# UNIVERSIDAD POLITÉCNICA SALESIANA

# SEDE QUITO

## CARRERA DE COMPUTACIÓN

## EVALUACIÓN DE UN ESCENARIO DE SEGURIDAD DE LOS ENTORNOS VIRTUALIZADOS EN EL DATA CENTER DE LA CARRERA DE COMPUTACIÓN, DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO – CAMPUS SUR

Trabajo de titulación previo a la obtención del

Título de: Ingeniera en Ciencias de la Computación

AUTOR: SASKIA REBECA GUERRERO GARRIDO

TUTOR: JORGE ENRIQUE LÓPEZ LOGACHO

Quito – Ecuador

2024

**CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN**

Yo, Saskia Rebeca Guerrero Garrido con documento de identificación N° 1752138022 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucros la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 21 de febrero del 2024

Atentamente,

Saskia Rebeca Guerrero Garrido

1752138022

**CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA**

Yo, Saskia Rebeca Guerrero Garrido con documento de identificación N° 1752138022, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Proyecto Técnico: "Evaluación de un escenario de seguridad de los entornos virtualizados en el Data Center de la Carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito - Campus Sur", el cual ha sido desarrollado para optar por el título de: Ingeniera en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 21 de febrero del 2024

Atentamente,

Saskia Rebeca Guerrero Garrido

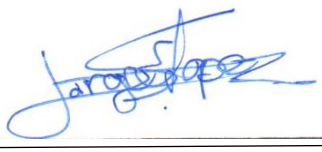
1752138022

## CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Jorge Enrique López Logacho con documento de identificación N° 1712082484, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: EVALUACIÓN DE UN ESCENARIO DE SEGURIDAD DE LOS ENTORNOS VIRTUALIZADOS EN EL DATA CENTER DE LA CARRERA DE COMPUTACIÓN, DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO - CAMPUS SUR, realizado por Saskia Rebeca Guerrero Garrido con documento de identificación N° 1752138022, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 21 de febrero del 2024

Atentamente,



Ing. Jorge Enrique López Logacho, MSc.

1712082484

## DEDICATORIA

Dedico este trabajo a aquellos que han sido faros de luz en mi travesía académica. A mis padres, y hermanos cuyo amor incondicional ha sido mi mayor apoyo, y cuya dedicación a mi educación ha sido un regalo invaluable. A mi familia extendida, por su constante estímulo y comprensión. A mis amigos, cuyas risas han iluminado los días más oscuros y cuyo apoyo ha sido un recordatorio constante de que no estoy sola en este viaje.

A mis ingenieros, quienes han compartido generosamente su conocimiento y han guiado mi camino con paciencia y sabiduría. A todos aquellos que, de una forma u otra, han creído en mí y me han brindado su ayuda incondicional.

Y, finalmente, esta dedicatoria es para mí misma, como un recordatorio de la perseverancia, la resistencia y el esfuerzo dedicados a alcanzar este sueño. Este logro no solo representa el final de un capítulo, sino el comienzo de nuevas y emocionantes aventuras.

Saskia Rebeca Guerrero Garrido

## AGRADECIMIENTO

Agradezco a Dios por haberme concedido la fortaleza, la claridad mental y la perseverancia necesaria durante todo este proceso de mi carrera.

Quiero expresar mi sincero agradecimiento a mi tutor de tesis: Jorge Enrique López Logacho por su dedicación, sabiduría y paciencia infinita. Su orientación experta y apoyo constante fueron fundamentales para dar forma y estructura a mis ideas, llevándome más allá de mis propios límites intelectuales.

A mi lector José Luis Aguayo Morales por impartir su conocimiento y ayuda en el proceso del trabajo de titulación.

Finalmente, agradezco a todos los ingenieros, que, de alguna manera, contribuyeron a mi crecimiento académico y personal.

Saskia Rebeca Guerrero Garrido

## ÍNDICE DE CONTENIDOS

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

## RESUMEN

En el presente proyecto técnico indica como la virtualización se ha ido implementando dentro de las industrias y como a la vez existe un aumento en los ataques virtuales, es por lo que, dentro del Data Center de la Carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito – Campus Sur, se va a replicar un entorno virtualizado para evaluar mediante herramientas que busquen brechas de seguridad que exploten las vulnerabilidades, para posteriormente documentar los resultados obtenidos.

La metodología que mejor se adapta a este proyecto técnico es el método Mehari que consiste en realizar una auditoría, evaluación de riesgos o evaluación de seguridad en el cual permite analizar las vulnerabilidades y amenazas que se expone el Data Center.

En conclusión, el realizar una evaluación hacia un entorno virtualizado permite identificar los posibles riesgos al que se están exponiendo y así evitar que la información se pierda o sea utilizada para fines maliciosos.



**Palabras clave:** máquinas virtuales, vulnerabilidades, Windows, Ubuntu, entorno virtualizado, máquina objetivo, evaluación, escaneos, explotación, Data Center.

## ABSTRACT

This technical project indicates how virtualisation has been implemented within industries and how at the same time there is an increase in virtual attacks, which is why, within the Data Centre of the Computer Science Department of the Salesian Polytechnic University, Quito - South Campus, a virtualised environment will be replicated to evaluate using tools that search for security gaps that exploit vulnerabilities, and subsequently document the results obtained.

The methodology that best suits this technical project is the Mehari method, which consists of carrying out an audit, risk assessment or security assessment in which the vulnerabilities and threats that the Data Centre is exposed to are analysed.

In conclusion, carrying out an assessment of a virtualised environment makes it possible to identify the possible risks to which it is exposed and thus prevent information from being lost or used for malicious purposes.



**Keywords:** virtual machines, vulnerabilities, Windows, Ubuntu, virtualised environment, target machine, assessment, scans, exploitation, Data Center.

# INTRODUCCIÓN

Realizar una evaluación significa que se debe tomar en cuenta las medidas para mitigar riesgos o brechas de seguridad que no se hayan identificado. Según Gallardo (2018):

> En el ámbito de la tecnología informática, las máquinas virtuales representan una solución cada vez más adoptada por las empresas debido a su flexibilidad y capacidad para funcionar como sistemas informáticos. Sin embargo, esta misma flexibilidad también plantea un desafío importante en términos de seguridad, ya que las máquinas virtuales pueden ser vulnerables a posibles ataques que pongan en riesgo la integridad de la información alojada en ellas, incluyendo la posibilidad de robo de la máquina completa.

El crecimiento de la virtualización es evidente en los últimos años, convirtiéndose en un estándar dentro de las industrias. Esta adopción se debe, en gran medida a los beneficios que ofrece en términos de capacidad de almacenamiento y procesamiento en infraestructuras cada vez más reducidas. Sin embargo, el aumento de la virtualización también ha llevado a un aumento en la sofisticación y frecuencia de los ataques virtuales, lo que subraya la importancia de abordar adecuadamente la seguridad en los sistemas virtualizados.

Es fundamental implementar estrategias de seguridad adecuadas a las particularidades de cada entidad para resguardar tanto los sistemas operativos como la información contenida en las máquinas virtuales.

En este contexto, el presente trabajo tiene como objetivo evaluar el escenario de seguridad de los entornos virtualizados en el Data Center. A través de herramientas y con una metodología que se adapte y ayude a garantizar la confidencialidad e integridad de los datos almacenados y transmitidos, así como para mitigar riesgos y prevenir accesos no autorizados. Con ello, se busca reforzar la infraestructura de seguridad y proporcionar una mayor protección tanto para estudiantes y docentes que utilizan las máquinas virtuales.

## ANTECEDENTES

Desde hace algunos años, las máquinas virtuales han ido tomando un gran apogeo ya sea a nivel empresarial o personal, ya que funciona como una máquina física donde se puede realizar varias pruebas y si existe algún daño, solo se pierde la información de la máquina virtual. Según Gallardo (2018):

> Las máquinas virtuales (virtual machines), a diferencia de un equipo físico, las máquinas virtuales funcionan como sistema informático virtual con su propia CPU, memoria, interfaz de red y almacenamiento, que, si bien representa flexibilidad para el administrador, también significa una vulnerabilidad que puede ser explotada para robar la máquina completa, incluyendo su contenido.

En los últimos años la virtualización ha experimentado una considerable aceptación dentro de las empresas, convirtiéndose en un estándar de la industria. Esta adopción se debe principalmente a los beneficios relacionados con las capacidades de almacenamiento y procesamiento en infraestructuras cada vez más reducidas. Según Universidad de Veracruz (s.f.)

> La seguridad se vuelve un elemento crucial para mitigar las amenazas informáticas y evitar que los sistemas virtualizados se vean afectados por posibles incidentes. Los riesgos cibernéticos pueden impactar los sistemas, independientemente de si están desplegados en entornos físicos o virtuales. Sin embargo, las estrategias de protección varían según las características específicas de cada entorno, especialmente al tener en cuenta que la gestión de sistemas virtualizados se realiza a través de un hipervisor.

Por ello, se debe tener en cuenta la protección de datos que tienen las máquinas virtuales para evitar exponer los datos ante personas que hagan mal uso. Según Universidad de Veracruz (s.f.)

Cuando se busca salvaguardar los sistemas operativos y la información almacenada en máquinas virtuales, se pueden aplicar diversas estrategias de seguridad adaptadas a la infraestructura específica de cada organización. En el contexto de la protección contra amenazas maliciosas, una opción directa es la instalación de software de seguridad en cada sistema virtualizado, una medida que preserva la privacidad de la información contenida en el sistema informático y se alinea con entornos virtuales. Este método de seguridad, conocido como protección basada en agentes (agent-based), contrasta, no obstante, con el objetivo de maximizar la eficiencia de los recursos de hardware.

Se debe tener en cuenta que al implementar máquinas virtuales e instalar un software de seguridad consume recursos lo que provoca que el incremento sea exponencial afectando el rendimiento y sobre todo el entorno virtual. Según Universidad de Veracruz (s.f.)

Similar a cualquier otro software, un antivirus consume los recursos de todas las máquinas virtuales en las que está presente, incluyendo tanto espacio en disco como memoria. La razón radica en que una herramienta antimalware dentro de cada sistema requiere su propio motor de análisis y detección de códigos maliciosos, además de actualizaciones que son independientes tanto del software en sí como de la base de datos de firmas de malware. Este consumo de recursos aumenta de manera proporcional al número de máquinas virtuales, generando una demanda lineal. En el modelo tradicional cliente-servidor, cuando el antivirus realiza actualizaciones o exploraciones, estas operaciones se llevan a cabo simultáneamente en todas las máquinas virtuales. De manera análoga, al identificar malware, el antivirus tiende a ponerlo en cuarentena o iniciar procesos de escaneo y limpieza en toda la máquina virtual, implicando un mayor consumo de recursos.

## PROBLEMA

El presente proyecto busca dar respuesta a la interrogante de ¿Cómo se evalúa el escenario de seguridad de los entornos virtualizados en el Data Center, en términos de protección contra la pérdida de datos, acceso no autorizado y la mitigación de riesgos contra la pérdida de datos?

En la actualidad, la virtualización se ha convertido en una práctica común en los entornos de los Data Centers, ofreciendo beneficios significativos en términos de eficiencia y flexibilidad. Sin embargo, junto con estos avances también surgen desafíos en cuanto a la seguridad de los entornos virtualizados. La evaluación del escenario de seguridad en estos entornos se vuelve muy importante para garantizar la protección de datos, el acceso autorizado y la mitigación de riesgos. Es por ello por lo que se detallará los elementos que se consideran importantes para esta evaluación.

- **Protección de datos:** Se deben aplicar medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos almacenados y transmitidos en los sistemas virtualizados. Usando algoritmos criptográficos para cifrar los datos, así dando garantía de que se encuentran asegurados los datos que tienen las máquinas virtuales. (Universidad Nacional de Córdoba, s.f.)
- **Acceso autorizado:** Se debe mantener la seguridad en los entornos virtualizados y prevenir accesos no autorizados a los sistemas y datos sensibles. Además, tener un control sobre los roles que cumplen las personas que tienen acceso evitando actividades sospechosas. (Universidad Nacional de Córdoba, s.f.)
- **Mitigación de riesgos:** Es fundamental para reducir la exposición a amenazas y minimizar los impactos de posibles incidentes de seguridad en los entornos virtualizados. (Universidad Nacional de Córdoba, s.f.)

El proceso de evaluación de vulnerabilidades implica tener un objetivo claro frente a las amenazas que podrían afectar la seguridad e integridad. Según Paredes (2022):

> Al realizar una evaluación de vulnerabilidades, pruebas, análisis con algunas técnicas se evita que el riesgo sea profundo. Además, aplicar regularmente parches y actualizaciones de seguridad en los sistemas y software utilizados en los entornos virtualizados. Al aplicar estos conceptos en la evaluación práctica permitirá identificar áreas de mejora y tomar medidas efectivas para fortalecer la seguridad en los entornos virtualizados.

## JUSTIFICACIÓN

Cuando se busca proteger los sistemas operativos y la información en las máquinas virtuales, se pueden aplicar enfoques de seguridad adaptados a la infraestructura de cada organización. Por ejemplo, la instalación de software antimalware en cada sistema virtualizado puede brindar protección contra códigos maliciosos.

Además, un antivirus en cada máquina virtual consume recursos como espacio en disco y memoria, lo que incrementa linealmente con el número de máquinas virtuales. Las actualizaciones, exploraciones y limpieza de malware también pueden generar un mayor consumo de recursos. Las máquinas que se encuentran en el Data Center; son muy importantes ya que contiene información valiosa, entre ellas está: academia, tesis, docentes, investigación, es por ello por lo que se debe conocer el estado de seguridad que tiene dichas máquinas.

Se debe tener en cuenta que, en el contexto de los ciberataques son cada vez más sofisticados y frecuentes, es fundamental fortalecer la seguridad y protegerse contra invasores y criminales cibernéticos. Lo que provoca que el software malicioso para escritorios virtuales sea vulnerable, además se desconoce las brechas de seguridad latentes en el Data Center, motivo por el cual, se va a realizar una evaluación de la seguridad de la infraestructura de tecnología de la información (TI), para que estudiantes y docentes que hacen uso de máquinas virtuales tengan una mayor

seguridad y confianza de la infraestructura, además si existe un posible ataque el personal se encuentre preparado para brindar el adecuado protocolo de seguridad ante tal evento.

Para contar con los procesos y procedimientos adecuados de seguridad los mismos que deberían incluir tecnologías, procesos y usuarios, y ofrecer protección de red, control de aplicaciones y gestión de endpoints sin comprometer el rendimiento del sistema o la productividad de los usuarios.

## OBJETIVOS GENERALES Y ESPECÍFICOS

### *Objetivo General*

Evaluar un escenario de seguridad de los entornos virtualizados en el Data Center de la Carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito – Campus Sur.

### *Objetivos Específicos*

- Definir el estado inicial del escenario físico y lógico del Data Center de la Carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito – Campus Sur, en lo relacionado con la protección de datos y el acceso no autorizado.
- Establecer las herramientas para la evaluación del escenario.
- Documentar los resultados obtenidos de la evaluación del escenario.

## METODOLOGÍA

La metodología con mayor adaptación a este proyecto es el método Mehari, donde se basa en analizar los riesgos que se podrían presentar en la seguridad.

Es una metodología diseñada para respaldar a los responsables de la seguridad informática en una empresa, llevando a cabo un análisis exhaustivo de los factores de riesgo fundamentales. Según Alemán & Rodríguez (s.f.):

> Evalúa cuantitativamente, de acuerdo con la situación específica de la organización, dónde se necesita realizar el análisis. Además, integra los objetivos estratégicos existentes con nuevos métodos operativos a través de una política de seguridad, manteniendo los riesgos a un nivel previamente acordado. Mehari propone un módulo especializado para examinar los intereses vinculados a la seguridad, respaldado por un método de análisis de riesgos que utiliza herramientas de apoyo.

Esto implica que, permite realizar un análisis profundo mediante herramientas que ayuden a una evaluación correcta.

Por tal motivo, su objetivo se basa en los estándares de la ISO/IEC 27001:27005 (2010). "El principal objetivo es proporcionar un método para la evaluación y gestión de riesgos, en el dominio de la seguridad de la información, conforme a los requerimientos ISO/IEC 27001:27005:2010, por medio de un conjunto de herramientas y elementos necesarios para su implementación". (Alemán & Rodríguez, s.f.)

Es por eso por lo que el proyecto técnico necesita una evaluación de la seguridad del entorno virtualizado. "Los aspectos fundamentales de esta metodología son: diseño de un modelo de riesgo, evaluación de la eficiencia de las políticas de seguridad previamente planteadas en la organización y capacidad para valorar y simular los niveles de riesgo." (Alemán & Rodríguez, s.f.)

Este método permite tomar las medidas correctas para tener mejor protección de la seguridad, ya que permite realizar un análisis exhaustivo de lo que se está buscando que en este caso es evaluar la seguridad que tiene el Data Center. Según Alemán & Rodríguez (s.f.):

> Mehari se presenta principalmente como un método para realizar auditorías y evaluaciones de riesgos en sistemas. Su gestión fue concebida y desarrollada para llevar a cabo un examen exhaustivo y preciso de los riesgos en sistemas informáticos. Este

> procedimiento consta de tres módulos: la evaluación o análisis de riesgos, la evaluación de seguridad (con enfoque en el análisis de vulnerabilidades) y el análisis de amenazas. (párr. 25).

Para esta evaluación se va a relacionar sobre el marco de referencia de la ISO 27001. Al implementar esta norma, se pueden aplicar enfoques de seguridad adaptados a la infraestructura específica de la organización, abordando aspectos clave como la protección de datos, el acceso autorizado y la mitigación de riesgos.

Lo que proporciona un marco de trabajo para establecer un sistema de gestión de seguridad de la información eficaz. Al levantar el escenario físico y lógico del Data Center, se puede obtener una visión clara de los componentes y la arquitectura de la infraestructura, lo que servirá como base para identificar los activos de información críticos y evaluar los riesgos asociados.

Mediante el cumplimiento de los requisitos de la norma y la aplicación de buenas prácticas de seguridad, se busca garantizar la confidencialidad, integridad y disponibilidad de la información alojada en el Data Center. Para aplicar la norma se realizará mediante los siguientes pasos:

- **Realizar un análisis de riesgos:** Identificar y evaluar los riesgos asociados con los entornos virtualizados. Esto implica identificar activos, amenazas y vulnerabilidades, y determinar el impacto y la probabilidad de ocurrencia de los riesgos.
- **Proponer la implementación de herramientas de seguridad:** Basándose en los resultados del análisis de riesgos, establecer e implementar herramientas de seguridad para mitigar los riesgos identificados.
- **Documentar:** Documentar los controles de seguridad implementados de seguridad de la información en los entornos virtualizados que tiene el Data Center.

# CAPÍTULO I

## LEVANTAMIENTO DEL ESCENARIO FÍSICO Y LÓGICO DEL DATA CENTER.

En este capítulo se presentará al Data Center de la Carrera de Computación se posiciona como un bastión tecnológico en el ámbito académico, proporcionando servicios, asegurando la integridad y confidencialidad de la información que maneja, además las políticas de seguridad y las prácticas de infraestructura se entrelazan para garantizar un equilibrio entre la accesibilidad de recursos y la protección de datos sensibles.

El realizar un levantamiento implica realizar una evaluación para identificar los posibles riesgos y vulnerabilidades que podría sufrir el Data Center.

En el ámbito de la virtualización, se aborda cómo los hipervisores y las redes virtuales se entrelazan para ofrecer un entorno eficiente y conectado. Además, las políticas de uso del servicio de virtualización delinean las condiciones bajo las cuales se gestionan y utilizan las máquinas virtuales, garantizando un equilibrio entre accesibilidad y seguridad.

### *Definición del Data Center*

Un Data Center es un espacio físico que se utiliza para alojar sistemas informáticos, servidores, equipos de almacenamiento de datos, dispositivos de red, entre otros. Su principal función es gestionar y almacenar datos, aplicaciones y recursos informáticos para el correcto funcionamiento ya sea de organizaciones, empresas incluso servicios en línea.

Existe diferentes tipos de Data Center como: empresariales, proveedores de servicios, colocation, hiperescala, académicos entre otros.

El Data Center de la Carrera de Computación, es un centro de datos académico, su principal objetivo es brindar servicios de infraestructura tecnológica y recursos informáticos avanzados para satisfacer las necesidades de investigación, enseñanza y aprendizaje de la comunidad académica. En el cual cuenta con un clúster de servidores que está conformado por:

Tres servidores XL230A, estos tipos de servidores están diseñados para entornos de alto rendimiento, virtualización, además su almacenamiento tiene una mayor capacidad lo que garantiza un rendimiento óptimo. Estos servidores están clusterizados teniendo un total de capacidad de 96 núcleos, 3 TB en RAM y 90 TB de almacenamiento. (Hewlett Packard Enterprise, 2021)

Se posee un modelo de servidor XL190R en el cual se encuentra configurados los Apollo 1, 2, 3 y 5. Este servidor tiene un rendimiento para poder trabajar en escritorios virtuales sin sobre cargar los procesadores en su rendimiento. (HPE, s.f.)

