis of both the physical and logical characteristics required for this type of laboratory will be conducted, enabling an evaluation of the benefits and limitations from the perspective of the instructor in charge.

This work seeks to provide an educational solution that will contribute to the development of the skills of future professionals at our institution in the field of network security, in a safe and accessible environment, while maintaining the focus and standards necessary for information security based on ISO 27001.

Keywords:

Information and Communication Technologies
SDG 4- Quality Education
SDG 9 - Industry, Innovation and Infrastructure
SDG 16 - Peace, Justice and Strong Institutions

ÍNDICE

INDICE DE TABLAS

INDICE DE FIGURAS

1. INTRODUCCIÓN

En la actualidad, la seguridad de la información es un factor clave para organizaciones de todo tipo y tamaño. Con el aumento constante de las amenazas cibernéticas y la creciente dependencia de los sistemas informáticos y redes interconectadas, resulta fundamental adoptar prácticas de seguridad en redes que sean efectivas.

En este sentido, la norma ISO 27001, creada por la Organización Internacional de Normalización (ISO), ofrece un marco completo para la gestión de la seguridad de la información. Esta norma brinda directrices y mejores prácticas para identificar, evaluar y gestionar los riesgos asociados a la seguridad de los datos.

El proyecto se alinea principalmente con la línea de investigación de Tecnologías para la Información y la Comunicación dentro del área de Ingeniería Informática. Esta línea de investigación abarca la implementación y mejora de tecnologías y sistemas de información que son fundamentales para la ciberseguridad y la gestión de la información.

Además, el proyecto también puede tener componentes de Ingeniería de Software si se consideran las herramientas y software necesarios para implementar y gestionar el laboratorio virtualizado, así como el desarrollo de soluciones prácticas para mejorar la enseñanza en seguridad de la información.

El proyecto se alinea principalmente con los siguientes Objetivos de Desarrollo Sostenible (ODS):

ODS 4: Educación de Calidad: Este proyecto busca proporcionar un entorno de aprendizaje práctico y seguro, mejorando así la calidad de la educación en el área de ciberseguridad. Esto ayuda a desarrollar habilidades y competencias esenciales en los futuros profesionales.

ODS 9: Industria, Innovación e Infraestructura: Al proponer un laboratorio de prácticas de seguridad en redes virtualizado alineado con estándares internacionales como la ISO 27001, el proyecto fomenta la innovación y mejora la infraestructura educativa y tecnológica.

ODS 16: Paz, Justicia e Instituciones Sólidas: La implementación de prácticas de seguridad en redes que cumplen con la ISO 27001 contribuye a la creación de sistemas de información seguros y confiables, lo que es fundamental para mantener la paz y la justicia en el ámbito digital.

El enfoque en la ciberseguridad y el cumplimiento de normas internacionales también tiene el potencial de contribuir indirectamente a otros ODS relacionados con la sostenibilidad y la eficiencia de los sistemas educativos y tecnológicos.

1.1. Antecedentes

El proyecto "Diseño de un Laboratorio de Seguridad de la Información para el Tecnológico de Antioquia", realizado por Daniel Eduardo Cardona Zapata y Ana María Sánchez Piedrahita, tuvo como propósito sugerir a la Facultad de Ingeniería de Antioquia la creación de un laboratorio especializado en seguridad informática. Este espacio estaría equipado con los recursos necesarios para que los estudiantes de diversos programas puedan realizar prácticas que incluyan pruebas de seguridad, identificación de vulnerabilidades y medidas de prevención ante posibles amenazas cibernéticas. [1]

Por otro lado, el proyecto "Laboratorio de Ciberseguridad en un Entorno Empresarial Virtualizado", llevado a cabo en 2015 por Javier Gómez Velázquez como parte de su proyecto de grado, busca aportar al conocimiento en ciberseguridad de los futuros ingenieros en tecnologías y servicios de telecomunicación. La meta fue proporcionar a los estudiantes un entorno donde puedan aplicar de forma práctica los conocimientos teóricos adquiridos en asignaturas relacionadas con la ciberseguridad, favoreciendo el desarrollo de sus capacidades técnicas en este ámbito. [2]

Los siguientes proyectos fueron elaborados como tesis de grado en la FCyT, a pesar de no ser de la misma carrera se agregan como referencias:

El proyecto final de grado “DISEÑO DE UN LABORATORIO PARA PRÁCTICA DE SISTEMAS DE PROTECCIONES ELÉCTRICAS DE POTENCIA BASADO EN DISPOSITIVOS PROGRAMABLES UTILIZADOS EN SUBESTACIONES DE ALTA TENSIÓN PARA LA FCYT DE LA UNCA” escrito por Juan Paolo Gonzales Rolón, el cual se enfoca en realizar un diseño de un laboratorio para las prácticas de protecciones de sistemas eléctricos, haciendo énfasis en las subestaciones de alta tensión. [3]

El proyecto final de grado “DISEÑO DE UN LABORATORIO DE ENSAYOS PARA LA CERTIFICACIÓN DE EFICIENCIA ENERGÉTICA EN APARATOS DE REFRIGERACION AUTOCONTENIDOS Y ACONDICIONADORES DE AIRE” escrito por Álvaro Gustavo Torres Zarza, el cual tiene como objetivo, la de realizar un diseño de un laboratorio de ensayos para las certificaciones de eficiencia energética, en el área de aparatos de refrigeración autocontenidos y también acondicionadores de aire, de tal manera que se pueda garantizar niveles óptimos de eficiencia en los equipos evaluados. [4]

El proyecto final de grado “DISEÑO DE UN LABORATORIO DE ENSAYOS DE RUTINA DE TRANSFORMADORES DE DISTRIBUCIÓN PARA LA FACULTAD DE CIENCIAS Y TECNOLOGÍAS DE LA UNCA” escrito por Francisco Marín Sanabria el cual tiene como objetivo el diseñar un laboratorio de ensayos de rutina, con énfasis en transformadores de

distribución monofásico y trifásico, con una potencia aparente de hasta 500 kVA, para Facultad de Ciencias y Tecnologías. [5]

El proyecto final de grado "IMPLEMENTACIÓN DE UN LABORATORIO DE MECÁNICA DE SUELOS PARA LA FACULTAD DE CIENCIAS Y TECNOLOGÍAS DE LA UNIVERSIDAD NACIONAL DE CAAGUAZÚ" escrito por Celia Noemi Báez Vázquez y Jazmín Rocio de Jesús Aquino Gorostiaga, el cual propone la creación de un laboratorio, con todos los equipos y procedimientos actualizados y necesarios que cumplan con los estándares necesarios para la realización de ensayos y experimentos. [6]

El proyecto final de grado "Políticas de seguridad en Sistemas de Información para el rectorado de la Universidad Nacional del Caaguazú en el año 2017" del autor Justino Rodrigo Rojas Sartorio tuvo el objetivo de establecer un modelo de política correspondiente a la seguridad de la información dentro del Rectorado de la Universidad Nacional Del Caaguazú basado en el Plan Nacional de Ciberseguridad. [7]

1.2. Justificación

En la actualidad, vivimos en una sociedad altamente interconectada e impulsada por la tecnología, donde los datos y la información fluyen constantemente a través de redes digitales. Esta creciente dependencia de la tecnología digital ha dado lugar a un entorno en el que la ciberseguridad se ha convertido en una cuestión de vital importancia.

La ciberseguridad es esencial para proteger los derechos fundamentales de las personas en la era digital. En un contexto donde la información personal y confidencial se almacena y se comparte a través de dispositivos y plataformas en línea, la integridad y la confidencialidad de estos datos se convierte en prioridades primordiales. La pérdida o el acceso no autorizado a esta información puede tener consecuencias devastadoras, incluyendo el robo de identidad, la exposición de datos financieros, médicos, y la violación de la privacidad.

Además, en el ámbito empresarial, la ciberseguridad es un pilar fundamental para garantizar la continuidad de las operaciones y la protección de la propiedad intelectual y la información estratégica. Las organizaciones enfrentan constantemente amenazas cibernéticas que pueden provocar la interrupción de los servicios, pérdidas financieras y daños a la reputación.

La relevancia de la ciberseguridad va más allá de los dominios individuales y empresariales, extendiéndose en el ámbito de la seguridad nacional y la estabilidad global. Los ciberataques, que pueden funcionar como instrumentos de espionaje y armas en contextos cibernéticos, destacan la imperativa necesidad de preservar las infraestructuras críticas de una nación, tales como centrales eléctricas y sistemas de transporte.

Por último, la ciberseguridad también es un requisito legal y ético. La regulación y el cumplimiento de normativas de ciberseguridad son fundamentales para proteger los derechos individuales y garantizar prácticas comerciales éticas.

En el contexto actual, la ciberseguridad se ha convertido en un campo esencial y en constante evolución, crucial para garantizar la protección de la información en el mundo digital. A pesar de la importancia de esta disciplina, la falta de un laboratorio de ciberseguridad en la Facultad de Ciencias y Tecnologías ha limitado significativamente la capacidad de los estudiantes para adquirir experiencia práctica y aplicar sus conocimientos teóricos en situaciones del mundo real.

Con este proyecto se pretende aportar a la Facultad de Ciencias y Tecnologías un proyecto de laboratorio de ciberseguridad, dedo que el conocimiento teórico debe de poder aplicarse a la práctica, el realizar la implementación de un laboratorio fomentaría las habilidades para nuestro entorno, donde los estudiantes pueden adquirir un amplio conocimiento y este los prepare de una mejor manera para un mercado laboral en donde es sabido que se valoran las habilidades prácticas.

El principal beneficiario de este proyecto será la Facultad de Ciencias y Tecnologías, ya que con ello podrá desarrollar de forma más óptima a los alumnos de la carrera de Ingeniería en Informática.

1.3. Objetivos

1.3.1. Objetivo general

- Proponer un laboratorio de prácticas de seguridad en redes virtualizado basado en la norma ISO 27001.

1.3.2. Objetivos específicos

- Identificar los requisitos de seguridad informática de la norma ISO 27001.
- Determinar las características físicas y lógicas necesarias para la implementación de un laboratorio de prácticas de seguridad en redes virtualizado basado en la norma ISO 27001.
- Analizar la viabilidad de un laboratorio de prácticas de seguridad en redes virtualizado basado en la norma ISO 27001.

2. METODOLOGÍA

2.1. Alcance de la investigación.

Este estudio tuvo un enfoque descriptivo, centrado en el análisis de los requisitos de la norma ISO 27001 y también de las características necesarias para llevar a cabo la implementación del laboratorio de prácticas de seguridad en redes virtualizado. Además, se realizó una investigación, sobre las herramientas tecnológicas y recursos necesarios para su correcto desarrollo.

2.2. Técnicas e instrumentos de recolección de datos.

Para este estudio, utilizamos como herramienta una encuesta la cual tiene como objetivo el obtener datos numéricos sobre lo que piensan los estudiantes sobre el acceder a un laboratorio de seguridad en redes virtualizado tanto como evaluar su nivel de comprensión sobre conceptos claves necesarios y su percepción sobre el aprendizaje desarrollado en el área de seguridad en redes.

2.3. Métodos y análisis de datos.

Alcance de la investigación: Investigación descriptiva, ya que se enfoca en analizar y describir requisitos y características basados en la norma ISO 27001, las cuales son necesarias para la implementación de un laboratorio de prácticas de seguridad en redes virtualizado.

Análisis de datos: Investigación exploratoria, ya que se pretende explorar y familiarizarse con un objetivo poco conocido o novedoso.

3. BASES TEÓRICAS

Fases de la implementación de la norma ISO27001

- Análisis y evaluación de riesgos.
- Implementación de controles.
- Planes o contingencias de vulnerabilidades.
- Alcance de la gestión dentro de las políticas implementadas.
- Medición de las amenazas que se conozcan y/o que puedan afectar la integridad de los activos.
- Auditorías internas y externas dentro de un seguimiento.

La norma ISO 27001 se fundamenta principalmente de la identificación y análisis de las principales amenazas para minimizar los riesgos que puedan verse vinculados y permitiendo aportar a la identificación de dichos riesgos [8]

Los riesgos pueden ser identificados como cualquier evento y tipo que haga efecto a la integridad de los activos como “Críticos, activos y pasivos”

- Críticos: una vez no se identifica el riesgo, este se convierte en una amenaza la cual pasa a dañar por completo la información y genera una pérdida total de los activos.
- Activos: una vez que se identifican las amenazas se pueden detener dentro del proceso o ejecución, de tal forma que se evite pérdidas o daños en dicho proceso.
- Pasivas: se tienen identificadas y controladas las amenazas que estos pueden ser

La norma ISO 27001 establece un conjunto de parámetros y controles de seguridad los cuales deben ser implementados para garantizar la protección de la información. En el contexto de este laboratorio de prácticas con enfoque virtualizado, se han identificado los siguientes controles como prioritarios, debido a que la aplicación directa de las mismas corresponde a las medidas de seguridad en redes:

Control A.5.1.1: Política de seguridad de la información [8]: Este control hace énfasis en la necesidad de contar con una política de seguridad de la información la cual sea relevante y que este establecida de acuerdo a los objetivos propuestos de la organización.

Control A.6.1.1: Roles y responsabilidades de seguridad de la información [8]: Este control establece que es de mucha importancia y necesidad definir y asignar roles y responsabilidades para todos los usuarios dentro de la organización, de forma que cada uno tenga una responsabilidad.

Control A.7.2.2: Capacitación en seguridad de la información [8]: Este control establece que, se debe de asegurar que tanto como los alumnos como los encargados del laboratorio reciban la capacitación necesaria y concientización sobre la seguridad de la información periódicamente.

Control A.11.1.2: Controles de entrada física [8]: Este control hace énfasis en no solo contar con controles lógicos, sino también físicos para poder restringir el acceso a las áreas en donde se pueden acceder a información importante.

Control A.12.1.3 Gestión de la capacidad [8]: Este control exige que todos los recursos de los sistemas informáticos tanto como los recursos de red, procesamientos y almacenamientos, sean todos gestionados de forma que se garantice su disponibilidad y rendimientos adecuados para poder satisfacer las demandas actuales y futuras.

