



**UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL  
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO  
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES**

**TEMA:  
Estudio de las Threats Tools y la Ciberseguridad en las  
empresas.**

**AUTOR:  
Borja Hernández, Donald Stefano**

**Trabajo de Integración Curricular previo a la obtención del título de  
INGENIERO EN TELECOMUNICACIONES**

**TUTOR:  
Ing. Efraín Oswaldo Suarez Murillo, MGs**

**Guayaquil, Ecuador  
06 de septiembre del 2023**



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO**  
**CARRERA DE INGENIERÍA EN TELECOMUNICACIONES**

**CERTIFICACIÓN**

Certificamos que el presente trabajo fue realizado en su totalidad por **Borja Hernández, Donald Stefano** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR:

---

**Ing. Efraín Oswaldo, Suarez Murillo, MGs**

DIRECTOR DE CARRERA

---

**M. Sc. Bohórquez Escobar, Celso Bayardo**

Guayaquil, a los 06 día del mes de septiembre del año 2023



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO  
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES**

**DECLARACIÓN DE RESPONSABILIDAD**

Yo, **Borja Hernández, Donald Stefano**

**DECLARO QUE:**

El trabajo de titulación **Estudio de las Threats Tools y la Ciberseguridad en las empresas**, previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

**Guayaquil, a los 06 día del mes de septiembre del año 2023**

**Borja Hernández, Donald Stefano**



UNIVERSIDAD CATÓLICA  
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO  
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES**

### **AUTORIZACIÓN**


Yo, **Borja Hernández, Donald Stefano**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **Estudio de las Threats Tools y la Ciberseguridad en las empresas**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

**Guayaquil, a los 06 día del mes de septiembre del año 2023**

**Borja Hernández, Donald Stefano**

## INFORME SOFTWARE ANTIPLAGIO REPORTE COMPILATIO

 CERTIFICADO DE ANÁLISIS  
major

TESIS TRABAJO FINAL DONALD BORJA

4%  
Coincidencias

0  
Textos entre comillas  
17% coincidentes con la base de datos

24  
Libros no reconocidos

Nombre del documento: TESIS TRABAJO FINAL DONALD BORJA.doc  
ID del documento: 674821e1215e83a28e1e010330910ef6e301  
Tamaño del documento original: 12,1 KB

Depositar: Efraim Oswaldo Suarez Murillo  
Fecha de depósito: 08/05/21  
Tipo de carga: Interfaz  
Fecha de fin de análisis: 08/05/21

Número de palabras: 14.782  
Número de caracteres: 88.419



---

ING. EFRAIN OSWALDO SUAREZ MURILLO  
Revisor - COMPILATIO

Reporte Compilatio del trabajo de titulación de la Carrera de Ingeniería en Telecomunicaciones: **Estudio de las Threats Tools y la Ciberseguridad en las empresas**, del estudiante **Borja Hernández, Donald Stefano** se encuentra al 4 % de coincidencias.

## **DEDICATORIA**

A mis hermanas Fanny y Haydee, quienes con amor me salvaron cuando era aún un niño con pocos años de vida. A mis padres, que con perseverancia y esfuerzo me ayudaron a seguir este camino hasta el final, y dejarme llegar a cumplir con una meta de vida que no solo es un cierre sino un inicio. A mi mejor amigo que siempre me ayudo y brindo todo su apoyo a lo largo de todo este tiempo, y en general a todas las personas que me brindaron su apoyo e hicieron posible esto.

**EL AUTOR**

**BORJA HERNADEZ, DONALD STEFANO**

## **AGRADECIMIENTOS**

Le agradecer a Dios por crear las ciencias y permitirme obtener esta sabiduría y darme la fuerza necesaria para poder obtenerla. A mi familia por darme su apoyo y paciencia, también les agradezco a mis profesores de vida el Señor Alfredo Cuentas Ramos, la Señora María Daniela Rivera Molestina que me nutrieron en temas laborales, morales e intelectuales. A mis amigos, compañeros de trabajo y docentes por su ayuda y sugerencias durante todo este tiempo.

EL AUTOR

BORJA HERNANDEZ, DONALD STEFANO

## INDICE GENERAL

INDICE GENERAL.....	VIII
ÍNDICE DE FIGURAS.....	X
RESUMEN.....	XI
ABSTRACT.....	XII
Capítulo 1: Descripción general de trabajo de titulación .....	2
1.1.    Introducción.....	2
1.2.    Antecedentes.....	2
1.3.    Definición del Problema.....	4
1.4.    Justificación y alcance.....	5
1.5.    Objetivos del Problema de Investigación.....	5
1.5.1  Objetivo General.....	5
1.5.2  Objetivo Específico.....	6
1.6.    Hipótesis.....	6
1.7.    Metodología de Investigación.....	6
Capítulo 2: Fundamentación teórica.....	7
2.1  Ciberseguridad.....	7
2.1.1  Ventajas de la Ciberseguridad.....	9
2.1.2  Desventajas de la Ciberseguridad.....	10
2.2  Herramientas contra amenazas.....	11
2.3  Tecnologías del uso de Herramientas contra amenazas.....	13
2.3.1  Tecnologías del uso de ciberseguridad.....	13
2.3.1.1  Entorno basado en IA.....	13
2.3.1.2  Entorno basado en humanos.....	14
2.3.1.3  Entorno Híbrido.....	14
2.3.1.4  Área de sistemas.....	14
2.4  Fundamentos y Técnicas de las Herramientas contra amenazas...	14
2.4.1  Caza de amenazas.....	17
2.4.2  Conciencia y Formación en Ciberseguridad.....	18
2.5  Hacking Ético.....	20
2.5.1  Sombrero Blanco.....	21
2.5.2  Sombrero Gris.....	22
2.5.3  Sombrero Negro.....	24
2.6  Equipo Azul, Rojo y Purpura en Hacking Ético.....	25
2.6.1  Equipo Azul.....	26
2.6.2  Equipo Rojo.....	27
2.6.3  Equipo Purpura.....	28
2.7  Virus Computacionales.....	30
2.7.1  Tipos de virus.....	31
2.8  Encriptado de Datos.....	33
2.8.1  Encriptado por Ransomware.....	35
2.9  Virus de Computadora Históricas.....	36
2.9.1  Mydoom.....	37
2.9.2  Sobig.....	37
2.9.3  Klez.....	37
2.9.4  ILOVEYOU.....	38
2.9.5  WannaCry.....	38



Capítulo 3: Instalación y Programación .....	40
3.1 Características del Equipo.....	40
3.1.1 Máquina Virtual Kali Linux.....	40
3.1.2 Instalación y Configuración de Kali Linux.....	42
3.1.3 Inicio de máquina virtual.....	44
3.1.4 Uso de los núcleos del equipo.....	45
3.1.5 Almacenamiento.....	46
3.1.6 Configuración de Red.....	47
3.2 Parrot aplicación de pruebas de infiltración.....	48
3.2.1 Instalación Parrot Security.....	48
3.2.3 Instalación de Parrot en Máquina Virtual.....	49
3.2.4 Configuración del Parrot en Virtual Box.....	50
Capítulo 4: Metodología y estudios del proyecto .....	54
4.1 Metodología analítica explicativa.....	54
4.2 Características del área de estudio.....	54
<b>4.3 Cálculos de costo de cursos de ciberseguridad.....</b>	<b>56</b>
<b>4.3.1 Certificación CISSP.....</b>	<b>57</b>
<b>4.3.2 Certificado CISA.....</b>	<b>58</b>
4.3.3 Certificado Security+.....	59
4.3.4 Certificado CEH.....	60
4.3.5 Certificación CISM.....	61
4.3.6 GSEC.....	61
4.3.7 Certificación SSCP.....	62
4.3.8 Certificación CASP.....	63
4.3.9 Certificado GCIH.....	64
<b>4.3.10 Certificación OSCP.....</b>	<b>65</b>
4.5 Referencias de Presupuesto.....	66
<b>CONCLUSIONES Y RECOMENDACIONES .....</b>	<b>67</b>
Conclusiones.....	67
<b>Recomendaciones.....</b>	<b>68</b>
Bibliografía.....	69

## ÍNDICE DE FIGURAS

Figura 2. 1 Mapa de Cursos y Habilidades en Ciberseguridad .....	8
Figura 2. 2 Arquitectura de seguridad multicapa de defensa en profundidad. ....	17
Figura 2.3 El impacto de la caza de amenazas en sus operaciones de seguridad .18	
Figura 2. 4 Las 7 Tácticas Defensivas y Procesos.....	20
Figura 2. 5 Interconexión entre los equipos de hacking ético.....	26
Figura 2. 6 Operación de proceso de ataque y defensa.....	27
Figura 2. 7 Cualidades de cada equipo.....	29
Figura 2. 8 Diagrama del cambio de equipos.....	30
Figura 3. 1 página de descarga.....	40
Figura 3. 2 Kali Linux 2023 de 10G.....	41
Figura 3. 3 Aplicación Máquina Virtual Kali Linux.....	42
Figura 3. 4 Ventana de configuración de Máquina virtual.....	43
Figura 3. 5 Selección de disco duro para la máquina virtual .....	43
Figura 3. 6 Ventana principal de la máquina virtual .....	45
Figura 3. 7 Ventanda de Selección de nucleos.....	46
Figura 3. 8 Ventana de Almacenamiento .....	47
Figura 3. 9 Ventana de Red .....	48
Figura 3. 10 Aplicación Parrot Security .....	49
Figura 3. 11 Ampliación Parrot en ISO .....	49
Figura 3. 12 Versión Security Edition Parrot.....	50
Figura 3. 13 Parrot en Máquina Virtual Funcionando.....	50
Figura 3. 14 Parrot en Máquina Virtual Instalador Grafico.....	51
Figura 3. 15 Panel de Control del Parrot.....	51
Figura 3. 16 Ventana de Selección de Región.....	52
Figura 3. 17 Ventana de Selección de idioma del teclado .....	52
Figura 3. 18 Ventada de Creación de User y Password.....	52
Figura 3. 19 Ventana final de descarga de controladores y herramientas .....	53
Figura 3. 20 Finalización de instalación .....	53

## RESUMEN

En este proyecto de investigación tiene como punto principal dar a demostrar la importancia que tienen los conocimientos de las herramientas de amenazas cibernéticas y de la ciber-seguridad que nos rodea en la actualidad, esta investigación no solo busca mostrarles el amplio abanico que existe en las amenazas cibernéticas, sino como se podrían prevenir si se usaran las herramientas adecuadas para encontrar las fallas tanto humanas como de los software y hardware que se emplean en este ambiente, otro de los puntos a exponer son de los Virus computacionales más usados que han amenazado a la sociedad computacional a lo largo de los años tanto nuevos como los más viejos, también vamos a centrarnos en las vulnerabilidades que tiene los Switcher, Router's y otros equipos electrónicos en general que usen puertos de conexión Ethernet, Bluetooth, Infrarrojo, USB de todos los tipos, conexiones LAN, entre otras. Se utilizará información de ataques que han ocurrido en tiempo real, también demostraremos mediante esquemas cómo funcionan los ataques. Al concluir se dará una explicación de por qué es importante invertir en un área especializada en la protección de datos cibernéticos en la compañía.

**Palabras claves: Ciberseguridad, Virus Computacionales, Vulnerabilidades.**

## **ABSTRACT**

In this research project has as main point to demonstrate the importance of knowledge of cyber threats and cybersecurity tools that surrounds us today, this research not only seeks to show the wide range that exists in cyber threats, but how they could be prevented if you use the right tools to find both human failures and software and hardware that are used in this environment, Another of the points to expose are the most used computer viruses that have threatened the computer society over the years both new and older, we will also focus on the vulnerabilities that have the Switcher, Router's and other electronic equipment in general that use Ethernet connection ports, Bluetooth, Infrared, USB of all types, LAN connections, among others. We will use information of attacks that have occurred in real time, we will also demonstrate through diagrams how the attacks work. At the end, an explanation will be given as to why it is important to invest in an area specialized in the protection of cyber data in the company.

**Keywords:**     **Cybersecurity, Computer Viruses, Vulnerabilities**

# **Capítulo 1:**

## **Descripción general de trabajo de titulación**

### **1.1. Introducción.**

La ciberseguridad en el mundo interconectado actual, en el que la tecnología desempeña un papel fundamental en nuestra vida personal y profesional. El panorama de las amenazas se ha ampliado debido al rápido progreso de la tecnología digital, lo que hace que las organizaciones y las personas sean vulnerables a diferentes ciber-amenazas. Dado que las consecuencias de un ciberataque pueden ser desastrosas, la ciberseguridad se ha convertido en una preocupación fundamental para gobiernos, empresas y particulares por igual.

La ciberseguridad es un componente vital de nuestra vida digital en un mundo en el que la tecnología está firmemente integrada en todos los ámbitos de nuestras vidas. Es fundamental para salvaguardar la información sensible, defenderse de las ciber-amenazas, garantizar la integridad y datos de las empresas, asegurar la seguridad nacional y garantizar la seguridad y la privacidad de las personas. Las organizaciones y los individuos pueden reducir los riesgos haciendo hincapié en la ciberseguridad.

### **1.2. Antecedentes.**

El campo de la ciberseguridad surgió como respuesta a las crecientes amenazas y vulnerabilidades del mundo digital. Comenzó a cobrar fuerza a finales del siglo XX, a medida que las redes informáticas se extendían e interconectaban. Al principio se centró en proteger los sistemas informáticos personales, pero a medida que avanza la tecnología, también lo hacen el alcance y la complejidad de la ciberseguridad.

En los primeros años:

El concepto de ciberseguridad se remonta a la década de 1970, cuando los sistemas informáticos eran utilizados principalmente por instituciones académicas y organizaciones gubernamentales. En aquella época, la principal preocupación era proteger estos sistemas de accesos no autorizados. El primer virus informático notable, llamado virus Creeper, apareció en 1971, demostrando la necesidad de tomar medidas para combatir los programas maliciosos. La evolución de Internet y la expansión de las amenazas:

Con la llegada de Internet, la década de 1990 marcó un importante punto de inflexión en la ciberseguridad. A medida que Internet crece, también lo hace la posibilidad de que se produzcan ciberataques. El uso generalizado del correo electrónico y el aumento de la conectividad entre ordenadores han creado nuevas oportunidades que los ciberdelincuentes pueden explotar. Durante este periodo, aumentaron los virus, gusanos y otros programas maliciosos dirigidos contra las vulnerabilidades de los sistemas operativos y los programas informáticos. Iniciativas y normas gubernamentales:

Los gobiernos de todo el mundo se están dando cuenta de la importancia de la ciberseguridad y están empezando a tomar medidas para hacer frente a la creciente amenaza. En Estados Unidos, se aprobó la Ley de Seguridad Informática de 1987 para aumentar la seguridad y la privacidad de los sistemas informáticos federales. En la década de 2000, se desarrollaron varios marcos y normas de ciberseguridad, como la ISO/IEC 27001, que proporciona directrices para establecer un sistema de gestión de la seguridad de la información.

Ampliación del panorama de las ciber-amenazas:

Con el rápido desarrollo de la tecnología y la creciente dependencia de los sistemas digitales, el panorama de las ciber-amenazas se ha ampliado drásticamente. Los ciberataques se han vuelto más sofisticados, y no solo se dirigen a particulares y empresas, sino también a infraestructuras críticas y organismos gubernamentales. La proliferación de dispositivos móviles, computación en la nube e Internet de las cosas (IoT) ha aumentado aún más

la superficie de ataque e introducido nuevas vulnerabilidades. Desarrollo y especialización de la ciberseguridad:

A medida que las amenazas cibernéticas se vuelven más sofisticadas, el campo de la ciberseguridad continúa evolucionando y abarca una amplia gama de disciplinas. Abarca áreas como la seguridad de redes, la seguridad de aplicaciones, la protección de datos, la respuesta a incidentes y la gestión de riesgos. La creciente demanda de profesionales de la ciberseguridad ha llevado al desarrollo de certificaciones profesionales, programas académicos y organizaciones profesionales dedicadas a la ciberseguridad.

Retos actuales y perspectivas de futuro:

El panorama actual de la ciberseguridad se caracteriza por amenazas persistentes avanzadas, ciber-espionaje patrocinado por el Estado, ataques de ransomware y sofisticadas técnicas de piratería informática. Las organizaciones y los particulares se enfrentan a una batalla constante para adelantarse a los ciberdelincuentes y proteger la información sensible. A medida que la tecnología siga evolucionando, la ciberseguridad seguirá siendo una cuestión crítica que requiere innovación constante, colaboración e inversión en investigación y desarrollo. En conclusión, el campo de la ciberseguridad ha evolucionado con el avance de la tecnología digital y la creciente sofisticación de las ciber-amenazas. Ha pasado de centrarse exclusivamente en la seguridad de los ordenadores personales a adoptar un enfoque interdisciplinar destinado a proteger los sistemas, las redes y las infraestructuras críticas. A medida que las ciber-amenazas siguen evolucionando, los profesionales y las organizaciones de ciberseguridad deben permanecer vigilantes, adaptables y proactivos para proteger la información y preservar la integridad de los ecosistemas digitales.