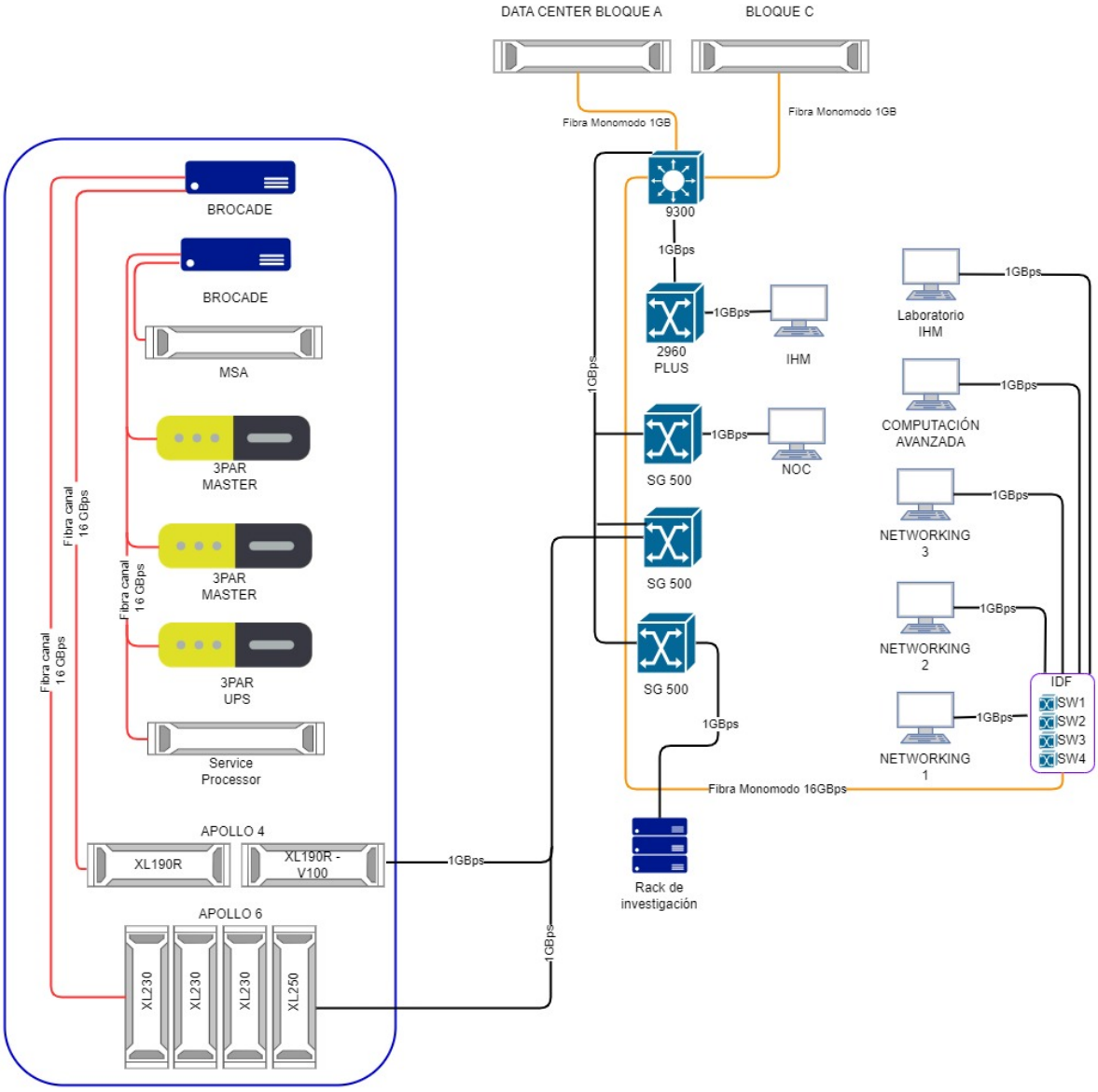
Por otro lado, también poseen el modelo de servidor XL250A que se encuentra configurado el Apollo 4, permite reducir el nivel de carga de trabajo, dando como resultado una nivelación a los entornos virtuales. Este se encuentra trabajando de manera independiente ya que es el clúster. (HPE, s.f.)

Por último, el modelo del servidor XL190R está configurado el Apollo 6, este servidor ya está mencionado anteriormente, la diferencia es que trabaja de manera independiente ya que se encuentra alojado las máquinas virtuales para la parte de investigación. (HPE, s.f.)

A continuación, se indica el diagrama de red del Data Center.

**Figura 1**

*Diagrama de red del Data Center*




*Nota.* Esquema de cómo se encuentra conectada la red desde el Data Center del bloque "A" hacia el Data Center de la Carrera de Computación. Elaborado por: El Autor.

Ahora se explicará cómo se encuentra conectado el Data Center de la Carrera de Computación y cómo funciona:

El Data Center de la Carrera de Computación, está bajo las políticas del Data Center del Bloque A, en el cual se encuentra conectado mediante la fibra monomodo, esta fibra óptica permite trasmitir señales de manera eficiente a largas distancias, de acuerdo con el ancho de

banda. Tiene dos conexiones hacia el Data Center de producción y los switches IDF que se encuentra en el laboratorio de Networking 1.

En los laboratorios de Networking 2, Networking 3 y Computación Avanzada se encuentra conectado al laboratorio de Networking 1, el mismo que llega la conexión al Data Center.

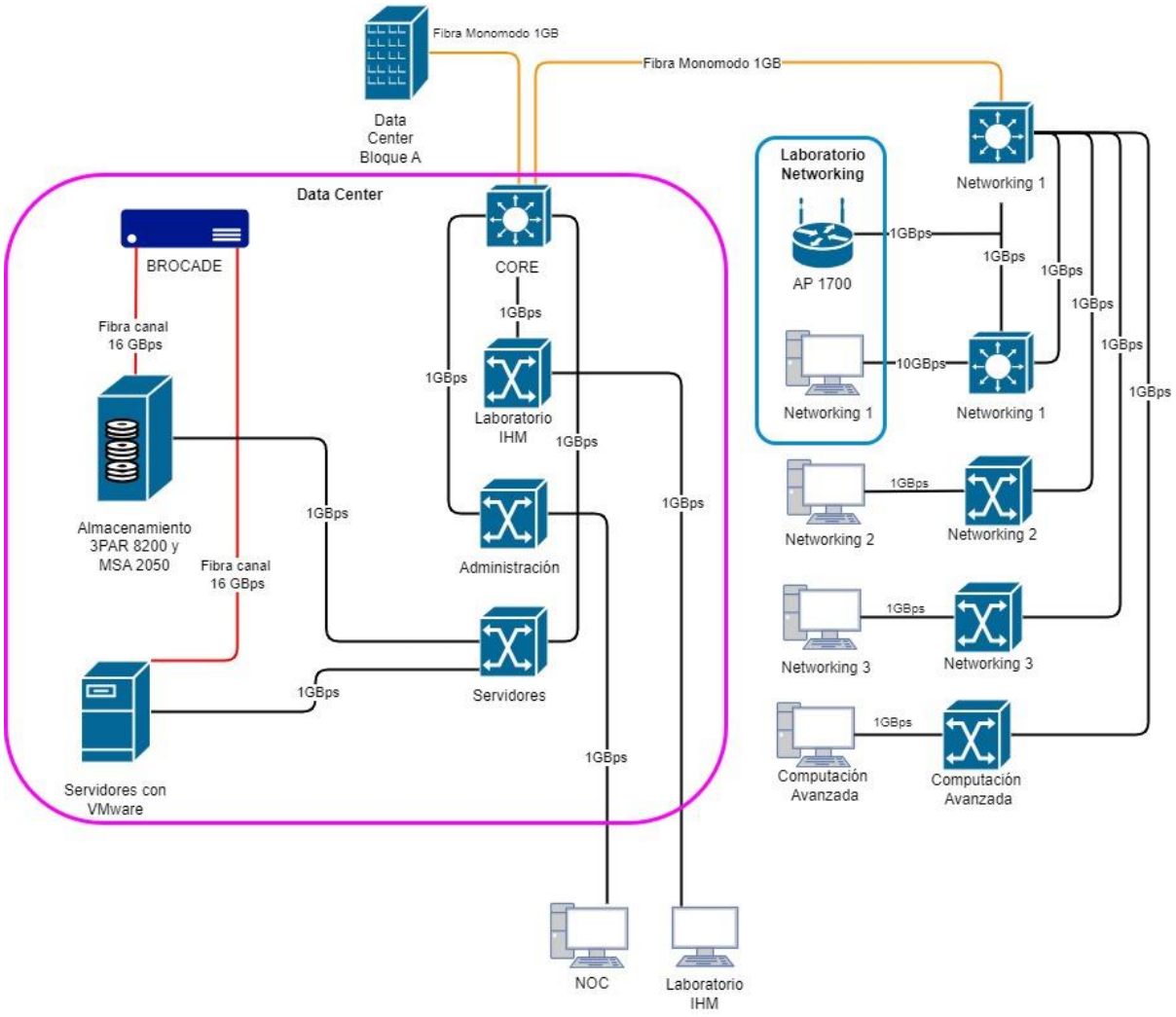
El laboratorio de IHM se encuentra conectado directamente al switch “Laboratorio IHM” del Data Center, el NOC está conectado al switch “Administración”.

El BROCADE (switch SAN) utiliza fibra de canal de 16 GBps, ya que la velocidad de datos es alta lo que permite facilitar la transferencia de datos, la cual está conectada al almacenamiento (3PAR 8200 y MSA 2050), y a los servidores VMware (Apollo 4, Apollo 6 y Clúster (servidores Apollo). Y este almacenamiento y servidores VMware están conectados al servidor “Servidores”.

A continuación, se indica el diagrama del Data Center de la Carrera de Computación:

**Figura 2**

*Diagrama General del Data Center*




*Nota.* Esquema sobre la conexión entre el Data Center del Bloque A y el Data Center de la Carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito – Campus Sur. Fuente: (Data Center de la Carrera de Computación, 2023).

**Políticas de seguridad que se rige el Data Center de la Carrera de Computación, bajo el Data Center del bloque A.**

A continuación, se explica las políticas que se acoplan al plan del proyecto, donde se dividen en temas y subtemas. Cabe mencionar que esta información es pública y fue recopilada de la página oficial de la Universidad Politécnica Salesiana.

Nota: La numeración que se indica es en base a las políticas que tiene la Universidad Politécnica Salesiana.

*Gestión de la seguridad de la información*

## *4.3 CONTROLES DE SEGURIDAD DE LA INFORMACIÓN*

Al implementar controles de seguridad permite garantizar confidencialidad e integridad de los datos de los usuarios, a continuación, se indican las políticas que se rige dentro de la Universidad Politécnica Salesiana.

### 4.3.1 Evaluación de Riesgo de la Información

Se realiza una evaluación para identificar el nivel de criticidad que tiene la información, para tomar las respectivas medidas, a continuación, se prescribe lo siguiente:

> 4.3.1.1 El grado de control de la seguridad requerida depende de la sensibilidad y criticidad de la información. El primer paso para determinar el nivel adecuado de seguridad es un proceso de evaluación de riesgos, cuyo fin será identificar y clasificar la naturaleza de la información que la UPS posee, las consecuencias adversas de las brechas de seguridad y la probabilidad de que ocurran esas consecuencias. (Universidad Politécnica Salesiana, 2022, pág. 3)

Esto indica que se debe determinar un equilibrio para tener una buena protección de la información.

Cada departamento de la Universidad Politécnica Salesiana debe asumir la responsabilidad de tener en cuenta y tomar medidas sobre la evaluación de riesgos, a continuación, se prescribe lo siguiente:

> 4.3.1.2 Dada la naturaleza descentralizada de la estructura de la UPS, la evaluación del riesgo debe llevarse a cabo en primera instancia por sus diferentes departamentos y ésta debe ser coherente con los principios generales de esta Política. (Universidad Politécnica Salesiana, 2022, pág. 3)

Al tener una estructura descentralizada, los departamentos pueden tener información en específico donde ellos crean que sea necesario.

Al realizar una evaluación se debe tener en cuenta el conocimiento y la importancia de la información para evitar riesgos o vulnerabilidades, a continuación, se prescribe lo siguiente:

> 4.3.1.3 La evaluación del riesgo debe identificar los activos de información del departamento, definir la propiedad de dichos activos, y clasificarlas en función de su sensibilidad y/o criticidad para el departamento o la UPS en su conjunto. En la evaluación de riesgos, los departamentos deben considerar el valor de los activos, las amenazas a ese activo y su vulnerabilidad. (Universidad Politécnica Salesiana, 2022, pág. 3)

Esta evaluación permite comprender los riesgos sobre los activos de información y tomar decisiones sobre la criticidad del caso.

Se destaca la importancia de tener una operación continua y una adaptación favorable acorde a la evolución y las circunstancias, a continuación, se prescribe lo siguiente:

> 4.3.1.6 Las evaluaciones de riesgos de seguridad de información deben ser repetidos periódicamente como parte de la ejecución operacional normal y cuando se realicen cambios en la infraestructura, los sistemas informáticos y los procesos de la UPS. (Universidad Politécnica Salesiana, 2022, pág. 3)

Esto explica que la seguridad de la información siempre debe estar en constante revisión y actualización.

### 4.3.4 Protección de información confidencial

La protección de la información es una prioridad para garantizar que la información se encuentra en un entorno seguro. “El tratamiento de la Información Confidencial estará

contemplado en el documento Política de Datos Personales de la UPS y clasificación de la información" (Universidad Politécnica Salesiana, 2022, p. 4). Esto implica que tienen en cuenta los controles, políticas y procedimientos que realiza internamente la Universidad Politécnica Salesiana.

### 4.3.5 Acceso remoto

Se debe establecer reglas claras y procedimientos para todos los que hagan uso del acceso remoto, esto con la finalidad de reducir el riesgo de seguridad. "4.3.5.1 Cuando se requiera de acceso remoto, éste debe ser controlado mediante una política de control de acceso definida y los controles deben ser estrictos manteniendo el principio del mínimo acceso necesario". (Universidad Politécnica Salesiana, 2022, p. 4). Es decir que se debe otorgar el acceso solo a personas que realmente lo necesiten.

Se debe tener métodos y estándares específicos para tener un control y acceso de manera segura hacia la información. "4.3.5.2 Todo acceso remoto debe ser controlado por protocolos de control de acceso seguro usando los niveles apropiados de encriptación y autentificación". (Universidad Politécnica Salesiana, 2022, p. 4)

### 4.3.8 Uso de dispositivos o medios portátiles

Permite garantizar que los medios removibles sean seguros y tener un control sobre la información. "4.3.8.1 Se deben definir procedimientos para la administración de medios removibles con el fin de asegurar que ellos estén apropiadamente protegidos de accesos no autorizados". (Universidad Politécnica Salesiana, 2022, p. 4)

El dueño de la información es responsable de examinar y verificar los permisos. "4.3.8.2 El dueño de la información debe revisar los permisos sobre los activos de información a su cargo antes de que éstos sean llevados fuera de la UPS". (Universidad Politécnica Salesiana, 2022, p. 4). Esto implica que es importante tener una supervisión y control de la información.

Recomiendan que la mayor parte de la información sobre la protección de datos personales sean encriptados en todos los dispositivos que hagan uso. “4.3.8.3 En el caso de datos personales, se recomienda que todos los dispositivos y medios portátiles deben ser encriptados cuando la pérdida de dicha información pueda causar daño o angustia a los individuos”. (Universidad Politécnica Salesiana, 2022, p. 5)

La clave de encriptación nunca debería estar en los dispositivos que se están protegiendo, ya que podría existir un porcentaje alto de vulnerabilidad. “4.3.8.4 La frase de encriptación de un dispositivo no debe ser almacenada en el mismo dispositivo”. (Universidad Politécnica Salesiana, 2022, p. 5)

### 4.3.10 Controles criptográficos

Tener técnicas criptográficas para la información sensible donde sea compartida solo para el personal autorizado. “4.3.10.1 Se deben definir procedimientos para soportar el uso de técnicas criptográficas para asegurar que solo el personal autorizado pueda tener acceso a información confidencial”. (Universidad Politécnica Salesiana, 2022, p. 5). En ese sentido, tener procedimientos claros permite que las técnicas criptográficas sean efectivas.

Para asegurar la información, los departamentos deben cumplir con los requisitos tanto internos como externos sobre la seguridad de la información, donde se maneje todos los protocolos de manera segura. “4.3.10.2 Se debe definir una política de criptografía y administración de claves, y verificar su cumplimiento con el fin de asegurar que los datos estén apropiadamente asegurados y que los requerimientos tanto internos como externos han sido cumplidos”. (Universidad Politécnica Salesiana, 2022, p. 5)

## Levantamiento del escenario

El levantamiento del escenario en el contexto de la seguridad de los entornos virtualizados en el Data Center es de vital importancia para comprender y evaluar la

infraestructura en la que se desarrollan las operaciones informáticas. Este proceso proporciona una visión detallada tanto de los componentes físicos como de los aspectos lógicos.

El levantamiento del escenario también facilita la identificación de posibles vulnerabilidades y riesgos presentes en los sistemas virtualizados. Mediante herramientas que permite analizar, se pueden descubrir puntos débiles en la seguridad, brechas en la protección de datos y accesos no autorizados que puedan poner en peligro la confidencialidad e integridad de la información alojada en las máquinas virtuales.

La información obtenida a través del levantamiento del escenario también sirve de base para la implementación de medidas de seguridad. Al contar con un panorama claro de la infraestructura, se puede tener una evaluación más precisa, dando una protección eficaz y minimizando los riesgos asociados. En resumen, el levantamiento del escenario es una fase fundamental en la evaluación de la seguridad de los entornos virtualizados, proporcionando los datos necesarios para fortalecer la infraestructura y garantizar la integridad de la información frente a las crecientes amenazas que existe hoy en día.

**Componentes físicos del Data Center**

Un Data Center se encuentra compuesto por, sistemas de almacenamiento, servidores, hardware para garantizar un funcionamiento interrumpido.

Un procesador es el cerebro de un computador o de un servidor el cual permite controlar el flujo de datos, en el caso del servidor al ser de gama alta puede trabajar en paralelo lo que hace que las tareas sean más rápidas, ya que pueden trabajar con grandes cantidades de datos.

Un procesador asume la responsabilidad de la mayoría de las funciones de una computadora. Su tarea principal es el manejo de la transferencia de datos, asegurando el funcionamiento eficiente del ordenador. Para lograr esto, requiere recibir y ejecutar comandos específicos. Los dos principales fabricantes de procesadores, Advanced Micro Devices (AMD)

e Intel, desempeñan un papel crucial en la industria, produciendo procesadores para una variedad de dispositivos, incluyendo PC, portátiles y dispositivos móviles. Los distintos tipos de procesadores cumplen funciones específicas a diversas velocidades, adaptándose al tipo de sistema en el que operan. (Navas, 2018)

**Infraestructura de procesamiento**

***Procesadores con Hyper-Threading Tecnología (HT)***

Este tipo de tecnologías mejora el rendimiento y eficiencia del procesador ya que maneja múltiples subprocesos de manera simultánea.

La tecnología Hyper-Threading Intel® (Intel® HT) optimiza la utilización de los recursos del procesador al permitir la ejecución de múltiples subprocesos en cada núcleo. Este enfoque no solo mejora el rendimiento general del software que emplea varios subprocesos, sino que también incrementa la capacidad de procesamiento del sistema. (Tecnología Intel® Hyper-Threading, s.f.)

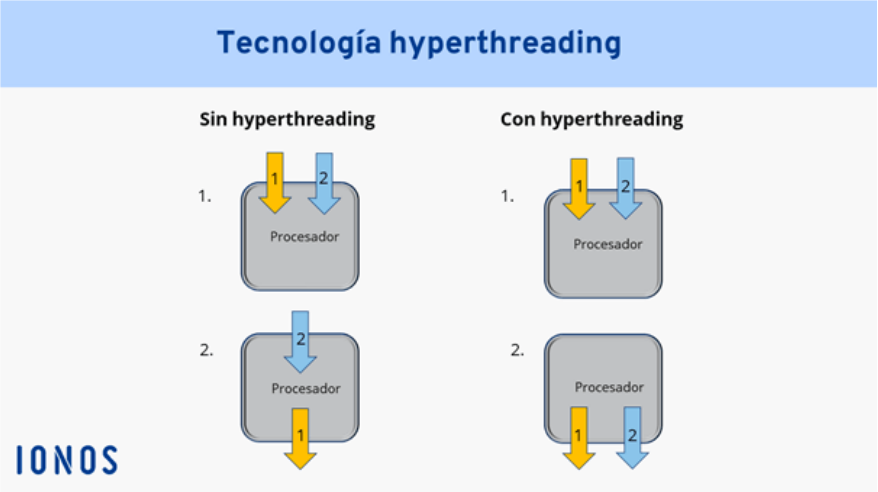
***¿Cómo funciona?***

El HT cumple con una función muy importante en la parte de rendimiento de procesadores especialmente en los servidores que tiene la capacidad de aumentar los hilos en el núcleo físico.

En la actualidad, el Hyperthreading (también conocido como HT) desempeña un papel crucial en numerosos procesadores. Conforme se incrementa la cantidad de núcleos en un procesador, la presencia de Hyperthreading duplica los hilos disponibles, convirtiéndolo en una tecnología fundamental, especialmente en entornos como servidores. Este avance contribuye significativamente a la capacidad de procesamiento de estos sistemas. (GEEKNETIC, s.f.)

**Figura 3**

*Procesadores con Hyper Threading*




*Nota.* Referencia de núcleo físico, donde explica cómo se comporta al tener dos núcleos virtuales y lógicos. Fuente: (Digital guide IONOS, 2021).

***Núcleo (Core)***

Esta unidad de procesamiento es independiente y se puede ejecutar varias tareas al mismo tiempo. “Los núcleos de un procesador son procesadores más pequeños integrados en la CPU principal. El número de núcleos indica la cantidad de procesadores de una CPU”. (Ghimiray, 2022)

Al tener núcleos múltiples permiten mayor eficiencia y productividad en las tareas, teniendo en cuenta el rendimiento y la capacidad que tienen estos núcleos. Según (Breixo, 2021):

> Básicamente, la idea del núcleo nace de multiplicar diversas partes destinadas a la lógica para así tener varios procesadores en uno. Así, en un solo paquete se tiene lo que se comporta como varias CPUs separadas, lo cual se combina mediante técnicas de programación paralela para conseguir un paralelismo real de los programas, o simplemente para poder ejecutar varios programas distintos a la vez.