Control A.13.1.1 Control de Redes [8]: Este control se establece debido a la necesidad de proteger la seguridad y operatividad de las redes de información a través de mecanismos tales como el control de acceso, la segregación de redes y la monitorización de tráfico.

Control A.13.2.1 Seguridad en la transferencia de información [8]: Este control exige la protección de la información transferida dentro de las redes y hacia redes externas, de forma que se minimicen todos los posibles riesgos de interceptación de datos o modificación de datos.

Control A.14.1.2: Protección de aplicaciones en redes públicas [8]: Este control exige la implementación de medidas de protecciones, las cuales pueden ser cifrado y autenticaciones de forma que se pueda asegurar la integridad y confidencialidad de la información transmitida a través de todas las redes públicas.

Control A.16.1.1: Gestión de incidentes de seguridad [8]: Este control exige el tener establecido un procedimiento el cual seguir para reportar y gestionar incidentes de seguridad.

Control A.18.2.3: Revisión Independiente de la seguridad de la información [8]: Este control exige que se realicen de forma preventiva en un periodo determinado evaluaciones del cumplimiento de los controles de seguridad.

Análisis de las herramientas físicas y lógicas necesarias para el laboratorio de seguridad en redes.

Una vez que hemos analizado la información correspondiente a la identificación de todos los requerimientos, se determina que, para la correcta implementación del laboratorio con el fin de garantizar su éxito, son necesarias un conjunto de herramientas físicas y lógicas, las cuales se detallaran a continuación:

Herramientas físicas:

- Servidores

Son quipos informáticos que proporcionan diversos servicios (llamadas de también como roles) a computadoras conectadas mediante una red ya sean de WAN o LAN.

Dentro de la jerarquía de los servidores podemos encontrar algunas como:

- Servidores web
- Servidores de almacenamiento

- Servidores de bases de datos
- Servidores de acceso remoto
- Servidores de correo
- Servidores de servicios (DNS, AD, DHCP, entre otros)

La enseñanza de la configuración y puesta en marcha de los mencionados servidores facilitara al alumno el entendimiento de conceptos que son fundamentales y están orientados a la seguridad de la información, como lo son Políticas de grupo, Permisos sobre archivos, Configuración de tipos de almacenamientos, instalación de sistemas operativos destinados a servidores, entre otros.

- Equipos para el usuario

Son aquellos equipos informáticos los cuales serán utilizados para pruebas puntuales de la seguridad en redes

- Switches

Los switches son los dispositivos que permitirán la comunicación de datos entre los múltiples equipos conectados en la red.

Podemos categorizar los switches en:

- Switches Desktop
- Switches perimetrales no gestionables
- Switches gestionables
- Switches de prestaciones medias
- Switches de prestaciones altas

Los mencionados switches abarcan todas las capas básicas de conexión a la red y también permiten realizar una óptima configuración de los diferentes protocolos de comunicación entre los equipos a utilizar.

- Enrutadores

El enrutador es un dispositivo el cual se encarga de la comunicación entre una o varias redes.

Tipos de enrutadores:

- Brouter: También conocido como enrutador de puente y que funciona como puente y como enrutador.
- Fresadora de núcleo: Es un dispositivo central, el cual crea una conexión de red y facilita que la transmisión de datos dentro de la una red privada. Estos operan exclusivamente en el núcleo de la red, y no es capaz de enviar o recibir cualquier tipo de información a redes externas. La distribución de los datos queda simplemente limitada a la red interna conectada, ya que este tipo de router, no cuenta con la capacidad de intercambiar información con redes externas.

- Enroutador virtual: Este enroutador consiste en un tipo de software el cual permite que un dispositivo tenga la capacidad de funcionar como un enroutador.
- Enroutador inalámbrico: A pesar de su nombre este dispositivo posee una conexión alámbrica al modem, y este es el cual le enviar las señales de datos de internet. Pero para este luego, no es necesario el contar con una conexión por cable para poder transportar la información para los dispositivos conectados a su red. Este enroutador utiliza las antenas que posee, las cuales enviar ondas infrarrojas o de radio, las cuales transportan todos los paquetes de datos necesarios.
- Enroutador con cable: Este tipo de enroutador posee dos conexiones físicas, como mínimo, La primera, es la conexión directa que existe entre el modem de internet y el enroutador, el cual hace posible al enroutador el poder recibir y enviar paquetes de información a través del modem. La segunda conexión, es entre los dispositivos que estén conectados con la red local del enroutador.

Herramientas Lógicas:

- Virtualizadores

Los Virtualizadores son softwares, los cuales permiten crear y gestionar máquinas virtuales (VMs) dentro de un mismo equipo físico. A través de la virtualización, un equipo físico, puede contar con múltiples sistemas operativos de manera aislada y simultáneamente dentro de la misma, y hacer como si cada uno de ellos tuviera su propio equipo independiente.
Podemos categorizar los Virtualizadores en los siguientes tipos:

- De hardware a servidor: Este tipo de virtualización permite el poder ejecutar múltiples sistemas operativos en un mismo servidor físico, los cuales funcionan como servidores independientes, permitiendo así que un solo equipo físico pueda actuar como varios servidores.
- De red: Este tipo de virtualización permite el poder crear redes virtuales dentro de una misma red física, pudiendo dividir y asignar diferentes recursos de red tales como ancho de banda y conexiones, a diferentes entornos virtuales. Así también este tipo de virtualización nos permite el que cada entorno pueda contar con sus propias políticas de seguridad y configuración.
- De almacenamiento: Este tipo de virtualización consiste en crear capas de abstracción entre el almacenamiento físico y todos los sistemas que lo utilizan. Permitiendo así poder agrupar varios recursos de almacenamiento físico, y convertirlos en un único recurso ya que de esta forma podemos hacer que sea más fácil de gestionar y escalar.
- De memoria: Este tipo de virtualización nos permite el poder hacer uso de la memoria física de un sistema de forma más eficiente, dándole a entender a las máquinas virtuales

que tienen más memoria disponible de forma física.

- De software: Este tipo de virtualización hace que sea posible que existan aplicaciones que se ejecuten cada una de manera independiente del sistema operativo o del hardware en el que están instalados, de forma que esto facilita la portabilidad y también el aislamiento de cada una de las aplicaciones.
- De datos: Este tipo de virtualización consiste en crear una capa de abstracción entre todos los datos y todas las aplicaciones las cuales las están utilizando. De forma que todos los datos pueden agruparse en diferentes fuentes, pero en una sola vista virtualizada, permitiendo así el acceder a todos ellos sin tener cuidado de la ubicación física o formato del dato.
- De escritorio: Este tipo de virtualización permite el poder ejecutar escritorios completos en las máquinas virtuales que están alojadas en los servidores, donde cada usuario puede acceder a su propio entorno virtualizado, pero desde cualquier dispositivo como si fuera un ordenador propio.

También necesitamos sistemas operativos, los cuales podemos categorizar en dos:

- Sistemas Operativos Open Source

  Estos sistemas operativos son de costo nulo, o casi nulo, cuya idea principal es la de proveer al usuario final un entorno con el cual pueda interactuar con el hardware ya sea de forma gráfica o no.
- Sistemas Operativos licenciadas

  Estos tipos de sistemas operativos son aquellos cuyos fabricantes nos dan la autorización de su uso mediante licencias, en donde podemos encontrar los siguientes tipos de licencia:
  - OEM: Este tipo de licencia usualmente la obtenemos al adquirir el equipo. Su principal distintivo es una calcomanía visible en el hardware del equipo. Estos no pueden ser transferibles entre equipos.
  - FPP: Este tipo de licencia son aquellas las cuales adquirimos en la caja del software, y estos si pueden ser transferidos de un equipo a otro, ya que no está vinculada directamente al hardware.
  - Open, Select y Open Value: Este tipo de licencias pueden ser ya sea de una OEM O FPP las cuales usualmente están ligadas a un contrato de permanencia durante el cual pueden tener las actualizaciones de las versiones, está destinada para empresas, ya que son solo ofrecidas en cantidad.

Sistemas de protección perimetral.

Estos softwares son herramientas las cuales son utilizadas para prevenir la intrusión de amenazas,

acceso no autorizado, controlar el tráfico que entra y sale, para defenderse de ataques, manejar la integridad de los datos, etc. Podemos encontrar algunos sistemas de protecciones perimetral tales como:

- Snort: Este software es un sistema de detección y prevención de intrusiones (IDS/IPS) el cual es empleado para detectar y bloquear ataques.
- Suricata: Este software es un sistema el cual analiza el tráfico de red y también puede ser utilizado como un IDS/IPS ya que podemos monitorizar el tráfico de red para poder encontrar anomalías en la red.
- OSSEC: Este software es de código abierto, y es utilizado para la detección de intrusos, a través del monitoreo de logs y de todas las actividades en la red.
- Bro (Zeek): Este software ofrece una visibilidad completa de todo el tráfico que ocurre en la red y también es utilizada para la detección de intrusos.
- Cisco Identity Services Engine (ISE): Esta es una plataforma que proporciona soluciones para la autenticación, autorización y auditoria de dispositivos y también usuarios los cuales tengan intención de acceder a la red.
- Pulse Secure: Es una plataforma diseñada para garantizar el acceso a una red a solamente ciertos usuarios autorizados, protegiendo así la red de amenazas.

Antivirus

Los antivirus son softwares los cuales nos protegen de posibles amenazas para nuestros sistemas, ya sean de clientes o servidores. Los antivirus pueden de tipo personal y empresarial.

Podemos clasificar los antivirus de la siguiente forma:

- Invasivos: Este tipo de antivirus que monitorizan el 100% del equipo y por tanto tiene un alto impacto en el consumo de los recursos del equipo.
- De carga media: Este tipo de antivirus poseen políticas preestablecidas, mediante las cuales pueden tener otros módulos configurados tales como firewall.
- De un solo uso: Este tipo de antivirus son herramientas específicas, las cuales generalmente se utilizan para realizar análisis puntuales.

Cifradores o Descifradores

Son utilidades los cuales están dedicados a cifrar o descifrar datos, únicamente con el fin de brindar seguridad de la información y protección de los datos.

Teniendo en cuenta el concepto de virtualizador, podes nombrar dos de los principales y más efectivos Virtualizadores, los cuales son VirtualBox y VMware. Estos dos son las principales herramientas de virtualización, tanto como también las más conocidas.

VirtualBox es un virtualizador de código abierto el cual es muy robusto, esta herramienta pertenece

a la compañía Oracle Corporation y es bien conocido por su compatibilidad con las arquitecturas x86 y AMD 64/Intel 64 y por su excelente rendimiento. Esta herramienta es más bien dirigida a clientes del ámbito empresarial, ya que permite el crear y tener múltiples sistemas operativos en una misma caja virtual o máquina virtual y al mismo tiempo seguir con un sistema operativo principal.

En la actualidad esta herramienta de virtualización es compatible con máquinas con un sistema operativo principal basado en Linux, Windows MacOS y Solaris, demostrando así su capacidad de adaptabilidad a cualquier sistema base, además este también permite el uso de varios sistemas operativos, los cuales pueden ser tanto versiones anteriores del escritorio como también servidores de Microsoft Windows, DOS, todas las versiones de Linux, etc.

Por otro lado, tenemos la herramienta VMware, el cual también es una empresa líder en el ámbito de software de virtualización, esta herramienta nos promete una conectividad segura y una experiencia muy fluida.

Este Virtualizador cuanta también con una herramienta gratuita, de nombre “VMware Studio” el cual ayuda tanto a los desarrolladores como a profesionales de TI a crear y también poder distribuir dispositivos virtuales.

Haciendo una comparación entre ambos, podemos destacar que, si bien ambos son gratuitos, por el lado de VirtualBox, nos podemos encontrar en su versión gratuita con funciones básicas, y si deseamos tener funciones avanzadas, se debe de comprar un paquete, como también para su uso comercial y en varios dispositivos.

Por el lado de VMware también podemos encontrar que cuenta con su versión gratuita, para uso personal y educativo, y que, si deseamos su versión comercial, necesitamos una licencia. La versión pro de esta herramienta tiene una cuota para poder tener acceso a las funciones comerciales.

En el apartado de características, podemos encontrarnos con las siguientes diferencias más importantes:

En el apartado de interfaz de usuario y amigable al usuario, podemos ver que VirtualBox, tiene una interfaz bastante centralizada y sensible, por tanto, fácil de usar. Por otro lado, VMware puede tener múltiples interfaces ya que tiene que soportar múltiples productos.

En modos de red, en VirtualBox podemos ver que cuenta con las redes NAT, puenteado, solo host, en nube y genérica, mientras que, en VMware solo puenteada, solo host, y NAT.

En el ámbito de la virtualización tanto de software y de hardware, podemos ver que VirtualBox es capaz de soportar la virtualización de ambos, mientras que VMware solo admite la virtualización de hardware.

Como podemos ver cada herramienta de virtualización cuenta con sus ventajas y desventaja, lo que nos lleva a ver también las principales ventas o pros de cada uno frente a otro.

Por el lado de VMware podemos ver que esta plataforma tiene una seguridad mejorada, lograda con la implementación de un marco de confianza nulo.

Puede ser utilizado como una plataforma en donde realizar pruebas seguras, de forma que se puedan evaluar dentro actualizaciones y parches, antes de que se apliquen en máquinas físicas.

Tiene una gran variedad de soluciones de recuperación ante desastres, tales como VMware Cloud Disaster Recovery, Site Recovery Manager y VMware Site Recovery.

Cuenta con una optimizada gestión de los centros de datos, además también una mayor eficiencia y también flexibilidad a la hora de realizar operaciones de datos.

Y por el lado de VirtualBox nos encontramos un sistema sólido, el cual puede soportar varios sistemas operativos en un mismo equipo, permitiendo tener aplicaciones heredadas en un hardware nuevo, y también proporcionar un acceso remoto y seguro a las aplicaciones.

Podemos decir que en parte reduce los costos ya que funciona en todos los escritorios y es fácil de adaptar.