### **1.3. Definición del Problema.**

La cuestión de la ciberseguridad para una empresa alude a los retos y peligros particulares a los que se enfrenta una organización a la hora de proteger sus recursos informáticos, su información sensible y su coherencia operativa frente a los ciber-peligros. Incluye la protección frente a una serie de

posibles ataques, como las filtraciones de información, el ransomware, los peligros internos, los intentos de suplantación de identidad y otros ejercicios perniciosos centrados en los marcos, sistemas y representantes de la empresa. El problema se agrava por la creciente modernidad y determinación de los ciberdelincuentes, así como por el avance del escenario de peligro que continuamente presenta vulnerabilidades y vectores de asalto sin utilizar. Esto requiere la ejecución de medidas de seguridad enérgicas, como FireWalls, marcos de detección y anticipación de Frameworks, convenciones de encriptación, controles de acceso y revisiones de seguridad estándar. Además, las empresas deben contribuir a la preparación de representantes, programas de concienciación y capacidades de reacción ante incidentes para moderar el efecto de los incidentes de seguridad, minimizar el tiempo de inactividad, garantizar los datos confidenciales y mantener la confianza de clientes y socios. En última instancia, el éxito de la ciberseguridad para una empresa incluye un enfoque proactivo e integral para reconocer, evaluar y aliviar los peligros, garantizando al mismo tiempo la flexibilidad y agudeza de los recursos y operaciones avanzadas.

#### **1.4. Justificación y alcance.**

Debido a los altos ataques que asechan constantemente, no solo las empresas sino a toda entidad que tenga importante información digital sensible, se busca fomentar y explicar la suma importancia que tiene esta área en una empresa para poder evitar cualquier fuga o ataque interno, esto generara confianza a lo accionista e inversionista ayudando en el crecimiento sano de la compañía

#### **1.5. Objetivos del Problema de Investigación.**

##### **1.5.1 Objetivo General.**

Mejorar el uso de la ciberseguridad de la empresa, garantizando el aseguramiento de recursos avanzados, información delicada y coherencia



operativa frente a ataques cibernéticos, explicar cómo estos ataques avanzan con el pasar del tiempo.

### **1.5.2 Objetivo Específico.**

- Aumentar la concienciación y preparación de los representantes.
- Reforzar la seguridad de la organización.
- Crear componentes de reacción y recuperación de incidentes.

### **1.6. Hipótesis.**

El uso de un programa de ciberseguridad coordinado con una área de sistemas entrenado, que cuente con la concienciación y preparación de los trabajadores, medidas de seguridad mejoradas y un sistema de reacción ante incidentes bien definidos, reducirá la probabilidad y el efecto de los ataques cibernéticos y los incidentes en los recursos informáticos, la información y la coherencia operativa de la empresa.

### **1.7. Metodología de Investigación.**

El tipo de investigativo empleado en este documento va categorizado en tres maneras análisis teórico, descriptivo y demostrativo, que se planteara en el ámbito de las áreas de sistemas encargadas de la seguridad digital de las compañías en general del país.

La metodología empleada para esta investigación es la analítica debido a que en el trabajo realizado se exponen los diferentes temas pertinentes para lograr hacer entender la importancia de estas áreas en una compañía o entidad importante que maneje datos sensibles o de suma importancia.

## **Capítulo 2:**

### **Fundamentación teórica**

#### **2.1 Ciberseguridad.**

La ciberseguridad, también conocida como seguridad de los datos, consiste en proteger las estructuras informáticas, los sistemas y la información contra el acceso no autorizado, la utilización, la divulgación, la perturbación, la alteración o la devastación. Incluye la ejecución de medidas para anticipar o minimizar los daños derivados de asaltos, robos o cualquier acceso no autorizado a los marcos de datos.

Existen diferentes tipos o categorías de ciberseguridad que se centran en distintos ángulos de la seguridad de los marcos informáticos, los sistemas y la información. He aquí algunos tipos comunes de ciberseguridad:

- Network Security.
- Application Security.
- Information Security.
- Endpoint Security.
- Cloud Security.
- Incident Response.
- Disaster Recovery.
- Social Engineering.

Estos son sólo algunos tipos de ciberseguridad. Es crucial recordar que la ciberseguridad es una industria en constante evolución, con nuevos tipos de amenazas y métodos de seguridad que aparecen todo el tiempo. En la figura 2.1 se muestra un mapa de como seria las distintas habilidades que se debe tener para frontear en esta área.



Una de las temáticas más complicadas de este tema es el error que comete la gente al asumir que un experto en ciberseguridad y un ingeniero en sistemas o de cómputo son lo mismo, sin embargo, está claro decir que las habilidades para brindar esas funciones se las puede obtener mediante certificaciones y estudios adicionales, no son ejes en las carreras que se las confunde.

Las obras hidroeléctricas generalmente tienen múltiples operaciones, produciendo agua potable, agua de riego, control de mareas y fallas de inundaciones, servicios de navegación y también esta energía de fuerza que indicamos.

La energía hidroeléctrica es actualmente la mayor fuente de energía renovable dentro del sector eléctrico. Se basa en patrones de caída generalmente estables y puede verse afectado negativamente por sequías causadas por el cambio climático o, de hecho, por cambios en los ecosistemas, lo que también produce este problema y afecta estos patrones de caída.

### **2.1.1 Ventajas de la Ciberseguridad.**

- Las medidas de ciberseguridad proporcionan seguridad frente a una amplia gama de amenazas cibernéticas, como intentos de pirateo, contaminación por malware, filtraciones de información y acceso no autorizado. Mediante la aplicación de fuertes medidas de seguridad, las organizaciones pueden reducir el riesgo de ciberataques y defender sus datos confidenciales.
- La ciberseguridad garantiza la privacidad y la protección de la información delicada. El cifrado, los controles de acceso y las convenciones de comunicación segura ayudan a evitar el acceso no autorizado o la divulgación de datos. Esto arraiga la creencia entre clientes, cómplices y socios, cultivando conexiones sólidas y el cumplimiento de los controles de protección.

- Una ciberseguridad exitosa contribuye a la progresión del comercio minimizando las perturbaciones causadas por las ciber-ocurrencias. Las medidas proactivas, como la organización de la reacción ante incidentes, los refuerzos de información y los procedimientos de recuperación ante catástrofes, ayudan a las organizaciones a recuperarse rápidamente de los ciberataques, minimizando el tiempo de inactividad y las pérdidas económicas.
- La ciberseguridad marca la diferencia a la hora de garantizar la notoriedad de una organización y generar confianza entre clientes y cómplices. Demostrando su compromiso con la seguridad y reduciendo eficazmente los ciber-peligros, las empresas pueden mantener su notoriedad, conservar la confianza de sus clientes y atraer a clientes modernos.

### **2.1.2 Desventajas de la Ciberseguridad.**

- Actualizar medidas de ciberseguridad sólidas puede ser complejo y desorbitado. Las organizaciones tienen que contribuir en el marco de la seguridad, el programa informático, la preparación de los trabajadores y la comprobación y el mantenimiento progresivos. Las pequeñas empresas con activos limitados pueden descubrir que es difícil asignar las reservas y el dominio adecuados para garantizar una ciberseguridad integral.
- Los marcos de ciberseguridad pueden crear aspectos positivos erróneos (aclamando ejercicios auténticos como amenazas) o negativos erróneos (quedándose cortos a la hora de distinguir peligros reales). Esto podría dar lugar a aspectos de despilfarro, ampliación de la carga de trabajo o posibles grietas de seguridad en caso de que no se supervisen legítimamente. Ajustar el descubrimiento de peligros viables con la minimización de advertencias falsas puede ser todo un reto.
- El escenario de la ciberseguridad avanza continuamente, con peligros no utilizados, vectores de asalto y vulnerabilidades que aumentan de forma rutinaria. Mantenerse al día con la naturaleza avanzada de los ciber-peligros

requiere una observación incesante, medidas de seguridad proactivas y actualizaciones estándar de las convenciones de seguridad. La incapacidad para adaptarse a los peligros no utilizados puede hacer que las organizaciones queden indefensas ante los ataques.

- El error humano sigue siendo uno de los puntos más débiles de la ciberseguridad. A pesar de las estrictas medidas de seguridad adoptadas, la falta de atención por parte de los clientes, el incumplimiento de las normas de seguridad o los errores involuntarios pueden debilitar los esfuerzos de ciberseguridad. Los ataques de construcción social, como el phishing, abusan de las vulnerabilidades humanas, enfatizando la importancia de progresar en la instrucción del cliente y en las campañas de concienciación.

## **2.2 Herramientas contra amenazas.**

Las herramientas de amenazas, también conocidas como herramientas de hacking o de seguridad ofensiva, son aplicaciones o utilidades de software utilizadas por los profesionales de la ciberseguridad para simular y evaluar diversas ciberamenazas y vulnerabilidades. Estas herramientas son esenciales en ciberseguridad porque ofrecen información valiosa sobre los puntos débiles de un sistema, red o aplicación. Al emular las tácticas y técnicas empleadas por los actores maliciosos, los expertos en ciberseguridad pueden identificar vulnerabilidades, probar controles de seguridad y desarrollar estrategias de defensa eficaces. Las herramientas de amenazas permiten la evaluación proactiva y sistemática de vulnerabilidades, pruebas de penetración y auditorías de seguridad, ayudando a las organizaciones a adelantarse a los posibles atacantes y reforzar su postura general de ciberseguridad.

Una de las razones clave por las que las herramientas de amenazas son esenciales en ciberseguridad es su capacidad para descubrir vulnerabilidades y debilidades que de otro modo podrían pasar desapercibidas. Estas herramientas pueden escanear redes, aplicaciones y sistemas en busca de fallos de seguridad comunes, configuraciones erróneas y vulnerabilidades de software. Al identificar estos puntos débiles, las organizaciones pueden abordarlos de forma proactiva, parchear las vulnerabilidades y aplicar medidas de seguridad adicionales para

mitigar los riesgos potenciales. Este enfoque proactivo ayuda a prevenir el acceso no autorizado, las violaciones de datos y otras actividades maliciosas que podrían conducir a importantes daños financieros y de reputación .

Otro aspecto crucial de las herramientas de amenazas en ciberseguridad es su papel en la preparación y respuesta a incidentes cibernéticos del mundo real. Al simular ataques y evaluar las defensas de una organización, estas herramientas ayudan a evaluar la eficacia de los controles de seguridad y las capacidades de respuesta ante incidentes. Permiten a los profesionales de la ciberseguridad simular escenarios, analizar el impacto de posibles violaciones y perfeccionar los planes de respuesta a incidentes. Además, las herramientas de amenazas ayudan a los equipos de seguridad a comprender la evolución de las técnicas y tácticas empleadas por los ciberdelincuentes, manteniéndolos informados sobre las últimas tendencias en el panorama de las amenazas. Este conocimiento dota a las organizaciones de los conocimientos necesarios para adaptar y mejorar de forma proactiva sus defensas de ciberseguridad, reduciendo en última instancia el riesgo de éxito de los ciberataques.

Existen varias herramientas que por lo general sería una lista interminable, ya que mucho depende de cómo sea el área de aplicación y que vulnerabilidad estes buscando en tu entorno de seguridad, este es un pequeño listado de las más usadas de manera semi-gratuita:

- Tripwire IP360
- Nessus vulnerability scanner
- Comodo HackerProof
- Nexpose community
- OpenVAS Vulnerability Scanner
- Nikto
- Wireshark
- Aircrack-ng
- Retina network security scanner

## **2.3 Tecnologías del uso de Herramientas contra amenazas.**

Los escáneres de vulnerabilidades utilizan una combinación de tecnologías para identificar vulnerabilidades de seguridad y errores de configuración en sistemas, redes y aplicaciones. Estas son algunas de las tecnologías clave utilizadas habitualmente por los escáneres de vulnerabilidades.

Es importante tener en cuenta que los escáneres de vulnerabilidades pueden emplear una combinación de tecnologías, junto con algoritmos y criterios propios, para proporcionar una evaluación completa de las vulnerabilidades y capacidades de escaneado. Las características y tecnologías específicas utilizadas pueden variar dependiendo del diseño, propósito y proveedor del escáner.

### **2.3.1 Tecnologías del uso de ciberseguridad.**

Existen varias tecnologías utilizadas en ciberseguridad para proteger sistemas, redes y datos de las ciber-amenazas. Estas son algunas tecnologías comunes empleadas en el campo de la ciberseguridad:

- Firewalls
- Sistemas de Detección y Prevención de Intrusiones (IDPS)
- Software Antivirus y Antimalware
- Encriptación
- Redes Privadas Virtuales (VPN)
- Gestión de Eventos e Información de Seguridad (SIEM)
- Autenticidad con Múltiples Pasos (MFA)
- Escáneres de Vulnerabilidades

#### **2.3.1.1 Entorno basado en IA**

En un entorno basado en IA, los avances en falsos conocimientos se utilizan para mecanizar y mejorar las formas de ciberseguridad. Los cálculos de IA pueden analizar enormes volúmenes de información, identificar diseños



y reconocer peculiaridades o peligros potenciales con mayor eficacia que las estrategias manuales convencionales. Los dispositivos de ciberseguridad impulsados por IA pueden realizar tareas.

#### **2.3.1.2 Entorno basado en humanos**

Un entorno basado en humanos en ciberseguridad incluye expertos dotados que utilizan su habilidad, implicación y capacidades básicas de reflexión para analizar, reaccionar y supervisar los ciber-peligros. La intervención humana sigue siendo imprescindible por varias razones.

#### **2.3.1.3 Entorno Híbrido**

Combinar las innovaciones basadas en la IA con la habilidad humana crea un entorno de ciberseguridad capaz. Los marcos de IA pueden preparar y analizar grandes cantidades de información con rapidez, mientras que los expertos humanos aportan la comprensión, la imaginación y la versatilidad necesarias para gestionar ciber-peligros complejos y crecientes de forma viable.

#### **2.3.1.4 Área de sistemas.**

Los ingenieros de sistemas tienen un conjunto de conocimientos diferentes que abarcan equipos informáticos, marcos de trabajo, convenciones de organización, administración de bases de datos, virtualización y organización de marcos. Superan las expectativas en la organización, optimización y resolución de problemas dentro de los marcos y sistemas. Centrados en la planificación, el uso y la asistencia, los ingenieros de estructuras garantizan el funcionamiento, la ejecución y la integración coherentes de los distintos componentes de las estructuras. Su destreza garantiza la calidad y competencia inquebrantables de los marcos, sistemas y cimientos informáticos.

### **2.4 Fundamentos y Técnicas de las Herramientas contra amenazas.**

Las armas coherentes en la lucha cibernética hacen referencia a los aparatos o programas utilizados para la observación, los sistemas de exploración y la propulsión de ataques o el abuso de vulnerabilidades. Estos

aparatos son la base de los ejercicios de ciber guerra. Aunque no varíen conceptualmente de los utilizados en las pruebas de infiltración ordinarias, su objetivo y efecto se amplían totalmente en una situación de lucha cibernética. A diferencia de los analistas de infiltración, que a menudo se ven limitados a utilizar instrumentos "peligrosos", la lucha cibernética permite la utilización de tales instrumentos, incluso si tienen efectos negativos sobre el objetivo. Mientras que los aparatos comerciales pueden ser utilizados por las fuerzas de lucha cibernética apoyadas por los países, es menos probable que las personas o los pequeños grupos dispongan de ellos. En cualquier caso, las personas dotadas utilizan regularmente dispositivos gratuitos, que pueden ser profundamente viables, pero menos informatizados en comparación con las alternativas comerciales. (Threat Modeling Tools: A Taxonomy, 2022).

En el programa de seguridad de una organización, la localización de riesgos incluye diferentes perspectivas, reconociendo la posibilidad de que se produzcan infracciones incluso con medidas de protección enérgicas. Combina la innovación y el dominio humano para distinguir a tiempo los signos de una brecha. Un programa completo de localización de peligros y reacción depende de una combinación de individuos, formas e innovación para identificar tanto los peligros conocidos como aquellos oscuros dentro del entorno organizado.

