# CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

CARLOS EDUARDO DONOSO RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

OCTUBRE

2023

# CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

CARLOS EDUARDO DONOSO RAMIREZ

Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team

Director De Curso:

JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

OCTUBRE

2023

**CONTENIDO**

## LISTA DE FIGURAS

## LISTA TABLAS

## GLOSARIO

BLUETEAM: Equipo encargado de defender la infraestructura y sistemas de una organización contra amenazas cibernéticas.

CIBERSEGURIDAD: Conjunto de medidas y prácticas destinadas a proteger sistemas, redes y datos contra amenazas cibernéticas, 5, 7, 8, 12, 13, 14, 15, 16, 17, 18

FIREWALLS: sistema o dispositivo diseñado para proteger una red o un sistema informático al controlar y filtrar el tráfico de datos que entra y sale de la red., 11

HACKING ÉTICO: práctica de utilizar las habilidades y conocimientos de un hacker para identificar y resolver vulnerabilidades y debilidades en sistemas, 9

PURPLE TEAM: Enfoque que combina las capacidades de RedTeam y BlueTeam para mejorar la seguridad cibernética., 5, 7, 8, 10, 11, 14, 17

REDTEAM: Equipo especializado en simular ataques cibernéticos para identificar debilidades de seguridad., 5, 7, 8, 9, 10, 12, 14, 16

## RESUMEN

Este informe técnico tiene la finalidad de suministrar estrategias de contención mediante el análisis de riesgos y vulnerabilidades en la infraestructura TI, proporciona un análisis de las estrategias RedTeam y BlueTeam aplicadas en el contexto de la ciberseguridad, con un enfoque en su integración para crear un equipo Purple Team, se presentan políticas de seguridad y recomendaciones destinadas a fortalecer la postura de la seguridad cibernética de la organización. El presente informe se basa en el estudio realizado en diferentes etapas ejecutadas del seminario



**Palabras clave: RedTeam, BlueTeam, Purple Team.**

# INTRODUCCIÓN

En la era digital actual, la ciberseguridad se ha convertido en una prioridad para todas las organizaciones, debido a la creciente cantidad de amenazas cibernéticas, el presente informe tiene como finalidad examinar en detalle estrategias de contención y análisis de riesgo implementando estrategias RedTeam y BlueTeam, con la finalidad de realizar una integración con enfoque Purple Team, concluir con el seminario de investigación donde se abarco la parle legal y ética que debe portar un profesional en ciberseguridad, de igual manera, proyectar los resultados del ataque simulado a la organización Hacker House y el protocolo ejecutado para la contención del ataque informático proporcionar políticas de seguridad y recomendaciones para el fortalecimiento de la ciberseguridad dentro de la organización y se enfatizará la importancia de la inversión en ciberseguridad.

# 1. OBJETIVOS

## 1.1 OBJETIVO GENERAL

Presentar resultados de las estrategias de contención establecidas mediante el análisis de riesgo contemplados bajo las estrategias RedTeam y BlueTeam en el contexto de la ciberseguridad, proponer políticas y recomendaciones para fortaleces la seguridad en las organizaciones.

## 1.2 OBJETIVOS ESPECÍFICOS

- Informar aspectos relevantes de las actividades ejecutadas, como leyes establecidas para la protección de datos y contención de ataque informático
- Resumen de actividades para la intrusión de seguridad en Hacker House
- Explorar las ventajas de la integración de equipos en un enfoque Purple Team y presentar mejores prácticas para su implementación.
- Diseñar políticas de seguridad efectivas, abordar áreas críticas como el acceso, la gestión de parches y actualización, la evaluación de riesgos y la concientización del personal.

# 2. DESARROLLO DEL TRABAJO

## 2.1 ASPECTOS ÉTICOS, LEGALES Y DESARROLLO ATAQUE SIMULADO BAJO UN AMBIENTE CONTROLADO EMPRESA HACKER HOUSE

Dentro del desarrollo de las 4 etapas del seminario se entablo ejercicios para desarrollar la estrategia en los equipos RedTeam y BlueTeam, comenzando con el análisis de documentación para la validación del cumplimiento de las normas legales establecidas en Colombia para la protección de datos, “leyes 1273 de 2009[1] y 1581[2] de 2012”, como la importancia del código de ética en la ejecución de la ingeniería. Se evidenciando inconsistencias en documento de confidencialidad, haciendo énfasis en la violación de los artículos 269A “acceso abusivo a sistemas informáticos”, 269C “interceptación de datos informáticos” los cuales pueden incurrir en el pago de100 a 1.000 SMMLV y la pena de prisión de 36 a 72 meses, dentro del documento se incumple la Ley 1581 de 2012 encargada de regular a las organizaciones mediante la superintendencia de industria y comercio, en donde se visualiza la sustracción de información de manera ilegal y sin consentimiento del titular. Figura1