También puede ser utilizado para realizar pruebas de versiones tanto como parches nuevos antes de aplicarlos a una maquina física.

La herramienta de VirtualBox ofrece espacios seguros y cifrados de trabajo, tanto como también la capacidad de realizar despliegues muy fácilmente y rápidos en la nube.

Monitoreo de Recursos en el entorno virtualizado.

Teniendo en cuenta el punto de gestión de capacidad, en donde se realizará el control de los recursos del entorno virtualizado entenderemos lo siguiente:

En un entorno de plataforma virtualizado, el monitoreo continuo de los recursos es esencial y fundamental para asegurar el rendimiento óptimo de todas las máquinas virtuales (VMs) y así evitar problemas que puedan impactar de manera negativa en la operación del laboratorio. Los sistemas de monitoreo nos permitirán observar en tiempo real el uso de que estamos teniendo de todos los recursos claves del servidor, tales como CPU, memoria RAM, almacenamiento y red, de esta forma estaremos asegurando que todos estos recursos no se vean comprometidos por sobrecargas, las cuales puedan afectar la estabilidad y eficiencia del laboratorio.

De forma que la razón principal de implementar un sistema de monitoreo en el laboratorio es la de detectar y prevenir cualquier problema de rendimiento que podamos que tener, que sea relacionado con el uso excesivo de nuestros recursos, ya que el llegar a utilizar un porcentaje alto de ya sea CPU, memoria RAM o almacenamiento puede llevar a un rendimiento débil e incluso la detención servicios. Por lo cual es vital la supervisión eficaz para mantener la operabilidad del laboratorio y

garantizar que las pruebas se realicen sin ningún tipo de interrupción.

Herramientas de monitoreo

Existen varias herramientas de monitoreo que podemos utilizar, las cuales serán útiles para nuestro objetivo, y podemos citar algunas.

- Nagios

Esta es una herramienta de monitoreo de sistemas, redes, y aplicaciones en tiempo real, el cual permite supervisar toda la disponibilidad y rendimiento de los servidores y servicios, ofreciendo así también alertas y notificaciones ante problemas de rendimientos y fallos.

Aplicación para el laboratorio

Alertas de rendimiento: se establecerán límites para el uso de recursos, generando así alertas una vez que detecten condiciones las cuales podrían afectar la operación del laboratorio.

- Zabbix

Es una plataforma de monitoreo el cual proporciona una visión integral de toda la infraestructura de TI, este incluyendo redes, servidores, y aplicaciones. También ofrece funciones avanzadas tales como la recopilación de datos, análisis y visualización.

Aplicación en el laboratorio:

Paneles y Reportes: Se configurarán paneles de control y reportes en Zabbix de forma que nos facilitara el análisis del rendimiento y así también la identificación de posibles cuellos de botella.

- VSphere Performance Monitor

Es una herramienta nativa que trae VMWare que nos proporciona información detallada sobre el rendimiento de nuestros recursos en el entorno virtualizado gestionados por VMWare Sphere.

Aplicación en el laboratorio:

Monitoreo de VMs: se utilizará para supervisar el uso de la CPU, RAM y almacenamiento en cada máquina virtual, proporcionada por el propio entorno generándonos datos en tiempo real y gráficos sobre el rendimiento.

Optimización de recursos: Facilitara la identificación de recursos que se están sobre utilizando o infrautilizando, permitiendo así realizar ajustes para mejorar la eficiencia del entorno virtualizado.

- Windows Performance Monitor

Es una herramienta la cual está integrada en Windows Server y la cual permite la supervisión del rendimiento del sistema operativo, estos incluyendo el uso de CPU, RAM, y otros recursos.

Aplicación en el laboratorio:

Monitoreo en servidores Windows: se configurará de forma que se puedan supervisar el rendimiento de los servidores Windows dentro del laboratorio, de forma que nos proporcionará datos específicos sobre el uso de recursos del sistema operativo.

Análisis de tendencias: Se utilizara para recopilar datos históricos sobre el uso de recursos, ayudando a seguir e identificar patrones, de forma que podemos realizar ajustes proactivos en la configuración del sistema.

Beneficios del monitoreo.

A parte de los ya mencionados anteriormente debemos de tener en cuenta los siguientes puntos como beneficios importantes para nuestro laboratorio virtualizado.

- Detección proactiva de problemas: La supervisión continua de nuestro equipo, permite la identificación temprana de problemas en el rendimiento permitiendo así dar una respuesta rápida y efectiva.
- Optimización de recursos: las herramientas de monitoreo nos proporcionaran información valiosa para ayudar a ajustar la asignación de recursos de nuestras VMs y así poder optimizar el uso de la infraestructura.
- Estabilidad y fiabilidad: un monitoreo adecuado asegura que el laboratorio pueda operar de forma estable y confiable, garantizando así que todas las pruebas y prácticas que deseamos realizar se puedan ejecutar sin interrupciones correspondientes a problemas de recursos.

Teniendo en cuenta el control que se debe aplicar a las redes primero debemos de entender a qué hacemos énfasis. Al hablar de configuraciones de redes virtuales aisladas, que sean mediante el uso de VLANs y firewall, hacemos referencia al esquema en el que las máquinas virtuales (VMs) del laboratorio virtualizado se organizara en las redes lógicas, aunque físicamente estén compartiendo la misma infraestructura de red.

El aislamiento y protección de los que serán estas redes se lograra utilizando tecnologías como VLANs (Redes de Área local Virtuales), firewall y sistemas de detección de intrusos (IDS).

Estos funcionan de la siguiente manera:

- VLANs

una VLAN, permite la segmentación de una red física en varias redes lógicas. Esto da lugar a que podemos tener múltiples grupos de máquinas virtuales o servidores en una misma red física, pero que todas estén aisladas entre sí, es como si estuvieran en redes físicas separadas. Es decir, podemos de esta forma, tener una VLAN que sea destinada para estudiantes, donde realizaran pruebas y experimentos de seguridad, como así también una VLAN separada, la cual será para servidores críticos, tales como un servidor de base de datos o un servidor. Así también una red VLAN para los equipos de administración y monitoreo que estarán a cargo de gestionar y controlar el laboratorio.

Lo que lograremos con este aislamiento es que, si ocurre un ataque o vulnerabilidad a la red VLAN

de estudiantes, todos los demás no se vean comprometidos.

- Firewalls

Un firewall actúa como una barrera de seguridad el cual controla todo el trafica de las redes, este es el encargado de permitir y bloquear las conexiones en función de políticas de seguridad definidas. En un entorno como nuestro laboratorio, este puede configurarse en las máquinas virtuales o entre las VLANs de forma que se pueda utilizar para filtrar e inspeccionar el tráfico que entra o sale de nuestra red.

Utilizaremos esto para configurar cada VMs y permitir solamente el tráfico de puertos específicos y bloquear todos los demás puertos. Así también, bloquear las direcciones IPs no autorizadas o bien, limitar el acceso a ciertos servicios desde las direcciones IP específicas. Evitando así en nuestra VLAN, que maquinas no autorizadas accedan a recursos críticos en nuestra red.

- Sistema de detección de intrusos (IDS)

Es un sistema de detección de intrusos, es una herramienta la cual monitorea el tráfico de red, y todos los eventos de las máquinas, de forma que podamos detectar actividades sospechosas o maliciosas. A diferencia de lo que es un firewall, el cual bloquea el tráfico que no deseamos, el IDS detecta y notifica sobre posibles amenazas de seguridad tales como, intentos de hacking, escaneos de puertos o violaciones en las políticas de seguridad.

Implementaremos herramientas de IDS tales como Snort o Suricata, las cuales no servirán para monitorizar el tráfico existente entre las máquinas virtuales.

Estos IDS pueden detectar:

- Escaneo de puertos: Si un estudiante intenta escanear puertos los cuales estén abiertos en el servidor de prácticas, el IDS nos notificará.
- Ataques de fuerza bruta: Si alguien intenta acceder a nuestra red utilizando múltiples contraseñas fallidas, el IDS puede generar una alerta que nos permita tomar acciones preventivas tales como bloquear temporalmente la IP de origen.
- Anomalías en el tráfico de red: Si se detecta un volumen muy alto e inusual de tráfico, en un puerto o protocolo no habitual, el IDS es capaz de identificarlo como una posible señal de un ataque DDoS (Denegación de Servicio Distribuido).

- Certificación SSL/TLS (secure sockets layer/ transport layer security)

Es utilizado para cifrar la comunicación entre clientes y servidores a través de las redes públicas. Este cifrado nos asegura que todos los datos transmitidos no puedan ser interceptados ni leídos por terceros no autorizados.

Esta certificación se podrá implementar el laboratorio. Para obtenerla debemos recurrir a una autoridad certificadora (CA) confiable o se utilizaran certificados autofirmados para entornos de

prueba. Estos certificados se deberán instalar en los servidores web y de aplicaciones dentro de nuestro laboratorio.

Acto siguiente se deberá actualizar las configuraciones del servidor para poder forzar el uso de TLS y entonces deshabilitar las versiones anteriores y menos seguras de la SSL/TLS. Luego se implementarán procedimientos para realizar la renovación y actualización periódica de los certificados SSL/TLS, de forma que estemos seguros que los certificados estén siempre válidos y que las configuraciones del cifrado estén siempre actualizadas.

- VPN (Virtual Private Networks)

Los VPNs nos proporcionaran un canal seguro y cifrado para poder realizar la comunicación entre las redes o entre un usuario y una red. Esto será útil para proteger la información que se transfiere entre redes aisladas o entre los entornos de red ya sean remotos o locales.

Configuraremos el VPN desplegando servidores VPN utilizando soluciones como OpenVPN, o WireGuard, los cuales nos permitirán la conexión segura entre nuestras diferentes VLANs dentro de nuestro laboratorio, o entre el laboratorio y redes externas que pueden ser simuladas.

Las conexiones VPN serán configuradas para poder utilizar el cifrado robusto tales como AES-256, y autenticación fuerte mediante los certificados o claves pre compartidas. Y se establecerán políticas de acceso que restrinjan las conexiones VPN solo a usuarios o sistemas que estén autorizados.

Implementaremos herramientas de monitoreo para supervisar el tráfico de VPN, y así poder garantizar que todas las conexiones sean seguras. Y luego se realizarán auditorias periódicas para poder verificar las integridad y seguridad de las conexiones VPN.

- Autenticación de dos factores(2FA)

Para protección del acceso a aplicaciones: Lo que hará la autenticación en dos factores es añadir una capa adicional de seguridad a todo el proceso de autenticación, ya que requiere de dos formas de verificación para poder permitir el acceso. Generalmente, esto implica que el que usuario debe de tener una contraseña y luego además un código (el cual normalmente es enviado a un dispositivo móvil o generado por una aplicación de autenticación).

Habilitaremos la 2FA en todas las aplicaciones críticas y sistemas de administración las cuales estén dentro del laboratorio.

Las aplicaciones web y servicios utilizados en el laboratorio, todas serán configuradas para requerir 2FA en el proceso de inicio de sesión. Esto implica que se debe de ajustar todas las configuraciones en las aplicaciones y posiblemente integrarlas con servicios de identidad que puedan soportar 2FA.

Teniendo en cuenta todo esto tendremos altos beneficios en nuestro laboratorio, aplicando el

aislamiento de redes y minimizando así el riesgo de que un fallo o ataquen una VM comprometa nuestro entorno. Aplicando el control de acceso, de forma que podemos limitar el tráfico, y prevenir el acceso no autorizado, de forma que aseguramos que solo el tráfico legítimo y deseado pueda llegar a nuestros servidores. Aplicando el monitoreo proactivo, de forma que tengamos una supervisión continua del entorno, detectando y alertando sobre cualquier actividad que sea sospechosa o malintencionada, mucho antes de que este pueda causar daños. Aplicando la certificación SSL/TLS, VPNs, y la autenticación en dos factores (2FA) en el laboratorio, garantizaremos la protección adecuada de toda la información y seguridad de las aplicaciones. Ya que estas tecnologías trabajaran en conjunto para tanto como cifrar la información, como asegurar la comunicación entre nuestras redes, protegiendo el acceso a las aplicaciones críticas. Proporcionando así un entorno de prueba seguro y confiable, que podrá ser utilizado para las prácticas de seguridad en redes.

Teniendo en cuenta todo lo anterior debemos de enfocarnos en identificar y especificar las características físicas y lógicas requeridas para nuestra implementación del laboratorio de prácticas de seguridad en redes virtualizado. Utilizando siempre como guía y margen la norma ISO 27001, consideraremos los requisitos mínimos de hardware y lógica la cual nos garantice un entorno seguro, escalable y eficiente para nuestras prácticas académicas.

Primero debemos de entender que queremos decir con requisitos de hardware. toda la infraestructura física de nuestro laboratorio la cual debe de ser capaz de soportar múltiples máquinas virtuales (VMs) que se estén ejecutando simultáneamente.

Entonces, para ello podemos requerir los siguientes componentes mínimos:

- Servidor principal de servidores

Este servidor será nuestro corazón del laboratorio, ya que proporcionará la capacidad de procesamiento y memoria para poder ejecutar las demás máquinas virtuales (VMs). El laboratorio puede contar con decenas de VMs que simulen distintos equipos o sistemas de red y un servidor físico y principal tendrá el poder de alojar y manejar todas las demás VMs de manera eficiente.

Para ellos debemos de tener una maquina con un potencial decente el cual pueda manejar todos estos procesos un procesador multi-core (mínimo de 8 núcleos) ya que cada máquina virtual necesita tener capacidad de procesamiento, y este tipo de procesador permite distribuir toda la carga entre varias VMs, debemos de tener en cuenta que mientras más núcleos poseamos, mas VMs podemos ejecutar sin que el sistema se ralentice.

- RAM

La memoria RAM es fundamental para que las VMs porque cada máquina virtual consumirá una parte de la RAM. Entonces mientras más memoria RAM, más capacidad para tendremos para

correr múltiples VMs y por supuesto sin comprometer el rendimiento. Por tanto 64 GB sería el punto de partida y mientras más mejor.