El reconocimiento y la reacción ante los riesgos es el perfeccionamiento proactivo para distinguir los ejercicios nocivos que suponen un peligro para la seguridad de una red. Incluye el reconocimiento expeditivo de peligros potenciales y la actualización de actividades adecuadas para neutralizarlos o aliviarlos, minimizando el efecto potencial sobre la organización.

Las herramientas de vigilancia, son aquellos que utilizamos para acumular datos, la mayoría de las veces en estado inactivo, sobre los sistemas y marcos contra los que podríamos requerir actividad en un sentido coherente. Dichos esfuerzos pueden incluir la recopilación de datos de sitios web abiertos, la búsqueda de registros de servidores del Marco de Títulos Espaciales (DNS), la recopilación de metadatos de archivos abiertos, la

recuperación de datos excepcionalmente específicos mediante el uso de motores de búsqueda, o cualquiera de otros ejercicios similares. Para la observación, podemos utilizar datos acumulados de fuentes como:

- Sitios web.
- Motores de búsqueda.
- Google hacking.
- Búsquedas WHOIS/consultas DNS.
- Metadatos.
- Dispositivos de búsqueda especializados como Maltego.

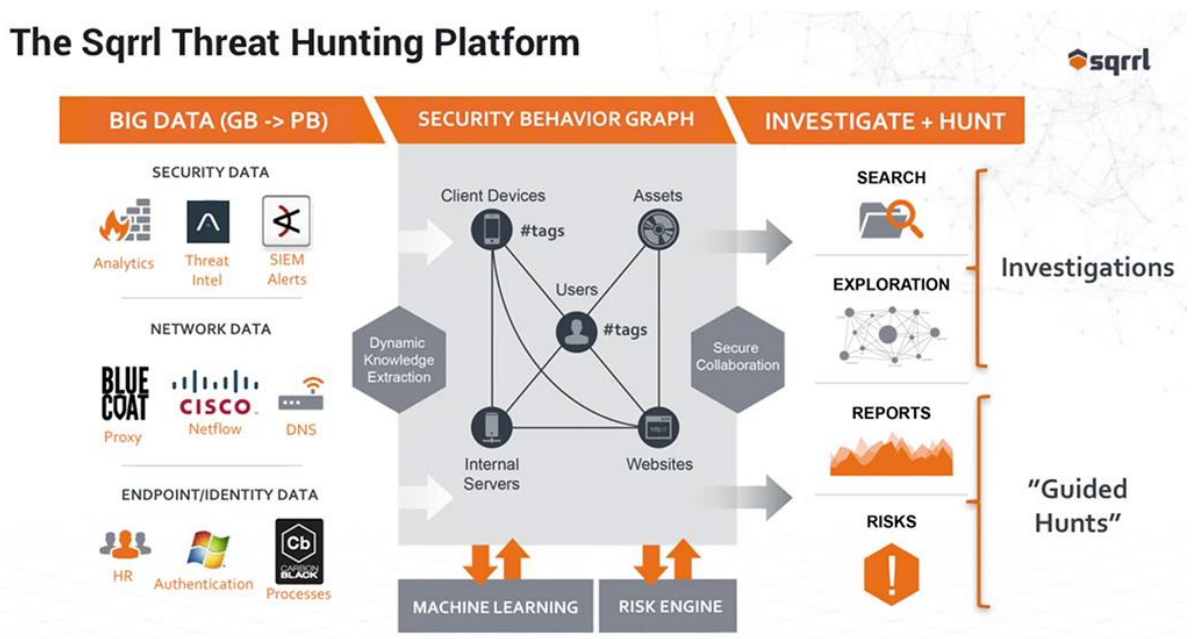
Las herramientas de escaneo son la categoría de dispositivos que utilizamos para descubrir más datos casi de nuestro entorno de destino, los marcos dentro de él, y los elementos sutiles de esos sistemas. Con tales instrumentos, seremos muy generales, en el caso de ejecutar limpiezas de ping, hasta cierto punto más específico, en el caso de ejecutar miradas de puerto, o excepcionalmente particulares, en el caso de obtener estándares o identificar clientes en marcos específicos. Algunos aparatos comunes utilizados para filtrar incorporan:

- Nmap.
- Nessus.
- OpenVAS.



La persecución de amenazas cibernéticas se separa de la localización de riesgos, porque va más allá de la observación inactiva para cazar eficazmente peligros basados en la comprensión de los comportamientos de los actores de peligro. Depende de la mejora de la especulación, las miradas dinámicas y la investigación legal o tal vez que exclusivamente en función de las alarmas o punteros de compromiso. Acepta que se ha producido o se producirá una brecha, provocando que el personal de seguridad persiga eficazmente los peligros en su entorno en lugar de depender exclusivamente del envío de los aparatos más recientes. La vigilancia y las medidas proactivas son básicas para una ciberseguridad convincente, dado el constante avance de los peligros y las vulnerabilidades.

Figura 2. 3 El impacto de la caza de amenazas en sus operaciones de seguridad



Fuente: (Zorz, 2020)

### 2.4.2 Conciencia y Formación en Ciberseguridad.

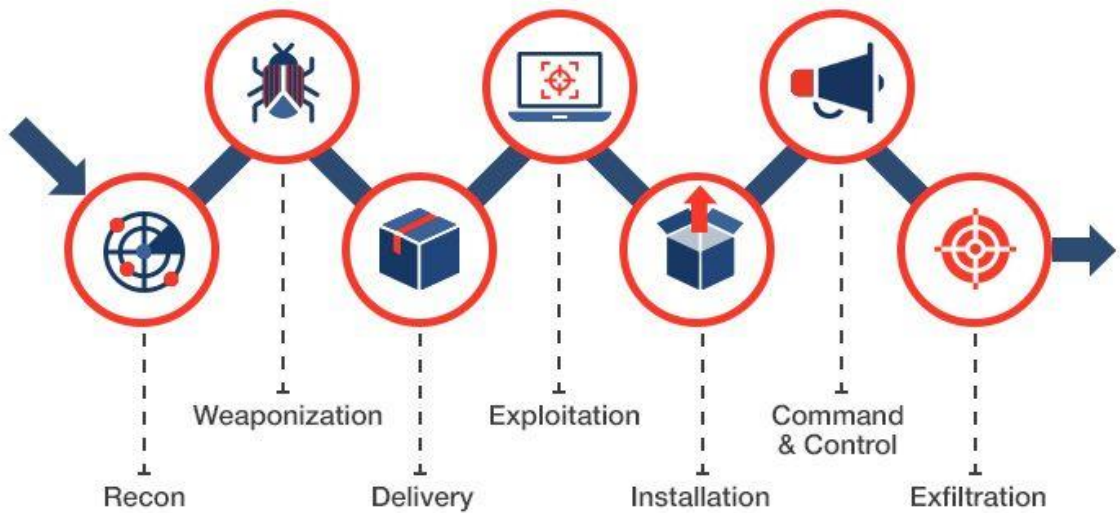
A la hora de defenderse contra los ciberataques, la atención se centra principalmente en salvaguardar la información sensible, como la Información de Identificación Personal (PII) o la Información Sanitaria del Paciente (PHI).

El compromiso de tales datos puede conducir al robo de identidad y a actividades fraudulentas, que van desde pérdidas financieras a transacciones no autorizadas. En los sectores militar y gubernamental, la exposición de información sensible puede tener graves consecuencias, como la pérdida de vidas humanas y un cambio en la dinámica de poder. Aunque existen leyes para proteger estos datos, siguen evolucionando, y cada estado promulga normas más estrictas de protección de datos y privacidad. (*the Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice* by Steve Winterfeld, Jason Andress | Perlego, 2012)

El factor humano plantea una importante vulnerabilidad de seguridad, ya que las personas pueden socavar inadvertidamente medidas de seguridad cuidadosamente planificadas por pereza, descuido o errores honestos. Las medidas técnicas y las políticas por sí solas son insuficientes para hacer frente a esta vulnerabilidad. La formación y la disciplina son esenciales para inculcar la concienciación y la comprensión de los riesgos de seguridad y para promover comportamientos adecuados que mejoren la seguridad. La formación a nivel de mando es crucial para garantizar un entorno centrado en la ciberseguridad que refleje el clima de la organización.

Aunque las medidas técnicas y las políticas tienen por objeto prevenir las actividades malintencionadas, es vital educar a las personas y hacer cumplir sistemáticamente los protocolos de seguridad en todos los niveles de la organización. Al fomentar la concienciación y la formación, las organizaciones pueden establecer una postura de seguridad más sólida y mitigar los riesgos asociados a los factores humanos.

Figura 2. 4 Las 7 Tácticas Defensivas y Procesos.



Fuente:(Security, 2023)

## 2.5 Hacking Ético.

El Hacking Ético, también conocido como pruebas de infiltración, se ha desarrollado como una llamada en reacción a las preocupaciones en desarrollo que abarcan la piratería informática y la ciberseguridad en nuestro mundo cuidadosamente asociado. En esta era informatizada, en la que casi todo está en línea e interconectado, la necesidad de proteger la información delicada de programadores perniciosos es primordial.

El Hacking Ético hace alusión a los ejercicios de hacking que se llevan a cabo con el consentimiento expreso del propietario del sistema objetivo y se rigen por valores morales y éticos. Incluye los esfuerzos autorizados para eludir o romper las medidas de seguridad con el fin de distinguir las vulnerabilidades, las brechas de información y los peligros potenciales. Los programadores morales, o analizadores de entrada, se rigen por las leyes y normas cibernéticas territoriales y organizativas a la hora de realizar sus evaluaciones.

El objetivo esencial de un Programador Moral es revelar las deficiencias en la seguridad de un sistema en algún momento antes de que los programadores nocivos puedan abusar de ellas. Al recrear los esfuerzos de piratería del mundo real, ofrecen asistencia a las organizaciones para reconocer vulnerabilidades y aplicar rápidamente parches de seguridad para prescindir de los posibles focos de paso de los agresores. Este enfoque proactivo permite a los grupos de seguridad vigilar los marcos de forma viable y proteger la información delicada.

El Hacking Ético desempeña un papel crucial a la hora de garantizar la seguridad y la agudeza de los marcos informáticos. Al ir un paso por delante de los peligros potenciales, los programadores morales contribuyen a reforzar las medidas de ciberseguridad y a garantizar que no se produzcan violaciones de la información, lo que a la larga contribuye a crear un entorno informático más seguro tanto para las personas como para las organizaciones. (Erickson, 2008)

### **2.5.1 Sombrero Blanco.**

Los programadores de sombrero blanco, también conocidos como hackers éticos, desempeñan un papel crucial en el descubrimiento de vulnerabilidades en programas, equipos y sistemas que los hackers malintencionados pueden explotar. A diferencia de sus homólogos, los hackers de sombrero negro, los hackers de sombrero blanco operan con la debida autorización y únicamente con fines defensivos. Revelan todas las vulnerabilidades identificadas a sus empleadores y también pueden notificarlas a los proveedores para facilitar las correcciones necesarias para los sistemas afectados. Entre las técnicas más utilizadas por los hackers de sombrero blanco se encuentran las pruebas de penetración y las evaluaciones de vulnerabilidades. (Kim, 2015)

Los hackers de sombrero blanco trabajan como analistas de seguridad de la información, investigadores de ciberseguridad, probadores de penetración y consultores para empresas y organismos públicos. Emplean



metodologías de hacking para evaluar y mejorar la seguridad de los sistemas, operando con integridad y con el permiso explícito de los propietarios de los sistemas. Estos profesionales suelen tener formación académica y de investigación, con el objetivo de conocer mejor las ciber-amenazas y educar a otros sobre ellas. Ayudan a las organizaciones a preparar planes de contingencia para combatir los ataques cibernéticos y se adhieren a las regulaciones de seguridad como HIPAA, PCI DSS y GDPR.

Habilidades que se desarrollan:

- Descubrir y solventar vulnerabilidades antes que los hackers de sombrero negro puedan abusar de ellas.
- Crear dispositivos que puedan distinguir los ciberataques y aliviarlos o cuadrarlos.
- Fortalecer la seguridad general del programa y los componentes del equipo.
- Construir programas informáticos de seguridad como antivirus, antimalware, antispymware, honeypots, cortafuegos, etc.

### **2.5.2 Sombrero Gris.**

Los hackers de sombrero gris se sitúan entre los hackers de sombrero blanco y los hackers de sombrero negro, mostrando una mezcla de comportamientos éticos y no éticos en sus técnicas de hacking. Aunque a menudo poseen habilidades técnicas similares a las de los hackers de sombrero blanco, no siempre se adhieren a las prácticas éticas. Por ejemplo, pueden buscar vulnerabilidades en sitios web, aplicaciones o sistemas informáticos sin la debida autorización, aunque normalmente no tienen intención de causar daños. Los hackers de sombrero gris llaman la atención sobre las vulnerabilidades existentes, lanzando ciberataques similares a los de los hackers de sombrero blanco contra servidores y sitios web de empresas o gobiernos. Estos ataques sacan a la luz lagunas de seguridad,

pero no causan daños directos, aunque sin el conocimiento o consentimiento del propietario.

Algunos hackers de sombrero gris optan por divulgar públicamente información sobre vulnerabilidades una vez que han sido corregidas, mientras que, en otros casos, primero se ponen en contacto con las empresas afectadas para informarles. Si una empresa no responde o no toma medidas rápidas, el hacker puede decidir divulgar públicamente la información, aunque el fallo no se haya corregido. Los hackers de sombrero gris suelen hacer esto para ganar reconocimiento y establecer su reputación dentro de la comunidad de la ciberseguridad, ayudándoles indirectamente a avanzar en sus carreras como expertos en seguridad. Sin embargo, este paso puede dañar la reputación de las empresas cuyas vulnerabilidades de seguridad o exploits se revelan públicamente.

Los piratas informáticos de sombrero gris pueden carecer de la intención criminal o maliciosa de los piratas informáticos de sombrero negro, pero también operan sin el conocimiento previo o el consentimiento de los sistemas que piratean. Aunque los hackers de sombrero gris informan sobre vulnerabilidades en lugar de explotarlas por completo, pueden solicitar un pago a cambio de proporcionar información detallada sobre lo que han descubierto.

Información que proveen:

- Corregir errores o vulnerabilidades.
- Reforzar las defensas de seguridad de la organización.
- Proporcionar recomendaciones, soluciones o herramientas para parchear vulnerabilidades.

### **2.5.3 Sombrero Negro.**

Los programadores de sombrero negro son ciberdelincuentes que rompen ilícitamente los marcos con expectativas perniciosas. La definición de hacking sombrero negro es la búsqueda de acceso no autorizado a los sistemas informáticos. Una vez que un programador de sombrero negro encuentra un fallo de seguridad, intenta abusar de él, normalmente incrustando una infección u otro tipo de malware como un troyano.

Los ataques de ransomware son otra estratagema favorecida que los programadores de sombrero negro utilizan para chantajear recogidas monetarias o violar marcos de información.

Los programadores de sombrero negro son personas diabólicas que necesitan utilizar sus habilidades especializadas para estafar y extorsionar a otros. Por regla general, tienen el dominio y la información necesarios para entrar en sistemas informáticos sin la autorización de los propietarios, abusar de las vulnerabilidades de seguridad y saltarse las convenciones de seguridad. Para formar dinero en efectivo, están dispuestos a realizar todos los ejercicios ilícitos como:

- Enviar correos electrónicos y mensajes SMS de phishing.
- Componer, transmitir y ofrecer malware como infecciones, gusanos, troyanos, etc.
- Envío de ciberataques como denegación dispersa de beneficios (DDoS) para moderar o colapsar los sitios web.
- Ganar dinero en efectivo para hacer vigilancia política y corporativa.
- Encontrar y utilizar indebidamente bases de datos defectuosas y vulnerabilidades de programas.

- Ofrecer datos monetarios e identificables en la Web opaca.
- Ejecutar extorsiones presupuestarias y delitos relacionados con el robo de personalidad.
- Transmitir peligros cibernéticos peligrosos como ataques de fuerza bruta, scareware, botnets, ataques man-in-the-middle, campañas de malvertising, etc.
- Extorsionando a las víctimas utilizando ransomware y spyware para codificar, bloquear, tomar, ajustar y borrar su información.
- Los programadores oscuros suelen pedir dinero en efectivo como chantaje para permitir el acceso a los registros, el marco, las bases de datos o todo el dispositivo.
- También shakedown víctimas, debilitando a descubrir su información privada, registros comerciales, fotografías individuales, grabaciones, etc, a la luz en caso de que no pagan.