[1] (senado, 04) senado Secretaria de Ley 1273 de 2009 [En línea] // secretaria de senado. - 2023 de 08 de 04. - http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.
[2] (Publica, 2012) Publica Funcion Ley 1581 de 2012 [En línea] // Funcion Publica. - 18 de 10 de 2012. - https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

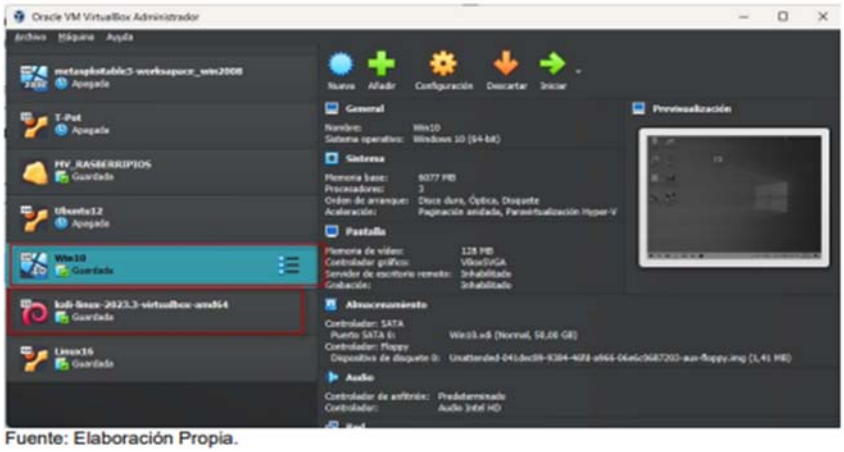
*Figura 1 Irregularidad contrato de confidencialidad.*

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación ilegal de información, accesos abusivos a sistemas informáticos".

Fuente: Anexo 3 – Acuerdo

Al demostrar las irregularidades que se presentaron el documento, se procede a realizar un caso de practica en ambiente controlado, donde se puede iniciar a evidenciar el desarrollo de estrategias RedTeam y BlueTeam, para esta puesta se procedió con una prueba de intrusión de seguridad a la empresa Hacker House en una maquina objeto, mediante las herramientas Virtual Box[3] y Kali Linux[4] en donde se procede a ejecutar un ambiente seguro, aislado y controlado. Para este momento se aprecia la intervención del equipo RedTeam utilizando la herramienta Virtual Box con la que se preparara la imagen de Windows 10 como maquina objetivo. Sobre esta también se realizará la instalación de la imagen de Kali Linux (equipo atacante).

*Figura 2 Instalación VirtualBox*



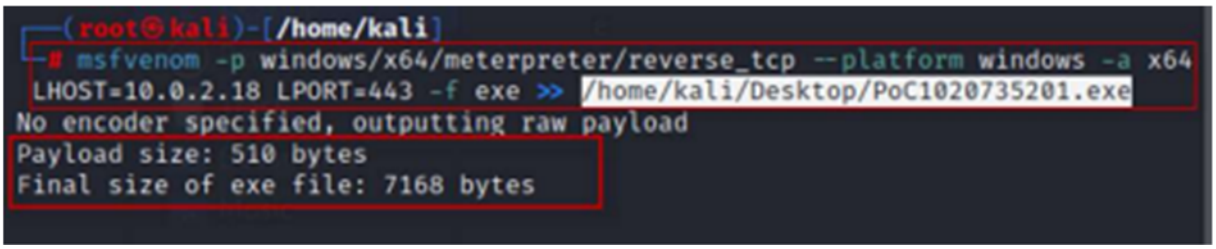

Fuente: Elaboración Propia.

[3] (ORACLE VM)Hipervisor VirtualBox [página web]. [Consultado el 5 septiembre de 2023]. Disponible en Internet:

[4] (KALI LINUX)Penetration Testing and Ethical Hacking Linux Distribution. Kali Linux [página web]. [Consultado el 28 agosto de 2023]. Disponible en Internet: .

Para realizar el escaneo de red se implementó la herramienta Legion[5] que se encuentra preinstalada en Kali Linux encontrando que equipos son vulnerables para proceder con el ataque, en este caso la IP10.0.2.17 fue a la que se le practico el ejercicio de intrusión, con el sistema operativo Windows 10. Dentro del ejercicio se utilizó Msfvenom, herramienta preinstalada en Kali Linux, la cual nos permite generar Payload (cargas maliciosas), con el fin de vulnerar una plataforma especifica.