- Tecnología de virtualización

Y por supuesto debemos de tener en cuenta que nuestro procesador soporte la virtualización por hardware ya sea Intel VT-x o AMD-v, ya que esta tecnología es la que permite que nuestros servidores puedan ser ejecutados en una máquina virtual de forma eficiente, de forma así que podemos reducir la sobrecarga de recursos y también mejorando el rendimiento en general de nuestra máquina virtual. Sin esta tecnología, nuestro servidor no podrá manejar las VMs de manera óptima.

- Almacenamiento

El apartado de almacenamiento de datos también es esencial porque las VMs necesitan espacio en el disco y para ellos los discos de estado sólido (SSD) con la tecnología NVMe nos ofrecen una velocidad de lectura/escritura significativamente más rápida que los discos duros (HDD) y esto es importante, ya que mediante esto podemos lograr que:

Nuestras VMs se inicien mucho más rápido y funcionen de manera más eficiente.

Los datos que se manipulen dentro puedan ser movidos y copiados mucho más rápido, lo cual puede ser crucial para ahorrar tiempo y que los estudiantes puedan realizar múltiples tareas a la par y guardar o restaurar estados de las VMs.

Y podemos decir lo mismo que antes, mientras más memoria, más capacidad y estabilidad tendremos.

- Conexión de red

Una buena conectividad de red rápida y estable es vital para que nuestras máquinas virtuales se comuniquen entre sí con el exterior. Para lo cual podemos tener en cuenta que podríamos tener una conexión de 1 Gbps como mínimo la cual es la velocidad estándar en muchos laboratorios y también oficinas. La cual puede ser suficiente para nuestras simulaciones.

Y de ser posible una conexión de 10Gbps en los servidores ya que de esta forma podremos manejar nuestro tráfico de red de manera más eficiente ya que esto nos permitiría el poder transferir grandes cantidades de datos rápidamente entre nuestras VMs o a través de nuestras VLANs, y sin cuello de botella.

- Sistema de alimentación ininterrumpida

Y claro tener una UPS (Sistema de alimentación ininterrumpida), ya que nuestro laboratorio debe de estar protegido contra posibles interrupciones de energía. El UPS nos brindará la seguridad y garantía de que nuestro servidor continúe trabajando y funcionando en caso de un corte de energía momentáneo y también de guardar a salvo las maquinas físicas, como también evitar que se puedan

perder o corromperse datos en los cuales se estuviesen trabajando en el momento.

Teniendo en cuenta la información brindada por el docente encargado del área, al contar un laboratorio de prácticas tendríamos estas principales ventajas;

1. Acceso directo a las herramientas especializadas: los estudiantes podrán acceder directamente a todas las herramientas necesarias para poder realizar las diversas prácticas. Esto eliminará toda necesidad de configurar el entorno cada vez que los estudiantes deseen realizar algún tipo de práctica, lo cual permitirá agilizar los trabajos y aprovechar de forma más efectiva los tiempos de clase.
2. Eficiencia y comodidad: Contando con una infraestructura lista para utilizarla, esto facilitará el proceso de enseñanza y aprendizaje, ya que el docente o los docentes encargados podrán concentrarse en el tema clave sin perder el tiempo en la preparación de todos los equipos, resultando así también una mayor eficiencia en la hora de la enseñanza.
3. Mejora en la calidad de la enseñanza: Al contar con un laboratorio virtualizado, este nos brindara la oportunidad de poder realizar también prácticas de configuraciones reales de seguridad de la información, como la implementación de firewall, sistemas de detección de intrusiones, VLANs, entre otros. Esto permitirá a los estudiantes que se puedan enfrentar a escenarios reales en un entorno controlado, lo cual facilitara significativamente la comprensión y también la preparación para el mundo laboral.
4. Cumplimiento del estándar ISO 27001: al implementar el laboratorio alineado a la norma ISO 27001 tendremos por seguro que nuestras practicas realizadas cumplirán con los estándares reconocidos a nivel mundial. Esto no solo nos garantizará estar en un entorno de aprendizaje seguro, sino que también preparará a los estudiantes para las exigencias del mercado laboral, donde estos estándares son más que necesarios de conocer y entender.

Y por otro lado tener como desventajas las siguientes:

1. Dependencia de recursos personales: Al no contar con un laboratorio de prácticas, los estudiantes se ven forzados a utilizar sus propios dispositivos y redes para realizar prácticas, lo cual limita el acceso a las herramientas especiales necesarias. Sumando además el hecho de no contar con un entorno el cual este controlado. Las oportunidades de aprender de esta forma se ven reducidas de esta forma.
2. Pérdida de tiempo en configuraciones: Una parte significativa se tiene que ver para la preparación de la clase y el entorno de trabajo, lo cual se traduce en un retraso en el avance de los temas importantes, lo cual afecta a la eficiencia del proceso y aprendizaje del mismo.
3. Riesgo de errores técnicos: Al trabajar en redes no controladas, los estudiantes están mas

expuestos a cometer errores los cuales pueden comprometer la seguridad y el funcionamiento de sus equipos. Este riesgo limita muchas posibilidades de aprender y experimentar las clases prácticas.

4. Enfoque teórico predominante: al no contar con un entorno practico, las clases tienden a ser más teóricas, lo cual reduce la oportunidad de desarrollar las habilidades que deberían de ser aplicadas. Esto resulta en una formación menos completa, ya que toda teoría sin llevarla a la práctica, no puede preparar de manera óptima a los estudiantes, de forma que estén preparados para encontrarse con desafíos reales que se encontraran en el ámbito profesional.
5. No alineados con la ISO 27001: al no contar con un laboratorio, no se cumpliría con la norma ISO 27001, entonces las practicas realizadas no seguirían los estándares de seguridad establecidas por la ISO, y esto podría restar competitividad a los estudiantes, quienes al no contar con los conocimientos necesarios podrían no estar completamente preparados para cumplir con las expectativas de las organizaciones que utilizan estas normativas.

Teniendo en cuenta todo lo anterior podemos realizar un presupuesta básico y avanzado de forma de cumplir con las normativas de la ISO 27001.
Básica:

Tabla 1. TABLA DE PRESUPUESTO SERVIDOR BÁSICO.

Componente	Marca/Modelo	Precio (GS)
Procesador	Intel Core i3-12100	1.082.000
Placa base	ASUS PRIME H610M-E D4	841.000
RAM	Adata XPG 32GB DD4 (2X16)	636.000
Almacenamiento	WD GREEN 120 GB	816.000
Fuente de poder	GIGABYTE GP-P650B 650W	600.000
Switch de red	TP-LINK TL-SG108	245.000
UPS	APC BACK 600VA, 120V	705.000
		4.925.000

Tabla 2. TABLA DE PRESUPUESTO DE SERVIDOR AVANZADO.

Avanzado:

Componente	Marca/Modelo	Precio (GS)
Procesador	AMD EPYC 9654	80.000.000
Placa base	GIGABYTE MZ72-HB0	10.000.000
RAM	Kingston Server Premier 512GB(8X64GB) DDR5 ECC	25.000.000
Almacenamiento	Samsung 990 Pro 2TB NVMe (x2, RAID 1)	7.000.000
	HDD Seagate Exos 18TB (x4, RAID 10)	11.000.000
Fuente de poder	Corsair AX1600i(1600W, Titanium)	3.000.000
Switch de red	Cisco Catalyst C9300-24T	30.000.000
UPS	APC Smart-UPS SRT 3000VA	12.000.000
Total		178.000.000

Cada componente fue seleccionado por su potencial y capacidad de trabajo y compatibilidad en este presupuesto, comenzando por el CPU el cual a día de hoy es uno de los procesadores en el área de servidores más potentes del mercado y es capaz de ofrecer un muy alto rendimiento aún bajo trabajos intensivos. La placa base que lo acompaña es uno de los más compatible con dicho CPU, y que también tiene la capacidad de gestionar múltiples GPUs, ranuras de NVMe, y la capacidad de funcionar con diversas configuraciones de RAID avanzadas, motivo por el cual es elegido, teniendo en cuenta una posible actualización. La memoria RAM es la mejor opción existente actualmente en cuanto a servidores, ya que no solamente cuenta con una velocidad de trabajo elevada, sino que también corrige errores de forma automática, de ahí el nombre de ECC (Error-Correcting Code Memory).
En cuanto al almacenamiento por un lado tenemos 2TB de NVMe en RAID 1 ya que, esta configuración de RAID hace que los datos se duplican para poder proteger toda la información importante.
Y por otro lado 18TB de HDD, en RAID 10, el cual combina rendimiento y seguridad, es decir RAID 1 + RAID 0. Mientras que el RAID 1 es el encargado de crear copias exactas de los datos, el RAID 0 se encarga de divide los datos, fragmentarlos y distribuir entre los discos de forma que se obtiene una mejora en el rendimiento.
La fuente de alimentación es una de las más eficientes y que cuenta con la certificación de Titanium, lo cual significa que genera pérdidas de energía menores a los demás y proporciona una mayor fiabilidad en operaciones de tiempo continuo.
La Switch elegida es la mejor e ideal para servidores, ya que cuenta con soporte avanzado para VLANs, así como también calidad de servicios y la capacidad de poder manejar tráfico de datos muy pesados.
Y para todo esto necesitamos una UPS acorde a lo que necesitamos, por tanto, UPS APC Smart-UPS SRT 3000VA nos proporcionara energía ininterrumpidas durante nuestros cortes eléctricos, protegiendo así, nuestro servidor y también sus datos

Si bien ya se ha expuesto las normativas a tener en cuenta, debemos de enfatizar en el hecho de que dicho servidor debe de tener un espacio dedicado, alejado de los demás equipos, polvo y la

humedad, ya que son equipos delicados. Estos deben de estar a una temperatura controlada, es decir entre 18ºC y 24º C o bajo un sistema de enfriamiento especial para su optimo funcionamiento. Debe de estar restringido a personas no autorizadas, y tener mucho cuidado de quien puede tener acceso al mismo.

También de ser posible el considerar tener un generador, en caso de largas o múltiples desconexiones eléctricas, así como también usar tanto cables como conectadores que tengan certificaciones de calidad, para así evitar riesgos de cortocircuito.

Es también recomendable el tener configurado un sistema de respaldo que este automatizado, para poder evitar pérdidas en caso de que existan fallos.

4. RESULTADOS Y ANÁLISIS

Implementación de controles de la ISO 27001 para el laboratorio de prácticas de seguridad en redes virtualizado.

Control A.5.1.1: Política de seguridad de la información [8]: Este control hace énfasis en la necesidad de contar con una política de seguridad de la información la cual sea relevante y que este establecida de acuerdo a los objetivos propuestos de la organización.

Aplicación en el laboratorio: En el laboratorio al decidir y obtener una política de seguridad la cual este definida de acuerdo con los objetivos de nuestro laboratorio, este será nuestra guía y norma para mantener la integridad del laboratorio y proteger la información de los participantes del laboratorio.

Para ello, se proponen las siguientes políticas de seguridad de la información:

- Congreso Nacional de Paraguay, Ley N° 6822/2021 de Protección de Datos Personales [9].
- Congreso Nacional de Paraguay, Ley N° 4017/2010 de Delitos Informáticos [10].
- Dirección General de Tecnologías de la Información y Comunicación, Plan Nacional de Ciberseguridad [10]
- Equipo de Respuesta ante Emergencias Informáticas, CERT-PY: Equipo de Respuesta ante Emergencias Informáticas [11].

Responsable: Responsable de Seguridad de la Información.

Control A.6.1.1: Roles y responsabilidades de seguridad de la información [8]: Este control establece que es de mucha importancia y necesidad definir y asignar roles y responsabilidades para todos los usuarios dentro de la organización, de forma que cada uno tenga una responsabilidad.

Aplicación en el laboratorio: Se asignarán roles tanto a los docentes, alumnos y parte administrativa encargada del laboratorio, en orden de que cada uno de ellos tengan permisos limitados a su capacidad. Por ejemplo, los alumnos solamente tendrán acceso a realizar las prácticas y ejercicios brindados por el docente encargado, mientras que los encargados del laboratorio pueden tener el control total sobre toda la infraestructura.

A continuación, se detallan los roles y las responsabilidades correspondientes:

1. **Responsable de Seguridad de la Información**

   Funciones:

   - Definir y mantener las políticas de seguridad de la información para el laboratorio.
   - Supervisar el cumplimiento de las normas de seguridad, como ISO 27001, dentro del laboratorio.
   - Gestionar los riesgos de seguridad de la información en la infraestructura virtualizada del laboratorio.
   - Asegurar que las prácticas de seguridad se alineen con las políticas y objetivos educativos del laboratorio.

2. **Administrador de Sistemas y Redes**

Funciones:

- Configurar y mantener la infraestructura de red y los sistemas del laboratorio virtualizado.
- Implementar controles de seguridad técnicos como firewalls, segmentación de red y controles de acceso.
- Monitorear el tráfico de red y detectar cualquier actividad anómala o no autorizada dentro del laboratorio.
- Gestionar las configuraciones de las máquinas virtuales y los recursos necesarios para las prácticas de los alumnos.
- Proporcionar mantenimiento y actualizaciones periódicas de los sistemas operativos y herramientas utilizadas en el laboratorio.

3. Analista de Seguridad

Funciones:

- Realizar análisis de vulnerabilidades y pruebas de penetración en la infraestructura virtualizada del laboratorio.
- Evaluar la eficacia de los controles de seguridad implementados dentro del laboratorio, como las políticas de acceso y los sistemas de protección de datos.
- Generar informes sobre incidentes de seguridad, recomendaciones de mejora y seguir procedimientos de mitigación de riesgos.
- Participar en la capacitación de los estudiantes en la identificación de vulnerabilidades comunes en redes y sistemas.

4. Auditor

Funciones:

- Realizar auditorías internas de seguridad de la información en el laboratorio, evaluando la efectividad de las políticas y controles.
- Verificar el cumplimiento de los procedimientos de seguridad establecidos, como la gestión de accesos y la protección de datos personales.
- Proponer mejoras en el sistema de gestión de seguridad de la información (SGSI) dentro del laboratorio.
- Evaluar la correcta implementación de los controles técnicos, tales como el control de acceso y la protección de las máquinas virtuales.