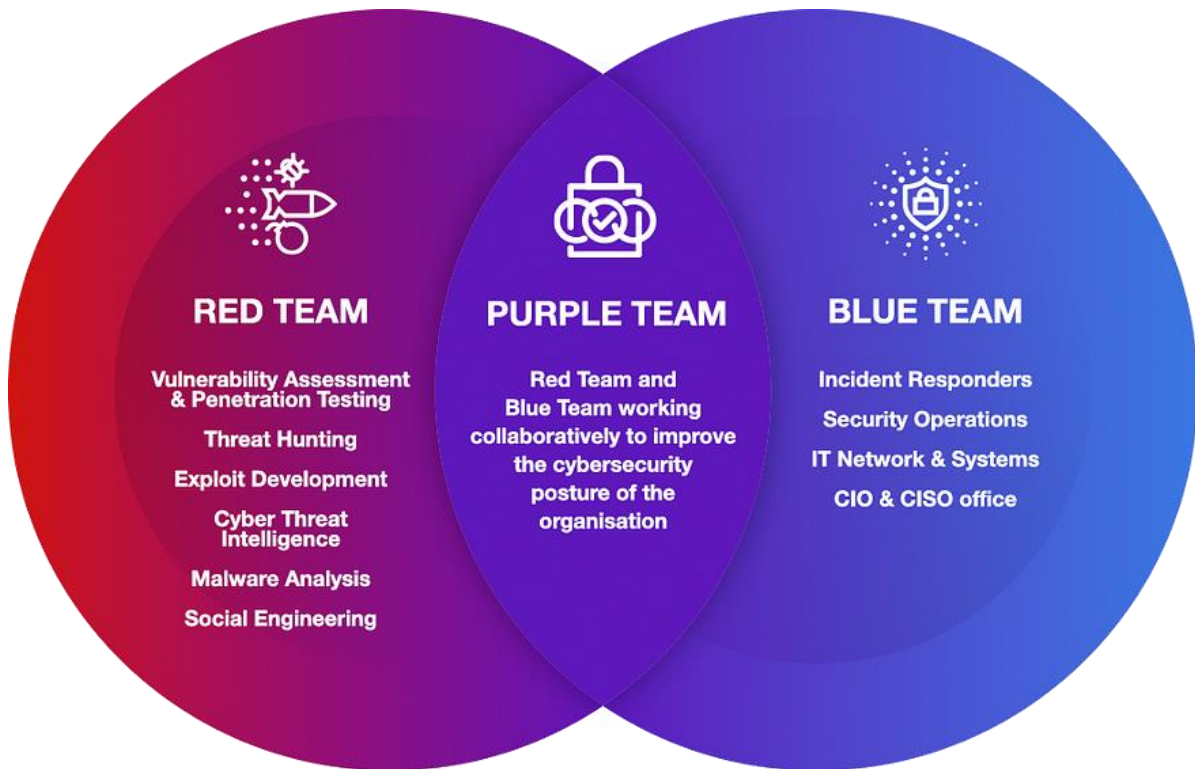
## **2.6 Equipo Azul, Rojo y Purpura en Hacking Ético.**

En el mundo del hacking moral, existen distintos grupos y enfoques para mejorar la ciberseguridad y proteger los marcos de posibles peligros. El grupo rojo, el grupo azul y el grupo púrpura hablan de puntos de vista y partes inconfundibles dentro del campo. Cada grupo contribuye a la seguridad general de una organización a su manera. Comprender los contrastes entre estos grupos es vital para construir técnicas de precaución viables y avanzar en la flexibilidad de la ciberseguridad.

Comprender las partes y los puntos de vista de los grupos rojo, azul y morado es vital para las organizaciones que buscan establecer sistemas de seguridad sólidos. Al comprender un enfoque integral que combine procedimientos hostiles y de protección, las organizaciones pueden reconocer

vulnerabilidades, mejorar sus resistencias y asegurar de forma proactiva sus recursos rentables frente al avance de los ciber-peligros.

Figura 2. 5 Interconexión entre los equipos de hacking ético.



Fuente: (Consultores, 2022)

### 2.6.1 Equipo Azul.

Los Equipos Azules, son grupos de seguridad interior atentos a la protección contra los auténticos asaltantes cibernéticos. Los Grupos Azules se distinguen de los grupos de seguridad estándar por adoptar una actitud de cuidado constante contra los asaltos, lo que da forma a su misión y punto de vista. Estos guardias proactivos desempeñan un papel vital en la escena de la ciberseguridad.

La figura 2.6 se distingue a un Grupo Azul en los ejercicios de protección estándar en un ambiente hostil cibernético. Los Grupos Azules muestran una

mentalidad proactiva centrada en la defensa sin pausa, el descubrimiento del peligro y la reacción. Van más allá de las medidas de defensa convencionales, buscando eficazmente formas de mejorar la seguridad y proteger a las organizaciones contra los ciber-peligros.

Figura 2. 6 Operación de proceso de ataque y defensa.



Fuente: (Paganini, 2017)

### **2.6.2 Equipo Rojo.**

Los equipos rojos se centran en la seguridad ofensiva y su objetivo es encontrar y explotar puntos débiles en las defensas de una organización. Prueban a fondo los sistemas de control y respuesta de los equipos azules, simulando ataques reales a la red de una organización. Utilizando las mismas herramientas y técnicas que los atacantes reales, el equipo rojo puede identificar vulnerabilidades críticas que necesitan reparación. La información obtenida de estas operaciones se utiliza para mejorar la postura de seguridad de la organización en su conjunto.

Las lecciones aprendidas de las operaciones de los equipos rojos desempeñan un papel importante en la mejora de la postura global de seguridad de una organización. Al identificar vulnerabilidades y puntos débiles, las organizaciones pueden tomar medidas proactivas para reforzar sus defensas. La información recopilada a partir de estos despliegues nos ayuda a tomar decisiones estratégicas y a impulsar mejoras en nuestras políticas, procedimientos y tecnologías de seguridad.

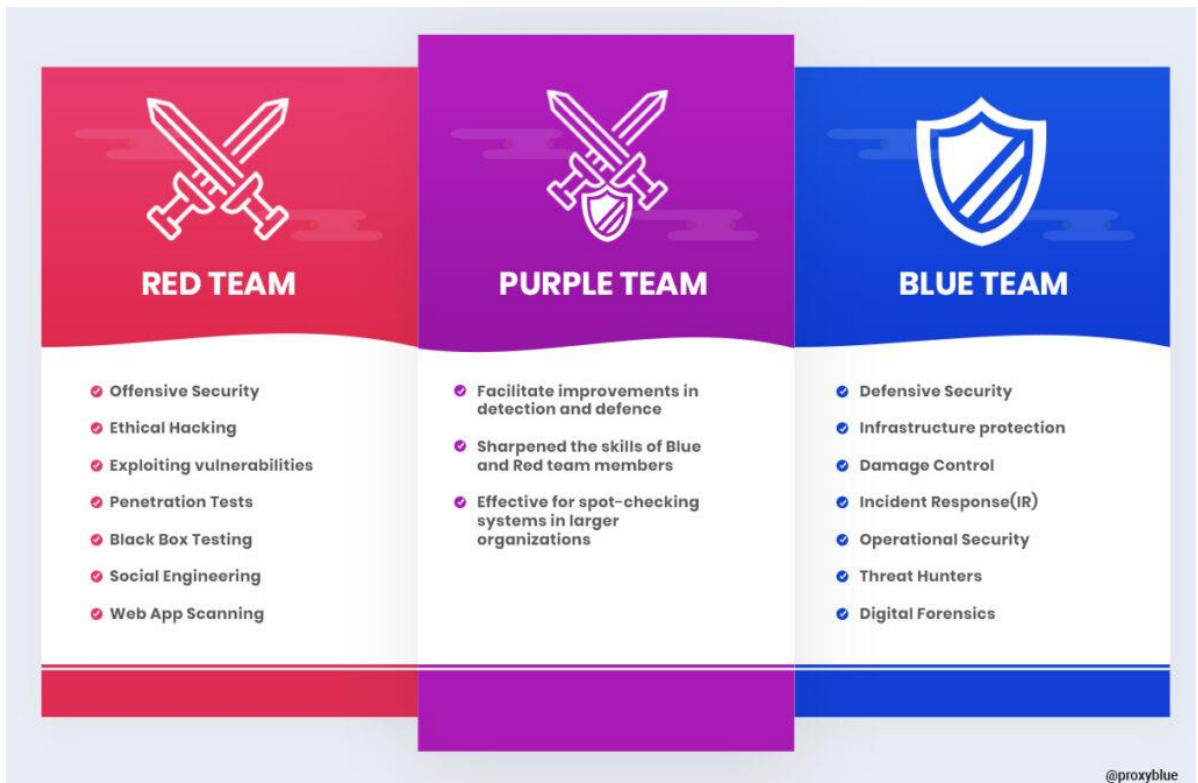
### **2.6.3 Equipo Púrpura.**

El concepto de Equipo Púrpura en ciberseguridad representa una mentalidad cooperativa entre atacantes y defensores, que trabajan juntos en el mismo bando. Sin embargo, debe considerarse una característica más que un equipo dedicado. El verdadero propósito del equipo rojo es identificar áreas de mejora dentro del equipo azul. En consecuencia, las organizaciones con interacciones eficaces entre los equipos rojo y azul pueden no necesitar un equipo púrpura separado.

El término "equipo púrpura" es más beneficioso cuando los grupos no familiarizados con las técnicas de ataque buscan aprender cómo piensan los atacantes. Esto puede incluir equipos de respuesta a incidentes, detección o desarrollo. Involucrarse con hackers de sombrero blanco permite a estos grupos adquirir ideas y conocimientos, sirviendo como ejercicio para el equipo púrpura.

Si los equipos rojo y azul funcionan eficazmente, la necesidad de un equipo púrpura dedicado puede disminuir. El concepto de equipo púrpura puede existir como principio rector, animando al equipo rojo a realizar pruebas específicas y establecer objetivos concretos. Implica elementos de las capacidades de defensa y detección del equipo azul, trabajando en colaboración con ambos equipos para analizar la cooperación y recomendar los ajustes necesarios para los ejercicios en curso o las mejoras futuras. (Consultores, 2022)

Figura 2. 7 Cualidades de cada equipo



Fuente: (Taylor, 2022)

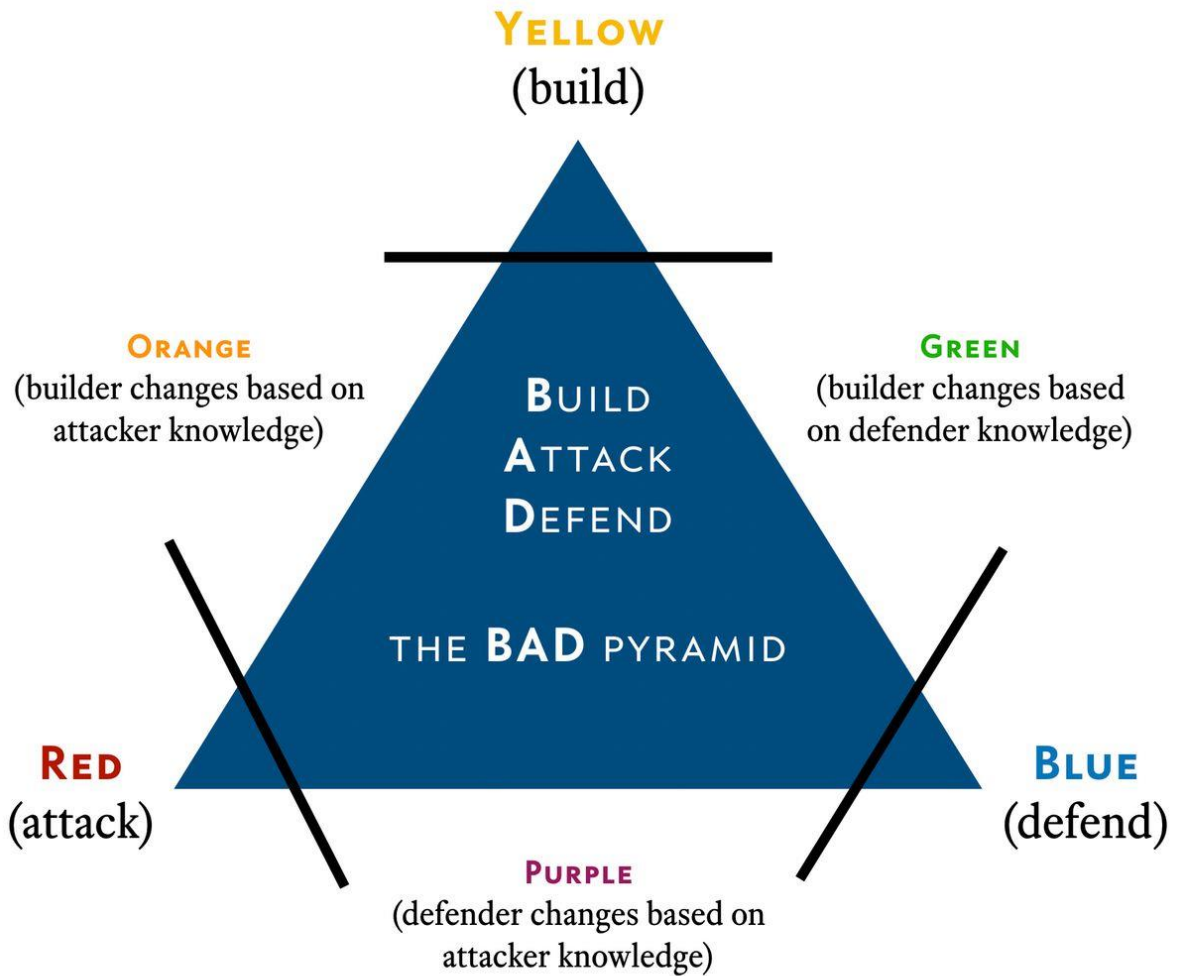
Además de los conocidos conceptos de equipo rojo, azul y morado, a lo largo de los años se fueron haciendo charlas y cesiones con experto para definir que pueden existir otros tipos de equipo, como el naranja que sería el nuevo morado.

En esa charla introdujo el concepto de equipo Amarillo, que son los constructores, y luego los combinó con el Azul y el Rojo para producir los otros colores. Creo que esto es extremadamente inteligente, pero se ah discrepado un poco con algunas de las caracterizaciones de las combinaciones.

Aun no se puede hablar de manera cómo equipos ya que aún no se definieron todos los colores, ya que creo que en la mayoría de los casos se trata de mentalidades o funciones, más que de grupos de personas dedicadas.



Figura 2. 8 Diagrama del cambio de equipos.



DANIEL MIESSLER 2019  
BASED ON WORK BY APRIL WRIGHT

Fuente: (Miessler, 2023)

## 2.7 Virus Computacionales.

Un virus informático puede ser un programa peligroso que puede duplicarse y propagarse de un ordenador a otro, normalmente sin la información o el consentimiento del usuario. A diferencia de las infecciones naturales, las infecciones informáticas pueden causar daños a los registros, adulterar la información, reducir la ejecución del marco o incluso tomar datos delicados.

Comprender el concepto de infección informática y sus distintos tipos es vital para adoptar medidas de ciberseguridad convincentes.

Las infecciones informáticas están planeadas para conectarse a programas o registros reales, permitiéndoles ejecutarse y proliferar. Normalmente son creadas por ciberdelincuentes con fines malévolos, con el objetivo de perturbar los sistemas informáticos, tomar datos o acceder a ellos sin autorización. Las infecciones pueden propagarse a través de diferentes medios, como conexiones de correo electrónico, sitios web contaminados, programas informáticos comprometidos o dispositivos de capacidad desmontable.

Las infecciones informáticas son un peligro incansable para los sistemas informáticos y los clientes de todo el mundo. Entender el concepto de infecciones informáticas y los diferentes tipos es básico para actualizar las medidas de seguridad con éxito. La utilización de un programa antivirus potente, la actualización frecuente de los programas informáticos y los sistemas de trabajo, la práctica de hábitos de navegación seguros y la precaución con las conexiones de correo electrónico y las descargas pueden ayudar a evitar las infecciones informáticas y aliviar sus posibles efectos.

### **2.7.1 Tipos de virus.**

Con el debido pasar de los tipos la tecnología ayuda a que los virus computacionales evolucionen a un ritmo sumamente veloz, haciendo complicado la determinación de muchos y generando dudas de su existencia a aquí tenemos unos ejemplos de los que a pesar de que se modifican con el tiempo mantienen ciertos rasgos que nos permite determinarlos.

- Virus de infección de archivos: Estos virus infectan archivos ejecutables como los archivos .exe y .com. Una vez que se ejecuta el archivo infectado, el virus se activa y se propaga a otros archivos ejecutables del sistema. Los virus de infección de archivos pueden hacer daño modificando o dañando los archivos infectados.