***Unidad central de procesamiento***

El procesador o CPU es un recurso clave, su correcta planificación constituye uno de los puntos centrales en el diseño de un buen Sistema Operativo.

Al tratarse de la unidad de procesamiento tiene dos trabajos en el cual mide el rendimiento y velocidad, y por otro lado verifica que los datos sean correctos. “La funcionalidad del procesador se divide en dos partes: el área de ejecución es la encargada de la velocidad y rendimiento del procesador mientras que el área de control comprueba que los datos sean correctamente asignados a las celdas de memoria” (Barionuevo, Apolloni, & Piccoli, 2009)

***Compute Unified Device Architecture (Cuda Core)***

Permite ejecutar en paralelo múltiples operaciones, lo que significa que la velocidad es mejor comparada a lo tradicional. Permite aprovechar la potencia de las GPUs para resolver problemas que tengan las diferentes áreas. Un ejemplo de esto es aplicaciones de procesamiento gráfico permite que se ejecute las operaciones de forma múltiple.

***Memoria Caché***

La caché es un nivel de almacenamiento de datos de alta velocidad que guarda una porción de información, generalmente temporales. Esta estrategia posibilita una respuesta más rápida a las solicitudes futuras de esos datos en comparación con el acceso a la ubicación principal de almacenamiento. La función principal de la caché es mejorar la eficiencia al permitir el acceso rápido a datos que han sido recuperados o procesados previamente. (AWS, s.f.)

Función de la memoria caché:

- ***Caché L1:*** Se encuentra muy cercano al procesador y es rápido, pero tiene poca capacidad. (Ros, 2019)
- ***Caché L2:*** Tiene una mejor capacidad que la L1. (Ros, 2019)

- ***Caché L3:*** Su capacidad es mayor, pero su nivel es inferior a la velocidad de los otros. (Ros, 2019)
- ***Caché L4:*** Es utilizado para mejorar el rendimiento de las GPUs. (Ros, 2019)

***Unidad de Procesamiento Gráfico (GPU)***

Al tener grandes cargas de trabajo gráfico, las GPU permiten acelerar estas cargas tanto de gráficas como de cálculos. "GPU es un acrónimo de Graphics Processing Unit. Es decir, unidad de procesamiento gráfico. Es el cerebro y el corazón de una tarjeta gráfica, el núcleo de la tarjeta gráfica". (Gr, 2023)

La GPU, o Unidad de Procesamiento Gráfico, es el acrónimo de Graphics Processing Unit en inglés. Esta unidad es esencialmente el cerebro y el corazón de una tarjeta gráfica, siendo el núcleo que se encarga de procesar y gestionar las tareas relacionadas con los gráficos y la representación visual en un sistema informático. (López, 2022).

Las Unidades de Procesamiento Gráfico (GPUs) tienen una función crucial en el procesamiento y generación de información visual que se visualiza en las pantallas de dispositivos. Estas unidades se encargan de diversas tareas, como la representación de texturas, la gestión de la iluminación, la aplicación de sombras y otros efectos gráficos, especialmente en entornos que demandan un alto rendimiento, como juegos y aplicaciones gráficas intensivas.(Gr, 2023)

**Infraestructura de almacenamiento**

***Storage***

El Storage permite preservar la información manteniendo los datos de manera segura y efectiva.

El almacenamiento de datos consiste en la conservación de información empleando una tecnología específicamente desarrollada para mantener los datos y que se encuentren accesibles siempre que sean necesarios. El almacenamiento de datos se refiere al uso de

medios de grabación para conservar los datos utilizando PC y otros dispositivos. Las formas más frecuentes de almacenamiento de datos son el almacenamiento de archivos, el almacenamiento en bloque y el almacenamiento de objetos, cada uno de los cuales resulta adecuado para un fin diferente. (Hewlett Packard Enterprise Development España, s.f.)

***Unidad de disco duro***

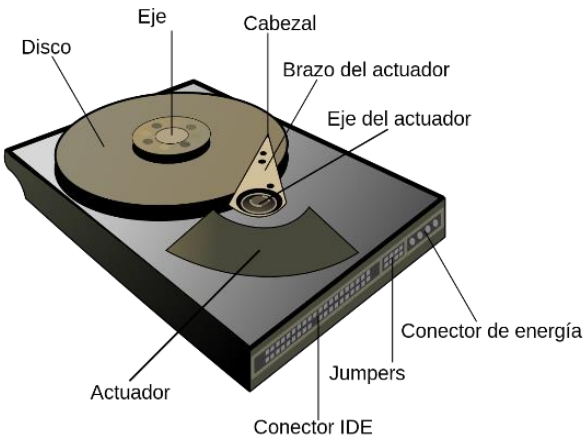
Dispositivos de almacenamiento de datos que utilizan medios magnéticos u ópticos para almacenar información de manera persistente.

***Tipos de discos:***

**Discos Duros (HDD - Hard Disk Drive**): Son componentes informáticos que tiene como propósito de estos dispositivos es preservar datos de forma duradera, en contraste con la memoria RAM., los datos en un disco duro no se borran cuando se apaga el sistema, lo que permite la retención a largo plazo de la información almacenada. (Férnandez, 2023)

**Figura 4**

*Unidad de disco duro o disco rígido*




*Nota.* Imagen referente, indicando con nombres cada una de las partes que tiene la unidad de disco duro. Fuente: (Wikipedia, 2023)

**Discos de Estado Sólido (SSD - Solid State Drive):** Guardan información en microcircuitos con memorias flash conectadas entre sí., comúnmente basadas en la tecnología NAND. Estas

memorias son no volátiles, lo que significa que retienen la información incluso cuando el disco se encuentra desconectado, ofreciendo una forma eficiente y rápida de almacenar y acceder a datos. (Férnandez, 2023)

**Figura 5**

*Disco de estado sólido*

*Nota*. Microchip para almacenar los datos. Fuente: (Qloudea Blog Especialistas en servidores NAS, 2021)

**Discos Ópticos:** Tiene la función de almacenar datos en formato digital. Este disco tiene una forma circular y los datos se guardan en surcos microscópicos que se crean durante el proceso de grabación utilizando un láser específico. (Férnandez, 2023)

***Número de unidad lógica (LUN)***

El almacenamiento virtual tiene la capacidad de permitir o prohibir el acceso a un servidor específico que posee una conexión física al dispositivo de almacenamiento adyacente. Los Niveles Lógicos de Unidad (LUN) se utilizan para identificar dispositivos SCSI, como discos duros externos conectados a una computadora. Cada dispositivo se asigna con un número de LUN que sirve como su dirección única.(Dell, s.f.)

**Figura 6**

*Funcionamiento de una LUN*

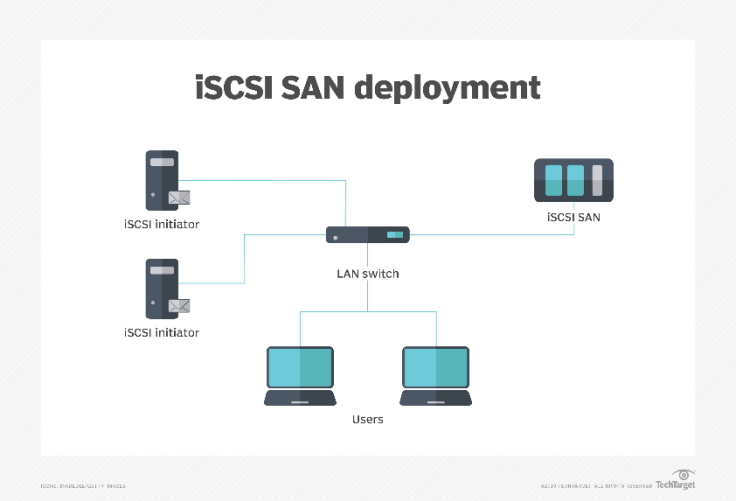

*Nota.* Explicación de cómo se conecta la LUN a los servidores. Fuente: (Krypton Solid, 2021)

### *Almacenamiento SAN iSCSI*

El almacenamiento de área de red iSCSI (SAN) resulta apropiado para pequeñas y medianas empresas que necesitan almacenar y transferir volúmenes significativos de datos a través de la red. (M, s.f.)

**Figura 7**

*Funcionamiento almacenamiento SAN iSCSI*



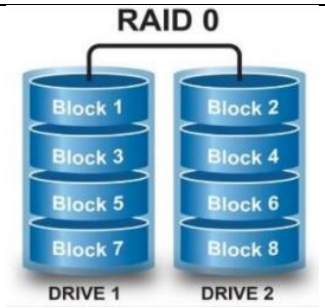
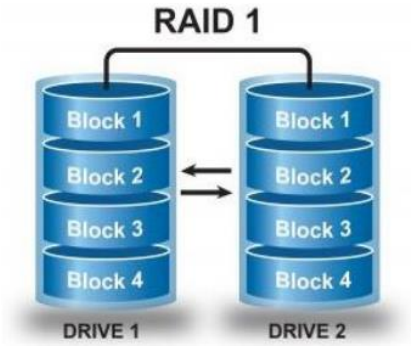
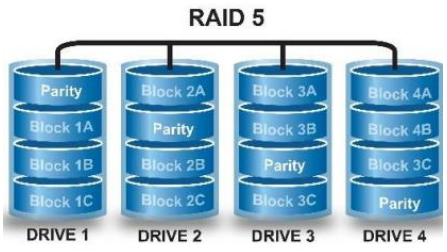
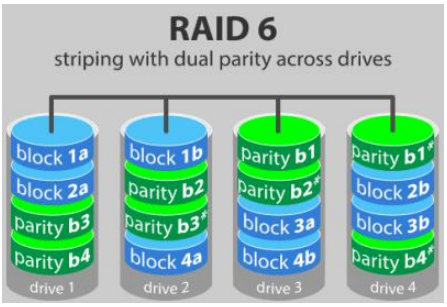

*Nota.* Funcionamiento de cómo se conecta el SAN iSCSI. Fuente: (TechTarget, 2019)

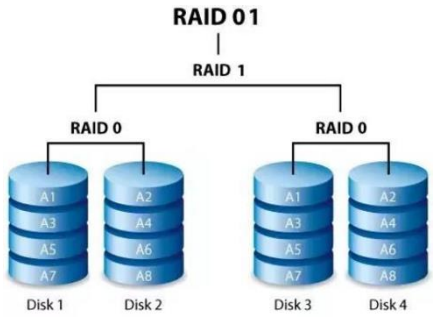
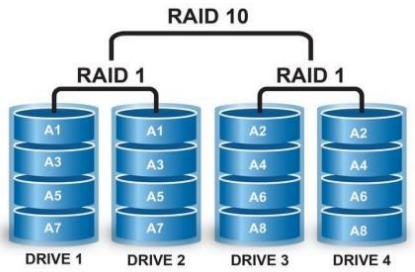
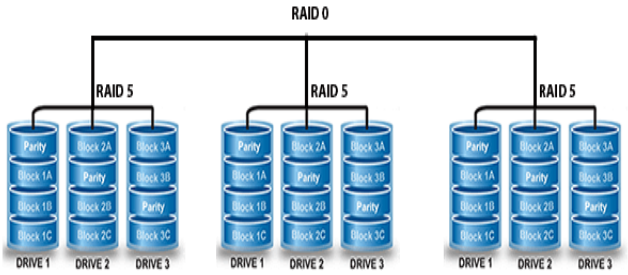
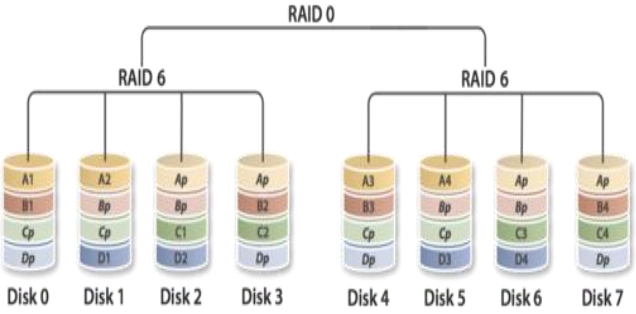
***Matriz de discos independientes (RAID)***

Es una tecnología de almacenamiento que combina múltiples discos duros para formar un solo volumen lógico de almacenamiento con el objetivo de mejorar el rendimiento, la redundancia o ambos. La idea principal detrás de RAID es proporcionar una mayor fiabilidad y rendimiento.

**Tabla 1**

*Tipos de Raid*

| Nombre | Descripción | Imagen |
|---|---|---|
| **RAID 0** | Denominado como striping o rayado, presenta un alto desempeño aunque carece de capacidad para tolerar fallos. |   |
| **RAID 1** | Identificado como espejo o mirroring, replica los datos de la unidad principal a una segunda sin pérdida de información y ofrece tolerancia a fallos. |   |
| **RAID 5** | Requiere al menos 3 discos, proporciona un rendimiento elevado y utiliza paridad para la recuperación de datos. |   |
| **RAID 6** | Requiere al menos 4 discos, ofrece tolerancia a fallos en dos discos, una redundancia elevada, con paridad dedicada a dos discos. |   |

| | | |
|---|---|---|
| **RAID 01** | Se divide en dos conjuntos de almacenamiento, RAID 0 y RAID 1, y es necesario que ambos tengan la misma cantidad de discos, con una capacidad limitada para la tolerancia a fallos. |  |
| **RAID 10** | Emplea al menos cuatro discos, logra un desempeño elevado, garantiza la redundancia de datos y asegura una rápida recuperación ante fallos. |  |
| **RAID 50** | Requiere al menos seis discos, con un rendimiento elevado en operaciones de lectura y un nivel medio en operaciones de escritura. |  |
| **RAID 60** | Necesita un mínimo de ocho discos para garantizar un rendimiento excepcional en las operaciones de lectura. |  |

*Nota.* Explicación de los tipos de raid y su utilización. Fuente: (Cueva & Vizcaíno, 2023)

Son los elementos y configuraciones que están relacionados con el software, la red y la gestión de los recursos de un Data Center, esto es fundamental para un buen funcionamiento y administración de la infraestructura tecnológica.

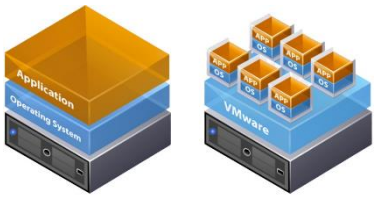
**Infraestructura de virtualización**

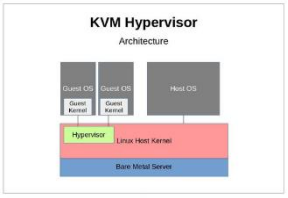
***Configuración de los hipervisores***

Es el software que permite realizar la virtualización, es decir crear varias máquinas virtuales en un solo servidor, este servidor es físico. Esto con la finalidad de aprovechar la capacidad y recursos del hardware físico. (Conzultek, s.f.) Existen hipervisores como:

**Tabla 2**

*Hipervisores más importantes dentro de la industria*

| Nombre | Descripción | Imagen |
|---|---|---|
| **VMware** | VMware vSphere/ESXi: este hipervisor es de tipo 1 o también conocido como "hipervisores bare metal" lo que hace es ejecutar directamente en el hardware de servidor, lo que permite crear y administrar varias máquinas virtuales en un solo servidor físico, permitiendo alta disponibilidad y tolerancia a fallos. (VMware, 2020) |   |
| **Hyper-V** | Esta plataforma virtual permite crear y gestionar máquinas virtuales en los servidores físicos, además tiene conexión de una máquina virtual y una herramienta de conexión remota. (Armstrong et al., 2023) |   |

| | | |
|---|---|---|
| **KVM** | Pueden ser instaladas en máquinas físicas de Linux para crear máquinas virtuales, es una solución de virtualización de código abierto. Cabe mencionar que se puede convertir cualquier máquina Linux en un hipervisor bare metal. (AWS, s.f.) |  |

*Nota.* Descripción de los hipervisores con mayor apogeo en creaciones de máquinas virtuales. Fuente: Elaborado por: El Autor.

***¿Cómo se encuentra configurado?***

Los hipervisores se encuentran instalados en cada servidor y todo se encuentra conectado al Vcenter Server, para que se obtenga un mayor control sobre cada una de las máquinas virtuales. Cabe mencionar que esta máquina virtual principal es donde se maneja toda la parte de la configuración de los hipervisores ya que se encuentra sobre uno de los servidores.

**Infraestructura de redes virtuales**

Las redes virtuales permiten la comunicación entre los recursos y las máquinas virtuales, esto con la finalidad de mejorar el rendimiento y seguridad facilitando la conectividad y segmentación. (VMware, 2020)

***¿Cómo es la infraestructura de la red virtual?***

En primer lugar, se realiza mediante VMware vShepere Hypervison ESXI 6.7 es un software que permite realizar la virtualización de máquinas virtuales en los servidores físicos, proporcionando alta capacidad de virtualización, disponibilidad y gestión centralizada, todo esto a través de vCenter Server.

VCenter Server al ser una aplicación que permite administrar y controlar de manera eficiente y escalable, todos los servidores se encuentran conectados a Vcenter Server. Proporcionando estabilidad en las máquinas virtuales.

**Tabla 3**

*Procesamiento de los servidores*

| ***Nombre del servidor*** | ***Modelo*** | ***Almacenamiento*** | ***Velocidad de procesamiento*** | | ***RAM*** |
|---|---|---|---|---|---|
| | | | ***Físicos*** | ***Lógicos*** | |
| **Apollo 1** | HPE XL230A | 1,2 TB | 32 | 64 | 500 GB |
| **Apollo 2** | HPE XL230A | 1,2 TB | 32 | 64 | 500 GB |
| **Apollo 3** | HPE XL230A | 1,2 TB | 32 | 64 | 500 GB |
| **Apollo 5** | HPE XL190R Gen10 | 1,8 TB | 32 | 64 | 500 GB |
| **Apollo 6** | HPE XL190R Gen10 | 1,8 TB | 32 | 64 | 500 GB |
| **Apollo 4** | HPE XL250A | 1,2 GB | 32 | 64 | 500 GB |

*Nota.* En la tabla se muestra los valores que tiene los servidores con sus respectivos modelos. Fuente: (Data Center de la Carrera de Computación, 2023).

**Tabla 4**

*Almacenamiento del Data Center*

| ***Sistema de almacenamiento*** | ***Modelo*** | ***Capacidad*** |
|---|---|---|
| **3PAR** | HPE 3PAR | 50 TB |
| **MASTER** | 8200 | |
| **3PAR UPS** | HPE 3PAR | 20 TB |
| | 8200 | |
| | MSA2050 | 50 TB |

*Nota.* La tabla indica la capacidad de almacenamiento que tiene los servidores. Fuente: (Data Center de la Carrera de Computación, 2023).

**Políticas de uso del servicio de virtualización**

Se definen las condiciones y restricciones que tiene el Data Center como gestionar y utilizar máquinas virtuales, además los recursos y servicios relacionados con la virtualización.

Las políticas que se llevan a cabo del Data Center son:

- Asignación de recursos.
- Seguridad.
- Administración de Usuarios y Permisos.
- Actualizaciones y Parches.
- Monitoreo y Auditorías.

***Sistemas de respaldo***

***¿Cómo lo respaldan?***

Es importante tener respaldos ya que permite recuperar los datos de manera rápida, además que es una capa adicional de seguridad. Según Garzón (2021):

> Los respaldos de máquinas virtuales permiten recuperarse rápidamente como desastres naturales, fallas de hardware, errores humanos, ataques de malware o incluso durante el proceso de migración o actualización. Si una máquina virtual se corrompe o se vuelve inaccesible, se puede restaurar desde una copia de seguridad, minimizando el tiempo de inactividad y las pérdidas de datos.

En el Data Center existe la política de respaldo bajo demanda, es decir que la persona que necesite un respaldo de la máquina virtual debe enviar un correo al departamento del Data Center para que realicen el procedimiento.

También existe respaldos bajo selección de elementos críticos por parte del Data Center, tales como: Vcenter Server, videos, acceso a los laboratorios (biométricos), máquinas de tesis orientados al doctorado, trabajos de doctorado o máquinas virtuales de investigación. Cabe recalcar que estos clones reposan en la misma arquitectura.

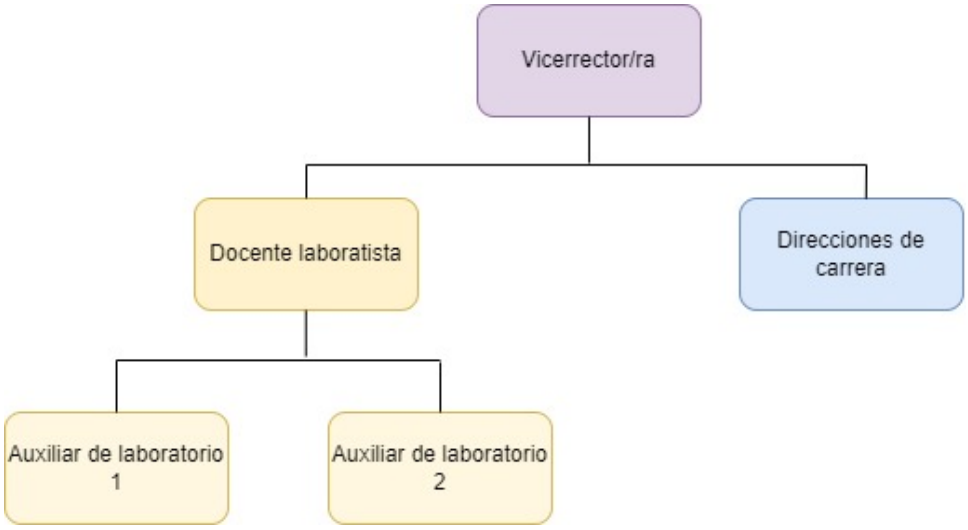
***Servicios que brindan prácticas de seguridad***

***Gobernanza***

La gobernanza para el Data Center empieza desde los auxiliares de laboratorio, donde realizan los pedidos, estándares y procedimientos ya sea por parte de docente laboratista, dirección de carrera de Computación, o Vicerrectorado; para luego ser revisado y aprobado por parte del docente laboratista (administrador) y Dirección de Carrera de Computación, finalmente llega a Vicerrectorado para verificar dichos cambios.