*Figura 3  Creación de Payload con msfvenom*




Fuente: Elaboración propia

Al ejecutar se crea un archivo .exe. el cual es utilizado para la infección del equipo víctima, para el laboratorio se implemento el Exploit Meterpreter[6] con Hendler (Herramienta que permite mantener una conexión activa y modo escucha contra la victima)

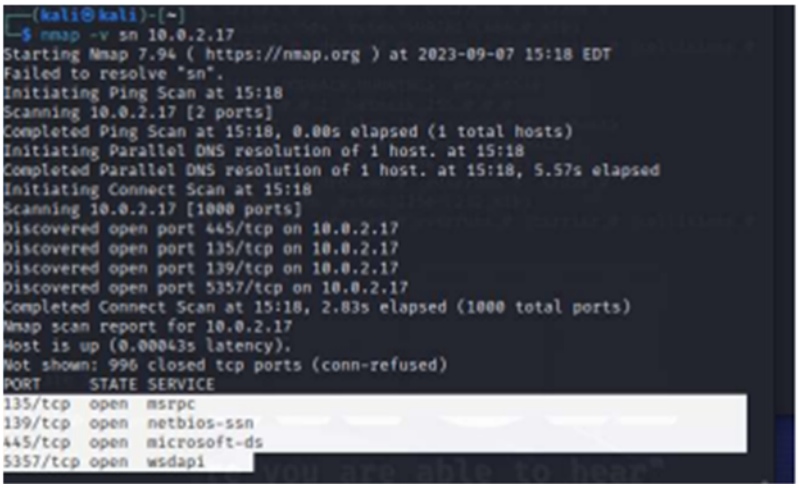
[5] (LEGION) Kali Linux Tools [Anónimo]. Kali Linux [página web]. [Consultado el 10, septiembre, 2023]. Disponible en Internet:
[6] (METASPLOIT) Penetration Testing Software, Pen Testing Security | Metasploit. Metasploit [página web]. [Consultado el 2, septiembre, 2023]. Disponible en Internet

*Figura 4 Metasploid*


Fuente: Elaboración propia

Desde nuestro equipo Kali Linux se realizó el uso de la herramienta Legion creando la carga útil mediante Msfvenom, con la dirección del cliente Kali Linux (10.0.2.18), esto con la finalidad de abrir una conexión remota para poder acceder a la información del pc. Con Legion (que hace uso de comandos de Nmap6 para el escaneo), también se puede determinar que puertos tiene abiertos este equipo.