- Virus del sector de arranque: Un virus del sector de arranque infecta el sector de arranque del disco duro de un ordenador o de otro dispositivo de almacenamiento. Estos se activan cuando arranca un dispositivo infectado, permitiendo que el virus se cargue en la memoria del ordenador. Los virus del sector de arranque pueden causar graves daños al sobrescribir archivos críticos del sistema e impedir que el ordenador arranque correctamente.

- Virus de macro: Los virus de macro se escriben utilizando el lenguaje de programación de macros y suelen infectar documentos y archivos de hojas de cálculo. Aprovechan las funciones de macro de aplicaciones como Microsoft Word y Excel para propagar y ejecutar código malicioso. Los virus de macro pueden corromper datos o robar información confidencial.

- Virus polimórficos: Los virus polimórficos tienen la capacidad de cambiar su código o apariencia para evitar ser detectados por el software antivirus. Revuelven o cambian su código con cada replicación, lo que dificulta su identificación y eliminación por parte de los programas antivirus. Los virus polimórficos suponen una amenaza importante porque pueden eludir los métodos de detección tradicionales.

- Gusanos: Los gusanos aprovechan las vulnerabilidades para acceder a los sistemas y utilizan las conexiones de red para propagarse a otros ordenadores. Pueden sobrecargar la red, consumir recursos del sistema y propagar otros programas maliciosos.

## 2.8 Encriptado de Datos.

El cifrado transforma los datos en otra forma o código, haciendo que sólo puedan leerlos quienes tengan acceso a la clave privada (formalmente conocida como clave de descifrado) o a la contraseña. Los datos cifrados se denominan comúnmente texto cifrado, y los no cifrados, texto plano. El cifrado es actualmente uno de los métodos de seguridad de datos más populares y eficaces utilizados por las empresas. Existen dos tipos principales de cifrado de datos. La criptografía asimétrica (también llamada criptografía de clave pública) y la criptografía simétrica.

En el entorno digital actual, en el que se almacenan y gestionan en línea grandes cantidades de información sensible, el cifrado desempeña un papel importante en la ciberseguridad. Actúa como mecanismo de defensa contra los ataques de fuerza bruta, el malware y el ransomware. El cifrado de datos protege tanto los datos digitales transmitidos (los llamados datos a bordo) como los datos digitales almacenados (los llamados datos en reposo). Protege los datos en entornos de nube y sistemas informáticos. (*What Is Encryption? Data Encryption Defined | IBM, n.d.*)

La fuerza del cifrado reside en la complejidad de las claves de cifrado utilizadas. Cuanto más compleja sea la clave, más seguro será el cifrado. Las claves complejas hacen que sea cada vez más difícil para terceros descifrar datos por fuerza bruta probando números aleatorios hasta adivinar la combinación correcta.

Ejemplo en código C de encriptado usando el método Caesar Cypher Algorithm.

```
//Simple C program to encrypt and decrypt a string  
  
#include <stdio.h>
```

```

int main()
{
    int i, x;

    char str[100];

    printf("\nPlease enter a string:\t");

    gets(str);

    printf("\nPlease choose following options:\n");

    printf("1 = Encrypt the string.\n");

    printf("2 = Decrypt the string.\n");

    scanf("%d", &x);

    //using switch case statements

    switch(x)
    {

    case 1:

        for(i = 0; (i < 100 && str[i] != '\0'); i++)

            str[i] = str[i] + 3; //the key for encryption is 3 that is added to ASCII
value

        printf("\nEncrypted string: %s\n", str);

        break;

```

```

case 2:

    for(i = 0; (i < 100 && str[i] != '\0'); i++)

        str[i] = str[i] - 3; //the key for encryption is 3 that is subtracted to
ASCII value

    printf("\nDecrypted string: %s\n", str);

    break;

default:

    printf("\nError\n");

}

return 0;

}

```

### 2.8.1 Encriptado por Ransomware.

El ransomware es un software malicioso utilizado por los ciberdelincuentes para bloquear el acceso a un ordenador o sistema de red y cifrar sus datos. A continuación, se pide un rescate a la víctima para exponer los datos. El ransomware se distribuye a través de campañas de correo electrónico spam y ataques dirigidos, y se requiere un vector de ataque para detectar la presencia de ransomware en los puntos finales.

Una vez infectado, el malware suele obtener acceso al dispositivo y cifra todo el sistema operativo o determinados archivos. Tras el cifrado, se pide un rescate a la víctima. El atacante suele esperar entre 24 a 48 horas para recibir el rescate solicitado de lo contrario la información quedaría perdida para siempre sin manera de poderla recuperar.

La naturaleza del ransomware como amenaza y cómo funciona se destaca la necesidad de protegerse eficazmente contra el ransomware con un software de seguridad fiable. Mediante la aplicación de medidas de seguridad sólidas, las personas y las organizaciones pueden minimizar el riesgo de ser víctimas de ataques de ransomware y proteger los datos valiosos de la extorsión.

## **2.9 Virus de Computadora Históricos.**

Robert Thomas creó Creeper en 1971, un programa que se movía entre ordenadores asociados a ARPANET y mostraba el mensaje "I'm the creeper:

Captúrame si lo desea" para usarlo de manera de estudio y poder comprender como se desenvuelve un programa entre computadoras de escritorio en ese entonces.

Wealthy Skrenta desarrolló Elk Cloner en 1982, considerada la primera infección informática que se propagó fuera de un centro de investigación. Skrenta lo creó como un truco, contaminando los ordenadores Apple II de sus amigos a través de un divertimento en un disquete (OpenMind).

A pesar de que Cohen no fue el primero en crear una infección informática, su compromiso fue fundamental. Llevó a cabo una investigación académica única sobre el concepto, y la estructura de su programa informático antivirus sigue siendo completa hoy en día (Robert Slade, OpenMind).

Las primeras infecciones eran básicamente exhibiciones mecánicas con afán no malicioso. El programa de Cohen apuntaba al tiempo de dispersión del grado en lugar del asalto. Creeper pretendía crear una aplicación portátil que pareciera trasladarse a la máquina que alojaba la información en lugar de al interruptor (OpenMind).

El principal código nocivo, Brain, se desarrolló en 1986. Realizado por dos hermanos pakistaníes, se centraba en los clientes de programas

informáticos robados. Aunque suave en sus impactos, Brain incluía los datos de contacto de los autores para que los clientes influenciados buscaran un remedio. Se propagó a través de disquetes, conduciendo a la fundación de las empresas antivirus para empezar (OpenMind)

### **2.9.1 Mydoom.**

Mydoom, el brote de infección informática más terrible de la historia, causó daños evaluados en 38.000 millones de dólares en 2004, pero su peaje ajustado a la inflación es realmente de 52.200 millones de dólares. También conocido como Novarg, este malware es en realidad un "gusano" que se propaga por correo electrónico masivo. En un momento dado, la infección Mydoom era responsable del 25% de todos los correos electrónicos enviados.

### **2.9.2 Sobig.**

La infección informática Sobig 2003 es en realidad otro gusano. Su alcance es similar al de la infección Mydoom. La cifra que alcanzo es de 30.000 millones de dólares podría ser una suma de todo el mundo, contando Canadá, Reino Unido, Estados Unidos, Europa y Asia. Unas cuantas adaptaciones del gusano fueron descargadas en rápida progresión, denominadas Sobig.A a través de Sobig.F, siendo Sobig.F la más dañina.

Este programa cibercriminal se disfrazaba de programa informático auténtico y se unía a los correos electrónicos. Perturbó la emisión de billetes en Discuss Canada y la obstrucción de otras empresas incalculables. A pesar de su gran alcance daño, el fabricante nunca fue capturado.

### **2.9.3 Klez.**

Es posible que Klez ocupe casi el tercer puesto en la lista de las infecciones informáticas más extremadamente malas de la historia. Con unos 20.000 millones de dólares en daños evaluados, contaminó casi el 7,2% de todos los ordenadores en 2001, es decir, 7 millones de PC. El gusano Klez enviaba correos electrónicos falsos, falsificaba remitentes reconocidos y, entre otras cosas, se esforzaba por desactivar otras infecciones.



Al igual que otras infecciones y gusanos, Klez se descargó con algunas variaciones. Contaminaba los registros, se replicaba a sí mismo y se propagaba por todo el organigrama de cada víctima. Permanecía durante mucho tiempo, y cada forma era más dañina que la anterior.

#### **2.9.4 ILOVEYOU.**

La infección ILOVEYOU del año 2000 funcionaba enviando una falsa "carta de amor" que parecía un registro de contenido seguro. Al igual que Mydoom, este agresor enviaba duplicados de sí mismo a cada dirección de correo electrónico de la lista de contactos de la máquina contaminada. En un abrir y cerrar de ojos tras su descarga el 4 de mayo, se había extendido a más de 10 millones de PC.

La infección fue creada por un estudiante universitario de Filipinas llamado Onel de Guzman. Al faltarle tiendas, compuso la infección para obtener contraseñas que le permitieran iniciar sesión en administraciones en línea que necesitaba utilizar sin coste alguno. Supuestamente no tenía ni idea de lo lejos que se propagaría su creación. Esta infección se conoce también como Loveletter.

#### **2.9.5 WannaCry.**

La infección informática WannaCry de 2017 es un ransomware, una infección que se apodera de tu ordenador (o registros en la nube) y los mantiene prisioneros. El ransomware WannaCry destrozó ordenadores en 150 países, causando enormes problemas de eficiencia, ya que las empresas, los centros de salud y las organizaciones gubernamentales que no pagaron se vieron obligadas a renovar sus sistemas desde cero.

El malware se propagó rápidamente por 200.000 ordenadores de todo el mundo. Cesó cuando un analista de seguridad de 22 años del Reino Unido encontró la forma de desactivarlo. Los ordenadores con marcos de trabajo desactualizados fueron golpeados con especial dificultad. Por eso, los especialistas en seguridad sugieren continuamente revisar los marcos de trabajo habitualmente.

El ransomware atacó de nuevo en septiembre de 2020, posiblemente uno de los mayores ataques de infección informática de la historia terapéutica afectó a Widespread Wellbeing Administrations. La cadena de clínicas de Estados Unidos, que tiene más de 400 áreas, fue supuestamente golpeada por un ransomware dañino. El ataque limitó la cancelación de cirugías e hizo que los trabajadores de la salud cambiaran a los registros en papel.

## **Capítulo 3:**

### **Instalación y Programación**

En este capítulo vamos a mostrar los pasos que se deberán tomar y que características debe tener un equipo computacional para poder tener estas aplicaciones y poder aplicarlas con eficiencia.

#### **3.1 Características del Equipo.**

Para que un equipo pueda soportar el trabajo para este tipo de situación debe tener las siguientes características.

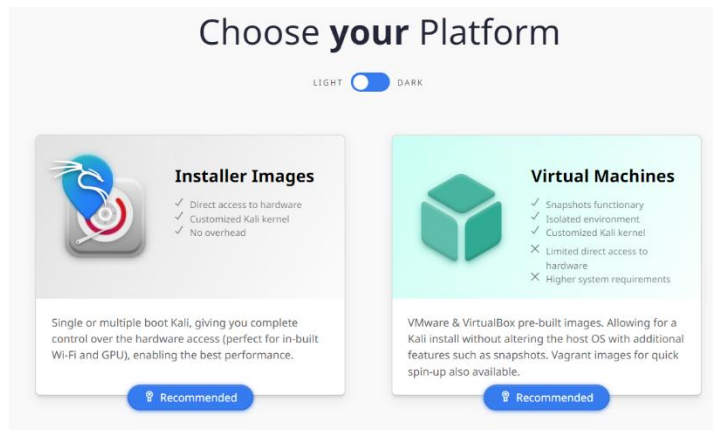
- **CPU:** procesador de i5 de 11 generación bitsx64
- **Espacio de almacenamiento:** 1 TERA o más
- **Memoria RAM:** 6 GB como mínimo para versión de escritorio y 16 GB recomendado
- **Tarjeta de red cableada** o Wi-Fi para las pruebas

Estas características pueden variar dependiendo del peso que vayas a poner en las actividades del equipo para ejecutar las actividades, pero por lo general serían las mínimas que debería tener el equipo para poder correr con facilidad lo que es la máquina virtual con la aplicación de escaneo de vulnerabilidades.

##### **3.1.1 Máquina Virtual Kali Linux.**

Para esta tesis vamos a usar esta aplicación de máquina virtual ya que viene con todos los paquetes necesarios y completos, esto nos permite tener todo tipo de alcances sin tener que estar buscando aditamentos adicionales.

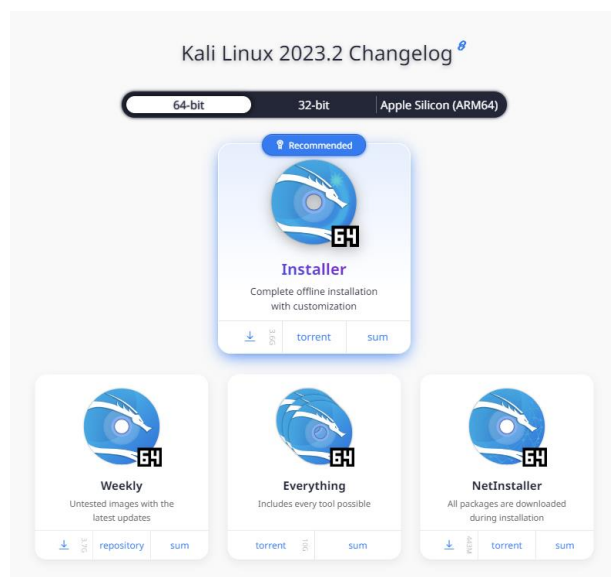
Figura 3. 1 página de descarga



Fuente(<https://www.kali.org/get-kali/#kali-platforms>)

En este caso como se está argumentando vamos a usar la versión completa que es la siguiente figura.

Figura 3. 2 Kali Linux 2023 de 10G



Fuente(<https://www.kali.org/get-kali/#kali-installer-images>)

Esta versión que es la que mantiene todas las herramientas para poder hacer las actividades que por lo general se hacen en todas las áreas computacionales como:

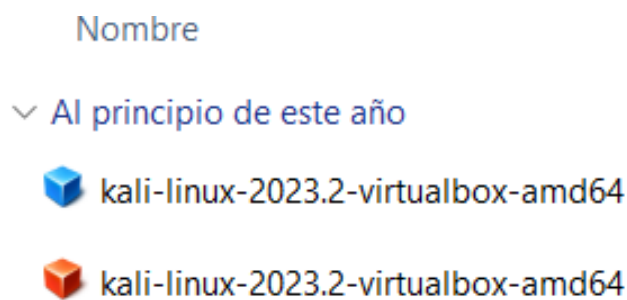
- Recopilación de información
- Análisis de vulnerabilidad

- Ataques inalámbricos
- Aplicaciones web
- Herramientas de explotación
- Pruebas de estrés
- Herramientas forenses
- Sniffing y Spoofing
- Ataques con contraseña
- Mantener el acceso
- Ingeniería inversa
- Herramientas de información
- Hacking de hardware

### 3.1 2 Instalación y Configuración de Kali Linux.

Al finalizar la descarga del archivo vamos a obtener lo que es un archivo WinRAR que contendrá el EXE del Kali Linux.

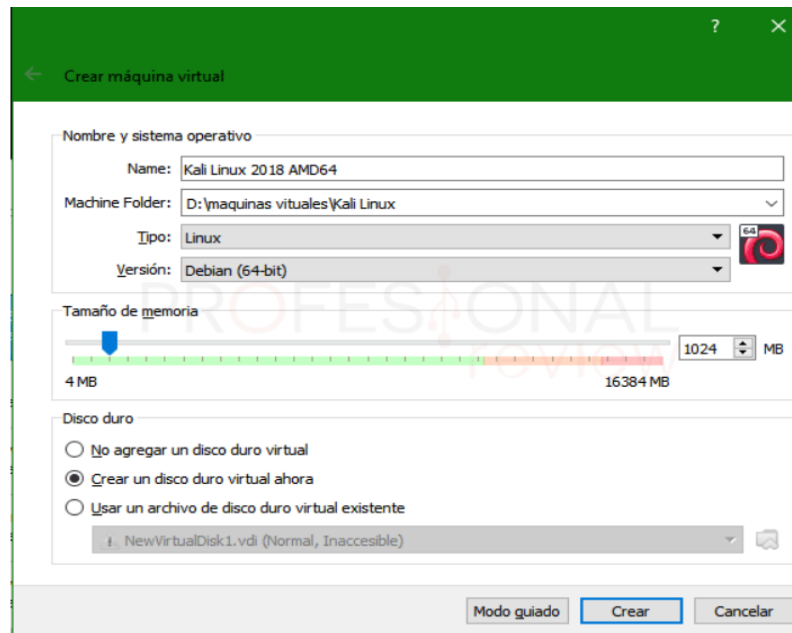
Figura 3. 3 Aplicación Máquina Virtual Kali Linux



Fuente (Equipo Personal)

Luego de iniciar los programas pasaremos a la ventana de configuración para poner las configuraciones que vayamos a usar como referencia sería mejor poner el modo experto para tener la todas las herramientas disponibles.