**Figura 8**

*Gobernanza del Data Center de Computación*




*Nota.* Explicación de la gobernanza que tiene el Data Center de la Carrera de Computación mediante una jerarquía. Fuente: (Data Center de la Carrera de Computación, 2023).

***¿Cómo es la administración del Data Center?***

**Administrador:** Cumple todas las funciones administrativas, Según Jorge López (2022):

- “Gestión de redes: Planificar, organizar, supervisar y control de elementos y recursos, para garantizar un buen nivel de servicio. Recursos usados en la conexión y comunicación de elementos, y recursos usados en las aplicaciones. (Diapositiva. 4)

  Tiene como objetivo tener la capacidad para reparar y evitar fallas, dar monitoreo general o de rendimiento, un correcto diagnóstico de condiciones insatisfactorias, manejo integrado de la red, reducir costo operación de la red, fácil uso de la red. (Diapositiva. 13)

- Gestión de la configuración: Control físico, lógico y eléctrico sobre la red. Además, está el manejo de inventarios, procesamiento y provisionamiento, gestión de cambios, verificación del estado de la red, presupuestos. (Diapositiva. 6)
- Gestión de cambios: Planificar, aprobar, ejecutar y documentar los cambios. Permite coordinar la implementación de cambio. (Diapositiva. 19)
- Gestión de contabilidad: Permite establecer cargos sobre el uso de recursos para identificar los costos, existe tres aspectos que son: (Diapositiva. 23)
    - Planificación: El primer aspecto es conocer los recursos de la red permite planificar el tipo de inversiones que necesita la red. (Diapositiva. 25)
    - Control: El segundo aspecto facilita el control de la información. (Diapositiva. 26)
    - Finanzas: El tercer y último aspecto, se establecen las políticas basadas en el consumo del mantenimiento de la red. (Diapositiva. 26)

  Permite tener mantenimiento sobre las cuentas, estadísticas de uso, recopilación de datos de uso. (Diapositiva. 29)

- Gestión de planificación: Permite determinar la optimización de la red, basándose en flujo de tráfico, requerimiento, cambios tecnológicos, futuras aplicaciones, rendimiento de la red. (Diapositiva. 33)
- Gestión de rendimiento: Evaluación del comportamiento de los elementos de la red, permite analizar datos relevantes para visualizar tendencias de alta utilización, define límites de utilización en la red, medición y gestión de tráfico. Tiene indicadores como, disponibilidad, tiempo de respuesta, retardos en la red, además permite capturar información de fallas. Tiene la capacidad de gestionar los recursos, capacidad y supervisión. (Diapositiva. 41-45; 48-50)
- Gestión de seguridades: Consiste en garantizar que los recursos informáticos estén disponibles para cumplir con su propósito, se realiza un análisis de las consecuencias y mediciones de los posibles riesgos tales como (virus, hackers y desastres naturales). Las funciones que cumple son, controlar y supervisar las actividades de auditoría; creación de una estrategia de implantación para integrar las medidas de seguridad." (Diapositiva. 55-57)

**Auxiliares de laboratorios:** Cumplen las funciones de:

- Brindar soporte técnico: Dar asistencia y soluciones a los usuarios de la Universidad Politécnica Salesiana (soporte remoto, persona, correo electrónico y telefónico), tener la habilidad para resolver problemas técnicos, cumplir con los pasos establecidos y habilidades para trabajar bajo presión.
- Creación de máquinas virtuales: Asignar la IP correspondiente a cada máquina virtual, crear y configurar la máquina virtual con el sistema operativo solicitado por el usuario, enviar al usuario el manual para ingresar a la máquina virtual, responder correos ante incidencias, dar soporte al usuario.

- Gestión de incidencias: Responder a eventos no planificados o interrupciones que pueden surgir inesperadamente. (Drew, 2022)

Se debe identificar, registrar, clasificar, analizar e intervenir la incidencia, para posteriormente dar un seguimiento y control.

**Fecha de operación del Data Center de Computación:** El Data Center lleva funcionando desde marzo del 2018, donde se han ido implementando más equipos para poder sustentar todas las necesidades que tienen los estudiantes y docentes de la Carrera de Computación y también de otras carreras, además realizan actividades como gestión administrativa y recursos, actualizaciones de los servidores, brindar soporte de usuario.

El Data Center trabaja con una alta disponibilidad y funcionamiento 24/7/365.

# CAPÍTULO II

## FUNDAMENTOS DE LA EVALUACIÓN DEL ESCENARIO

En este capítulo se explica las etapas que tiene el Pentesting, Enfocado en el Data Center de la Carrera de Computación, este proceso deliberado de pruebas de penetración se convierte en un pilar esencial para salvaguardar la integridad de los sistemas y datos. la prueba de penetración en entornos virtualizados no solo se revela como una técnica fundamental sino como un compromiso proactivo con la seguridad cibernética. Más allá de la mera conformidad con estándares, estas pruebas se erigen como guardianes activos, adaptándose a las amenazas emergentes y anticipando desafíos futuros.

**Pentesting:** Las pruebas de penetración, la búsqueda deliberada de vulnerabilidades potenciales en un sistema mediante el uso de técnicas de ataque, son una herramienta relevante para las personas interesadas en la seguridad de la información. (Böhme & Félegyházi, 2010)

### Etapa I

#### *¿Qué es la obtención de información?*

Es un conjunto de métodos a través de los cuales se lleva adelante técnicas que utiliza la persona para obtener información sobre lo que se desea. Esto es importante ya que gracias a la obtención de información permite detectar las vulnerabilidades. (Álvaro Chirou, 2023).

#### *¿Para qué sirve la información obtenida?*

Sirve para encontrar vulnerabilidades y explotarlas y que se tomé la mejor decisión ante estas vulnerabilidades. (Álvaro Chirou, 2023).

#### *¿Cómo sacar información?*

Se puede obtener mediante:

- Google hacking
- Footprinting

- Análisis de IP y DNS
- WHOIS
- OSINT
- Búsqueda de cuentas y credenciales
- Análisis de metadatos
- Que existan cambios históricos en la web o los movimientos que existen en internet.

**Etapa II (Enumeración)**

***¿Qué es?***

Se debe enumerar todo lo detectado sobre vulnerabilidades que se encontró en la etapa I. (Álvaro Chirou, 2023)

***¿Para qué sirve?***

Permite enumerar las máquinas o direcciones que pueden resultar lo más vulnerable posible. (Álvaro Chirou, 2023)

***¿Cómo hacer la enumeración?***

A través de:

- Detección de máquinas encendidas.
- Detección de los servicios que tiene la máquina (FTP, HTTP, etc.)
- Análisis de DNS
- Análisis de dominios
- Realizar escaneos

**Etapa III (Análisis de vulnerabilidades)**

***¿Qué es el análisis?***

Se centra en buscar vulnerabilidades internas a partir de la búsqueda de la etapa II. (Álvaro Chirou, 2023)

***¿Por qué se realiza esta fase?***

Para encontrar a mayor profundidad las vulnerabilidades y así realizar una ruta de ataque y ver que exploits se pueden usar. (Álvaro Chirou, 2023)

**Etapa IV (Explotación de vulnerabilidades)**

***¿Qué es explotación?***

Es una de las más importantes de las etapas, ya que con esta se penetrando a los sistemas tomando ventaja de las vulnerabilidades para realizar la explotación. (Álvaro Chirou, 2023)

***¿Por qué se usa la explotación?***

Se usa para entrar en el sistema y poder hackear en un entorno controlado. (Álvaro Chirou, 2023).

***Herramientas***

***1.1.1.1 Metasploit***

Es una plataforma de prueba de penetración y un conjunto de herramientas que permite encontrar vulnerabilidades, realizar pruebas de seguridad y evaluar la seguridad de sistemas y redes informáticas. (Arias, 2023)

***1.1.1.1.1 Características***

- Contiene una amplia variedad de exploits y módulos que se utilizan para atacar vulnerabilidades específicas en sistemas y aplicaciones. (Jacky, 2023)

- Permite crear una "Shell remota" esto quiere decir que una vez que se realizó una explotación exitosa, permite obtener el control y realizar en análisis de seguridad. (Jacky, 2023)
- Tiene una base de datos de vulnerabilidades, lo que permie que su actualización sea constante lo que incluye las últimas vulnerabilidades conocidas. (Jacky, 2023)
- Permite lanzar una serie de exploits y escaneos de seguridad en un sistema o red de manera eficiente. (Jacky, 2023)
- Tiene un Soporte Multiplataforma, es decir que se puede ejecutar en diferentes sistemas operativos. (Jacky, 2023)
- Permite eliminar la huella digital del atacante. (Jacky, 2023)

#### *1.1.1.1.2 Módulos*

- Auxiliary: Permite recopilar la información del sistema y realizar el escaneo de vulnerabilidades. (Álvaro Chirou, 2023)
- Exploits: Este módulo está enfocado en programas de explotación. (Álvaro Chirou, 2023)
- Posts: Cuenta con programas que permiten escalar privilegios, esto se realiza después de que ya se hayan infiltrado en el sistema. (Álvaro Chirou, 2023)
- Payloads: Está enfocado en el despliegue de acciones maliciosas. (Álvaro Chirou, 2023)
- Encoders: Permite que los programas de antivirus pasen por alto los ataques, evitando que sea detectado. (Álvaro Chirou, 2023)

### *1.1.1.2 Armitage*

Es una interfaz gráfica que trabaja en conjunto con el framework de Metaspolit. Según Caballero (2013):

Armitage representa una interfaz gráfica asociada al reconocido framework Metasploit. Su utilidad radica en la capacidad de explorar posibles vulnerabilidades en sistemas informáticos, permite realizar pruebas de penetración, está diseñada para usuarios que no están familiarizadas con las líneas de comandos.

#### *1.1.1.2.1 Características*

- Permite escanear y enumerar hosts en una red, identificar posibles vulnerabilidades.
- Facilita la selección y ejecución de exploits en hosts seleccionados.
- Se puede trabajar en conjunto en un entorno de prueba de penetración, lo que puede ser útil en evaluaciones de seguridad más grandes y complejas.
- Proporciona gráficos e información visual que ayuda a los usuarios a comprender mejor la topología de la red, las rutas de ataque y las relaciones entre hosts.

**Etapa V (Post-Explotación)**

***¿Qué es Post-Explotación?***

Es toda aquella acción que se realiza después de la fase de explotación. (Álvaro Chirou, 2023)

***¿Cómo hacer la Post-Explotación?***

- Buscar tener privilegios de administrador y llegar a obtener las credenciales.
- Asegurar de no dejar rastros ni huellas, es decir no dejar evidencia.
- Encontrar la información y eliminar los logs.
- Generar backdoors y persistencia, dejar una puerta trasera con la posibilidad de dejar por si descubren el método por el cual se está ingresando, poder ingresar nuevamente a pesar de que haya sido detectado la vulnerabilidad.
- Pivoting, saltar entre privilegios e ir resolviendo diferentes dificultades que se vayan presentando.

**Etapa VI (Documentación)**

***¿Qué es la documentación?***

Es un documento en el cual se presenta los hallazgos realizados durante el proceso, para llegar a los resultados esperados. (Álvaro Chirou, 2023)

***¿Por qué se tiene que presentar documentación?***

Es importante ya que mediante la documentación se puede presentar los métodos, herramientas que se utilizaron durante el proceso. (Álvaro Chirou, 2023)

***¿Qué debe ir en la documentación?***

- Métodos usados en el proceso.
- Todas las vulnerabilidades encontradas.
- Exploits utilizados para explotar las vulnerabilidades.
- Consejos de mejora en contra de esos ataques.
- Contratiempos y análisis de seguridad.

***Recolección de información***

***Footprinting***

Se refieren a los métodos de búsqueda en fuentes de información públicas, específicamente empleados en pruebas de penetración para descubrir vulnerabilidades. Este enfoque se utiliza estratégicamente para la preparación de posibles ataques. (Zola, 2021)

Existe dos tipos, que son los siguientes:

- **Footprinting activo:** Son técnicas y métodos en el cual el atacante recopila información utilizando una interacción directa con sistemas informáticos o con la red. (Tapia, 2021)
- **Footprinting pasivo:** Se le llama método sigiloso ya que recopila por medio de información pública. (Tapia, 2021)

***Archivo robot.txt***

Este archivo es muy común encontrarle en aplicaciones web, es una forma de decirle a los motores de búsqueda qué partes del sitio web pueden y no pueden rastrear, es decir que permite controlar que partes del sitio web son accesibles para los robots de búsqueda y cuáles no. (Valk, 2023)

***¿Qué utilidad tiene?***

Tiene como objetivo disuadir búsquedas en Google, es decir que no se indexa en las búsquedas. (Álvaro Chirou, 2023)

***Método whois***

Es un protocolo que permite consultar los datos de la página (dominio) que se está buscando. Este contiene nombre del propietario, números de teléfonos, dirección de correo electrónico. (Delavy, 2019)

***Metadatos***

Se trata de un conjunto de información que detalla el contenido de un objeto o recurso, contribuyendo a una búsqueda más precisa de información. Es importante tener en cuenta que los metadatos se gestionan como datos ocultos. (PowerData, s.f.)

**Escaneos y enumeración**

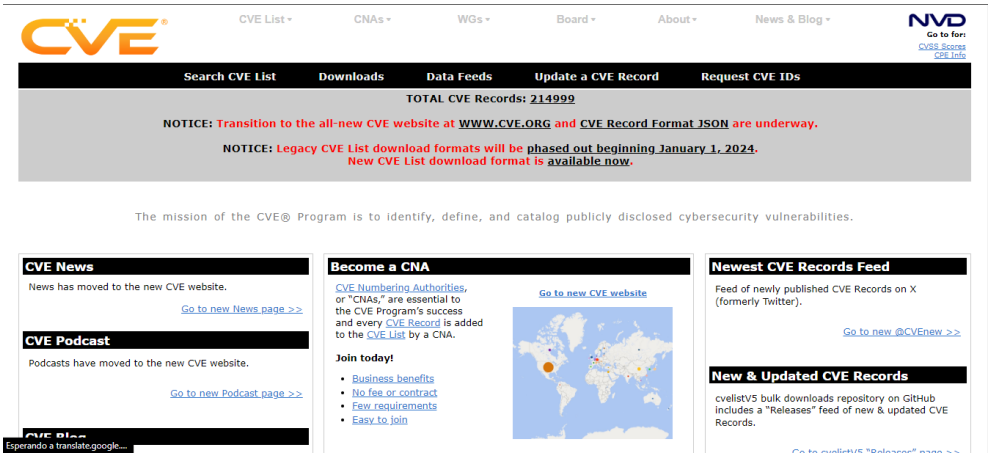
Se debe escanear y enumerar las vulnerabilidades encontradas, a continuación, se indicará algunos conceptos:

***CVE***

Es el intermediario entre la vulnerabilidad y la persona que va a explotar, es decir permite identificar, definir y catalogar vulnerabilidades catalogadas públicamente. (CVE, 2023)

**Figura 9**

*Página CVE*



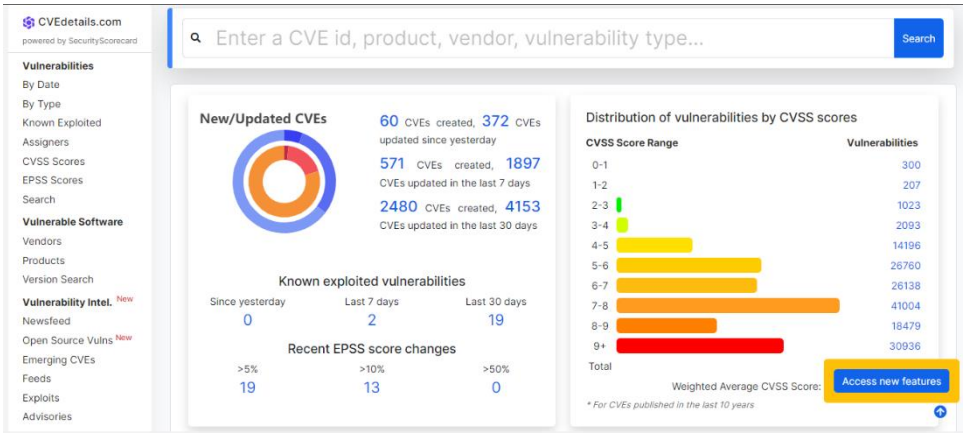

*Nota.* Esta página indica las vulnerabilidades de forma categórica. *Fuente:* (CVE, 2023)

### *CVE Details*

Permite encontrar datos sobre vulnerabilidades públicas, además tiene categorías: proveedores, productos, fecha de registro y tipo de vulnerabilidad. (KeepCoding, R, 2022)

**Figura 10**

*Página CVE Details*




*Nota*. CVE Details permite indicar en forma de datos las vulnerabilidades. Fuente: (CVE Details, 2023)

### Inventario de aplicaciones que utiliza el Data Center

En esta tabla se presentará las aplicaciones que más utilizan los estudiantes de la Universidad Politécnica Salesiana de la Carrera de Computación y de otras carreras. Además, también se presentará las aplicaciones que utilizan la parte de gestión y de monitoreo y las respectivas vulnerabilidades que podrían existir dentro de cada aplicación.

**Tabla 5**

*Vulnerabilidades de las aplicaciones*

| Aplicación | Vulnerabilidad |
|---|---|
| **Eclipse** | Las vulnerabilidades que se podrían dar son por parte de las bibliotecas que tiene java. Tal es el caso que en el año 2021 existió una vulnerabilidad en la biblioteca que da funcionalidad y creación de registros, lo que provocó que puedan realzar ataques por medio del código y así llegar a tener control sobre los servidores. (Tokio School , 2022) |
| **PostgreSQL** | En postgresql han existido hasta el momento 3 vulnerabilidades importantes que han logrado ser explotadas, lo han hecho mediante una inyección SQL y mediante Man-in-the-Middle lo que ha provocado que su ejecución sea inestable. La versión que ha sido más atacada es la 9.5.0. (Ciberseguridad, 2020) |
| **XAMPP** | En la versión 1.7.3 se encuentran las vulnerabilidades de tipo Disclosure y XSS, permiten que los ficheros se listen y se guarden en el servidor vulnerable y así poder atacar los clientes. (Adastra, 2013) |
| **Paquete de Office Professional Plus 2016** | Vulnerabilidades de ejecución remota de código en Microsoft Office, así como vulnerabilidades de seguridad en Microsoft Outlook 2016 Edición de 64 bits que podrían permitir la ejecución de código arbitrario al abrir un archivo modificado de forma malintencionada. Estas vulnerabilidades pueden ser explotadas por atacantes para realizar ataques de ejecución remota de código. (Soporte Técnico de Microsoft, 2022) |
| **Arduino** | Al ser un hardware de código abierto podría tener vulnerabilidades como inyecciones de código o de comando, al igual que podría existir vulnerabilidades al momento de ejecutar las bibliotecas. |
| **Android Studio** | Se han reportado vulnerabilidades como como dependencias no seguras, se puede ocasionar porque los desarrolladores de software no han integrado de la mejor manera las evaluaciones de seguridad y pruebas. Esto se puede dar a un amplio conjunto de ataques, ya sea ataques de inyección. Este impacto puede violar la seguridad de los datos o incluso la falta de disponibilidad en el servicio. (Android Devolopers, s.f.) |

| | |
|---|---|
| **TightVNC** | Mediante una falla en el uso incorrecto de la memoria se pudo llegar a tener fallos en la denegación de servicios, de igual manera esto fue favorable para los atacantes, lo que provoca que se puede ingresar un malware dentro de los sistemas de las personas que lo utilizan. (Kaspersky daily, s.f.) |
| **RDP - Acceso remoto dentro de la red de la Universidad** | Existe demasiadas vulnerabilidades del RDP. A continuación, se van a presentar las vulnerabilidades que podrían causar un impacto crítico dentro de la Universidad Politécnica Salesiana:<br>• Contraseñas débiles, la mayoría de las personas en los ordenadores tienen las contraseñas muy simples o débiles. Y al momento de acceder al acceso remoto de RDP, ocupan la misma contraseña, lo que lo hace más vulnerable a que se pueda realizar este tipo de ataques y de una manera sencilla.<br>• El puerto por defecto es el 3398, se recomienda cambiarlo ya que si no se lo realiza puede llegar a ser un blanco fácil de ataque e infectar todas las posibles máquinas que se encuentren con el RDP.<br>• Si el firewall de Windows no se encuentra actualizado y está habilitado el RDP pueden acceder al sistema. (Cloudfare, s.f.) (Microsoft, s.f.) |
| **VNC SERVER - VNC VIEWER (REALVNC)** | La vulnerabilidad más notoria es cuando en el proceso de autenticación existió un error en el diseño, donde al cliente y servidor se pide la contraseña, en ese caso al cliente no se le pide la contraseña lo que puede provocar un exploit que pueda acceder al servidor. (Hispasec, 2006) |
| **ANYDESK versión 8** | Las vulnerabilidades que se han ido arrastrando con las otras versiones, se pueden presentar en la versión 8, tal como denegación de servicios, vulnerabilidad en la interfaz XPC que produce ataques a las máquinas locales y escalamiento de privilegios. (CVE details, 2023) |
| **Ubuntu 22.04 (Sistema operativo más utilizado)** | La vulnerabilidad más reciente es que pueden enviar comandos arbitrarios mediante el SSH-agent. (Consultores, 2023) |

| | |
|---|---|
| **Windows 10, versiones 21H2 y 22H2 (Sistema operativo más utilizado)** | Esta debilidad, clasificada como "Zero Day", impacta al Servicio de Informes de Errores de Windows (WER).<br>La vulnerabilidad se manifiesta en un componente responsable de recopilar y enviar informes de errores a Microsoft. La falla reside en la forma en que WER gestiona solicitudes especialmente diseñadas, lo que posibilita que un atacante desarrolle un programa malicioso para aprovechar esta vulnerabilidad. Una vez ejecutado este programa malicioso, el atacante puede obtener acceso con privilegios elevados en el sistema. (CSIRT, 2023) |
| **Navegador Mozilla Firefox** | Una de las vulnerabilidades que tiene es que algunos datos que no deberían estar visibles lo están para terceros.<br>Otra vulnerabilidad a la denegación de servicios porque existe un error en el componente WASM JIT Analysis.<br>Pueden realizar un desbordamiento de buffer, haciendo un bloqueo a las páginas web totalmente explotable. (Cyber Zaintza, 2023) |
| **Navegador Google Chrome** | La vulnerabilidad Zero-Day es la que más afecta a Chrome, la última fue hacia la debilidad de heap-based buffer overflow donde bloquea aplicaciones y pueden ejecutar código arbitrario. (Hispasec, 2023) |
| **Navegador Microsoft Edge** | El atacante puede realizarlo de manera remota, ya que puede adquirir permisos superiores al sistema y esto provocaría poder instalar un software malicioso para poder sustraer la información confidencial o la información que el desea para poder extorsionar a los usuarios.<br>Otra vulnerabilidad que tiene es ataque de suplantación de identidad, donde pueden crear un sitio web o correo electrónico que parezca totalmente creíble y legible, lo que provoca que los usuarios revelen información personal o sensible. (CSIRT E. , 2023) |
| **Adobe** | La mayoría de las vulnerabilidades son críticas ya que pueden ejecutarlo a manera de ejecución remota de código arbitrario o que exista fuga de memoria afectando a los sistemas operativos. (Entelgy, 2022) |

*Nota.* Explicación detalla de las vulnerabilidades que tienen las aplicaciones que hacen uso los estudiantes de la Universidad Politécnica Salesiana. Elaborado por: El Autor.