5. Responsable de Capacitación

Funciones:

- Desarrollar y actualizar los programas de capacitación en seguridad de la información para los estudiantes y docentes.

- Fomentar la concienciación sobre la seguridad de la información entre los usuarios del laboratorio (alumnos, docentes y personal administrativo).
- Evaluar la efectividad de los programas de formación en seguridad y ajustar los contenidos en función de los resultados obtenidos en las prácticas.
- Organizar talleres y simulacros de incidentes para mejorar la respuesta ante situaciones reales de seguridad.

6. Gestor de Incidentes de Seguridad

Funciones:

- Coordinar la respuesta ante incidentes de seguridad dentro del laboratorio, asegurando una actuación rápida y eficaz ante cualquier vulnerabilidad o brecha de seguridad.
- Documentar y analizar los incidentes para detectar patrones y prevenir futuros problemas de seguridad.
- Establecer procedimientos a seguir ante incidentes como accesos no autorizados, ataques DDoS, malware, pérdida de datos, etc.
- Colaborar con el responsable de la seguridad de información en la mejora continua del SGSI y asegurar que todos los procedimientos de gestión de incidentes estén documentados y actualizados.
- Realizar simulacros de incidentes para evaluar la preparación del laboratorio ante situaciones de riesgo.

7. Personal de Soporte Técnico

Funciones:

- Proporcionar soporte técnico en la implementación de medidas de seguridad, como actualizaciones de software, instalación de parches de seguridad y configuración de máquinas virtuales.
- Ayudar a los usuarios finales (alumnos y docentes) a cumplir con las políticas de seguridad dentro del laboratorio, como la configuración adecuada de contraseñas y la gestión de accesos.
- Monitorear y reportar problemas de seguridad que puedan surgir durante las prácticas, como vulnerabilidades en las máquinas virtuales o el tráfico de red.
- Colaborar con el personal administrativo en la gestión de la infraestructura del laboratorio y garantizar que los recursos estén siempre operativos y seguros.

Control A.7.2.2: Capacitación en seguridad de la información [8]: Este control establece que, se debe de asegurar que tanto como los alumnos como los encargados del laboratorio reciban la capacitación necesaria y concientización sobre la seguridad de la información periódicamente.

Aplicación en el laboratorio: Antes de comenzar las practicas brindadas por el encargado del laboratorio o docente, los alumnos tendrían una capacitación sobre las buenas prácticas de seguridad. Esta capacitación es fundamental para que todos puedan comprender los riesgos y la importancia de conocer medidas de protección que se deben de tener durante todas las practicas.
Se propone el desarrollo de los siguientes puntos:

Tabla 3. TABLA DE PROPUESTA DE CAPACITACIONES.

Clase	Duración	Responsable	Objetivos	Contenidos
1	2 horas	Responsable de Capacitación	- Comprender conceptos básicos de seguridad.	- Conceptos de seguridad de la información.
			- Identificar riesgos y amenazas.	- Confidencialidad, integridad, disponibilidad.
				- Tipos de amenazas.
				- Introducción a ISO/IEC 27001.
2	2 horas	Responsable de Capacitación	- Conocer controles de seguridad.	- Tipos de controles de seguridad.
			- Realizar evaluación de riesgos.	- Herramientas de evaluación de riesgos.
				- Políticas de seguridad.
3	2 horas	Responsable de Capacitación, Gestor de Incidentes	- Comprender respuesta a incidentes.	- Proceso de gestión de incidentes.
			- Promover mejora continua.	- Roles y responsabilidades.
				- Mejores prácticas para la mejora continua.

Control A.11.1.2: Controles de entrada física [8]: Este control hace énfasis en no solo contar con controles lógicos, sino también físicos para poder restringir el acceso a las áreas en donde se pueden acceder a información importante.
Aplicación en el laboratorio: Solo los estudiantes de turno y el personal de turno podrá ingresar al laboratorio, se deberá de tener cerraduras, y de ser posible el uso de tarjetas de autenticación físicas para el acceso al laboratorio.
Para ello se hace las siguientes propuestas:

- Implementación de tarjetas de identificación para restringir el acceso al laboratorio únicamente a personas autorizadas (administradores, docentes y personal administrativo).
- Instalación de sistemas biométricos (como huella dactilar o reconocimiento facial) para reforzar la seguridad en el acceso al laboratorio, asegurando que solo las personas autorizadas puedan ingresar.
- Establecimiento de un sistema de control y registro para la entrada y salida de equipos y materiales del laboratorio, con el fin de evitar el robo o mal uso de los recursos.

- Implementación de medidas para garantizar que las estaciones de trabajo estén protegidas de accesos no autorizados, como el uso de bloqueos automáticos o contraseñas en las estaciones de trabajo.

Responsable: Administrador de sistemas y redes.

Control A.12.1.3 Gestión de la capacidad [8]: Este control exige que todos los recursos de los sistemas informáticos tanto como los recursos de red, procesamientos y almacenamientos, sean todos gestionados de forma que se garantice su disponibilidad y rendimientos adecuados para poder satisfacer las demandas actuales y futuras.

Aplicación en el laboratorio: en el diseño del laboratorio, se asegura que todos los recursos asignados a las máquinas virtuales, tales como CPU, RAM y almacenamiento serán suficientes para soportar múltiples entornos virtualizados trabajando simultáneamente. Se implementarán Sistemas de monitoreo que permitirán evaluar la capacidad de los recursos en tiempo real, asegurando que no se comprometa el rendimiento del entorno virtualizado durante toda la ejecución de las pruebas.

Se propone realizar controles:

- Supervisar y gestionar los recursos del sistema (servidores, redes, almacenamiento) para garantizar un rendimiento óptimo.
- Asegurar que la infraestructura del laboratorio pueda satisfacer las demandas actuales y futuras de los usuarios.
- Cálculos de concurrencia para analizar la capacidad adecuada de los componentes.

Para los cálculos de concurrencia se utilizarán las siguientes formulas:

Para EL CPU

$$\frac{\text{Número total de hilos} \times \text{Porcentaje de uso permitido}}{\text{Consumo de CPU por usuario}}$$

Para la memoria RAM

$$\frac{\text{RAM total disponible}}{\text{Consumo promedio de RAM por usuario}}$$

Para el ancho de banda

$$\frac{\text{Ancho de banda total disponible}}{\text{Consumo promedio de red por usuario}}$$

Control A.13.1.1 Control de Redes [8]: Este control se establece debido a la necesidad de proteger la seguridad y operatividad de las redes de información a través de mecanismos tales como el control de acceso, la segregación de redes y la monitorización de tráfico.

Aplicación en el laboratorio: El laboratorio contará con configuraciones de redes virtuales aisladas mediante el uso de VLANs y firewalls, donde cada segmento de red será monitorizado para controlar el tráfico entre las máquinas virtuales de forma que se podrá prevenir accesos no autorizados. Adicionalmente se implementará también sistemas de detección de intrusos (IDS) para identificar posibles violaciones de seguridad dentro del entorno virtualizado.

Para la implementación, se propone el uso de Suricata (IDS) para realizar las siguientes operaciones:

- Monitoreo de tráfico en tiempo real
- Análisis y detección de amenazas
- Integración con firewalls y segmentación de redes
- Pruebas periódicas

Y para ellos se realiza la siguiente propuesta de procedimiento para el manejo del control de redes son los siguientes:

1. Segmentación de Red

Objetivo: Aislar diferentes áreas de la red para mejorar la seguridad y el control de acceso.
Acciones:

- Crear VLANs separadas:
- VLAN estudiantes: para acceso a recursos educativos y servicios generales.
- VLAN profesores: para recursos exclusivos y herramientas pedagógicas.
- VLAN administrativa: para administración y gestión de datos sensibles.
- VLAN servidores: para mantener los servidores en una red aislada, protegiendo su acceso.

2. Control de Acceso

Objetivo: Asegurar que solo usuarios autorizados tengan acceso a los recursos de la red.
Acciones:

- Implementar 802.1X para autenticar dispositivos en la red, garantizando que solo los usuarios autorizados se conecten.
- Establecer un sistema de gestión de contraseñas robustas.
- Registrar direcciones MAC address para limitar el acceso a dispositivos específicos.
- Crear un portal cautivo para visitantes que requiera autenticación antes de acceder a los recursos de la red.

3. Monitoreo de Tráfico

Objetivo: Detectar y responder a amenazas en tiempo real.
Acciones:

- Implementar un sistema IDS/IPS (Intrusion Detection/Prevention System) para monitorear y prevenir intrusiones en la red.
- Centralizar los logs de todos los dispositivos para facilitar la auditoría y análisis de seguridad.
- Realizar monitoreo de tráfico en tiempo real para identificar actividades sospechosas.
- Configurar alertas automáticas que notifiquen al administrador de cualquier anomalía o intento de acceso no autorizado.

4. Políticas de Seguridad

Objetivo: Establecer directrices claras para el uso seguro de la red y los recursos.

Acciones:

- Documentar procedimientos de seguridad y las mejores prácticas para el uso de la red.
- Definir roles y responsabilidades para los administradores de red y usuarios, asegurando que cada uno entienda su papel en la protección de la red.
- Establecer horarios de acceso para limitar el acceso en horas no laborales, reduciendo riesgos.
- Crear una política de uso aceptable que describa los comportamientos permitidos en la red.

5. Protección Perimetral
Objetivo: Proteger la red contra accesos no autorizados desde el exterior.
Acciones:

- Configurar un firewall para filtrar el tráfico entrante y saliente, bloqueando accesos indeseados.
- Crear una DMZ (Zona Desmilitarizada) para servicios públicos accesibles externamente, protegiendo los sistemas internos.
- Implementar VPN para permitir acceso remoto de manera segura a la red.
- Filtrar contenido web para bloquear sitios maliciosos o inapropiados y reducir el riesgo de infecciones por malware.

6. Mantenimiento Continuo
Objetivo: Mantener la red protegida a largo plazo con medidas de mantenimiento regulares.
Acciones:

- Realizar actualizaciones periódicas de software y hardware para corregir vulnerabilidades conocidas.
- Establecer backups regulares de configuraciones y datos críticos para recuperación ante incidentes.
- Revisar mensualmente las configuraciones de red para garantizar que las políticas de seguridad se sigan correctamente.
- Aplicar parches de seguridad tan pronto como sean disponibles para prevenir vulnerabilidades.

7. Capacitación y Concientización
Objetivo: Asegurar que los usuarios y administradores comprendan y sigan las políticas de seguridad.
Acciones:

- Proveer inducción a nuevos usuarios sobre las mejores prácticas de seguridad en la red.
- Realizar actualizaciones trimestrales de capacitación para mantener a todos informados sobre las nuevas amenazas y políticas.

- Simular incidentes de seguridad para entrenar al personal en respuesta ante amenazas reales.
- Mantener la documentación actualizada sobre procedimientos y políticas de seguridad.

8. Gestión de Incidentes de Seguridad
Objetivo: Prepararse y responder eficazmente a incidentes de seguridad.
Acciones:

- Establecer un protocolo de respuesta detallado que especifique qué hacer en caso de un incidente de seguridad.
- Designar un equipo de respuesta a incidentes, preparado para actuar de inmediato en caso de detectarse una brecha de seguridad.
- Mantener un registro detallado de incidentes para analizar las causas y tomar medidas preventivas en el futuro.
- Elaborar un plan de continuidad que permita que el laboratorio recupere rápidamente su funcionamiento tras un incidente de seguridad.

Responsables: Administrador de Sistemas y Redes, responsables de seguridad de la información, analista de seguridad, auditor de seguridad, responsable de capacitación y gestor de incidentes
Control A.13.2.1 Seguridad en la transferencia de información [8]: Este control exige la protección de la información transferida dentro de las redes y hacia redes externas, de forma que se minimicen todos los posibles riesgos de interceptación de datos o modificación de datos.
Aplicación en el laboratorio: Para las prácticas de transferencia de información, se hará uso de VPNs y cifrados SSL/TLS de forma que la información transferida este protegido durante el tránsito del mismo. Adicionalmente este deberá ser supervisado en el tráfico de redes con el objetivo de detectar y prevenir posibles intentos de ataques.
Se propone el uso de TLS (Transport Layer Security) para proporcionar un protocolo de cifrado de extremo a extremo en las configuraciones, y garantizando la integridad de nuestros datos. Utilizando este protocolo para realizar las siguientes acciones:

- Cifrado de conexiones en servicios web y aplicaciones
- Aplicación en transferencias de correo electrónico y bases de datos
- Autenticación mutua
- Protección contra ataques MITM (Man-in-the-Middle)

Se propone los siguientes procedimientos a tener en cuenta para la protección y seguridad en la transferencia de información:
1. Cifrado de la Información en Tránsito
Objetivo: Asegurar que la información transferida dentro de las redes y hacia redes externas esté protegida contra interceptaciones o modificaciones.
Acciones:

- Implementar VPNs (Virtual Private Networks) para proteger las conexiones de red y cifrar toda la información transferida a través de redes públicas.

- Asegurar que todos los servicios web y aplicaciones que manejen información sensible utilicen certificados SSL/TLS para cifrar las conexiones entre los servidores y los clientes.
- Configurar TLS para garantizar la integridad y confidencialidad de los datos en tránsito, proporcionando un cifrado de extremo a extremo.

2. Protección en Transferencias de Correo Electrónico y Bases de Datos
Objetivo: Garantizar que los datos transferidos a través de otros canales, como correo electrónico o bases de datos, estén protegidos.
Acciones:

- Utilizar TLS para cifrar el correo electrónico durante su transmisión, protegiendo así tanto el contenido como los archivos adjuntos contra posibles interceptaciones.
- Implementar cifrado en las bases de datos para las conexiones de clientes y servidores, utilizando TLS en las conexiones de base de datos, asegurando que la información sensible esté cifrada tanto en reposo como en tránsito.