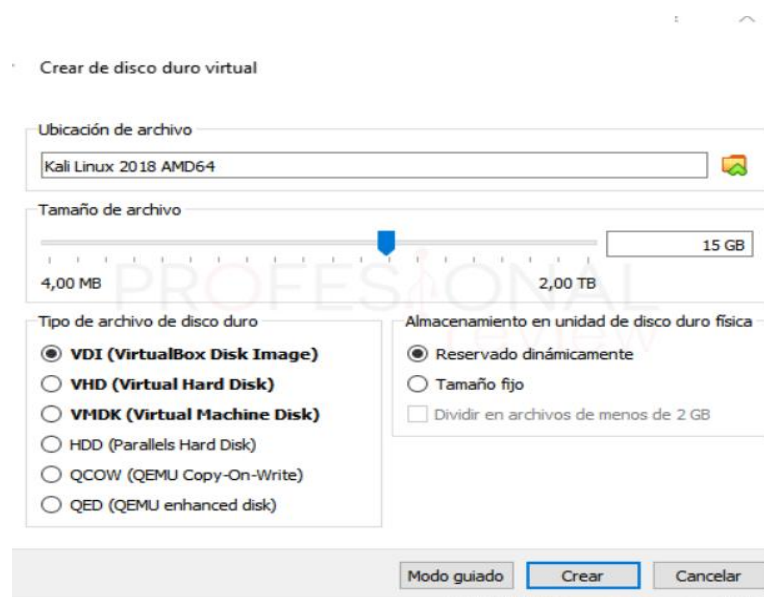
Figura 3. 4 Ventana de configuración de Máquina virtual



Fuente (Equipo Personal)

Ya ahora que tenemos puestas nuestras especificaciones para la creación de nuestra máquina virtual vamos a seleccionar el formato de disco duro que desearíamos ponerla dependiendo de la actividad que se hará.

Figura 3. 5 Selección de disco duro para la máquina virtual



Fuente (Equipo Personal)

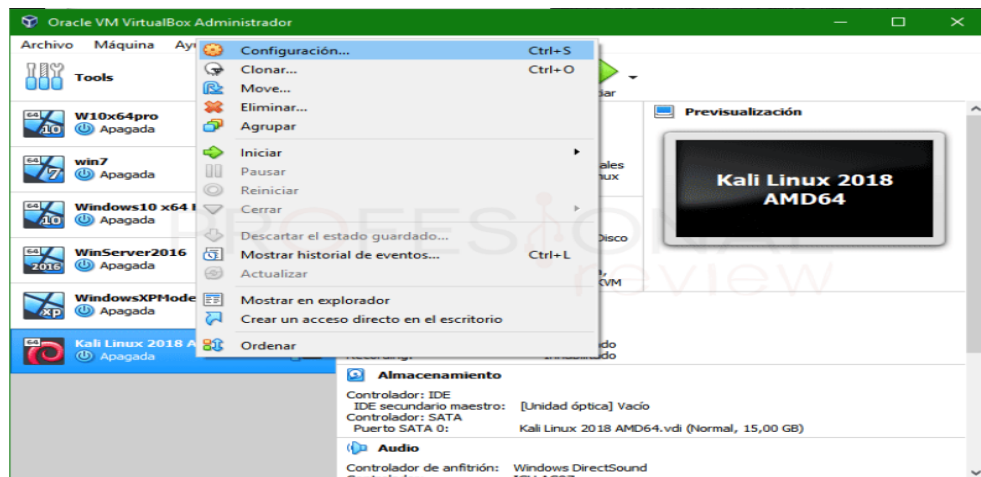
Como se observa en la imagen anterior vemos lo que es una variedad amplia de formas en las que podemos hacer uso de la partición o forma en la que va a generar el espacio proporcionado para la máquina virtual, nuestro caso vamos a usar 3 tipos que son los siguientes:

- **VDI (Imagen de Disco de Caja Virtual)** es la selección por defecto, es el sistema utilizado por Oracle VM VirtualBox, por lo que si no buscamos nada extravagante será la opción a elegir.
- **VMDK (Disco de Maquina de la Caja Virtual)** es el formato típico de VMWare (otro software de virtualización, semejante a VirtualBox). Se escogerá esta opción para contar con plena compatibilidad entre VMWare y VirtualBox y poder pasar sistemas operativos virtuales entre ambos softwares sin mayor problema.
- **VHD (Disco Duro Virtual)** es la opción a elegir si lo que queremos es crear un disco virtual versátil, que podamos recuperar cualquier archivo en su interior fácilmente. Se podrá utilizar como unidad de almacenamiento habitual y soporta particiones de todo tipo, como cualquier otro disco duro, además de varios usuarios por cada SO virtual instalado en él. Se utiliza sobre todo para Microsoft Virtual PC.

### **3.1.3 Inicio de máquina virtual.**

Una vez concluido con las configuraciones previas vamos a hacer lo que es la configuración principal de la máquina virtual en la que ahora seleccionaremos el sistema operativo que vamos a usar que por lo general son Windows y Linux que son los que nos permiten hacer configuraciones en Open Source.

Figura 3. 6 Ventana principal de la máquina virtual



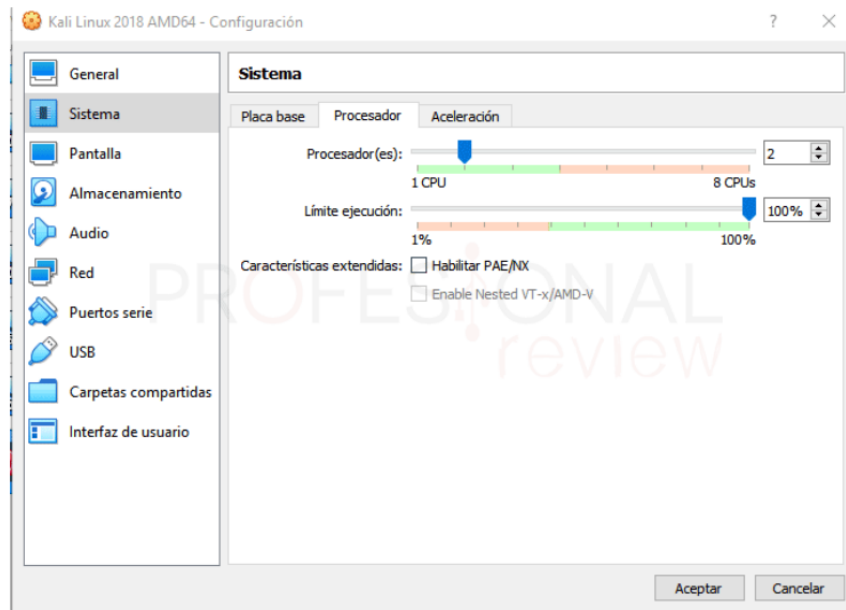
Fuente (Equipo Personal)

### 3.1.4 Uso de los núcleos del equipo.

En el apartado "Sistema" elegiremos el uso de dos núcleos del procesador, si tenemos más o queremos especificarlos todos, adelante. Obtendremos mayor velocidad si planeamos usar múltiples distribuciones.



Figura 3. 7 Ventana de Selección de núcleos

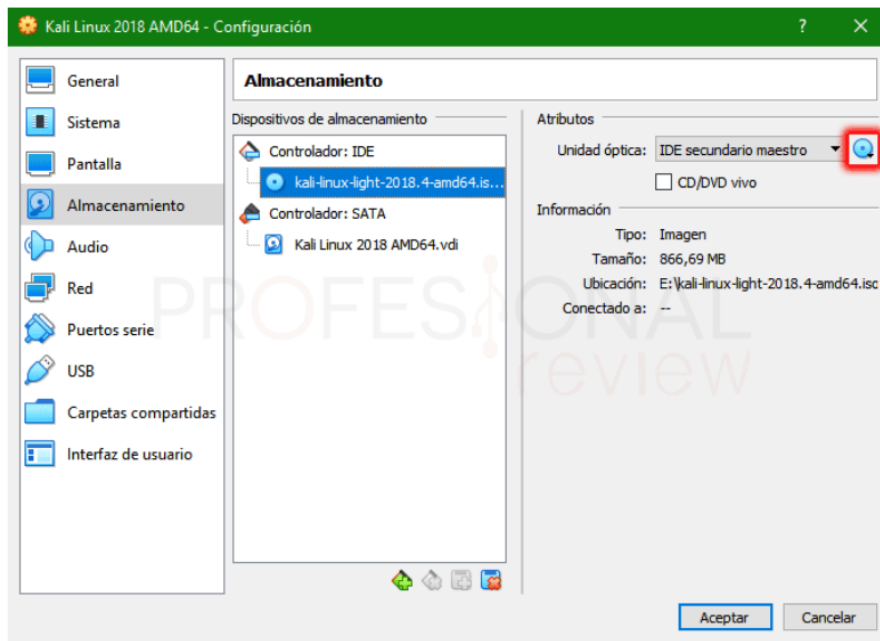


Fuente (Equipo Personal)

### 3.1.5 Almacenamiento.

Ahora iremos al apartado de Almacenamiento para seleccionar el tipo de almacenado que se usara dependiendo del tipo de descarga se o versión que se haya descargado.

Figura 3. 8 Ventana de Almacenamiento

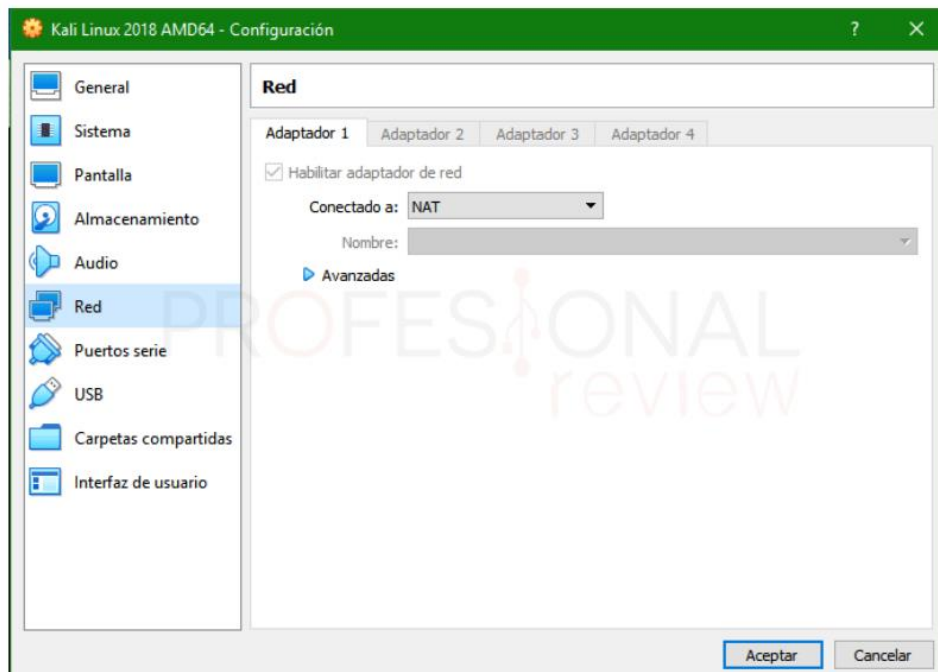


Fuente (Equipo Personal)

### 3.1.6 Configuración de Red.

En este apartado vamos a dejarlo tal como está, ya que en el modo que nos vota principalmente la instalación es en modo NAT, para poder tener internet a través de nuestro equipo en uso.

Figura 3. 9 Ventana de Red



Fuente (Equipo Personal)

### 3.2 Parrot aplicación de pruebas de infiltración.

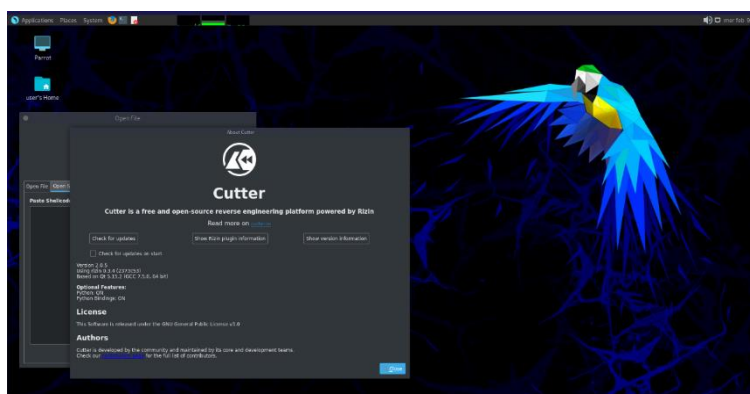
El marco está diseñado desde cero para ser seguro. Respaldo local para el cifrado de disco completo, voladura de revisiones rápidas de seguridad y un centro debían solidificado hace que el marco de la idealizar poner para almacenar información delicada.

Libre y de código abierto, y todo el código que alimenta el marco se hace accesible ya sea a través de nuestra tienda de programas Able o nuestros servidores GIT para que usted pueda examinar, personalizar y contribuir. Acceso gratuito al código que se ejecuta en tus dispositivos

#### 3.2.1 Instalación Parrot Security.

Para poder instalar esta aplicación en nuestro equipo iremos a la página principal para poder descargar el archivo y poder subirlo a nuestra máquina virtual ya antes instalada.

Figura 3. 10 Aplicación Parrot Security



Fuente (Equipo Personal)

Figura 3. 11 Ampliación Parrot en ISO

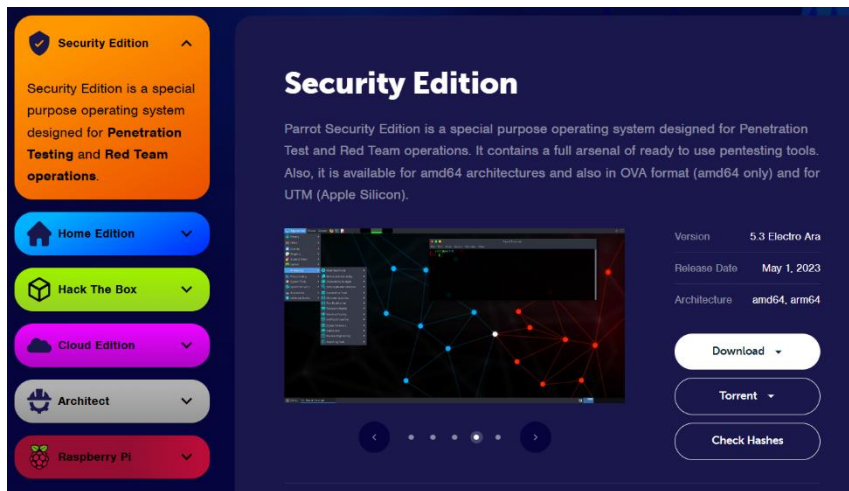
Nombre	Fecha de modificación	Tipo	Tam
Parrot OS	31/7/2023 22:07	Carpeta de archivos	
Parrot-security-5.3_amd64	31/7/2023 13:24	Archivo de image...	5.1

Fuente (Equipo Propio)

### 3.2.3 Instalación de Parrot en Máquina Virtual.

Al momento de entrar a la página principal de Parrot vamos a tener varias opciones o versiones para poder descargar, nosotros vamos a seleccionar la versión SECURITY EDITION ya que vamos a hacer un ataque de sombrero rojo en tiempo real.

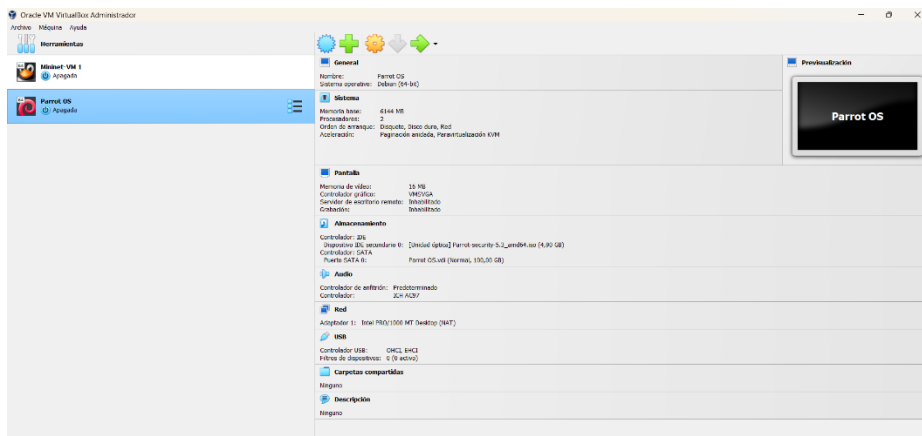
Figura 3. 12 Versión Security Edition Parrot



Fuente (Equipo Propio)

Una vez terminada la descarga del archivo abriremos nuestra máquina virtual para poder hacer la instalación del Parrot dentro de la maquina y poder realizar pruebas sin dañar nuestro propio equipo base.