A continuación, se indica las vulnerabilidades que podrían tener las aplicaciones tanto de la administración como de la gestión del Data Center.

**Tabla 6**

*Vulnerabilidades de las aplicaciones de administración y gestión*

| Aplicación | Vulnerabilidad |
|---|---|
| **VMware vRealize® Log Insight 8.10.2.0 - (Manejo de logs de servidores a nivel de VMware)** | Durante el año 2023 existió 4 vulnerabilidades donde dos fueron de estado crítico.<br>• El atacante aprovecha que hay control de acceso roto y pueda leer archivos arbitrarios en el sistema.<br>• El atacante puede generar una denegación de servicios (DoS).<br>• Esta vulnerabilidad es susceptible a la divulgación de información donde puede el atacante acceder a información sensible. (Lakshmanan, 2023) |
| **Vcenter Server 7** | Ha tenido varias vulnerabilidades, que se detallan a continuación:<br>• Permiten al atacante remoto Ejecutar comandos arbitrarios dentro del sistema.<br>• Esta vulnerabilidad se la ha llamado escritura fuera de límites, ya que el atacante, al estar dentro de la red del VCenter Server desencadena una escritura fuera de límites y envía paquetes que pueden llegar a provocar daños en la memoria.<br>• En esta vulnerabilidad, el atacante, que tiene acceso a la red, desencadena la vulnerabilidad de corrupción de memoria donde esquivan la |

| | |
|---|---|
| | autenticación, provocando los daños esperados por parte del atacante. (VMware, 2023) |
| **ESXI 7 UPDATE 3** | Esta vulnerabilidad es por desbordamiento donde se encuentra en el mismo segmento de la red ESXI ya que tiene acceso al puerto por defecto 427 lo que permite al atacante ejecutar de manera remota. (NIST, s.f.) |
| **Windows Server 2012** | Las dos vulnerabilidades más importantes que han sido para Windows Server 2012 son:<br>• Una vulnerabilidad llamada Zerologon, en el cual permite hacer escala de privilegios, si ingresa al dominio el atacante puede cambiar las contraseñas, esta vulnerabilidad ha sido calificada como crítica.<br>• Ataque al servidor DNS de Microsft donde si logra el desbordamiento puede ingresar como administrador y obtener todos los privilegios. (Pollack, 2021) |

*Nota.* La tabla explica detalladamente las vulnerabilidades que podría sufrir el Data Center. Elaborado por: El Autor.

**Penetración y explotación**

La penetración y explotación en el ámbito de la ciberseguridad son dos aspectos fundamentales en las pruebas de seguridad y evaluación de vulnerabilidades en sistemas informáticos. Según Guardiola (2020):

> El "penetration testing" o "pen testing" implica una simulación controlada de un ciberataque, donde expertos en seguridad informática buscan identificar y aprovechar vulnerabilidades en sistemas, redes o aplicaciones, con el objetivo de evaluar la

resistencia de los sistemas de seguridad y su capacidad de detección y respuesta ante posibles amenazas.

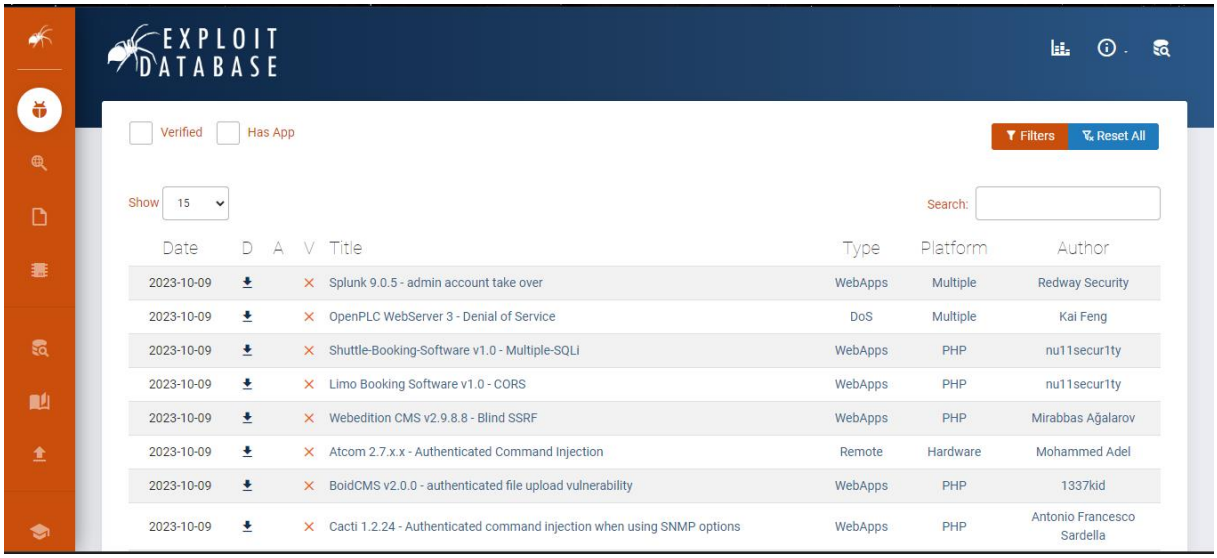
En contraste, la explotación se refiere al acto de aprovechar una vulnerabilidad o debilidad en un sistema con el propósito de comprometer su seguridad. Los ciberdelincuentes utilizan técnicas de explotación para obtener acceso no autorizado, robar información confidencial o causar daño a la infraestructura de TI.

Estos conceptos son esenciales para la evaluación y fortalecimiento de la seguridad cibernética, ya que posibilitan la identificación y corrección de vulnerabilidades antes de que sean aprovechadas por actores malintencionados. Las pruebas de penetración y la explotación ética son prácticas habituales en la ciberseguridad, llevadas a cabo de manera controlada y autorizada para mejorar la seguridad de los sistemas y resguardar la información sensible.

A continuación, se presenta una página web donde se puede encontrar vulnerabilidades dependiendo la necesidad.

**Figura 11**

*Página web Exploit DataBase*




*Nota.* Página web para encontrar las vulnerabilidades y luego realizar la post explotación. Fuente: (*OFFSEC's Exploit Database archive*, 2023)

**Importancia de la evaluación del escenario en entornos virtualizados**

Una buena evaluación permite identificar posibles vulnerabilidades que podría existir en la infraestructura virtual para poder mitigar los riesgos y fortalecer la seguridad. Además, una evaluación garantiza que se cumpla las normativas especialmente en entornos virtuales. Según Guardiola (2020), "Al identificar debilidades, se pueden implementar soluciones y realizar un seguimiento para garantizar que la seguridad siga siendo efectiva con el tiempo, dando una mejora continua de la seguridad, también ayuda a proteger datos importantes o sensibles ante posibles amenazas", además ayuda a los involucrados a tomar medidas preventivas contra riesgos y mantener una postura segura en un entorno de amenazas en constante evolución.

**Conceptos clave en la evaluación del escenario**

1. *Protección de datos:* Son datos que se recolectan, mantienen y procesan. (Biblioguias: Biblioteca de la CEPAL, s.f.). Permite garantizar que los datos son privados y evitar el uso inadecuado sobre los datos

   Ventajas:

   - Al realizar escalabilidad permite almacenar mayor cantidad de datos y ayuda en el ahorro de costes.
   - Los datos pueden ser almacenados en la nube, lo que permite realizar copias de seguridad en diferentes espacios y esto se puede llegar a evitar un riesgo o mitigarlo.
   - Se puede evitar brechas de seguridad mediante los respectivos controles que se implementen en las empresas, así aseguran los datos.
   - La empresa u organización al tener varios servidores deben ser resistentes ante el almacenamiento en la nube, por tal motivo se debe dar una protección sólida y garantizar que los datos no se encuentran expuestos a fines maliciosos.

- Si tiene protección y seguridad garantizan un buen servicio de calidad, confidencialidad, disponibilidad sobre los datos.
- Contar con herramientas que sean aprobadas, garantizadas y legales para que los usuarios se sientan seguros sobre sus datos.

2. *Acceso autorizado:* Es una medida de seguridad donde buscan proteger ya sean datos o información sensible que contenga la empresa. Esto con el fin de que solo personas que sean designadas o autorizadas puedan acceder a dicha información.

   Para garantizar el acceso autorizado, se toma en cuenta lo siguiente:

   - Cifrar los datos para que evitar que personas no autorizadas puedan leerlo.
   - Utilizar la técnica DLP, esto evita que los datos sean expuestos ya sea por negligencia del usuario, o con fines maliciosos. (Acronis, 2021)
   - Establecer políticas claras donde las personas involucradas tengan conocimiento al respecto y garantizar un acceso adecuado.
   - Al tener un buen monitoreo sobre el tráfico saliente se puede detectar anomalías dentro de la red, señales de violación al sistema.

3. *Mitigación de riesgos:* Es un proceso que trata de evitar o reducir un impacto que podría perjudicar a la empresa. Es por ello por lo que se explica a continuación algunas estrategias:

   - Identificar los riesgos y evaluar, para entender el tipo, nivel y solución para su respectiva mitigación.
   - Reducir la probabilidad de ocurrencia o impacto negativo ante un evento.
   - Denegación predeterminada en algunas aplicaciones de dudosa procedencia.
   - Monitorear y registrar todo tipo de actividades sospechosas.
   - Crear controles de acceso que sean adecuados a las prácticas de seguridad.
   - Dar un soporte inmediato ante posibles virus.

**Relación entre los mecanismos de evaluación y los fundamentos de seguridad**

La relación que existe entre la identificación y análisis de riesgo buscan implementar controles de seguridad para minimizar y controlar el riesgo.

El cual permite identificar, analizar y evaluar los riesgos y vulnerabilidades de un sistema u organización. Su objetivo principal es minimizar y controlar los riesgos que no han podido ser eliminados, estableciendo medidas preventivas. (FREMM, s.f.)

Algunos mecanismos y fundamentos son:

- Analizar los riesgos de seguridad permite determinar la probabilidad de que ocurra un evento riesgoso.
- Controles de seguridad se implementan las medidas para proteger la privacidad digital y prevenir el acceso no autorizado a los datos. (Safety Culture, 2023)
- Auditorias y evaluaciones permite verificar la efectividad de forma regular para tener respuestas favorables mediante planes de acción.

**Identificación de vulnerabilidades**

Los sistemas siempre estarán expuestos al peligro ya sea por amenaza o vulnerabilidad. Donde la vulnerabilidad pone en peligro al sistema, y es responsabilidad del administrador y su equipo detectar, evaluar y reducir. (Avenía, 2017)

Tipos de vulnerabilidades:

- *Vulnerabilidad física:* Las instalaciones inapropiadas en el espacio de trabajo, la escasez de recursos en los puestos de trabajo, la disposición caótica de los cables de alimentación y red, así como la ausencia de identificación del personal, al ser explotadas por amenazas, impactan directamente en los fundamentos esenciales de la seguridad de la información, especialmente en lo que respecta a la disponibilidad. (Avenía, 2017)

- *Vulnerabilidades naturales:* Son las condiciones de la naturaleza que puedan poner en riesgo la información. A menudo, la humedad, el polvo y la contaminación pueden causar daños a los bienes. (Avenía, 2017)
- *Vulnerabilidades de hardware:* Potenciales imperfecciones en la fabricación o configuración de los equipos de la empresa que podrían posibilitar un ataque o manipulación de esta. (Avenía, 2017)
- *Vulnerabilidades del software:* Configuraciones erróneas e instalación inapropiada de software, lo que podría conducir a un uso indebido de los recursos por parte de usuarios malintencionados. Las aplicaciones son componentes que facilitan la lectura de la información y posibilitan que los usuarios accedan a esos datos a través de medios electrónicos, como las páginas web de los navegadores de Internet. (Avenía, 2017)
- *Vulnerabilidades de medios de almacenamiento:* Los medios de almacenamiento son dispositivos físicos o magnéticos empleados para conservar información. Entre los tipos de medios de almacenamiento expuestos se encuentran los disquetes, CDs, así como los discos duros de servidores y bases de datos. (Avenía, 2017)
- *Vulnerabilidades de comunicación:* Esta clase de vulnerabilidad afecta a todos los datos que circulan por la red, independientemente del medio de transmisión, ya sea cable, satélite, fibra óptica o señales de radio. (Avenía, 2017)
- Vulnerabilidades humanas: Se refiere al perjuicio que las personas pueden causar a la información y al entorno tecnológico. La vulnerabilidad más significativa radica en la ausencia de medidas de seguridad adecuadas, particularmente en la adopción por parte de cada componente, especialmente los miembros internos de la empresa u organización. (Avenía, 2017)

***Factores de la vulnerabilidad***

- *Factores ambientales:* Guardan relación con la forma en que una comunidad emplea elementos no sostenibles de su entorno. (Avenía, 2017)
- *Factores económicos:* Uso inadecuado de los recursos disponibles para una gestión de riesgos apropiada. (Avenía, 2017)
- *Factores organizativos:* El nivel en que las comunidades se estructuran, coordinan y comprenden su vulnerabilidad, y por ende, representan una respuesta potencial a un desastre. Una ciudad que cuenta con un plan de gestión de riesgos implementado está menos susceptible a los impactos de un desastre. (Avenía, 2017)

***Casos reales de empresas que fueron afectadas por vulneraciones***

- *Microsoft Windows:* El sistema operativo es uno de los sistemas más comúnmente conectados a Internet y presenta varias vulnerabilidades críticas. Las más destacadas se encuentran en IIS, MS-SQL e Internet Explorer, que son ampliamente utilizados. (Avenía, 2017)
- *IIS:* Se describe en el Boletín de Seguridad de Microsoft MS01-033 y es una de las vulnerabilidades de Windows más explotadas. A lo largo de varios años, numerosos gusanos de red han sido creados para aprovechar esta vulnerabilidad, entre ellos 'CodeRed'. (Avenía, 2017)
- *El gusano de red spida:* Casi un año después de la aparición de CodeRed, se identificó utilizando una vulnerabilidad en MS-SQL Server para su propagación. Esto posibilitó que cualquier individuo con acceso a la red pudiera ejecutar instrucciones en el sistema. Aprovechando esta vulnerabilidad, el gusano configuraba la cuenta "Invitado" para permitir la apertura de archivos compartidos y su descarga, facilitando el acceso al sistema. (Avenía, 2017)

- *Gusano slammer:* Atacó servidores en sistemas Windows a través del método de MS-SQL: aprovechó una vulnerabilidad de desbordamiento de búfer en ciertas subrutinas encargadas del manejo de paquetes del servidor UDP. (Avenía, 2017)
- *Sasser:* Surgió a principios de mayo de 2003, se difundió de manera veloz y afectó a millones de computadoras alrededor del mundo. (Avenía, 2017)
- *Unix:* Ha empleado el servicio de finger, el cual posibilita a una persona externa a una red visualizar qué usuarios están conectados a equipos específicos o ubicaciones desde las cuales los usuarios obtienen acceso. (Avenía, 2017)
- *Sendmail:* Se creó para gestionar la transferencia de mensajes de correo electrónico en Internet; el gusano Morris empleó una vulnerabilidad a través de 'sendmail' para su explotación. (Avenía, 2017)

**Pruebas de penetración en escenarios virtualizados**

Una prueba de penetración, conocida como pen test o piratería ética, representa una técnica fundamental en el ámbito de la seguridad cibernética, empleada por organizaciones para descubrir, evaluar y destacar vulnerabilidades en su postura de seguridad. Estas pruebas, comúnmente llevadas a cabo por especialistas en piratería ética, ya sean empleados internos o terceros, buscan simular las estrategias y tácticas de un atacante real con el propósito de evaluar la resiliencia de los sistemas informáticos, redes y aplicaciones web de una entidad. (Mehta, 2022)

Además de fortalecer la seguridad, las pruebas de penetración también son utilizadas por las organizaciones para verificar su conformidad con las normativas y estándares de cumplimiento establecidos. (Mehta, 2022)

Las pruebas de penetración se sitúan como una medida proactiva en seguridad cibernética, ya que involucran mejoras continuas e iniciativas autónomas basadas en los informes generados

por la prueba. Este enfoque contrasta con estrategias no proactivas que carecen de la previsión necesaria para abordar y mejorar las vulnerabilidades a medida que emergen. (Mehta, 2022)

### *Tipos de Pentesting*

Existen tres tipos, que se detallan a continuación:

1. ***Caja negra o black box:*** Se trata del intento de comprometer el sistema informático sin conocimiento previo. Esta evaluación expone posibles fallos o vulnerabilidades de seguridad en la aplicación que podrían ser aprovechados por ciberdelincuentes en ataques externos, sin necesidad de acceder al sistema. Se proporciona únicamente la URL o la IP de la aplicación, y los casos de prueba se limitan para evitar la explotación de la funcionalidad interna de la aplicación. (Santos, 2023)
2. ***Caja gris o grey box:*** En esta evaluación, se proporciona información confidencial acerca de la aplicación, que incluye contraseñas de acceso y una descripción general de la arquitectura. Este suministro facilita la ampliación de los casos de prueba que se ejecutarán, lo que resulta en la detección de brechas de seguridad más críticas e importantes. (Santos, 2023)

   Centra los ataques en secciones particulares de la aplicación de forma muy específica. Aunque hereda todas las ventajas de una prueba de caja negra, demanda más tiempo, ya que involucra tanto ataques externos como internos, simulando la función de un usuario autenticado. (Santos, 2023)
3. ***Caja blanca o white box***: Se revela toda la información confidencial relacionada con la aplicación y el sistema, abarcando el diseño de la arquitectura, credenciales de acceso y, lo más vital, se comparte el código fuente para una revisión minuciosa en busca de posibles vulnerabilidades. Esta prueba es la más detallada, ofreciendo una auditoría completa de la seguridad del sistema. Sin embargo, su implementación lleva más tiempo debido a su elevada complejidad. (Santos, 2023)

**Figura 12**

*Tipos de Pentesting*


*Nota.* Explicación de los tipos de pruebas (caja negra, gris y blanca) con sus respectivas características. Fuente: (Santos, 2023)

**Obtención del escenario de pruebas (proceso de pentesting)**

Para realizar el escenario de pruebas se va a realizar mediante un escenario aislado, en el cual va a tener máquinas virtuales con sistemas operativos como Windows, Linux. Para ello se va a realizar en un laboratorio del Data Center, donde cumpla con los requisitos para poder realizar un ataque controlado a las máquinas virtuales.

# CAPÍTULO III

## EVALUACIÓN DE LOS RESULTADOS OBTENIDOS

Para realizar las pruebas pertinentes se llevó a cabo en una máquina virtual anidada con sistema operativo Windows 10, esta máquina virtual se encuentra en el Data Center, en cual se instaló las máquinas más solicitadas por los estudiantes y docentes que son: Windows 10 y Ubuntu 22.

La virtualización anidada es una configuración en la que se ejecuta una máquina virtual dentro de otra máquina virtual. Esto significa que se está virtualizando en un entorno controlado. Este enfoque se utiliza a menudo para propósitos de desarrollo y pruebas, por tal motivo para poder tener un ambiente controlado al momento de realizar las pruebas de explotación, no ponga en riesgo la integridad de la información o que exista intermitencia en la red.

### *Pruebas en la máquina virtual Ubuntu*

Para ello en el sistema operativo Ubuntu se va a hacer un escaneo de vulnerabilidades, para determinar que exploit se puede explotar en la máquina virtual.