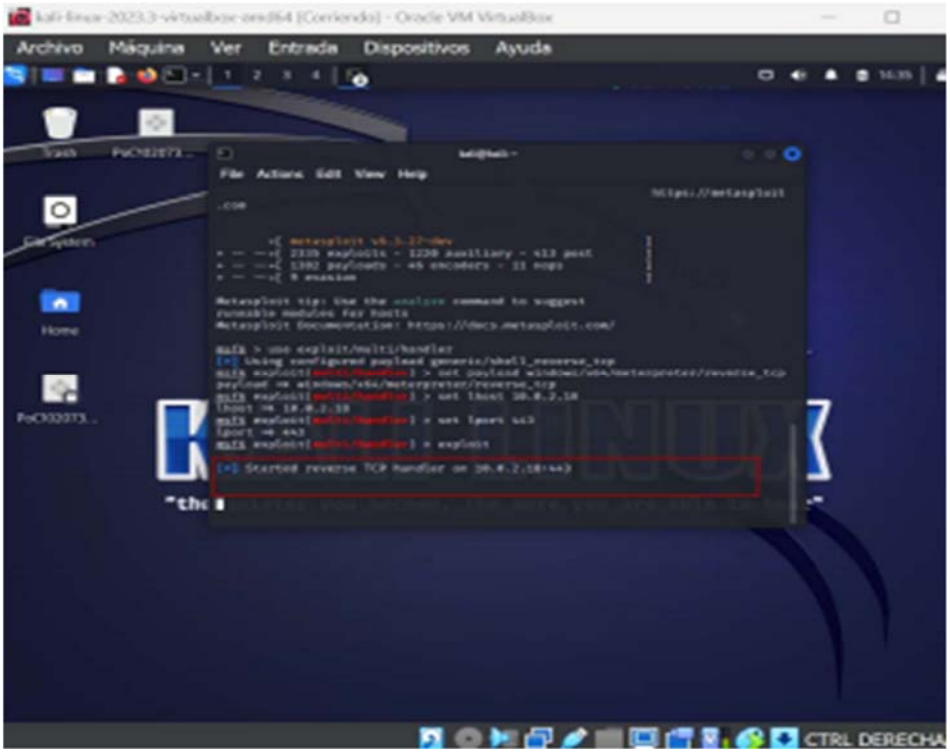
*Figura 5 Puertos abiertos Windows10*




Fuente: Elaboración propia

Luego de tener los datos para generar la carga útil mediante Metasploid generamos el Payload (.exe), que será compartido mediante WhatsApp Web. Una vez descargado el archivo .exe y ejecutado en el pc, se procede a ejecutar Metasploid desde Kali Linux, usaremos Hendler para determinar si tenemos conexión con la maquina “victima” mediante el puerto 443.

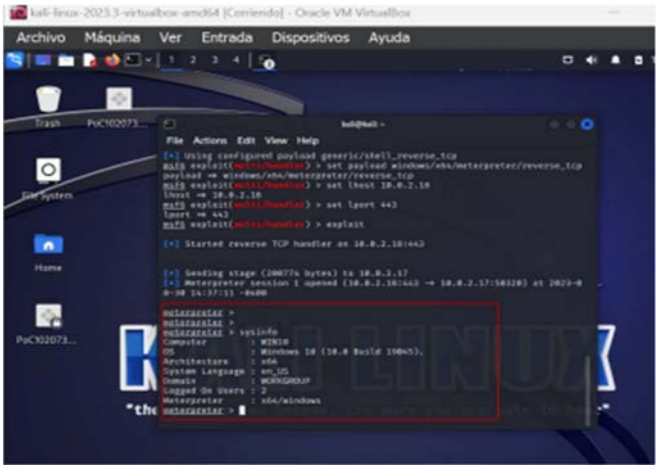
*Figura 6 Ejecucion Metasploid*




Fuente: Elaboración propia

La misma herramienta nos da la confirmación que la conexión hacia la maquina objetivo se encuentra en línea y podemos realizar la ejecución de comandos mediante Meterpreter, mediante este Payload podremos ejecutar tareas de forma remota desde nuestro equipo.

*Figura 7 Conexión remota*




Fuente: elaboración propia

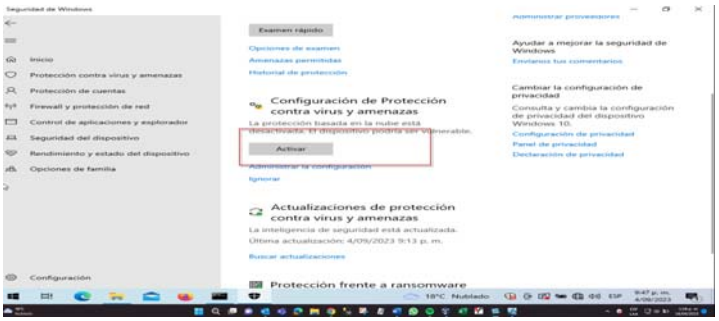
El ataque perpetrado se generó por una falta de sistemas de seguridad, que lograran evitar la ejecución del programa descargado desde WhatsApp Web, el programa al ser ejecutado de forma inconsciente por el administrador del equipo genero una conexión remota a un equipo atacante que se encuentra dentro de la misma red, al estar ejecutándose en modo silencioso o desatendido, el usuario no percibe que existe dicha conexión, adicional que tiene todos los privilegios sobre el equipo víctima para poder ejecutar cualquier tarea remota. Gracias a las diferentes herramientas que existen en la web se puede realizar un análisis detallado del ataque de ciber seguridad del que fue objeto la compañía, esto nos permite ver como se realizó y como impacto a la compañía, con la finalidad de tomar acciones para evitar que algo así se pueda volver a presentar.

Para subsanar el sistema que se vio comprometido en el ejercicio anterior debido al evento Payload visualizado en las máquinas virtuales, se llevan a cabo los siguientes pasos:

- Paso numero 1: Como primera medida de seguridad el equipo se debe aislar de la red corporativa, eliminarlo del dominio de red o desconectarlo de la red corporativa, con la finalidad de evitar riesgo de propagación.

- Paso numero 2: Una vez el equipo se encuentre aislado de la red, se debe realizar la verificación i/o activación del servicio de antivirus, una vez activado el servicio de antivirus se debe realizar un análisis en busca de virus o programas potencialmente malignos para el sistema.