Figura 3. 13 Parrot en Máquina Virtual Funcionando

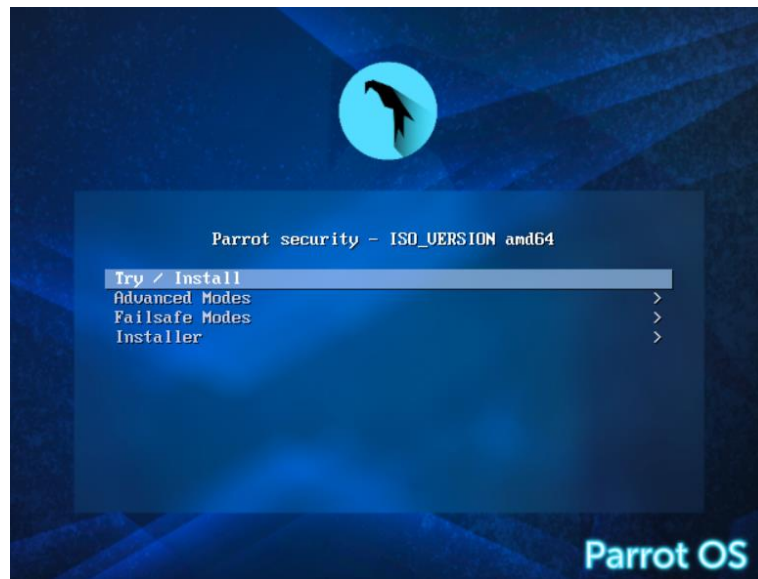


Fuente (Equipo Propio)

### 3.2.4 Configuración del Parrot en Virtual Box.

Al terminar de poner el ISO en la máquina virtual y darle una carpeta y espacio en el disco para trabajar vamos a abrir el programa en la máquina virtual para ahora si hacer las configuraciones necesarias y así nos permita acceder a su repertorio de herramientas.

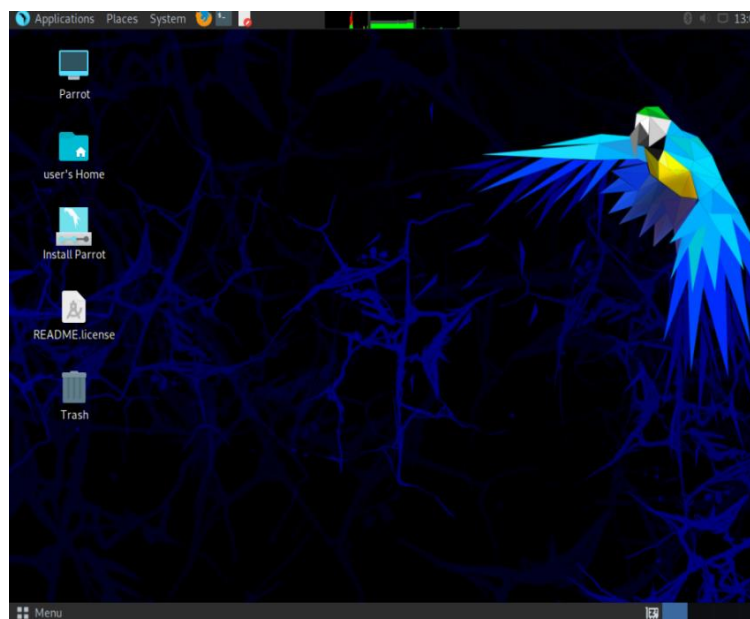
Figura 3. 14 Parrot en Máquina Virtual Instalador Grafico



Fuente (Equipo Propio)

Damos Enter en 'Try/ Instala' para poder comenzar con la instalación.

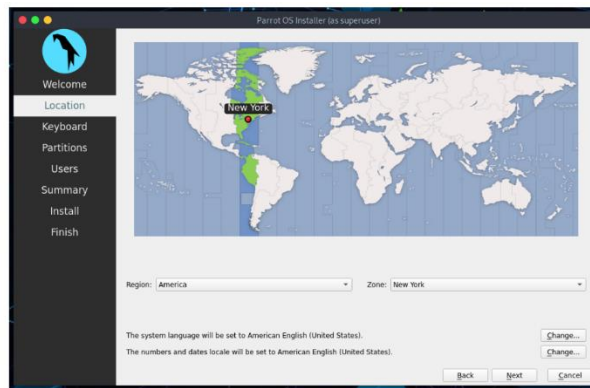
Figura 3. 15 Panel de Control del Parrot



Fuente (Equipo Propio)

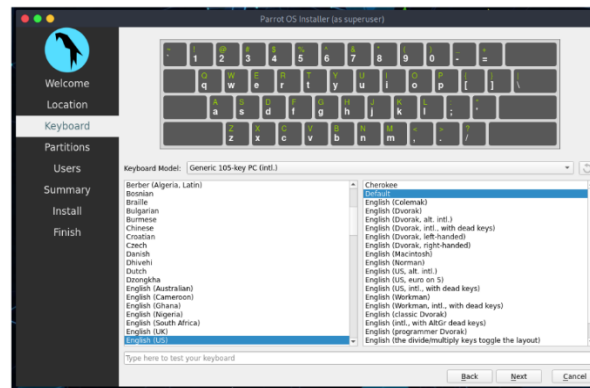
Una vez ya ingresado nos mostrará este panel donde iremos a la opción que se encuentra en la pantalla como 'Install Parrot' y comenzará a hacer la descarga de los archivos y nos pedirá indicarle la configuración que estaríamos deseando.

Figura 3. 16 Ventana de Selección de Región



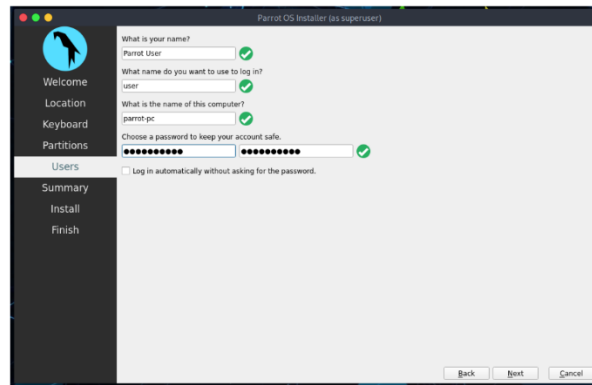
Fuente (Equipo Propio)

Figura 3. 17 Ventana de Selección de idioma del teclado



Fuente (Equipo Propio)

Figura 3. 18 Ventana de Creación de User y Password



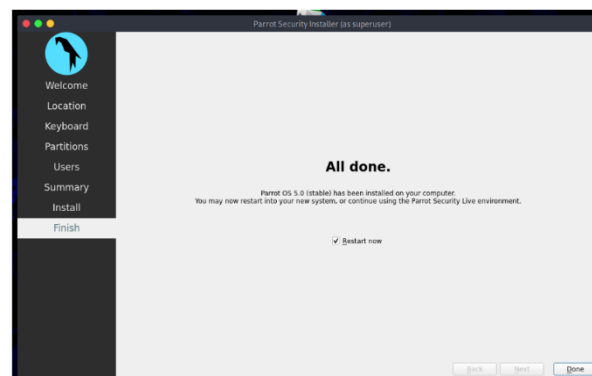
Fuente (Equipo Propio)

Figura 3. 19 Ventana final de descarga de controladores y herramientas



Fuente (Equipo Propio)

Figura 3. 20 Finalización de instalación



Fuente (Equipo Propio)

Una vez ya finalizado todo el proceso que nos pide y de haberle dado las configuraciones que necesitábamos para poder darle un ambiente decente a nuestro sistema Parrot vamos a reiniciar el equipo por completo para poder acceder a todo lo que se instaló.



## **Capítulo 4:**

### **Metodología y estudios del proyecto**

#### **4.1 Metodología analítica explicativa.**

La investigación o metodología es analítica y descriptiva por la forma en la que el problema se desarrolla y también se hará una demostración de lo explicado en esta investigación, en estos tipos de metodologías se busca aclarar y responder a las preguntas como, quien, donde y que.

#### **4.2 Características del área de estudio.**

La zona de estudio está situada tanto en el ambiente empresarial como en cualquier otra área que requiera de una suma protección de datos de suma importancia, esta puede ser una institución gubernamental, áreas militares, hasta el más mínimo y pequeño negocio ya que hoy en día estamos de pie a pie con la tecnología.

Una propuesta de ciberseguridad en el ámbito empresarial se centra en investigar y abordar los retos, peligros y oportunidades, específicos relacionados con la seguridad de los datos en el entorno empresarial. Estas son algunas de las características clave que puede encontrar en una propuesta de este tipo:

- **Enfoque empresarial:** La propuesta hará hincapié en la importancia de la ciberseguridad dentro del entorno comercial, apuntando a proteger la información comercial sensible, la propiedad intelectual, los datos de los clientes, los registros monetarios y otros recursos básicos.
- **Administración de riesgos:** La propuesta puede profundizar en las técnicas de evaluación de riesgos hechas a medida para las empresas, analizando el efecto potencial de los ciber-peligros en las operaciones, la reputación y la solidez monetaria de la organización.

- Coherencia del Comercio y Reacción ante Ocurrencias: La propuesta podría cubrir técnicas para mantener la progresión del comercio en medio de ocurrencias de ciberseguridad y la fundación de planes efectivos de reacción ante ocurrencias.
- Administración y enfoques de seguridad: La propuesta podría estudiar la creación de sistemas y enfoques de administración de la ciberseguridad vigorosos dentro de una empresa, garantizando que las medidas de seguridad estén suficientemente caracterizadas, actualizadas y mantenidas.
- Conciencia y preparación de la seguridad: Una propuesta de ciberseguridad centrada en la empresa podría destacar la importancia de preparar a los trabajadores en las mejores prácticas de ciberseguridad y crear una cultura consciente de la seguridad dentro de la organización.
- Administración de riesgos de terceros: Puede abordar los retos de supervisar los peligros de ciberseguridad planteados por terceros comerciantes y cómplices y proponer metodologías para moderar tales peligros.
- Investigación coste-beneficio: Analizar las compensaciones coste-beneficio de las especulaciones de ciberseguridad para las empresas, sopesando los costes de las medidas de seguridad frente a las posibles desgracias debidas a las brechas de seguridad.
- Sugerencias financieras: La proposición podría examinar los resultados financieros de los sucesos de ciberseguridad para las empresas, contando los impactos potenciales en los costes de las acciones, la cuota de escaparate y la creencia de los clientes.

- **Ciber-protecciones:** La propuesta puede abordar los beneficios y desafíos de las protecciones cibernéticas como instrumento de alivio de riesgos para las empresas.
- **Casos prácticos del sector:** La propuesta podría incorporar casos reales de incidentes de ciberseguridad y cómo reaccionaron las empresas ante ellos, extrayendo lecciones y buenas prácticas de estos encuentros.
- **Consideraciones éticas:** Atender a las sugerencias morales de los tonos de ciberseguridad dentro del entorno comercial, contando las preocupaciones de seguridad, el cuidado de la información y la franqueza.
- **Medidas de seguridad:** Analizar la viabilidad de las medidas de ciberseguridad mediante la utilización de medidas de ajuste y marcadores de ejecución.

#### **4.3 Cálculos de costo de cursos de ciberseguridad.**

Mientras que la mayoría de los expertos en ciberseguridad tienen como mínimo una licenciatura en informática, numerosas empresas se inclinan por candidatos que además tengan una certificación avalada y de grado superior o menciones en hackeo ético. Hay cientos de certificaciones disponibles, desde las comunes hasta las específicas de un proveedor, desde las de nivel básico hasta las avanzadas.

El avance del ser humano hace que cada día se vuelva a actualizar la base de conocimientos que uno debe tener en estas certificaciones por lo que estas certificaciones las de más alto nivel por lo general piden que hagas un examen de renovación para el título o mención que tengas, esto también nos hace entender que estar en estas áreas es un constante estudio y siempre viendo hacia el futuro.

Tabla 4.1 Certificaciones más frecuentes con sus costos.

Descripción	Precio total
CISSP (Profesional certificado en seguridad de sistemas de información)	749
CISA (Auditor certificado de sistemas de información)	760
Security+ (CompTIA Security+)	370
CEH (Certificado de Hacking Etico)	1199
CISM (Gestor certificado de seguridad de la información)	760
GSEC (Certificación de Seguridad Esencial)	2499
SSCP (Profesional certificado en seguridad de sistemas)	249
CASP (Profesional Avanzado de Seguridad)	466
GCIH (Gestor de incidentes certificado)	2499
OSCP (Profesional certificado en seguridad ofensiva)	999

#### 4.3.1 Certificación CISSP.

Para poder obtener la certificación CISSP de la organización de expertos en ciberseguridad (ISC) se encuentra entre las cualificaciones más solicitadas del sector. Obtener el CISSP demuestra que tiene experiencia en seguridad informática y que es competente en la planificación, ejecución y comprobación de un programa de ciberseguridad.

Esta certificación avanzada es para expertos en seguridad con experiencia que buscan progresar en sus carreras en partes como:

- Director de seguridad de datos - 181.529 dólares
- Presidente de seguridad - 61.655 dólares
- Construir la seguridad de TI - \$ 99.946
- Experto superior en seguridad - 108.379 dólares
- Investigador de afirmación de datos - \$85.083

Requisitos previos:

Para calificar y poder rendir el examen CISSP, necesitará cinco o mucho mas tiempo de experiencia de trabajo en al menos dos u ocho espacios de ciberseguridad. Estos incorporan la Seguridad y la Administración, Seguridad de Recursos, Ingeniería de Seguridad y Construcción, Comunicación y Seguridad, Personalidad y Llegar a la Administración, Evaluación de Seguridad y Pruebas, Operaciones de Seguridad, y la Seguridad de Mejora del programa informático.

#### **4.3.2 Certificado CISA.**

Para Esta certificación de la afiliación de expertos en TI ISACA marca la diferencia a la hora de ilustrar sus habilidades en el estudio de las vulnerabilidades de seguridad, la planificación y la actualización de los controles y el anuncio del cumplimiento. Es una de las certificaciones más reconocidas para las carreras en el examen de la seguridad cibernética.

El CISA está previsto para los expertos de TI de nivel medio que buscan progresar en ocupaciones como:

- Jefe de revisión de TI - 109.050 dólares
- Revisor de ciberseguridad - 77.583 dólares

- Investigador de seguridad de datos - \$83,109
- Constructor de seguridad informática - 99.946
- Jefe de extensión de TI - 94.137
- Supervisor del programa de cumplimiento - 91.915 dólares

Requerimientos:

Se requieren al menos cinco años de experiencia en revisión, control, seguridad o afirmación de TI o SI. Un título de dos o cuatro años puede sustituirse por uno o dos años de experiencia, por separado.

#### **4.3.3 Certificado Security+.**

Para CompTIA Security+ es una certificación de seguridad de nivel de entrada que aprueba las aptitudes centrales requeridas en cualquier parte de ciberseguridad. Con esta certificación, ilustrar su capacidad para estudiar la seguridad de una organización, la pantalla y la nube segura, portátil, y la web de las cosas (IoT) situaciones, conseguir que las leyes y los controles relacionados con el riesgo y el cumplimiento, y reconocer y reaccionar ante los episodios de seguridad.

Obtener tu certificación Security+ puede ayudarte en partes tales como:

- Director de área de trabajo de asistencia de oferta - \$80,298
- Diseño de seguridad - \$92,117
- Diseño de la nube - \$102,622
- Presidente de seguridad - \$61,655

- Evaluador informático - 74.108
- Diseñador de programas informáticos - \$88.568

Requerimientos:

Mientras que no hay necesidades estrictas para tomar el examen Security +, usted está facultado para ganar su certificación Organizar + para empezar y recoger al menos dos mucho tiempo de participación de TI con un centro de seguridad.