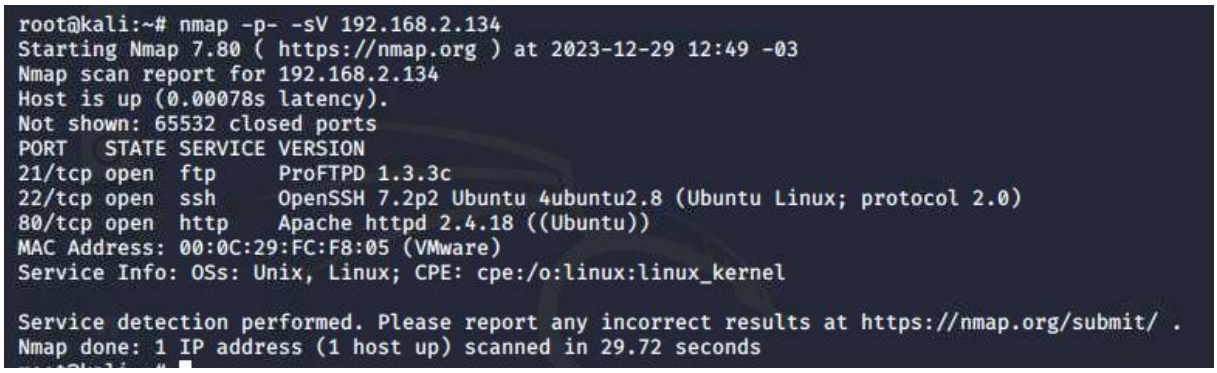
A continuación, se indican los pasos para obtener la información de la máquina virtual Ubuntu, cabe mencionar que la obtención de información se hace mediante el apoyo de Kali Linux:

Mediante el escaneo de nmap -sP, se lleva a cabo una exploración minuciosa de todos los puertos accesibles en el sistema objetivo, con el propósito adicional de reconocer los servicios activos en esos puertos mediante la detección de servicios.

nmap -p- -sV 192.168.2.134

**Figura 13**

*Escaneo con nmap*




*Nota.* Con esta línea de comando permite escanear con la IP de la máquina objetivo los puertos que están abiertos, el estado, el nombre del servicio y la versión. Elaborado por: El Autor.

Searchsploit, la tarea fundamental consiste en investigar y presentar detalles acerca de exploits, payloads, shellcodes y documentos vinculados a vulnerabilidades particulares presentes en bases de datos de exploits. (Chema, 2017)

searchsploit ProFTPD 1.3.3c

**Figura 14**

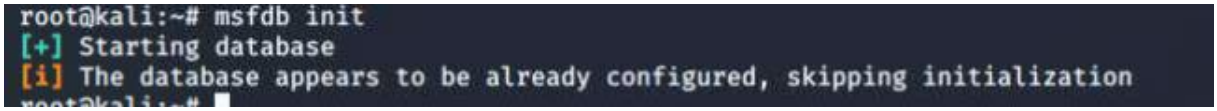
*searchsploit*


*Nota.* Con esta línea de comando permite buscar los exploit que tiene la versión del servicio. Elaborado por: El Autor.

Msfdb es un script que permite conectarse a Metasploit. (adamgalway, 2020)

**Figura 15**

*Base de datos msfdb*




*Nota.* Con esta línea de comando permite iniciar la base de datos de Metasploit. Elaborado por: El Autor.

Msfconsole, esta consola de Metasploit posibilita que los usuarios entren al Metasploit Framework mediante una interfaz de línea de comandos interactiva. (Ciberseg, 2021)

**Figura 16**

*Consola de Metasploit*


*Nota.* Con este comando permite ingresar a Metasploit. Elaborado por: El Autor.

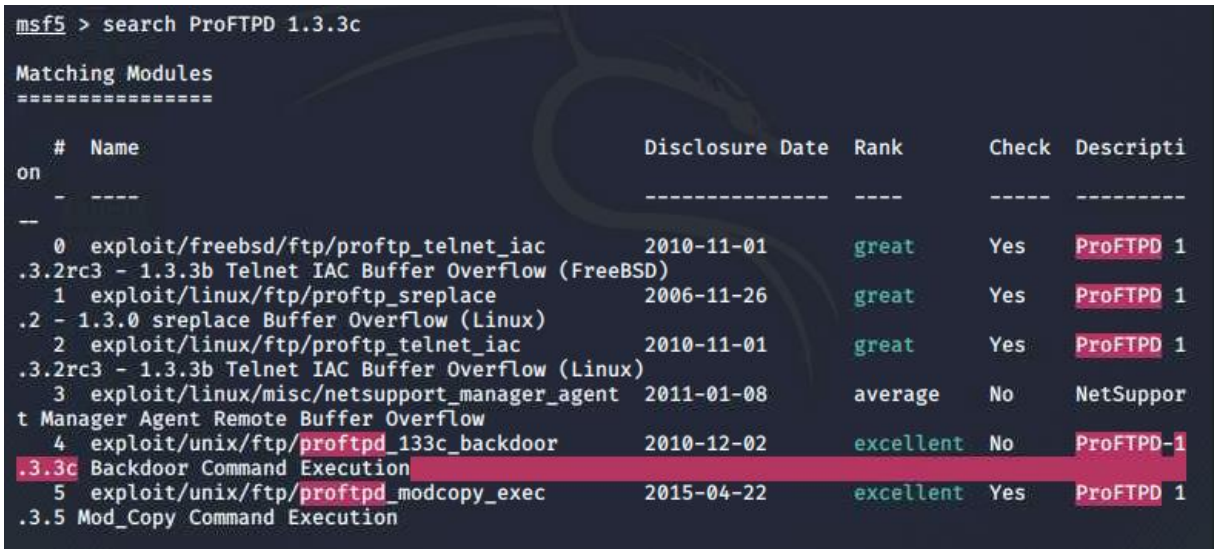
En segundo lugar, se indica las vulnerabilidades obtenidas, con el comando search:

Search, se busca nuevamente el servicio que se desea explotar. (Álvaro Chirou)

search ProFTPD 1.3.3c

**Figura 17**

*Consola de Metasploit*




*Nota.* Search es el comando que permite buscar el exploit. Elaborado por: El Autor.

Se usa el exploit mediante el comando use exploit/unix/ftp/proftpd_133c_backdoor

**Figura 18**

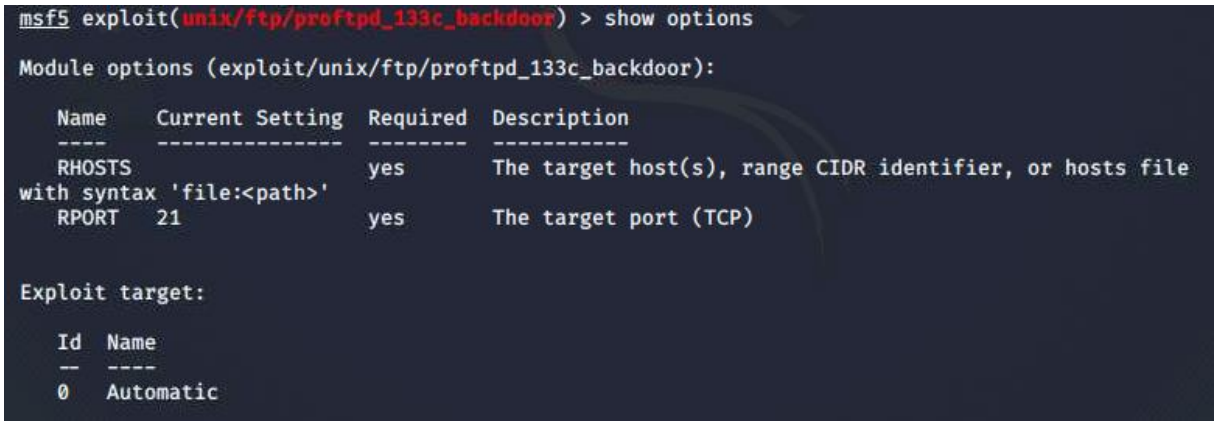
*Uso del exploit*


*Nota.* “Use” es el comando que permite ingresar al exploit. Elaborado por: El Autor.

El comando show options, indica los datos que se deben introducir en el exploit que se va a utilizar. (Álvaro Chirou)

**Figura 19**

*Ver opciones*




*Nota.* Show options es el comando que permite ver las opciones que tiene el exploit y validar si está asignado la IP en RHOSTS. Elaborado por: El Autor.

Set RHOSTS, se utiliza en Metasploit Framework para definir la dirección IP del objetivo en evaluación. (Caballero, 2018)

**Figura 20**

*Asignar IP*


*Nota.* Set RHOSTS es el comando para asignar la IP de la máquina objetivo. Elaborado por: El Autor.

Hydra, es una herramienta de prueba de penetración que se utiliza para realizar ataques de fuerza bruta y probar la seguridad de contraseñas.

hydra -l “marlinspike” -e nsr 192.168.2.134 ssh

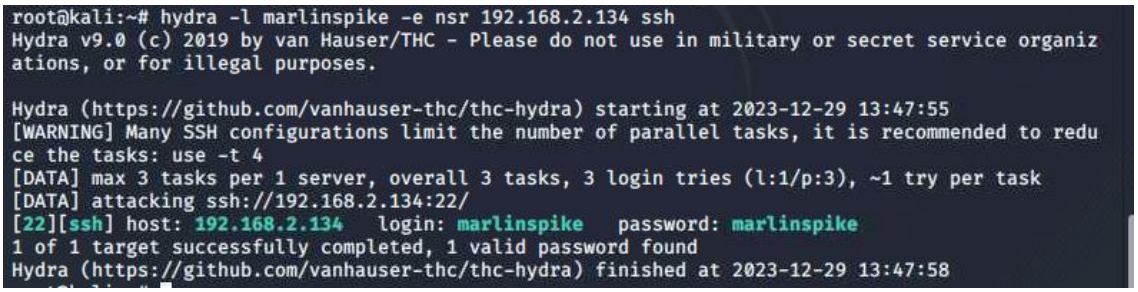
-l: especifica el nombre de usuario, en este caso es marlinspike

-e nsr: conjunto de caracteres que se utilizarán en el ataque de fuerza bruta.

SSH: Indica el protocolo o servicio al que se dirigirá el ataque, en este caso, SSH (Secure Shell).

**Figura 21**

*Herramienta Hydra*



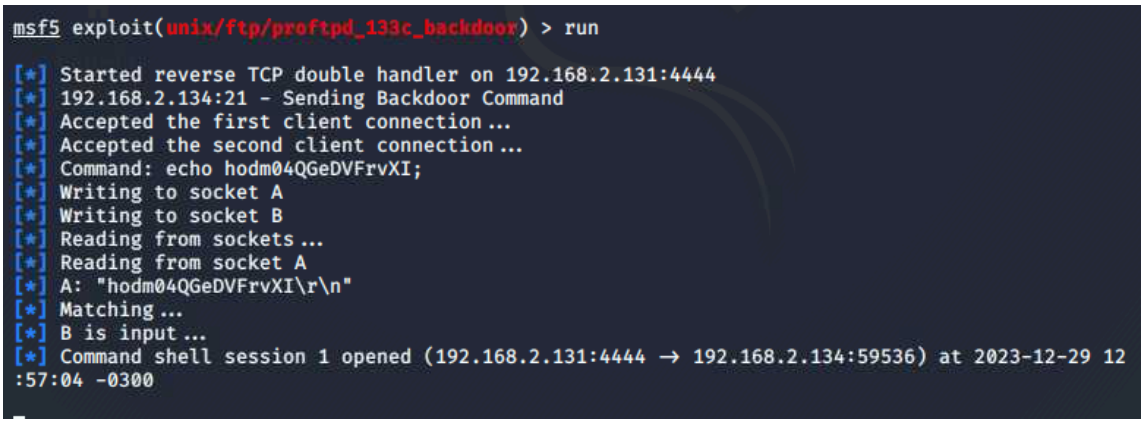

*Nota.* Se ingresa esa línea de comando para obtener el host, usuario y contraseña. Elaborado por: El Autor.

***Resultados de la máquina virtual Ubuntu***

Ahora se procede a ejecuta el exploit con el comando run.

**Figura 22**

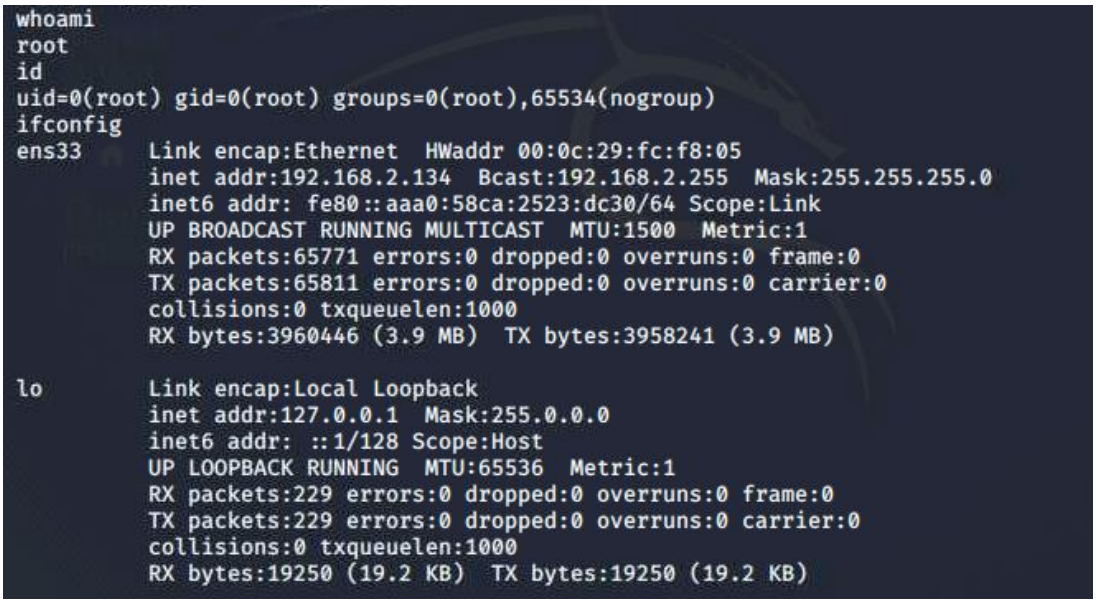
*Ejecutar el exploit*




*Nota.* Se ingresa esa línea de comando para ingresar a la máquina objetivo mediante Metasploit. Elaborado por: El Autor.

**Figura 23**

*Verificar máquina objetivo*

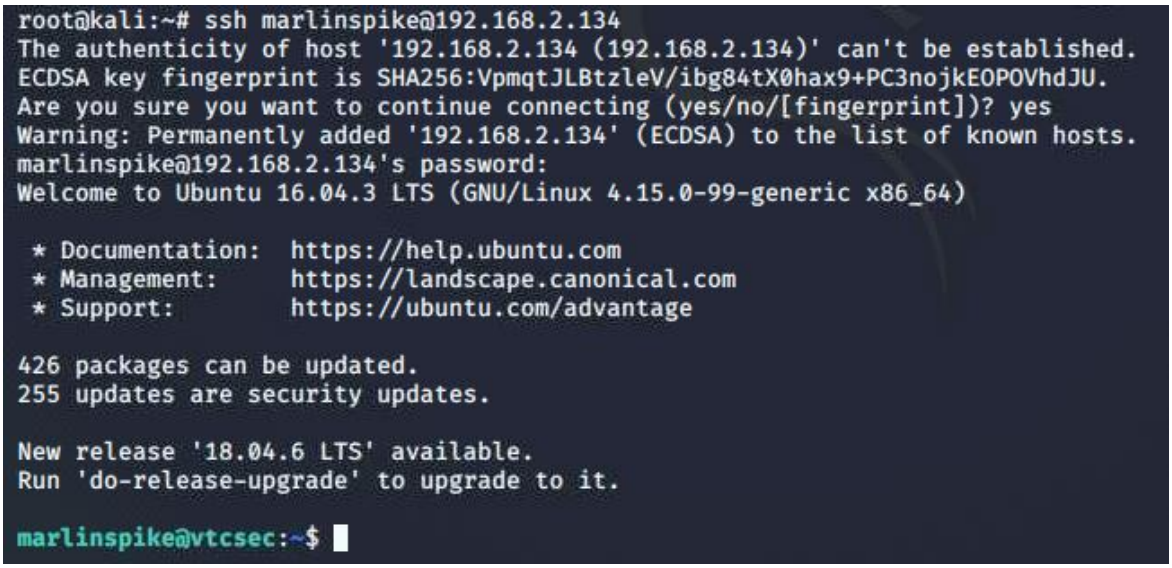



*Nota.* Se ingresa los comandos como, whoami, ifconfig para saber que se ha ingresado exitosamente a la máquina objetivo. Elaborado por: El Autor.

Se ingresa al SSH como normalmente se hace, y se ingresa a la máquina objetivo (Ubuntu):

**Figura 24**

*Verificar máquina objetivo mediante Hydra y SSH*

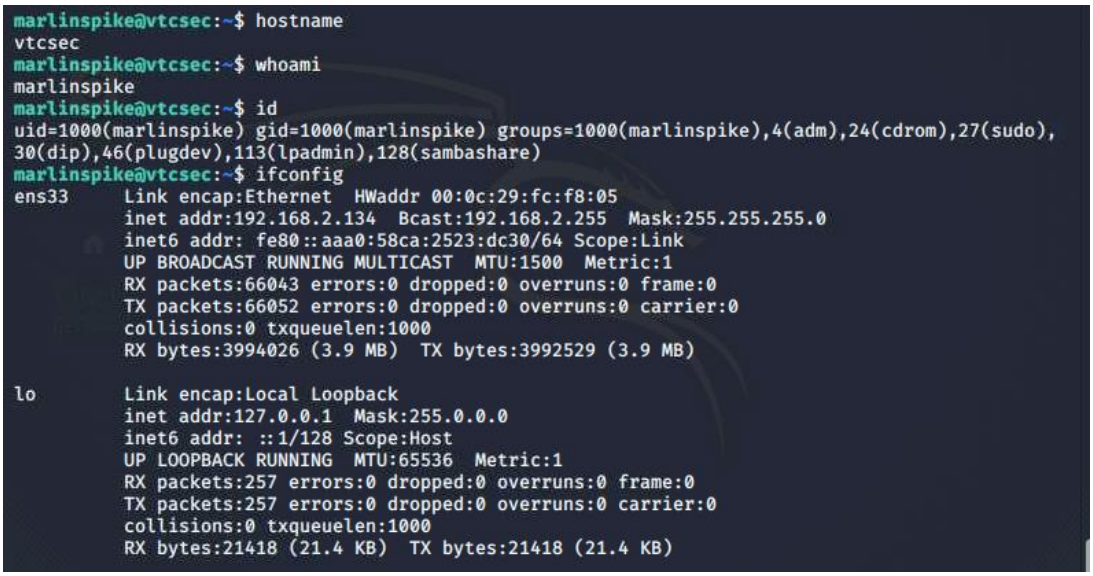



*Nota.* Se ingresa por SSH a la máquina objetivo, con las credenciales que se realizó con el comando hydra y así obtener acceso a la máquina. Elaborado por: El Autor.

Verificar máquina objetivo mediante Hydra y SSH

**Figura 25**

*Validar la máquina objetivo*

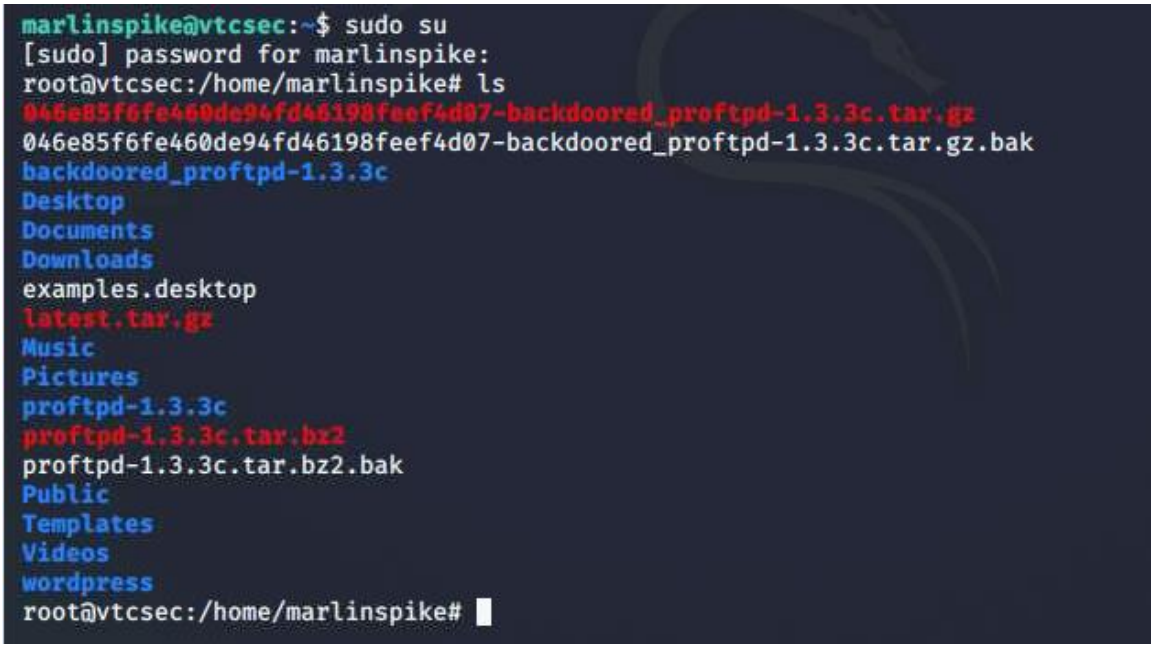



*Nota.* Se ingresar los comandos como, whoami, ifconfig para saber que se ha ingresado exitosamente a la máquina objetivo. Elaborado por: El Autor.

Se ingresa como root a la máquina objetivo (Ubuntu):

**Figura 26**

*Ingresar como usuario root a la máquina objetivo*




*Nota.* Se ingresa como usuario root a la máquina objetivo, para tener total acceso y control. Elaborado por: El Autor.

***Pruebas en la máquina virtual Windows***

Para realizar las explotaciones pertinentes en Windows, se encontró un virus llamado Bob Esponja o también conocido como Horror Bob en el cual es un .exe, que al momento de ejecutar desactiva Windows Defender y el administrador de tareas de manera inmediata llegando a dañar la máquina objetivo dejando sin acceso al usuario, es decir causando un daño irreparable a la máquina.