3. Autenticación Mutua
Objetivo: Asegurar que tanto el cliente como el servidor se autentiquen mutuamente durante la transferencia de información.
Acciones:

- Configurar la autenticación mutua utilizando certificados digitales para que ambas partes (cliente y servidor) puedan verificar la autenticidad de la otra antes de intercambiar información.
- Esto se puede aplicar en conexiones de bases de datos, aplicaciones web, y otros servicios críticos dentro del laboratorio.

4. Prevención contra Ataques Man-in-the-Middle (MITM)
Objetivo: Proteger las comunicaciones contra posibles ataques en los que un atacante se interpone entre el cliente y el servidor para interceptar o modificar la información.
Acciones:

- Utilizar TLS para proteger las conexiones y evitar que los datos sean interceptados o alterados por atacantes en un ataque MITM.
- Configurar los sistemas para verificar la validez de los certificados SSL/TLS durante cada sesión de comunicación, asegurando que el canal de comunicación no haya sido comprometido.

5. Monitoreo y Supervisión del Tráfico de Red
Objetivo: Detectar y prevenir intentos de ataques durante la transferencia de información.
Acciones:

- Implementar herramientas de monitoreo de red para supervisar el tráfico en tiempo real y detectar cualquier comportamiento sospechoso que podría indicar un intento de interceptación o modificación de datos.

- Realizar auditorías periódicas para verificar que las políticas de cifrado y protección estén siendo correctamente aplicadas.

Responsables: Administrador de Sistemas y Redes, responsables de seguridad de la información y analista de seguridad.

Control A.14.1.2: Protección de aplicaciones en redes públicas [8]: Este control exige la implementación de medidas de protecciones, las cuales pueden ser cifrado y autenticaciones de forma que se pueda asegurar la integridad y confidencialidad de la información transmitida a través de todas las redes públicas.

Aplicación en el laboratorio: Dentro de las practicas del laboratorio se simularán entornos en los que las aplicaciones estén expuestas a redes públicas, como internet, y para asegurar la protección de los datos, se implementarán certificados SSL/TLS para el cifrado de la información en tránsito, así como también VPNs para la conexión segura entre las redes. Adicionalmente también se configurarán mecanismos robustos de autenticación, como la autenticación en dos factores o en dos pasos (2FA), para proteger el acceso a las aplicaciones.

Se propone el uso de WAF (Web Application Firewall), para proteger las aplicaciones y los sistemas en las redes públicas contra accesos no autorizados y ataques cibernéticos.

Se le dará uso en los siguientes puntos:

- Protección contra ataques comunes
- Autenticación y Cifrado
- Monitoreo y análisis de tráfico
- Control de acceso

Y también se propone realizar el siguiente procedimiento para la protección de las aplicaciones en redes públicas:

1. Cifrado de la Información

Objetivo: Asegurar la confidencialidad e integridad de los datos transmitidos a través de redes públicas.

Acciones:

- Implementar certificados SSL/TLS en todas las aplicaciones web expuestas a redes públicas (como Internet) para cifrar las comunicaciones.
- Asegurar que el cifrado sea de grado adecuado para proteger la información durante su transmisión, evitando que los datos sean interceptados por terceros no autorizados.

2. Autenticación Segura

Objetivo: Garantizar que solo usuarios autorizados accedan a las aplicaciones.

Acciones:

- Implementar autenticación de múltiples factores (MFA), como la autenticación en dos pasos (2FA), para verificar la identidad de los usuarios antes de que puedan acceder a las aplicaciones.
- Utilizar autenticación robusta (por ejemplo, mediante certificados digitales o tokens de seguridad) para proteger las credenciales de los usuarios.

3. Uso de VPNs

Objetivo: Asegurar la conexión segura entre las redes del laboratorio y las aplicaciones expuestas a redes públicas.
Acciones:

- Implementar VPNs (Virtual Private Networks) para cifrar la conexión entre las redes internas del laboratorio y las aplicaciones accesibles a través de Internet.
- Garantizar que los túneles VPN sean fuertes y robustos, utilizando protocolos de seguridad avanzados como IPsec o OpenVPN para proteger la integridad de la comunicación.

4. Protección contra Ataques Comunes
Objetivo: Defender las aplicaciones y servicios contra amenazas conocidas que circulan por redes públicas.
Acciones:

- Implementar un WAF (Web Application Firewall) para filtrar el tráfico malicioso y proteger las aplicaciones de ataques comunes, como inyección SQL, cross-site scripting (XSS) y ataques de denegación de servicio (DDoS).
- Configurar el WAF para identificar y bloquear automáticamente solicitudes sospechosas y maliciosas en tiempo real.

5. Monitoreo y Análisis de Tráfico
Objetivo: Detectar y prevenir accesos no autorizados y amenazas en tiempo real.
Acciones:

- Configurar sistemas de monitoreo de tráfico para analizar las solicitudes que llegan a las aplicaciones, identificando patrones anómalos que puedan indicar un ataque.
- Utilizar herramientas de análisis de tráfico para realizar auditorías periódicas y detectar vulnerabilidades en la infraestructura de las aplicaciones expuestas.

6. Control de Acceso
Objetivo: Limitar el acceso a las aplicaciones basándose en roles y necesidades específicas.
Acciones:

- Implementar políticas de control de acceso basado en roles para asegurar que los usuarios solo tengan acceso a las aplicaciones y datos necesarios para sus tareas.
- Establecer permisos granulares para cada aplicación, asegurando que se mantenga un principio de mínimos privilegios.

Responsables: Administrador de Sistemas y Redes, responsables de seguridad de la información y analista de seguridad.
Control A.16.1.1: Gestión de incidentes de seguridad [8]: Este control exige el tener establecido un procedimiento el cual seguir para reportar y gestionar incidentes de seguridad.
Aplicación en el laboratorio: Este control exige que se cuente con un protocolo a seguir por parte de los estudiantes y administradores del laboratorio ante cualquier incidente de seguridad que pueda ocurrir durante el desarrollo de las practicas, las cuales puede ser intentos de ataques o intento de acceso no autorizado. Esto para poder facilitar la identificación del problema y vulnerabilidad, de forma que se puedan ajustar medidas para futuras ocasiones.

Las funciones principales para este control abarcan los siguientes puntos:

- Definir y mantener procedimientos para gestionar incidentes de seguridad.
- Coordinar la respuesta ante incidentes, asegurando una pronta recuperación y minimización de daños.

Para ello se propone el siguiente procedimiento:

1-Identificación del Incidente

Objetivo: Detectar y reconocer un incidente de seguridad en el laboratorio.

Acciones:

- Monitoreo continuo: Utilizar herramientas de monitoreo (como IDS, WAF y logs de servidor) para detectar actividad sospechosa.
- Alerta: El sistema de monitoreo o un usuario (administrador, docente o alumno) debe generar una alerta si se detecta un comportamiento anómalo, como intentos de acceso no autorizado, tráfico malicioso, o anomalías en las aplicaciones.
- Clasificación: Clasificar el incidente según su gravedad (bajo, medio, alto) para determinar la respuesta apropiada.

2-Contención del Incidente

Objetivo: Limitar el impacto del incidente y evitar su propagación.

Acciones:

- Aislamiento: Desconectar los sistemas afectados de la red para evitar que el ataque se propague a otras partes del laboratorio.
- Bloqueo de acceso: Utilizar firewalls o sistemas de gestión de acceso para restringir el acceso de usuarios no autorizados o maliciosos.
- Desactivación de servicios: Si es necesario, desactivar servicios o aplicaciones comprometidas hasta que se resuelva el incidente.

3. Erradicación del Incidente

Objetivo: Eliminar las causas del incidente y restaurar el entorno a su estado seguro.

Acciones:

- Análisis forense: Revisar logs, registros de red y sistemas para identificar cómo ocurrió el incidente y qué vulnerabilidades fueron explotadas.
- Eliminación de malware: Si el incidente involucra malware, eliminarlo completamente de los sistemas afectados.
- Parcheo de vulnerabilidades: Actualizar o corregir las vulnerabilidades que permitieron el incidente (por ejemplo, actualizando software, configuraciones de seguridad o aplicando parches).

4. Recuperación

Objetivo: Restaurar los sistemas afectados y permitir que el laboratorio vuelva a funcionar de manera normal.

Acciones:

- Restauración de servicios: Rehabilitar los servicios o aplicaciones afectados, asegurando que se hayan corregido las vulnerabilidades.
- Verificación de la integridad: Comprobar que los sistemas restaurados estén operativos y libres de amenazas adicionales.
- Monitoreo post-incidente: Aumentar la vigilancia sobre los sistemas para detectar cualquier signo de reaparición del incidente.

5. Análisis y Lecciones Aprendidas
Objetivo: Analizar el incidente para mejorar la respuesta ante futuros incidentes y fortalecer las políticas de seguridad.
Acciones:

- Informe del incidente: Elaborar un informe detallado que documente el incidente, las acciones tomadas, y los resultados de la respuesta. Este informe debe incluir detalles sobre cómo se detectó el incidente, las vulnerabilidades explotadas, las acciones de contención y erradicación, y el tiempo de respuesta.
- Revisión de políticas: Evaluar si las políticas y controles existentes fueron efectivos o si necesitan mejoras. Esto puede incluir cambios en la configuración de seguridad, capacitación adicional, o una revisión de las herramientas de monitoreo.
- Capacitación: Basado en el análisis del incidente, se pueden diseñar programas de capacitación adicionales para el personal y los estudiantes sobre la prevención de incidentes similares en el futuro.
- Simulacro de incidentes: Realizar simulacros de incidentes para mejorar la preparación y la capacidad de respuesta ante futuros incidentes reales.

6. Comunicación y Reporte
Objetivo: Informar a todas las partes interesadas sobre el incidente y sus resoluciones.
Acciones:

- Notificación interna: Comunicar al personal del laboratorio (administradores, docentes, personal administrativo) los detalles del incidente y las acciones tomadas.
- Informe a autoridades: Si el incidente involucra violaciones significativas de datos o actividad delictiva, como accesos no autorizados a datos sensibles, debe informarse a las autoridades competentes (por ejemplo, una agencia gubernamental de protección de datos o cibercrimen).
- Herramientas y Recursos
- Sistemas de detección de intrusos (IDS): Como Snort, Suricata, o Zeek, para detectar actividades sospechosas en la red.
- Firewalls: Configurados para bloquear tráfico malicioso, como iptables o pfSense.

- Sistemas de gestión de incidentes: Como Splunk o SIEM (Security Information and Event Management), para gestionar, rastrear y analizar incidentes en tiempo real.

Responsables: Responsable de seguridad de la información, administrador de sistemas y redes, analista de seguridad, gestión de incidentes y personal de soporte técnico.
Control A.18.2.3: Revisión Independiente de la seguridad de la información [8]: Este control exige que se realicen de forma preventiva en un periodo determinado evaluaciones del cumplimiento de los controles de seguridad.
Aplicación en el laboratorio: Cada determinado tiempo el laboratorio debe de ser auditado, con el objetivo de verificar que todos los controles de seguridad se estén cumpliendo y también verificar que no existan ningún tipo de vulnerabilidad.
Se propone realizar revisiones periódicas y para ello controlar los siguientes puntos, como objetivos a cumplir:

Tabla 4. TABLA DE AUDITORIA.

Categoría	Actividad	Cumple (Sí/No)
I. Políticas y Procedimientos		
	Verificar políticas de uso de la red, acceso a equipos, configuración de dispositivos y respuesta a incidentes.	
	Confirmar que estudiantes y personal estén al tanto de las políticas y procedimientos de seguridad.	
	Asegurar que los usuarios firmen un acuerdo de uso aceptable antes de acceder al laboratorio.	
II. Seguridad Física y Ambiental		
	Acceso restringido mediante tarjetas o claves.	
	Registro de entrada y salida del laboratorio.	
	Vigilancia con CCTV.	
	Inventario actualizado y almacenamiento seguro de equipos.	
	Protección física contra robos, daños o manipulación.	
	Sistemas de detección y extinción de incendios.	
	Planes de evacuación y protección ante desastres naturales.	
III. Seguridad de la Red y Dispositivos		
	Separación de la red del laboratorio de la red universitaria.	
	Segmentación interna para diferentes usuarios y proyectos.	

	Contraseñas seguras y desactivación de servicios innecesarios.	
	Implementación de firewalls, IDS/IPS y DLP en la red del laboratorio.	
	Monitoreo del tráfico de red para detectar anomalías.	
IV. Gestión de Vulnerabilidades y Parches		
	Realización de escaneos periódicos en equipos y dispositivos de red.	
	Uso de herramientas automatizadas para identificar vulnerabilidades.	
	Proceso de instalación oportuna de parches de seguridad.	
	Pruebas de los parches antes de implementación en el entorno de producción.	
V. Gestión de Incidentes de Seguridad		
	Plan de respuesta a incidentes adaptado al laboratorio.	
	Realización de simulacros periódicos para evaluar la eficacia del plan de respuesta.	
	Capacitación para el personal y estudiantes en la respuesta a incidentes.	
VI. Consideraciones Adicionales		
	Verificar la seguridad de la plataforma de virtualización y las máquinas virtuales si se utilizan.	
	Implementación de autenticación robusta y cifrado de comunicaciones para accesos remotos.	
	Establecer políticas claras sobre el uso de dispositivos personales en la red.	
VII. Revisión y Mejora Continua		
	Realización de auditorías internas o externas para evaluar la eficacia de las medidas de seguridad.	
	Revisión y actualización de políticas y procedimientos adaptados a nuevas amenazas y mejores prácticas.	
	Monitoreo continuo del panorama de amenazas para mantenerse informado.	

Responsable: Auditor de seguridad.

Teniendo todos los criterios mencionados, podemos hacer uso de la concurrencia para analizar y comparar la diferencia entre ambos servidores propuestos.