#### **4.3.4 Certificado CEH.**

El hacking ético, también conocido como hacking de sombrero blanco, entrence testing, o ruddy group, es el hackeo legal de organizaciones para emprender y revelar vulnerabilidades de algún tiempo antes de que lo hagan los actores nocivos. El EC-Council ofrece la certificación CEH Certificado de hackeo ético. Con el que podrá ilustrar sus capacidades en pruebas de entrada, descubrimiento de asalto, vectores y evasión.

La certificación CEH marca la diferencia a la hora de pensar como un programador y adoptar un enfoque más proactivo de la ciberseguridad. Considere esta certificación para ocupaciones como:

- Analista de infiltración - \$90.673
- Examinador de sucesos cibernéticos - \$62.445
- Examinador de perspectivas de riesgo - 101.393 dólares
- Modelador de seguridad en la nube - \$125.252
- Diseñador de ciberseguridad - \$91.933

Requisitos:

Usted será capaz de tomar el examen CEH en la remota posibilidad de que usted tenga dos o más años de experiencia de trabajo en seguridad de datos o en el caso de que el total de una preparación oficial de EC-Council.

#### **4.3.5 Certificación CISM.**

Con la certificación CISM, usted aprobará su dominio dentro del lado de la administración de la seguridad de datos, contando puntos como la administración, el avance del programa, y el programa, la ocurrencia, y la administración de riesgos.

Ocupaciones que utilizan el CISM incorporar:

- Supervisor IT - \$ 105.134
- Oficial de seguridad de marcos de datos - \$ 80.751
- Experto en peligro de datos - \$ 79.429
- Director de seguridad de datos - \$ 153.898
- Supervisor de administración de la información - 107.126 dólares

Requisitos previos:

Para exigir el examen CISM, se requiere un mínimo de cinco años o más en el are de administración de seguridad de datos.

#### **4.3.6 GSEC.**

Con esta certificación de la Worldwide Data Affirmation Certification (GIAC) es una credencial de seguridad de nivel de entrada para aquellos con algunos fundamentos en marcos de datos y organización. La obtención de



esta credencial aprueba sus aptitudes en tareas de seguridad como la defensa dinámica, organizar la seguridad, la criptografía, la reacción ocurrencia, y la seguridad de la nube.

Considere la posibilidad de tomar el examen GSEC en la remota posibilidad de que usted tenga un poco de conocimiento en TI y desea pasar a la seguridad cibernética. Las partes de trabajo que utilizan las habilidades ilustradas por el GSEC incorporan:

- Jefe de seguridad informática - 119.246 dólares
- Examinador científico informático - 76.419 dólares
- Analista de entrada - \$90,673
- Presidente de seguridad - 61.655
- Revisor informático - 74.108
- Diseño de avance de programas - \$128.410

Requisitos previos:

No hay requisitos previos particulares para exigir el examen GSEC. Prepárese para la victoria mediante la recopilación de algunos marcos de datos o la organización de la computadora encuentro para empezar.

#### **4.3.7 Certificación SSCP.**

Con esta certificación de seguridad media de (ISC), obtendrás las aptitudes para planificar, ejecutar y supervisar una base de TI segura. El examen pone a prueba la capacidad en llegar a los controles, la prueba de peligro reconocible y el examen, la organización de la seguridad, la reacción

ocurrencia, la criptografía, comunicaciones, marcos, y la seguridad de las aplicaciones.

El SSCP está diseñado para expertos en TI que trabajan de forma práctica con los marcos o recursos de seguridad de una organización. Esta credencial es adecuada para puestos como:

- Organizar el diseño de seguridad - \$ 107.889
- Presidente del marco - 78.885 dólares
- Creador de marcos - 111.721 dólares
- Examinador de seguridad - \$83,167
- Presidente de base de datos - \$84.034
- Experto en seguridad - \$106.486

Requisitos previos:

Los candidatos para el SSCP requieren al menos un año de trabajo remunerado en una o más de las regiones de pruebas. Esto podría cumplirse además con una licenciatura o maestría en un programa relacionado con la ciberseguridad.

#### **4.3.8 Certificación CASP.**

La certificación CASP está pensado para expertos en ciberseguridad que demuestran aptitudes avanzadas, pero necesitan seguir trabajando en innovación (en lugar de en administración). El examen cubre temas avanzados como el espacio de seguridad de la empresa, el examen de

riesgo, la ineficiencia del programa, la seguridad de la nube y las innovaciones de virtualización, y los métodos criptográficos.

El CASP puede abrir las aberturas para las partes progresado en la ingeniería, la administración de riesgos, y la integración de seguridad de la empresa. Títulos de trabajo concebibles incorporan:

- Diseñador de seguridad - \$126.281
- Diseño de seguridad - \$92,117
- Diseño de seguridad de aplicaciones - 119.261 dólares
- Investigador principal especializado - 101.493 dólares
- Investigador de indefensión - \$94.391

Necesidades:

No hay un prerrequisito formal para tomar el examen CASP. CompTIA sugiere que por así decirlo para expertos en seguridad cibernética con experiencia.

#### **4.3.9 Certificado GCIH.**

La obtención del GCIH prueba su comprensión de las operaciones hostiles, contando estrategias y vectores de asalto comunes y su capacidad para identificar, reaccionar y protegerse contra los asaltos. El examen de certificación abarca la gestión de incidentes, el examen de delitos informáticos, los usos indebidos de los programadores y los dispositivos de los programadores.

Esta certificación está dirigida a cualquier persona que trabaje en la reacción ante incidentes. Los títulos de trabajo podrían incorporar:

- Encargado de sucesos de seguridad - \$48,757.
- Planificador de seguridad - \$126,281
- Director del marco - \$78,885

Necesidades:

No hay requisitos previos formales para realizar el examen GCIH, a pesar del hecho de que es una gran idea tener una comprensión de las normas de seguridad.

#### **4.3.10 Certificación OSCP.**

El OSCP de Hostile Security ha terminado siendo una de las certificaciones más buscadas para los analistas de infiltración. El examen pone a prueba su capacidad para comprometer un arreglo de máquinas de destino utilizando numerosos pasos de uso indebido y entregar informes de prueba de entrada punto por punto para cada asalto.

El OSCP puede ser una gran opción para ocupaciones como:

- Analista de entrada - \$97,465
- Programador moral - \$105,548 dólares
- Analista de riesgos - \$57,612
- Examinador de seguridad de aplicaciones - \$96,140

Requisitos previos:

No hay requisitos previos formales para exigir el examen. Hostile Security sugiere el reconocimiento con la organización, Linux, Bash scripting, Perl o Python, así como la finalización del curso de Pruebas de Acceso con Kali.

#### **4.5 Referencias de Presupuesto.**

Para llevar a cada este estudio se tomó en referencia varios programas que podría ser utilizados para demostrar o explicar cómo funcionaría un ataque cibernético en tiempo real, para esto se hizo el estudio de las aplicaciones que podrían usarse en esta investigación:

Herramientas Opensource:

- Owasp zap
- Nikto
- Wapití
- W3af

Herramientas Privativas:

- Acunetix - \$4495 Versión estándar
- Netesparker - \$666 al mes
- Qualys - \$500 al mes

Teniendo en cuenta estas referencias y los costos, optamos como programa para nuestra explicación la aplicación Owasp zap que es una de las open source ya que nos permitirá ver de fondo los errores que una página web puede tener y no se pueden ver a simple vista

Esta aplicación también fue elegida por que dentro de nuestro marco de habilidades tenemos lo que es una dominación en los lenguajes para poder usarla y eso nos permite hacer uso de su totalidad.

## CONCLUSIONES Y RECOMENDACIONES

### Conclusiones

La ciberseguridad es de suma importancia para las empresas y organizaciones en la era informática. A medida que avanza la innovación, las empresas dependen cada vez más de una base avanzada, de la comunicación en línea y de la capacidad de información, lo que las hace impotentes ante una amplia gama de ciber-amenazas.

La ciberseguridad no es una opción, sino una necesidad crucial para que las empresas sobrevivan y prosperen en el escenario actual.

La creciente recurrencia y el avance de los ataques cibernéticos tienen el potencial de causar graves daños a la notoriedad de una organización, a su solidez financiera y a la confianza de sus clientes. Desde ataques de ransomware que pueden paralizar las operaciones hasta filtraciones de datos que descubren información delicada, los resultados de la falta de ciberseguridad pueden ser aniquiladores.

Además, a medida que el comercio mundial está más interconectado, la seguridad de la cadena de suministro y la administración de riesgos de terceros se han convertido en aspectos básicos de la ciberseguridad. Las empresas deben investigar y garantizar la seguridad de sus cómplices, vendedores y proveedores para evitar posibles vulnerabilidades que puedan ser mal utilizadas por artistas nocivos.

Por último, la importancia de la ciberseguridad va más allá de la protección de los recursos de la empresa. También se amplía a la defensa de la información y la seguridad de los clientes. Los clientes son cada vez más conscientes de los peligros relacionados con las fugas de información, y su confianza en la capacidad de una empresa para garantizar sus datos afecta específicamente a la reputación de la marca y a la fiabilidad de los clientes.

La ciberseguridad no es una extravagancia o un añadido para las empresas; es una parte indispensable de su metodología comercial. Las empresas que dan prioridad a la ciberseguridad y contribuyen con vigorosas medidas de seguridad ilustran su compromiso de garantizar a sus socios, mantener su notoriedad y asegurar la victoria a largo plazo en un panorama informático en constante evolución. A medida que los peligros cibernéticos avanzan, la necesidad de medidas de ciberseguridad sólidas se desarrollará, convirtiéndose en una necesidad continua para todas las empresas, en cualquier caso, de su estimación o industria.

## **Recomendaciones**

Para no sufrir de ataques o pérdidas de información sensible se recomienda que se tenga un área especializada en ciberseguridad o también se puede optar por la contratación de empresas externas encargadas a la preservación de información y que tienen los conocimientos indicados en esta área.

Capacitar al personal de todas las áreas sobre los errores que podrían llevar a generar un ataque o las falencias que podrían ocurrir a la hora de abrir algún correo malicioso o hasta una imagen de un número desconocido, ya que hoy en días existen muchas maneras que hasta desconocemos en las que nos podrían atacar de manera cibernética.

## Bibliografía

- Antonio, J. M. A. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciber-amenazas a la seguridad nacional y política exterior. Estudios Internacionales.
- Ciberseguridad, fundamental para la transformación digital. Edgar Parada Technical Solutions Manager - PDF
- Consultores, E. H. (2022, January 5). Red Team vs Blue Team vs Purple Team. - Ethical Hacking Consultores - Medium. Medium.
- Erickson, J. (2008, January). Hacking: The Art of Exploitation, 2nd Edition. O'Reilly Online Learning.
- Ferney, M. R. E. (2015, February 3). Hacking ético: una herramienta para la seguridad informática.
- Hacking ético con herramientas Python. (n.d.). Google Books.
- Hurel, L. M. (2023, April 1). La ceguera política de la ciberseguridad en Latinoamérica
- Kello, L. (2017). The virtual weapon and international order. Yale University Press.
- Kim, P. (2015). The Hacker Playbook 2: Practical Guide to Penetration Testing. Kim, Peter: 9781512214567 - AbeBooks.
- Klimburg, A., & Tirmaa-Klaar, H. (2021). Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU.
- Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. Kramer, S. Starr, L. Wentz (Eds.), Cyberpower and National Security (pp. 25-42). National Defense University Press.
- Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local.



- Revista Latinoamericana De Ingeniería De Software. 3(4), 161.
- Martín, P. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. Instituto Español de Estudios Estratégicos.
- Miessler, D. (2023, May 26). The difference between red, blue, and purple teams. Unsupervised Learning.
- Natalia, M. F. M. (2011). Análisis y estudio de los virus y antivirus informáticos del mercado local. Caso práctico elaboración de un virus que recopile la mayor cantidad de procesos que pueden causar daños en los computadores.
- Oluoha, O. U., Yange, T. S., Okereke, G., & Bakpo, F. S. (2021). Cutting Edge Trends in Deception Based Intrusion Detection Systems—A survey. *Journal of Information Security*, 12(04), 250–269.
- Paganini, P. (2017, October 6). Cyber Security: Red Team, Blue Team and Purple Team. Security Affairs.
- Penetration testing. (n.d.). Google Books.
- Phongchiewboon, A. (2018, July 1). Book review: Cybersecurity and Cyberwar: What Everyone needs to know. Retrieved from
- Pruna, F. X. J., Jeadá, P. V. Y., & Jumbo, J. L. C. (2020). Análisis de las características del sector microempresarial en Latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. *Revista Científica Ecociencia*, 7(1), 1–26.
- Security, N. (2023). What is Threat Hunting and how it can benefit your organisation? Nucleon Security
- Seguridad informática. (n.d.). Google Books.
- Steve Winterfeld, Jason Andress | Perlego. (2012, December 28). [PDF] The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in

Theory and Practice. Perlego.

Subramanian, J. (2023, February 12). RISE with SAP: 'Defense in Depth' Security Architecture with SAP S/4HANA Cloud, public edition. SAP Blogs

Taylor, C. (2022). Purple Team. CyberHoot.

Threat Modeling Tools: A Taxonomy. (2022, August 1). IEEE Journals & Magazine | IEEE Xplore.

What is encryption? Data encryption defined | IBM. (n.d.).

Zeadally, S. (2014a). Special issue on Cybersecurity, Cybercrime, Cyberwar. Journal of Homeland Security and Emergency

Zorz, Z. (2020, May 28). The impact of threat hunting on your security operations - Help Net Security. Help Net Security.



Presidencia  
de la República  
del Ecuador



Plan Nacional  
de Ciencia, Tecnología,  
Innovación y Saberes



**SENESCYT**

Secretaría Nacional de Educación Superior,  
Ciencia, Tecnología e Innovación

## DECLARACIÓN Y AUTORIZACIÓN

Yo, **Borja Hernández, Donald Stefano** con C.C: # 0926072679 autor del Trabajo de Integración Curricular: **Estudio de las Threats Tools y la Ciberseguridad en las empresas**, previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

**Guayaquil, 7 de agosto del 2023**

f. \_\_\_\_\_

Nombre: **Borja Hernández, Donald Stefano**  
C.C:0926072679



Presidencia  
de la República  
del Ecuador



Plan Nacional  
de Ciencia, Tecnología,  
Innovación y Saberes



SENESCYT

Secretaría Nacional de Educación Superior,  
Ciencia, Tecnología e Innovación

## REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

### FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Estudio de las Threats Tools y la Ciberseguridad en las empresas.		
AUTOR(ES)	Borja Hernández, Donald Stefano		
REVISOR(ES)/TUTOR(ES)	Ing. Efraín Oswaldo Suarez Murillo, MGs		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	06 de septiembre del 2023	No. DE PÁGINAS:	70
ÁREAS TEMÁTICAS:	Internet de las cosas, Protocolos de información, Tarjetas de desarrollo.		
PALABRAS CLAVES	Ciberseguridad, Virus Computacionales, Vulnerabilidades.		
RESUMEN/ABSTRACT (150-250 palabras):	<p>En este proyecto de investigación tiene como punto principal dar a demostrar la importancia que tienen los conocimientos de las herramientas de amenazas cibernéticas y de la ciber-seguridad que nos rodea en la actualidad, esta investigación no solo busca mostrarles el amplio abanico que existe en las amenazas cibernéticas, sino como se podrían prevenir si se usaran las herramientas adecuadas para encontrar las fallas tanto humanas como de los software y hardware que se emplean en este ambiente, otro de los puntos a exponer son de los Virus computacionales más usados que han amenazado a la sociedad computacional a lo largo de los años tanto nuevos como los más viejos, también vamos a centrarnos en las vulnerabilidades que tiene los Switcher, Router's y otros equipos electrónicos en general que usen puertos de conexión Ethernet, Bluetooth, Infrarrojo, USB de todos los tipos, conexiones LAN, entre otras. Se utilizará información de ataques que han ocurrido en tiempo real, también demostraremos mediante esquemas cómo funcionan los ataques. Al concluir se dará una explicación de por qué es importante invertir en un área especializada en la protección de datos cibernéticos en la compañía.</p>		
ADJUNTO PDF:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
CONTACTO CON AUTOR/ES:	Teléfono: +5939954785412	E-mail: <a href="mailto:donald.borja@cu.ucsg.edu.ec">donald.borja@cu.ucsg.edu.ec</a>	
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	Nombre: Ricardo Xavier Ubilla González	Teléfono: +593-99-952-8515	
	E-mail: <a href="mailto:ricardo.ubilla@cu.ucsg.edu.ec">ricardo.ubilla@cu.ucsg.edu.ec</a>		
<b>SECCIÓN PARA USO DE BIBLIOTECA</b>			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			