A continuación, se indica cómo se implementó el virus en la máquina objetivo:

En primer lugar, Gmail presenta una vulnerabilidad relacionada con la detección de virus, ya que no detecta o no logra reconocerlos. Esto conlleva a que al enviar correos electrónicos, los receptores podrían descargar archivos maliciosos en sus computadoras. En contraste, Outlook (Hotmail) permite cargar archivos, pero incorpora un mecanismo de seguridad más robusto. En este caso, aunque se permite la carga de archivos, al intentar descargarlos, Outlook detecta posibles amenazas de virus y bloquea la acción.

Se verifica que el archivo se haya descargado exitosamente.

**Figura 27**

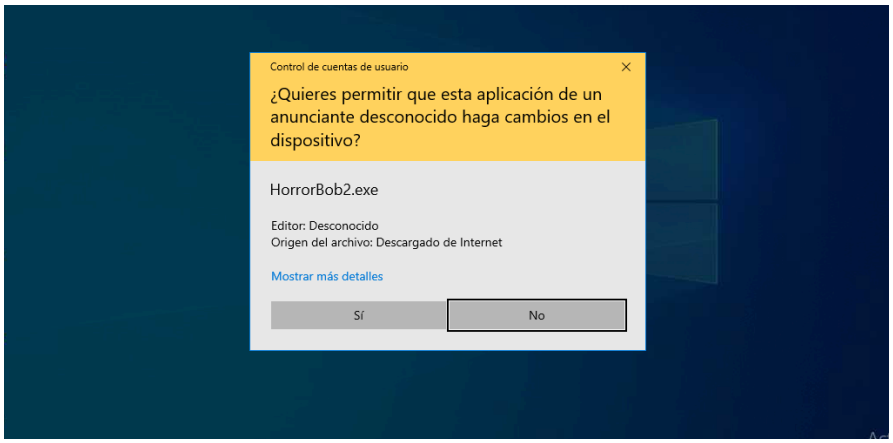
*Descarga del archivo*


*Nota.* El archivo que se descarga no da indicio de que sea malicioso. Elaborado por: El Autor.

Cuando ya se encuentra descargado, el usuario procede a ejecutar el archivo y permite los cambios en el dispositivo.

**Figura 28**

*Permitir cambios en el dispositivo*

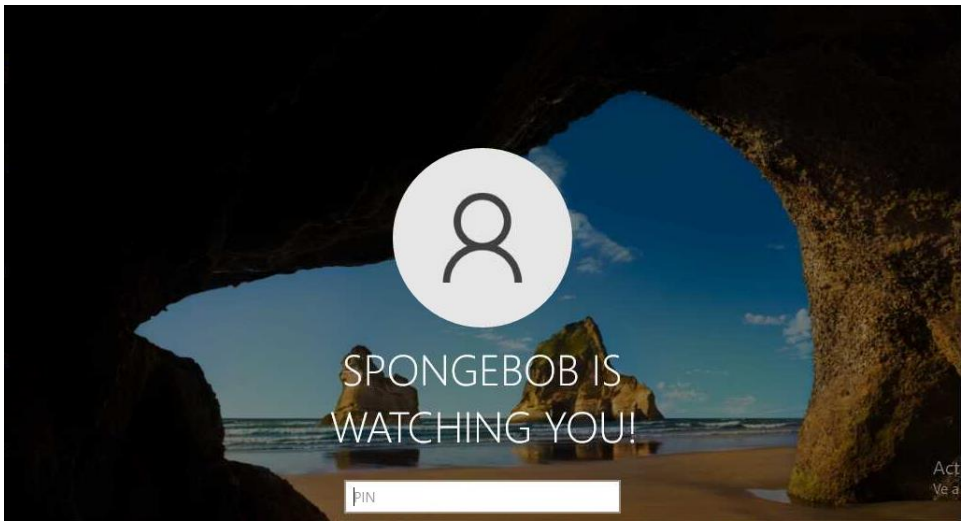



*Nota.* El .exe pide la autorización para realizar los cambios, como si fuera un archivo normal. Elaborado por: El Autor.

Después de efectuar las modificaciones en el dispositivo de la máquina objetivo, se lleva a cabo un reinicio. Al solicitar el PIN, el nombre del usuario ya no aparece; en su lugar, se presenta el mensaje: "SPONGEBOB IS WATCHING YOU!". A pesar de este cambio, el usuario sigue ingresando el PIN de manera habitual.

**Figura 29**

*Inicio de sesión*




*Nota.* En la imagen se muestra cómo se ha sustituido el nombre del usuario por el nombre que ingresó el programa malicioso. Elaborado por: El Autor.

Una vez ingresado el PIN, la pantalla de inicio se presenta de manera distinta, en el cual se restableció el tema de Windows por defecto. Esto modifica la apariencia de la pantalla, como se ilustra en la imagen adjunta.

**Figura 30**

*Pantalla inicial*

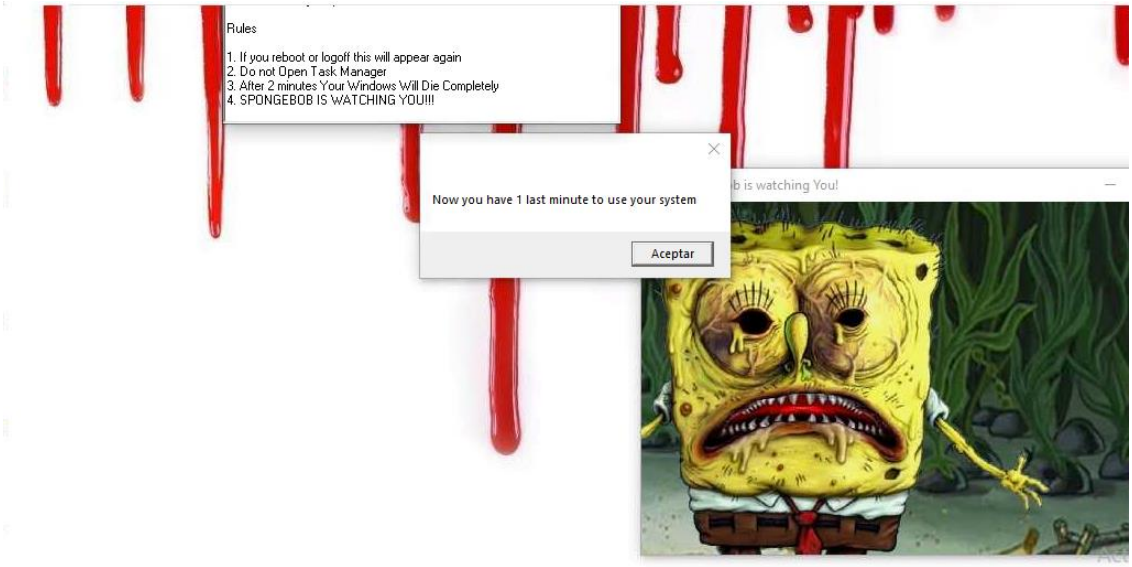

*Nota.* El fondo de pantalla se ha cambiado a lo esperado con el programa malicioso. Elaborado por: El Autor.

Al cabo de unos minutos empezará el escritorio a llenarse de mensajes y de imágenes, en el cual indica las normas a las que está sometida la máquina objetivo:

1. Si reinicia o cierra sesión esto aparecerá nuevamente.
2. No abra el administrador de tareas.
3. Después de 2 minutos Windows se apagará por completo.
4. Bob Esponja te está observando.
5. Ahora tienes un último minuto para estar en el sistema.

**Figura 31**

*Invasión mediante imágenes*



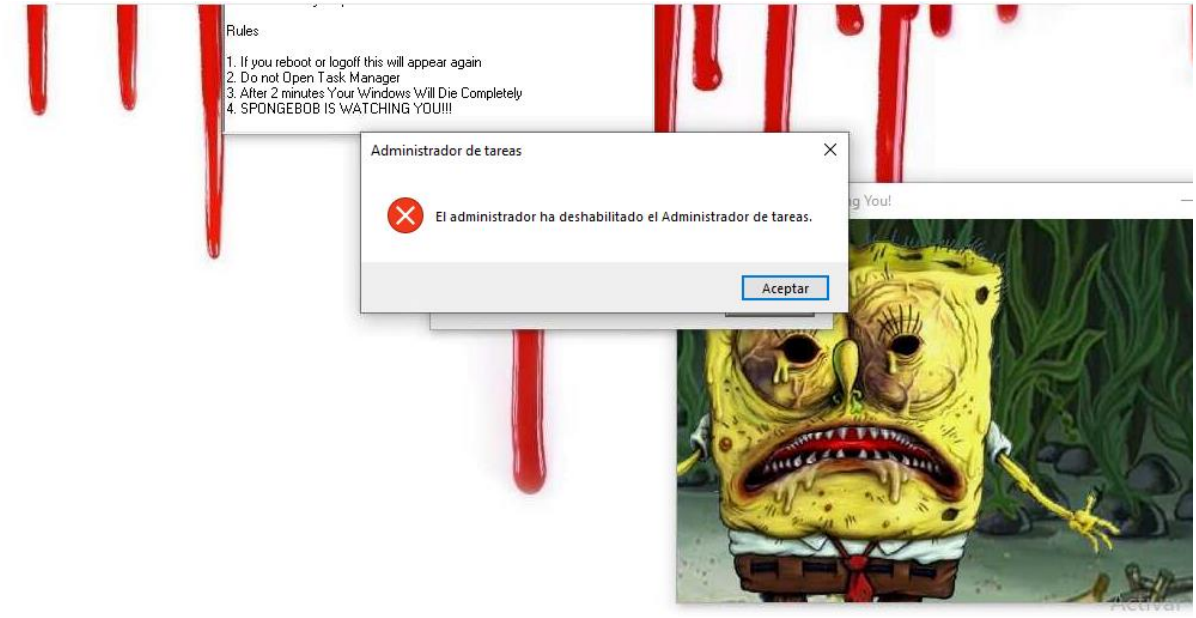

*Nota.* En la pantalla se muestra los cuadros de mensajes maliciosos, explicando las reglas que debe seguir el usuario. Elaborado por: El Autor.

***Resultados de la máquina virtual Windows***

Al momento de ingresar al administrador de tareas, se muestra el siguiente mensaje: "El administrador ha deshabilitado el administrador de tareas", dejando sin acceso al usuario.

**Figura 32**

*Administrador de tareas*

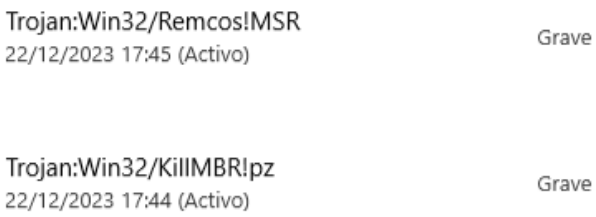



*Nota.* Bloqueo de acceso al administrador de tareas. Elaborado por: El Autor.

Se ingresa a la parte de seguridad para verificar el nivel de gravedad del virus.

**Figura 33**

*Estado del virus*

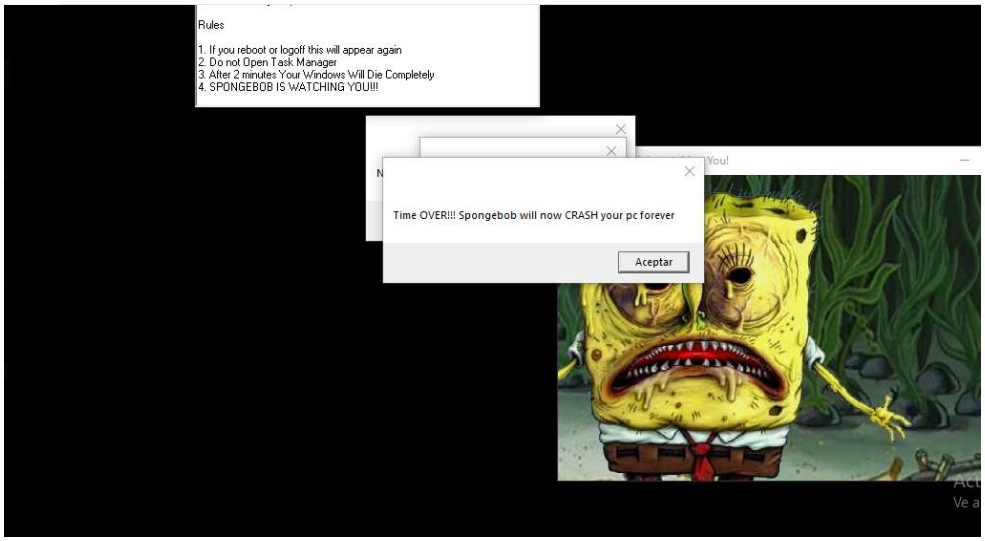



*Nota.* En esta imagen se puede evidenciar que el virus es de tipo troyano y el estado es grave. Elaborado por: El Autor.

Una vez transcurrido el minuto, el escritorio deja de funcionar y toma el siguiente aspecto.

**Figura 34**

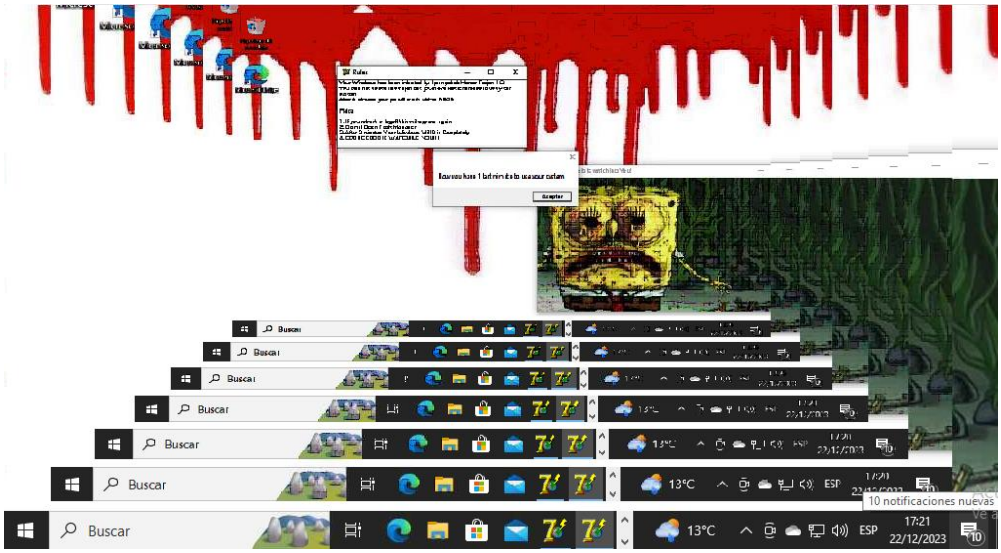
*Primer aspecto una vez ejecutado el virus*




*Nota.* En esta imagen se puede evidenciar como deja de funcionar todo el sistema y entra en estado de colapso. Elaborado por: El Autor.

**Figura 35**

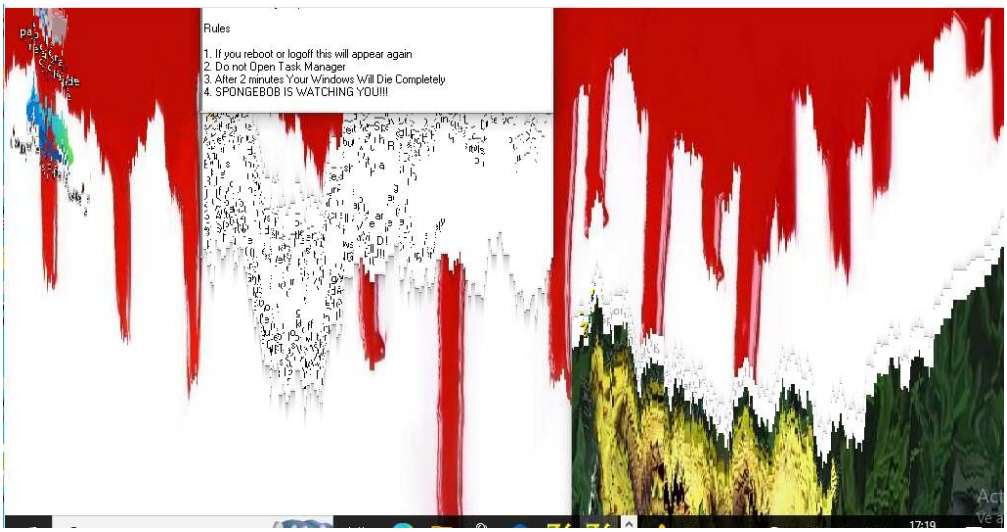
*Segundo aspecto*




*Nota.* En esta imagen se puede evidenciar como deja de funcionar todo el sistema y entra en estado de colapso. Elaborado por: El Autor.

**Figura 36**

*Tercer aspecto*

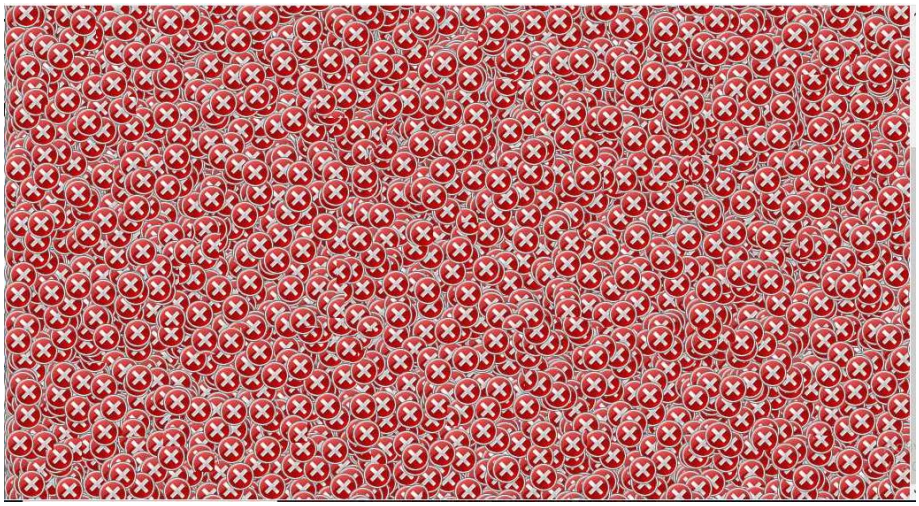



*Nota.* En esta imagen se puede evidenciar como deja de funcionar todo el sistema y entra en estado de colapso. Elaborado por: El Autor.

Finalmente la máquina objetivo queda obsoleta, lo que significa el ataque se realizó con éxito y el usuario ya no tiene control sobre su máquina.

**Figura 37**

*Máquina obsoleta*



*Nota.* En esta imagen se puede evidenciar como la máquina objetivo ha colapsado. Elaborado por: El Autor.

**Análisis de resultados sobre las máquinas virtuales**

Cabe mencionar que este trabajo de titulación se lo realizó con fines educativos para obtener más información sobre las máquinas virtuales y el nivel de control que pueden tener los estudiantes, docentes y personal a cargo del Data Center.

Para analizar los resultados con respecto a la máquina de Ubuntu se puede mencionar que, la seguridad en Ubuntu es considerablemente mejor que en Windows ya que fue un poco complicada poder atacar sin que rechace la conexión por parte de la máquina objetivo, para eso se realizó tomando en cuenta a los estudiantes al momento de obtener su máquina virtual, instalando y habilitando los puertos 21, 22 y 80.

Con la ayuda de Kali Linux que es un entorno especializado en la seguridad informática y pruebas de penetración (pentesting), se procede a realizar un barrido con nmap y la IP para obtener información sobre los puertos abiertos. Una vez realizado el análisis se recopila la información sobre posibles vulnerabilidades o ataques que se podrían generar a la máquina objetivo, con Metasploit se puede realizar la explotación y post explotación, en este caso se

obtuvo una respuesta favorable mediante el puerto 21, lo que permitió el ingreso a la máquina objetivo y se obtuvo toda la información que el atacante desea sin que se dé cuenta el usuario.

Lo que hace este tipo de exploit, es explotar la máquina objetivo mediante una puerta trasera maliciosa donde se encuentra en el archivo de ProFTPD, dando paso al atacante a tener todos los privilegios.

Otra forma de ataque que se realizó fue al puerto 22, utilizando el ataque de fuerza bruta mediante hydra que es una herramienta de pruebas de penetración (pentesting) y hacking ético diseñada para hacer ataques de fuerza bruta. Un ataque de fuerza bruta permite obtener todas las combinaciones posibles de contraseñas hasta encontrar la correcta, en este caso, se encontró de manera inmediata las credenciales de la máquina objetivo y una vez que se obtuvo se procedió a realizar un acceso normal a través de SSH, se ingresa la contraseña y se obtiene total acceso a la máquina, incluso puede cambiarse a usuario root.

Con respecto a Windows, como ya se mencionó con anterioridad en la parte de “resultados de la máquina virtual Windows”, mediante Gmail se envió un correo a la persona objetivo en este caso se creó un correo falso para realizar las pruebas pertinentes, en donde la persona objetivo ejecuta el programa y acepta los cambios en el dispositivo. En el cual, deja sin acceso al administrador de tareas y en un minuto el sistema deja de funcionar. Lo que provoca este virus al momento de su descarga es desactivar Windows Defender lo que provoca que sea más sencillo la propagación del virus.

Con respecto a la seguridad, Windows al ser el sistema operativo más utilizado por los usuarios a nivel mundial es blanco de mayores ataques cibernéticos, de igual manera las configuraciones por defecto no son tan seguros lo que ayuda a los atacantes a tener mayor éxito en realizar los ataques, y lo más importante que hay que destacar es que Windows ha sido más

vulnerable a malware, como virus con la finalidad de propagarse por el sistema operativo y causar daños en los archivos, como es el caso del virus Bob Esponja.