Entonces por el lado del servidor básico, haciendo una suposición de un uso del 10% por cada usuario del CPU, unos 200MB por cada usuario y unos 10Mbps de ancho de banda, con nuestro switch de 1Gbps, nos daría como resultado de la aplicación de las fórmulas los siguientes datos:

$$Cantidad\ de\ usuaris\ para\ el\ CPU: \quad \frac{8hilos \times 80\%}{10\%} = 64$$

$$Cantidad\ de\ usaurios\ para\ la\ memoria\ RAM: \frac{32GB \times 1024}{200MB} = 163$$

$$Cantidad\ de\ usuario\ para\ la\ Red: \frac{1000Mbps}{10Mbps} = 100$$

Mientras que para el servidor avanzado, utilizando los mismos valores de uso obtenemos los siguientes datos:

$$Cantidad\ de\ usuarios\ para\ el\ CPU: \quad \frac{192hilos \times 80\%}{10\%} = 1536$$

$$Cantidad\ de\ usaurios\ para\ la\ memoria\ RAM: \frac{32GB \times 1024}{200MB} = 1048$$

$$Cantidad\ de\ usuario\ para\ la\ Red: \frac{1000Mbps}{10Mbps} = 1000$$

Como resultado de las aplicaciones de las fórmulas obtenemos los siguientes resultados y podemos realizar la comparación.

Tabla 5. TABLA DE COMPARACION DE CONCURRENCIA DE SERVIDORES.

Recurso	Configuración Básica	Configuración Mejorada
Usuarios por CPU	64 usuarios	1536 usuarios
Usuarios por RAM	163 usuarios	2621 usuarios
Usuarios por Red	100 usuarios	1000 usuarios

Análisis de viabilidad.

Una vez hechas todas las comparaciones, y cumpliendo todos los requisitos necesarios, procedemos a analizar el proyecto, desde el punto de vista financiero, operativo y técnico.

Para ello hemos hecho una tabla en donde se aprecia todo el análisis desarrollado.

Tabla 6. TABLA DE ANALISIS DE VIABILIDAD.

<table>
<tr><th>Aspecto</th><th>Descripción</th><th>Análisis Financiero</th><th>Análisis Operativo</th><th>Análisis Técnico</th></tr>
<tr><td colspan="5">Financiero</td></tr>
<tr><td>Inversión Inicial</td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">- Hardware</td><td rowspan="2">Servidores, almacenamiento, red</td><td>Básica: GS 4.925.000</td><td>Responsables: Administrador de Sistemas y Redes</td><td>Procesador Intel i3-12100, 32GB RAM, SSD 120GB, switch TP-Link TL-SG108, UPS 600VA.</td></tr>
<tr><td>Mejorada: GS 178.000.000</td><td>Personal de Soporte Técnico</td><td>Mejorada: Procesador AMD EPYC, 512GB RAM ECC, NVMe 2TB, HDD 18TB RAID, switch Cisco Catalyst, UPS 3000VA.</td></tr>
<tr><td rowspan="2">Software</td><td rowspan="2">Sistema operativo, virtualización, herramientas (virtualización, simuladores de red, seguridad)</td><td>Costo total de software: 32.000.000 Gs</td><td>Operador principal: Administrador de Sistemas</td><td>Licencias de sistemas operativos, herramientas de virtualización y gestión de red.</td></tr>
<tr><td>Costo de licencias y software adicional: 10.000.000 Gs</td><td>Responsables: Gestor de Seguridad</td><td>Herramientas de simulación de redes, software de seguridad.</td></tr>
<tr><td rowspan="4">Seguridad</td><td rowspan="4">Firewall, IDS/IPS, software de cifrado</td><td>Costo total de seguridad: 40.000.000 Gs</td><td>Operador principal: Gestor de Seguridad</td><td rowspan="4">Implementación de firewall, IDS/IPS, software de cifrado de disco completo.</td></tr>
<tr><td>- Firewall: 20.000.000 Gs</td><td rowspan="3">Responsables: Administrador de Sistemas</td></tr>
<tr><td>- IDS/IPS: 15.000.000 Gs</td></tr>
<tr><td>- Cifrado: 5.000.000 Gs</td></tr>
<tr><td colspan="5">Operativo</td></tr>
</table>

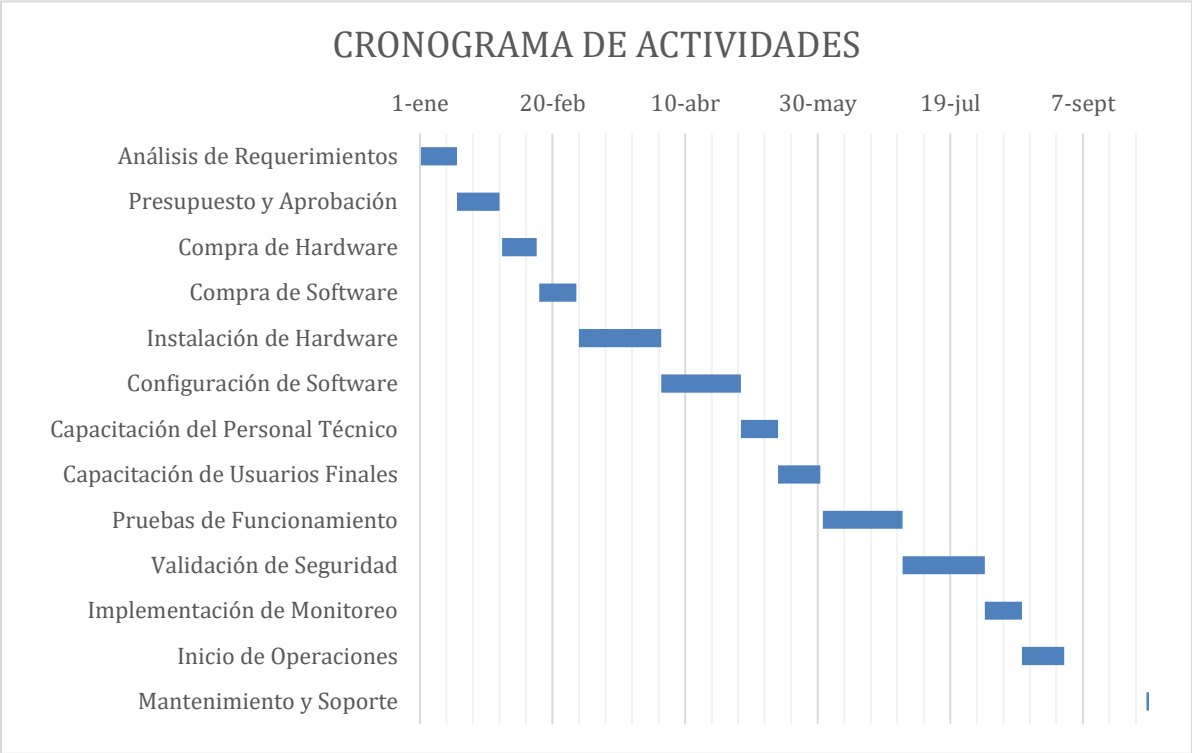
Accesibilidad	Acceso remoto para estudiantes y profesores	Costo de Internet (200 Mbps): 140.000 Gs/mes	Responsable: Administrador de Sistemas y Redes	Configuración de VPN, plataforma de acceso remoto segura (VPN, escritorio remoto).
		Certificado SSL/TLS: 64.000 Gs/año	Monitoreo continuo del acceso remoto	Ancho de banda adecuado para acceso concurrente.
Flexibilidad	Adaptación a diferentes cursos y necesidades	Hardware Básico: 4.925.000 Gs	Responsable: Administrador de Sistemas y Redes	Capacidad para crear redes virtuales, gestionar configuraciones y snapshots.
		Hardware Mejorado: 178.000.000 Gs	Responsable de Capacitación	
Gestión de Recursos	Uso eficiente de hardware y software	Auditorías ISO: 48.180.000 Gs/año	Responsables: Administrador de Sistemas y Redes, Analista de Seguridad	Implementación de sistemas de monitoreo como Zabbix, monitoreo de recursos.
		Costo Total Inicial (Servidor Básico): 85.289.000 Gs	Monitoreo de uso de recursos (CPU, memoria, almacenamiento)	Auditoría de recursos, reportes periódicos.
		Costo Total Inicial (Servidor Mejorado): 258.364.000 Gs		Implementación de cuotas de recursos.
Cumplimiento	Alineación con ISO 27001	Certificación ISO Inicial: 80.300.000 Gs	Responsable: Responsable de Seguridad de la Información, Auditor	Implementación de SGSI basado en ISO 27001, análisis de riesgos, controles de seguridad.
		Auditorías Recurrentes ISO: 48.180.000 Gs/año	Supervisión de auditorías externas	Documentación de políticas y procedimientos de seguridad.
Técnico				
Infraestructura				

Virtualización	Plataforma de virtualización (VMware, Hyper-V)	Licencia de VMware/Hyper-V: 10.000.000 Gs a 30.000.000 Gs	Operador principal: Gestor de Seguridad	Plataforma adecuada (VMware, Hyper-V), infraestructura que soporte virtualización.
Almacenamiento	Sistema de almacenamiento centralizado	Costo de SSD 2TB: 7.000.000 Gs	Operador principal: Gestor de Seguridad	Sistema de almacenamiento eficiente y redundante (RAID 10), seguridad en acceso y encriptación de datos.
		Costo HDD Seagate Exos 18TB (x4, RAID 10): 11.000.000 Gs	Responsables: Administrador de Almacenamiento y Seguridad	
Red				
Switches	Conectar y gestionar máquinas virtuales	Costo de Switch Cisco Catalyst C9300-24T: 30.000.000 Gs	Operador principal: Gestor de Incidentes	Configuración de switches virtuales, seguridad de red configurada para máquinas virtuales.
Firewall	Controlar tráfico de red entrante y saliente	Costo de Firewall (Software/Hardware): 5.000.000 Gs - 15.000.000 Gs	Operador principal: Gestor de Seguridad	Configuración de firewall virtual, monitoreo de tráfico.
Seguridad				
Control de acceso	Autenticación y autorización de usuarios	Costo de Software de Control de Acceso: 1.500.000 Gs	Operador principal: Gestor de Seguridad	Implementación de políticas de autenticación y autorización estrictas.
		Costo de Hardware de Control de Acceso: 3.000.000 Gs	Responsables: Administrador de Seguridad	Uso de herramientas de control de acceso.
Protección contra malware	Antivirus, antimalware	Costo de Antivirus/Antimalware: 2.000.000 Gs	Operador principal: Gestor de Seguridad	Implementación de protección contra malware, sistema de detección y respuesta.

Copias de seguridad	Sistema de backup y recuperación	Costo de Almacenamiento (RAID, NAS): 7.000.000 Gs	Operador principal: Gestor de Seguridad	Sistema automatizado de backups regulares, almacenamiento redundante.
		Costo de software de backup: 1.000.000 Gs	Responsables: Administrador de Sistemas	
Mantenimiento				
Actualizaciones	Actualizaciones de software y firmware	Costo de actualizaciones de software: 1.000.000 Gs/año	Operador principal: Gestor de Seguridad	Implementación de un sistema de gestión de actualizaciones.
		Costo de actualizaciones de hardware: 5.000.000 Gs	Responsables: Administrador de Sistemas	Actualización periódica de firmware y sistemas operativos.
Monitoreo	Supervisión del rendimiento y la seguridad	Costo de software de monitoreo (Nagios, Zabbix): 2.000.000 Gs	Operador principal: Gestor de Incidentes	Implementación de herramientas de monitoreo, capacitación para gestionar incidentes.
		Costo de equipos de monitoreo: 5.000.000 Gs (opcional)	Responsables: Administrador de Sistemas y Seguridad	
Inversión Total	Básica: 378.938.000 Gs			
	Mejorada: 498.364.000 Gs			

Una vez realizado el análisis exhaustivo, se procede a realizar el cronograma de actividades del proyecto:

Figura 1. CRONOGRAMA DE ACTIVIDADES.



El cronograma del proyecto de implementación del laboratorio de prácticas de seguridad en redes virtualizado, basado en la norma ISO 27001, se estructurará en diversas fases técnicas, cada una con actividades específicas que garantizarán el cumplimiento de los objetivos establecidos. En la fase de planificación, se implementará un análisis exhaustivo de los requerimientos técnicos, operativos y funcionales necesarios para el desarrollo del laboratorio, identificando las necesidades prioritarias y los objetivos que deberán alcanzarse. Posteriormente, se elaborará un presupuesto que incluirá la estimación de costos y recursos, el cual será sometido a evaluación y aprobación para asegurar la viabilidad económica y estratégica del proyecto antes de avanzar.

Durante la fase de adquisición, se procederá a la compra de hardware y software. En este proceso, se adquirirán los equipos físicos, como servidores, estaciones de trabajo y componentes de red, que deberán cumplir con las especificaciones requeridas para soportar el entorno virtualizado. De igual manera, se gestionará la adquisición de licencias y aplicaciones especializadas necesarias para la virtualización y la gestión de la seguridad, asegurando que estén alineadas con los estándares definidos por la norma ISO 27001.

En la fase de implementación, se llevará a cabo la integración de los componentes adquiridos. Se realizará, en primer lugar, la instalación del hardware, que incluirá el montaje físico y la conexión de los equipos. A continuación, se procederá con la configuración del software, ajustando las aplicaciones y plataformas para garantizar su correcta funcionalidad y su adaptación a los requerimientos del sistema.

La fase de capacitación se enfocará en preparar a los actores clave del proyecto. Se capacitará al personal técnico para que puedan operar, administrar y mantener el entorno virtualizado, mientras que los usuarios finales recibirán formación para utilizar de manera adecuada y segura las herramientas implementadas, promoviendo prácticas alineadas con los estándares de seguridad.

En la fase de pruebas y validación, se realizarán pruebas de funcionamiento con el objetivo de evaluar el desempeño técnico del sistema y verificar la integración correcta de todos los componentes. Asimismo, se llevará a cabo la validación de seguridad, donde se comprobará el cumplimiento de los controles de seguridad estipulados en la norma ISO 27001, asegurando la protección de los datos mediante la confidencialidad, integridad y disponibilidad.
Finalmente, en la fase de puesta en marcha, se implementará un sistema de monitoreo que permitirá supervisar de manera continua las operaciones del laboratorio virtualizado. Posteriormente, se iniciarán las operaciones, poniendo en funcionamiento el sistema de acuerdo con los objetivos previamente establecidos. Por último, se garantizará la sostenibilidad del proyecto mediante la fase de mantenimiento, donde se proporcionará soporte técnico continuo y se aplicarán actualizaciones necesarias para mantener la estabilidad, la eficiencia y la funcionalidad del laboratorio a largo plazo. Este enfoque, planeado meticulosamente, permitirá desarrollar un laboratorio virtualizado confiable, operativo y alineado con los más altos estándares internacionales de seguridad.