La seguridad de Linux al ser de código abierto puede ser un poco más estable debido a que se puede identificar y corregir rápidamente, la mayoría de las distribuciones viene con políticas de seguridad preconfiguradas al igual que las aplicaciones, esto no quiere decir que totalmente sea seguro, pero si brinda mayor enfoque en salvaguardar un poco más la seguridad del usuario. Linux ha recibido menos ataques de malware, pero a medida que va tomando popularidad y más usuarios hacen uso de este sistema operativo podría ser blanco de ataques por malware.

Otro propósito que se tiene en este proyecto técnico, es verificar si al momento de vulnerar una máquina el virus se propaga en otras máquinas, este no fue el caso ya que se probó de diferentes maneras a las máquinas y la máquina objetivo Ubuntu no influyó en la máquina objetivo Windows y viceversa, como ya se mencionó con anterioridad estas pruebas se realizaron en un ambiente controlado y aislado, esto con la finalidad de evitar afectar la integridad de las máquinas virtuales en uso por estudiantes y docentes de la Universidad Politécnica Salesiana.

Finalmente, no existe un sistema operativo totalmente seguro, se debe tener en cuenta que el usuario debe estar al tanto de la seguridad de su computador y dar el mantenimiento respectivo, ya sea parches de seguridad cuando sea necesario, actualizaciones de seguridad disponibles para el sistema específico, el usuario debe gestionar y configurar correctamente y bajo su responsabilidad el uso que dé al sistema operativo.

# CAPÍTULO IV

## CONCLUSIONES

Se concluye que, el tener máquinas virtuales se les debe dar el mismo mantenimiento y seguridad que una máquina física, ya que últimamente ha incrementado los ataques, lo que puede provocar la pérdida de información si no se realiza una copia de seguridad, incluso teniendo una copia puede sufrir pérdida de información.

Mediante las máquinas virtuales se determinó que se ha permitido crear entornos aislados y controlados para llevar a cabo pruebas de penetración sin comprometer el estado del Data Center con respecto a su seguridad, con la finalidad de evitar riesgos que comprometan los diferentes sistemas operativos y la información de los estudiantes y docentes que hagan uso de las máquinas.

Con las máquinas virtuales se concluye que se puede crear todo un entorno para emular o replicar escenarios de ataques para mejorar la seguridad en los entornos reales.

Se determinó que, se puede tener varios backups de las máquinas virtuales, con el propósito de, si existe un daño o se está realizando alguna experimentación y sufre algún daño la máquina virtual principal, se puede continuar con los backups generados.

Para realizar pruebas de penetración se concluye que se debe tener un aprendizaje ético siguiendo las leyes y políticas que se encuentren bajo los estatutos de las empresas, con el objetivo de tener un entorno controlado que no ponga en riesgo la información sensible.

Finalmente, mediante la investigación realizada se determinó que si existe una ataque a ESXi puede provocar la suspensión de los servicios ya que los servidores dejan de operar, lo cual provocaría la disminución del tiempo de prestación de servicios hasta la pérdida de información que se haya generado en ese lapso de tiempo, o a su vez si la máquina no posee un backup la

pérdida absoluta de dicha información. Adicional, se pudo apreciar que al tener máquinas virtuales no existiría contaminación fuera de la máquina virtual mientras estas se encuentren en diferentes segmentos de red.

## RECOMENDACIONES

Actualizar ZKACCESS a las versiones más recientes ya que podría ser blanco de ataque, si llegara a realizarse el ataque a los biométricos se podrían bloquear y no tendrían acceso a los laboratorios los docentes y personal administrativo. Otra consecuencia se podría dar que personas no autorizadas ingresen a las áreas restringidas como el NOC poniendo en peligro la seguridad de la información tanto de estudiantes, docentes como el departamento del Data Center, ya que un biométrico tiene como finalidad garantizar la seguridad y el acceso autorizado.

Como se utiliza RDP para acceder remotamente se recomienda tener contraseñas fuertes y cambiar cada cierto tiempo, se debe recordar que dependiendo de la cantidad de caracteres es la duración de las contraseñas, además se debería cambiar el puerto por defecto ya que los ataques con mayor continuidad es a ese puerto.

Al ser Windows el mayor blanco de ataque por medio de malware y al demorarse en mitigar los ataques, se recomienda que las máquinas virtuales tanto para estudiantes como docentes sea en el sistema operativo Linux (Ubuntu), ya que tiene mayor seguridad y evitaría que el Data Center sea posiblemente expuesto a estos ataques por malware.

Durante el 2023, ha existido varios ataques al navegador Chrome, de hecho, es el navegador que ha tenido más ataques de Zero Day lo que puede provocar que el atacante pueda realizar un BufferOverflow y obtener ejecución remota de comandos en el sistema, el total de vulnerabilidades que se han detectado es de 26447, por lo cual se recomienda bloquear este navegador como lo está el navegador Opera.

Realizar auditorías de seguridad periódicas para identificar posibles vulnerabilidades y realizar un monitoreo continuo para detectar actividades sospechosas, con el objetivo de identificar las

vulnerabilidades que posee el hipervisor ya que por medio del mismo podrían averiar el sistema principal afectando la disponibilidad.

## REFERENCIAS


Acronis. (24 de Junio de 2021). *Qué es la prevención de pérdida de datos?* Obtenido de ACRONIS: https://www.acronis.com/es-mx/blog/posts/data-loss-prevention/

Adamgalway. (2020, Mayo 1). *msfdb: Database Features & How to Set up a Database for Metasploit*. GitHub. https://github.com/rapid7/metasploit-framework/wiki/msfdb:-Database-Features-&-How-to-Set-up-a-Database-for-Metasploit/2a66094517649eff8ca8819951d0e2659d9b57b2

Adastra. (5 de Marzo de 2013). *WEB HACKING – Vulnerabilidades en XAMPP – Parte XXII*. Obtenido de The Hacker Way: https://thehackerway.com/2013/03/05/web-hacking-vulnerabilidades-en-xampp-parte-xxi/

Alemán, H., & Rodríguez, C. (s.f.). *Metodologías Para el Análisis de Riesgos en los SGSi*. Obtenido de Hemeroteca: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Android Devolopers. (s.f.). *Sugerencias de seguridad*. Obtenido de Android: https://developer.android.com/training/articles/security-tips?hl=es-419

Arias, A. (8 de Agosto de 2023). *Pruebas de Penetración: qué son y qué saber sobre ellas*. Obtenido de Tokio: https://www.tokioschool.com/noticias/pruebas-penetracion/

Armstrong, B., Ross, E., Coulter, D., Poggemeyer, L., & dknappettmsft. (3 de Agosto de 2023). *Información general sobre la tecnología Hyper-V*. Obtenido de Microsoft Learn: https://learn.microsoft.com/es-es/windows-server/virtualization/hyper-v/hyper-v-technology-overview

Avenía, C. (Noviembre de 2017). *Fundamentos de seguridad*. Obtenido de Fundación Universitaria del Área Andina: https://core.ac.uk/download/pdf/326424171.pdf

AWS. (s.f.). *¿Qué es una KVM? - Explicación sobre las máquinas virtuales basadas en el Kernel - AWS*. Obtenido de Amazon Web Services, Inc: https://aws.amazon.com/es/what-is/kvm/

AWS. (s.f.). *Información general sobre el almacenamiento en caché*. Obtenido de AWS: https://aws.amazon.com/es/caching/

Barionuevo, M., Apolloni, A., & Piccoli, F. (Octubre de 2009). *El Planificador de Procesos a trav´es de.* Obtenido de SEDICI: http://sedici.unlp.edu.ar/bitstream/handle/10915/20945/Documento_completo.pdf?sequence=1&isAllowed=y

Biblioguias: Biblioteca de la CEPAL. (s.f.). *Gestión de datos de investigación: Protección de los datos*. Obtenido de CEPAL: https://biblioguias.cepal.org/c.php?g=495473&p=4398118

Böhme, R., & Félegyházi, M. (2010). Optimal Information Security Investment with Penetration Testing. *Springer Link*. Obtenido de https://bibliotecas.ups.edu.ec:3401/chapter/10.1007/978-3-642-17197-0_2

Breixo, G. (13 de Febrero de 2021). *¿Qué es el núcleo de un procesador?* Obtenido de Profesional Review: https://www.profesionalreview.com/2021/02/13/nucleo-procesador/

buzonuv@uv.mx. (20 de Enero de 2016). *Conocimientos generales: ¿Qué hay de la seguridad de la información en ambientes virtualizados?* Obtenido de Universidad Veracruzana: https://www.uv.mx/infosegura/general/conocimientos_seguridad-4/

Caballero, J. (2013, Octubre 21). *Armitage: Administrador gráfico de metasploit - Hacking Ético*. Hacking Ético. https://hacking-etico.com/2013/10/21/armitage/

Caballero, A. (2018, Septiembre 4). (*Fundamentos de Metasploit Framework para la Explotación | Alonso Caballero / ReYDeS*. https://www.reydes.com/d/?q=Fundamentos_de_Metasploit_Framework_para_la_Explotacion

Chema, A. (2017, Enero 18). *Cómo buscar exploits automáticamente para elevar privilegios en GNU/Linux #Linux #Pentesting*. https://www.elladodelmal.com/2017/01/como-buscar-exploits-automaticamente.html

Ciberseguridad, C. N. (20 de Noviembre de 2020). *VULNERABILIDADES EN POSTGRESQL*. Obtenido de CNCS: https://cncs.gob.do/vulnerabilidades-en-postgresql/

Ciberseg. (2021, Diciembre 13). *¿Qué es Metasploit Framework y cómo funciona?* Ciberseguridad. https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Cloudfare. (s.f.). *¿Cuáles son los riesgos de seguridad del RDP? | Vulnerabilidades del RDP*. Obtenido de Cloudflare: https://www.cloudflare.com/es-es/learning/access-management/rdp-security-risks/

Consultores, E. H. (25 de Julio de 2023). *La nueva vulnerabilidad de OpenSSH expone los sistemas Linux a la inyección de comandos remotos*. Obtenido de Linkedin: https://es.linkedin.com/pulse/la-nueva-vulnerabilidad-de-openssh-expone-los-sistemas-linux

CSIRT, E. (20 de Septiembre de 2023). *Varias vulnerabilidades afectan al navegador Microsoft Edge (basado en Chromium)*. Obtenido de TELCONET: https://csirt.telconet.net/comunicacion/noticias-seguridad/varias-vulnerabilidades-afectan-al-navegador-microsoft-edge/

CSIRT, T. (22 de Agosto de 2023). *PoC para vulnerabilidad en Microsoft Windows*. Obtenido de TELCONET: https://csirt.telconet.net/comunicacion/noticias-seguridad/poc-para-vulnerabilidad-en-microsoft-windows/

CVE. (2023). *Common Vulnerabilities and Exposures*. Obtenido de https://cve.mitre.org/

CVE details. (2023). *Anydesk : Security Vulnerabilities Published In 2023*. Obtenido de CVE details: https://www.cvedetails.com/vulnerability-list/vendor_id-16953/Anydesk.html?page=1&year=2023&month=-1&order=1&trc=10&sha=5669a2027638e99c15f578fc7df4bf316a1d0b5b

Conzultek. (s.f.). *Conozca los tipos de virtualización y sus funciones*. https://blog.conzultek.com/productividad/conoce-los-tipos-de-virtualizacion-y-sus-funciones

Cyber Zaintza. (2 de Agosto de 2023). *Vulnerabilidades en Mozilla Firefox, Firefox ESR y Thunderbird*. Obtenido de Cyber Zaintza: https://www.ciberseguridad.eus/ultima-hora/vulnerabilidades-en-mozilla-firefox-firefox-esr-y-thunderbird

Delavy, E. (7 de Octubre de 2019). *Whois: conheça o protocolo de informações de domínios*. Obtenido de HostGator: https://www.hostgator.com.br/blog/o-que-e-whois/

Dell. (s.f.). *Sistemas de almacenamiento de Dell EMC Guía del producto de la función de nodo metro de PowerStore y Unity XT*. Obtenido de Dell Puerto Rico: https://www.dell.com/support/manuals/es-pr/dell-emc-metro-node/vplex_pub_product_guide/n%C3%BAmero-de-unidad-l%C3%B3gica-lun?guid=guid-bfbafbe3-cc91-42c2-92b3-3bc3c5fd258c&lang=es-mx#:~:text=Almacenamiento%20virtual%20al%20que%20se,se%20conectan%20a%20una

Drew. (25 de Noviembre de 2022). *¿Qué es la gestión de incidencias?* Obtenido de Drew: https://blog.wearedrew.co/concepts/que-es-la-gestion-de-incidencias

Entelgy. (14 de Julio de 2022). *Vulnerabilidades en productos Adobe*. Obtenido de Entelgy: https://www.entelgy.com/en/divisions/innotec-security/news-innotec-security/vulnerabilities/vulnerabilities-innotec-security/vulnerabilidades/vulnerabilidades-en-productos-adobe-202207141431

Férnandez, Y. (12 de Enero de 2023). *HDD vs SSD: diferencias y ventajas de ambos tipos de disco duro*. Obtenido de Xataka: https://www.xataka.com/basics/hdd-vs-ssd

FREMM. (s.f.). *¿Qué es la evaluación de riesgos y cómo los evaluamos?* Obtenido de FREMM: http://www.fremm.es/riesgoslaborales/autonomos/que_es_la_evaluacion.html

GEEKNETIC. (s.f.). *GEEKNETIC*. Obtenido de https://www.geeknetic.es/Hyperthreading/que-es-y-para-que-sirve#:~:text=A%20medida%20que%20se%20aumenta,muchos%20%C3%A1mbitos%20como%20los%20servidores.

Ghimiray. (19 de Enero de 2022). *Intel i5 o Intel i7: ¿qué procesador de Intel es el más adecuado para su equipo?* Obtenido de AVG: https://www.avg.com/es/signal/intel-i5-vs-i7

Gr, R. (10 de Febrero de 2023). *Qué es la GPU en un ordenador y por qué es importante*. Obtenido de ADSLZone: https://www.adslzone.net/esenciales/preguntas/que-es-gpu/

Gr, R. (10 de Febrero de 2023). *Qué es la GPU en un ordenador y por qué es importante*. Obtenido de ADSLZone: https://www.adslzone.net/esenciales/preguntas/que-es-gpu/

Hewlett Packard Enterprise. (2021, Enero 13). *HPE ProLiant XL230A Gen9 Server - Overview*.

https://support.hpe.com/hpesc/public/docDisplay?docId=c04483652&docLocale=en_US

Hewlett Packard Enterprise Development España. (s.f.). *¿Qué es el almacenamiento de datos?* Obtenido de Hewlett Packard Enterprise: https://www.hpe.com/es/es/what-is/data-storage.html

Hispasec. (15 de Mayo de 2006). *Grave vulnerabilidad en RealVNC*. Obtenido de UAD: https://unaaldia.hispasec.com/2006/05/grave-vulnerabilidad-en-realvnc.html

Hispasec. (28 de Septiembre de 2023). *Google responde a la explotación de una vulnerabilidad zero-day en Chrome*. Obtenido de UAD: https://unaaldia.hispasec.com/2023/09/google-responde-a-la-explotacion-de-una-vulnerabilidad-zero-day-en-chrome.html

*HPE ProLiant XL190R Gen10 Server*. (s.f.). PSNow. https://www.hpe.com/psnow/doc/a00022817enw

*HPE ProLiant XL250A Gen9 Server*. (s.f.). PSNow. https://www.hpe.com/psnow/doc/c04447895?jumpid=in_lit-psnow-red

*HPE ProLiant XL190R Gen10 Server*. (s.f.). PSNow. https://www.hpe.com/psnow/doc/a00022817enw

Jacky. (25 de Octubre de 2023). *What is Metasploit? The Penetration Testing Framework*. Obtenido de Sapphire: https://www.sapphire.net/cybersecurity/metasploit/

Kaspersky daily. (s.f.). *Vulnerabilidades en sistemas VNC de acceso remoto*. Obtenido de Kaspersky : https://www.kaspersky.es/blog/vnc-vulnerabilities/20680/

KeepCoding, R. (22 de Diciembre de 2022). *¿Qué es CVE Details?* Obtenido de KeepCoding Bootcamps. KeepCoding Bootcamps: https://keepcoding.io/blog/que-es-cve-details-ciberseguridad/

Lakshmanan, R. (25 de Enero de 2023). *VMware Releases Patches for Critical vRealize Log Insight Software Vulnerabilities*. Obtenido de The Hacker News Logo: https://thehackernews.com/2023/01/vmware-releases-patches-for-critical.html?m=1

López, J. (5 de Octubre de 2022). *Seguro que sabes lo que es una tarjeta gráfica, pero ¿qué es una GPU?* Obtenido de HardZone: https://hardzone.es/reportajes/que-es/gpu-caracteristicas-especificaciones/

M. (s.f.). *¿Qué es el almacenamiento iSCSI y cómo crear una SAN iSCSI?* Obtenido de Comunidad FS: https://community.fs.com/es/article/iscsi-storage-basics-plan-iscsi-san.html

Mehta, P. (1 de Abril de 2022). *Prueba de penetración (pen test)*. Obtenido de ComputerWeekly: https://www.computerweekly.com/es/definicion/Prueba-de-penetracion-pen-test

Microsoft. (s.f.). *MS15-082: Vulnerabilidades en RDP podrían permitir la ejecución remota de código: 11 de agosto de 2015*. Obtenido de Microsoft: https://support.microsoft.com/es-es/topic/ms15-082-vulnerabilidades-en-rdp-podr%C3%ADan-permitir-la-ejecuci%C3%B3n-remota-de-c%C3%B3digo-11-de-agosto-de-2015-1ffe98f4-6797-7e57-3321-7a039b4f1731

Navas, M. Á. (8 de Abril de 2018). *Tipos y velocidades de procesadores*. Obtenido de Profesional Review: https://www.profesionalreview.com/2018/04/08/tipos-velocidades-procesadores/

NIST. (s.f.). *NVD - CVE-2021-21974*. Obtenido de NIST: https://nvd.nist.gov/vuln/detail/CVE-2021-21974

Paredes, Ciberseguridad, M. (2022, Junio 28). *¿Pentest o Análisis de vulnerabilidades?* https://es.linkedin.com/pulse/pentest-o-an%C3%A1lisis-de-vulnerabilidades-paredes-ciberseguridad

Pollack, K. (16 de Noviembre de 2021). *LAS 10 PRINCIPALES VULNERABILIDADES DE WINDOWS SERVER EN 2021*. Obtenido de CalCom: https://www.calcomsoftware.com/las-10-principales-vulnerabilidades-de-windows-server-en-2021/#1472

PowerData. (s.f.). *Metadatos, definición y características*. Obtenido de https://www.powerdata.es/metadatos

*Redes virtuales*. (2020, April 27). VMware. https://www.vmware.com/es/topics/glossary/content/virtual-networking.html

Ros. (19 de Marzo de 2019). *Memoria caché: qué es y qué diferencias hay entre los tipos L1, L2 y L3*. Obtenido de MC: https://www.muycomputer.com/2019/03/19/memoria-cache-que-es-y-que-diferencias-hay-entre-los-tipos-l1-l2-y-l3/

Safety Culture. (19 de Junio de 2023). *¿Qué es una evaluación de riesgos de seguridad?* Obtenido de Safety Culture: https://safetyculture.com/es/temas/analisis-de-riesgo-en-seguridad/

Santos, J. (22 de Agosto de 2023). *¿Qué es el Pentesting? Tipos y cómo utilizarlo para prevenir ciberataques*. Obtenido de Delta Protect: https://www.deltaprotect.com/blog/que-es-pentesting#:~:text=Existen%20tres%20tipos%20de%20pruebas,encontrar%20vulnerabilidades%20en%20la%20seguridad

Soporte Técnico de Microsoft. (11 de Enero de 2022). *Descripción de la actualización de seguridad para Office 2016: 11 de enero de 2022 (KB5002052)*. Obtenido de Microsoft: https://support.microsoft.com/es-es/topic/descripci%C3%B3n-de-la-

actualizaci%C3%B3n-de-seguridad-para-office-2016-11-de-enero-de-2022-kb5002052-d5dafa42-2f6a-4122-9e95-d6168b4bf345

Tapia, D. (21 de Julio de 2021). *¿Qué es el FOOTPRINTING?* Obtenido de Atalanta: https://atalantago.com/footprinting/

Tecnología Intel® Hyper-Threading. (s.f.). Obtenido de INTEL: https://www.intel.la/content/www/xl/es/architecture-and-technology/hyper-threading/hyper-threading-technology.html

Tokio School . (10 de Agosto de 2022). *¿Que es una vulnerabilidad en Java y cómo encontrarla en tu código?* Obtenido de Tokio: https://www.tokioschool.com/noticias/vulnerabilidad-java/

Universidad Politécnica Salesiana. (23 de Marzo de 2022). *Política de seguridad de la información.* Obtenido de Universidad Politécnica Salesiana: https://www.ups.edu.ec/documents/20121/258112/Pol%C3%ADtica+de+Seguridad+de+la+Informaci%C3%B3n.pdf

Valk, J. d. (2 de Mayo de 2023). *The ultimate guide to robots.txt*. Obtenido de Yoast: https://yoast.com/ultimate-guide-robots-txt/

VMware. (22 de Junio de 2023). *VMSA-2023-0014*. Obtenido de VMware: https://www.vmware.com/security/advisories/VMSA-2023-0014.html

VMware, I. (25 de Agosto de 2020). *Hipervisor*. Obtenido de VMware: https://www.vmware.com/es/topics/glossary/content/hypervisor.html

Zola, A. (2023, Noviembre 2021). *footprinting*. Obtenido de TechTarget: https://www.techtarget.com/searchsecurity/definition/footprinting