Resultados de la encuesta.
Informe de la encuesta aplicada a alumnos los cuales ya cursaron la materia de seguridad en redes.
La encuesta realizada proporciono una visión general sobre la percepción de los estudiantes acerca de los contenidos desarrollados y los métodos utilizados en la enseñanza de la materia, en donde en los resultados se reflejan que varias áreas requieren una mayor atención de forma que se pueda mejorar la efectividad del curso, haciendo énfasis especial en lo que respecta a la preparación practica de la materia.
Una gran parte de los estudiantes (70%), considera que el conocimiento obtenido por la materia, no proporciono los conocimientos suficientes para poder comprender adecuadamente todos los riesgos y posibles soluciones en lo que respecta a la seguridad de la información, por lo que esta percepción sugiere que el enfoque del curso podría estar muy centrado en la teoría, sin aplicar y utilizar la suficiente practica que pueda ayudar a los estudiantes a interiorizar estos conceptos. De forma similar, muchos estudiantes (60%) no tuvieron la posibilidad de realizar prácticas de configuraciones de seguridad en redes tales como firewalls, VLANs o IDS, lo cual resalta una posible brecha entre la teoría impartida y la aplicación de lo impartido.
En cuanto al conocimiento obtenido referente a la ISO 27001 se encuentra también una disparidad, aunque una porción significativa de los alumnos (40%) esta familiarizada con la norma y comprende lo que implica dicha norma, mientras tanto por otra parte (43%) solo tiene un conocimiento superficial.
Por otro lado, la mayoría de los alumnos (79%) considera que un laboratorio de prácticas, habría mejorado su aprendizaje notoriamente, lo cual subraya la importancia de incorporar herramientas que sean interactivas en el proceso educativo. Este dato también sirve para dar pie a cuan beneficioso podría ser la aplicación práctica de los conocimientos desarrollados, con los cuales los alumnos se verían más familiarizados con el contenido, y logrando así una comprensión más profunda y completa.
En términos generales, los resultados sugieren que el curso de Seguridad en Redes podría verse altamente beneficiado, contando con la integración de un laboratorio de prácticas de seguridad en redes, el cual permitiría que los alumnos puedan aplicar lo aprendido de manera más tangible. Además, es crucial para el desarrollo de los futuros profesionales, para que puedan tener desarrollo profesional, obteniendo el conocimiento necesario sobre el área de seguridad en redes, tales como

la norma ISO 27001, asegurando así no solo la comprensión teórica, sino también la capacidad de solucionar problemas reales y poder implementar y gestionar las herramientas necesarias en escenarios reales.

En resumen, la implementación de un laboratorio de prácticas de seguridad en redes, es una necesidad para la mejora de la calidad de la enseñanza, brindando a los alumnos una experiencia más completa y también realista a las situaciones que se podrían encontrar en su futuro como profesional.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El proyecto para crear un laboratorio virtualizado de prácticas de seguridad en redes, basado en la norma ISO 27001, es una propuesta clave para mejorar las habilidades prácticas de los estudiantes en el área de seguridad informática. A través del análisis de las necesidades y las características necesarias, hemos podido identificar los aspectos técnicos y físicos que son cruciales para que este laboratorio funcione correctamente, además de asegurarnos de que se cumplan las mejores prácticas de seguridad.

Por un lado, hemos revisado los requisitos tanto lógicos (como el uso de virtualizadores, sistemas de protección perimetral, antivirus y cifrado) como físicos (equipos como servidores, switches, enrutadores, etc.) que permitirán mantener el laboratorio seguro y operando de forma eficiente. Sin estos componentes, sería muy difícil garantizar la estabilidad y la protección del entorno.

En cuanto al análisis de viabilidad, la parte técnica del proyecto es totalmente viable. Sin embargo, la gran barrera será el aspecto económico, ya que se requiere una inversión considerable en hardware, software y en la capacitación de los involucrados. A pesar de esto, los beneficios que aportaría el proyecto, tanto en el aprendizaje de los estudiantes como en el prestigio de la facultad, lo hacen una propuesta valiosa.

El cronograma de actividades está bien planificado, con fases claras que incluyen desde la evaluación de los requerimientos hasta el mantenimiento del laboratorio. Cada actividad está cuidadosamente organizada para asegurar que se cumpla con los plazos establecidos, garantizando que el proyecto avance de manera ordenada y sin contratiempos.

Aunque el proyecto enfrenta algunos desafíos financieros, los beneficios que puede generar a largo plazo justifican el esfuerzo. La creación de este laboratorio sería una excelente oportunidad para mejorar las competencias en seguridad de los estudiantes y contribuir al fortalecimiento de la infraestructura educativa de la facultad. No obstante, será esencial llevar a cabo un análisis económico más detallado para asegurarnos de que sea sostenible en el tiempo.

En resumen, el proyecto tiene un enorme potencial educativo y representa un paso importante hacia el cumplimiento de los estándares internacionales de seguridad informática. Si bien la viabilidad financiera es un reto, con una planificación adecuada se pueden encontrar soluciones para hacer que esta iniciativa sea una realidad, brindando grandes oportunidades para todos los involucrados.

5.2. Recomendaciones

Si en un futuro se desea implementar este proyecto, como recomendación primeramente se debería de realizar una evaluación detallada del presupuesto con el cual cuenta la facultad, ya que el implementar este proyecto conlleva ciertos costos significativos, tanto en material tecnológico, como también en licencias. Se podría hacer uso de apoyos financieros, ya sea a través de asociaciones con algunas empresas que sean del sector tecnológico o de ciberseguridad la cual podría ser una alternativa viable para cubrir estas necesidades.

Es de suma importante con también poder contar con un equipo de trabajo el cual este compuesto por puramente profesionales que posean experiencia en diversas áreas, ya sean virtualización, seguridad de la información y por supuesto redes. Ya que para implementar el laboratorio y que este cumpla con los requisitos de la norma ISO 27001, se necesitarían profesionales capacitados para poder gestionar y mantener estas tecnologías, tales como firewall, IDS, redes VLANs, y las herramientas de monitore. Por tanto, el trabajo en equipo seria esencial para mantener un entorno seguro y eficiente.

Además, es de suma importancia planificar de manera meticulosa y adecuada el mantenimiento y también la actualización del laboratorio. Dado que las tecnologías siempre tienden a estar en constante evolución, para ello será necesario tener actualizaciones de forma periódica de todos los sistemas. También se debería de mantener una supervisión constante de forma que se pueda asegurar que se cumplan todos los controles de seguridad requeridos por la norma ISO 27001.

También es muy importante tener cada etapa de proceso documentado, ya que esto no solamente serviría para aprender de la experiencia, sino que también de esta forma se podría garantizar, que el proyecto se mantenga siempre con las mejores prácticas de seguridad. La materialización de este proyecto no solamente mejoraría la calidad de educación de la institución, sino también podría ofrecer una muy importante y valiosa mejora, y oportunidad para adquirir nuevas experiencias prácticas en un entorno controlado y seguro, lo cual prepararía a los futuros profesionales a estar preparados para los futuros retos profesionales a los que se podrían enfrentar en el área laboral en el campo de la ciberseguridad.

Teniendo también en cuenta que la FCyT es miembro de la red Ciberlac, se podría llegar a un acuerdo para realizar capacitaciones tanto por parte de los docentes como también de los alumnos en el área de seguridad de la información y el uso del laboratorio de prácticas.

Como también es recomendable para los encargados del laboratorio el poder realizar cursos, diplomados o especializaciones en el área de ciberseguridad, y seguridad de la información teniendo en cuenta de que existen organizaciones en donde se puede obtener estas certificaciones tales como Coursera. Donde podemos encontrarnos con certificaciones profesionales y con instructores de la empresa de Google.

Además, también podemos encontrar Cisco Certified Network Associate (CCNA), de forma que realmente los encargados del laboratorio sean completamente expertos en el área y se pueda mantener en las correctas condiciones el laboratorio de prácticas de seguridad en redes virtualizado.

6. BIBLIOGRAFÍA

[1] D. E. CARDONA ZAPATA and A. M. SANCHEZ PIEDRAHITA, DISEÑO DE UN LABORATORIO DE SEGURIDAD DE LA INFORMACION PARA EL TECNOLÓGICO DE ANTIOQUIA, MARIA, 2019.

[2] J. Gómez Velázquez, Laboratorio de ciberseguridad en un entorno empresarial virtualizado.

[3] J. P. GONZÁLEZ ROLÓN, DISEÑO DE UN LABORATORIO PARA PRÁCTICA DE SISTEMAS DE PROTECCIONES ELÉCTRICAS DE POTENCIA BASADO EN DISPOSITIVOS PROGRAMABLES UTILIZADOS EN SUBESTACIONES DE ALTA TENSIÓN PARA LA FCYT DE LA UNCA.

[4] A. G. TORRES ZARZA, DISEÑO DE UN LABORATORIO DE ENSAYOS PARA LA CERTIFICACIÓN DE EFICIENCIA ENERGÉTICA EN APARATOS DE REFRIGERACION AUTOCONTENIDOS Y ACONDICIONADORES DE AIRE.

[5] F. J. MARIN SANABRIA, DISEÑO DE UN LABORATORIO DE ENSAYOS DE RUTINA DE TRANSFORMADORES DE DISTRIBUCIÓN PARA LA FACULTAD DE CIENCIAS Y TECNOLOGÍAS DE LA UNCA.

[6] J. R. D. J. AQUINO GOROSTIAGA and C. N. BÁEZ VÁZQUEZ, IMPLEMENTACIÓN DE UN LABORATORIO DE MECÁNICA DE SUELOS PARA LA FACULTAD DE CIENCIAS Y TECNOLOGÍAS DE LA UNIVERSIDAD NACIONAL DE CAAGUAZÚ.

[7] J. R. R. Sartorio, Políticas de seguridad en Sistemas de Información para el rectorado de la Universidad Nacional del Caaguazú en el año 2017.

[8] "ISO," [Online]. Available: https://www.iso.org/home.html.

[9] L. A. Luengas, J. C. Guevara and G. Sánchez, ¿Cómo desarrollar un laboratorio virtual? Metodología de diseño.

[10] "CISCO," [Online]. Available: https://www.cisco.com/c/es_ar/index.html.

[11] A. Roca López, Laboratorio de ciberseguridad en un entorno virtualizado, Almería, 2021.

[12] D. Britos, L. Vargas, S. Arias, N. Giraudo and G. Veneranda, Laboratorio Virtual y Remoto para la Enseñanza de Diseño, PARANA-ENTRE RIOS, 2013.

[13] D. D. Journal, Examining VMware, 2000.

[14] M. Soriano, Seguridad en redes y seguridad.

[15] ORACLE, Oracle VM VirtualBox.

[16] "Objetivos de Desarrollo Sostenible," [Online]. Available: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/.

[17] "NORMA ISO 27001," [Online]. Available: https://www.normaiso27001.es/.

[18] A. P. Lorandi Medina, G. Hermida Saba, J. Hernández Silva and E. L. de Guevara Durán, Los Laboratorios Virtuales y Laboratorios Remotos en la Enseñanza de la Ingenieria.

[19] A. C. Ballesteros and J. Tapia Zuñiga, DISEÑO E IMPLEMENTACIÓN DE UN LABORATORIO VIRTUAL DE CINEMATICA EN LA UNIVERSIDAD DE CORDOBA.

[20] "Global Suite Solutions," [Online]. Available: https://www.globalsuitesolutions.com/es/.

[21] MITIC, "MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION DEL PARAGUAY," [Online]. Available: https://www.mitic.gov.py.

[22] CERT-PY, "Equipo de Respuesta ante Emergencias Informáticas de Paraguay," [Online]. Available: cert.gov.py..

[23] DIGETIC, "Dirección General de Tecnologías de la Información y Comunicación," [Online]. Available: https://digetic.mil.py/.

7. ANEXOS

Encuesta

1. ¿Consideras que la materia de Seguridad en Redes te proporcionó los conocimientos necesarios para entender los riesgos y soluciones en seguridad informática?

- Sí
- No

2. ¿Qué tan claro tienes el concepto de firewall y su función en una red?

- Lo entiendo completamente
- Tengo una idea general, pero no estoy seguro/a
- No lo entiendo

3. ¿Durante la materia, tuviste la oportunidad de practicar configuraciones de seguridad en redes (como firewalls, VLANs, IDS, etc.)?

- Sí
- No
- Solo de forma teórica

4. ¿Qué tan familiarizado/a estás con la norma ISO 27001?

- La conozco y entiendo sus implicaciones en la seguridad de la información
- La he escuchado, pero no tengo claro qué implica
- No la conozco

Descripción breve de la norma ISO 27001: La ISO 27001 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información. Ayuda a las organizaciones a proteger sus activos de información de amenazas internas y externas mediante controles y procedimientos adecuados.

5. ¿Consideras que haber tenido un laboratorio virtualizado durante la materia habría mejorado tu aprendizaje práctico?

- Sí, definitivamente
- Tal vez
- No, creo que no habría hecho diferencia

6. En una escala del 1 al 5, ¿cómo evaluarías tu capacidad actual para diseñar e implementar medidas de seguridad en redes?

- 1 (muy bajo)
- 2
- 3 (regular)
- 4
- 5 (muy alto)

7. ¿Te sientes preparado/a para aplicar los conocimientos adquiridos en un entorno laboral real?
   - Sí, completamente
   - En parte
   - No

8. ¿Te gustaría haber tenido acceso a un laboratorio de prácticas con herramientas virtualizadas para realizar simulaciones de seguridad en redes?
   - Sí
   - No
   - Tal vez