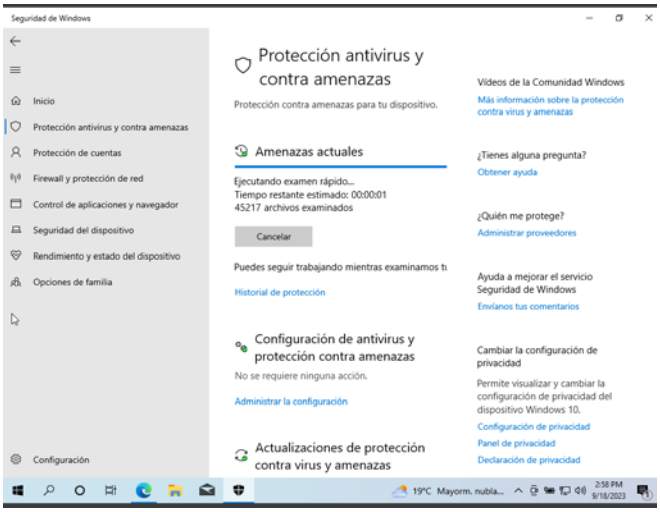
*Figura 8 Activación de antivirus*




Fuente: Elaboración propia

Se realizó un análisis del equipo en el cual se detectó y elimino él .exe que se encontraba en descargas del equipo, lo que imposibilita que equipo sea controlado de forma remota desde el equipo atacante.

*Figura 9 Escaneo de equipos*

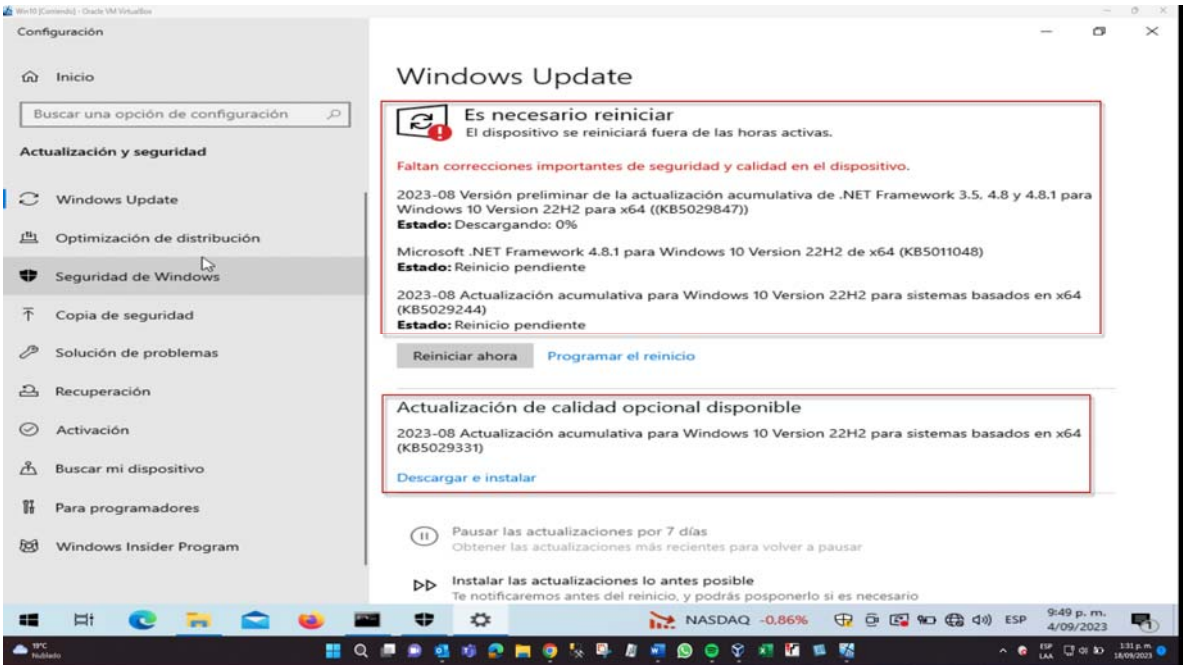



Fuente: Elaboración propia

Paso numero 3: Realizar la verificación del Firewall de Windows, si se encuentra activo o no, el Firewall se encontraba desactivado en el pc, se realizó la activación del Firewall para red de dominio, red privada y red local, lo que permite que el equipo pueda activar las defensas contra ataques por red.

Paso numero 4: Realizar la actualización del sistema operativo, aplicar los parches de seguridad disponibles, esto nos permite minimizar los riesgos de ataque y subsana las vulnerabilidades detectadas del sistema operativo, lo que en muchas ocasiones permite eliminar brechas de seguridad

*Figura 10 actualizaciones de S.O.*

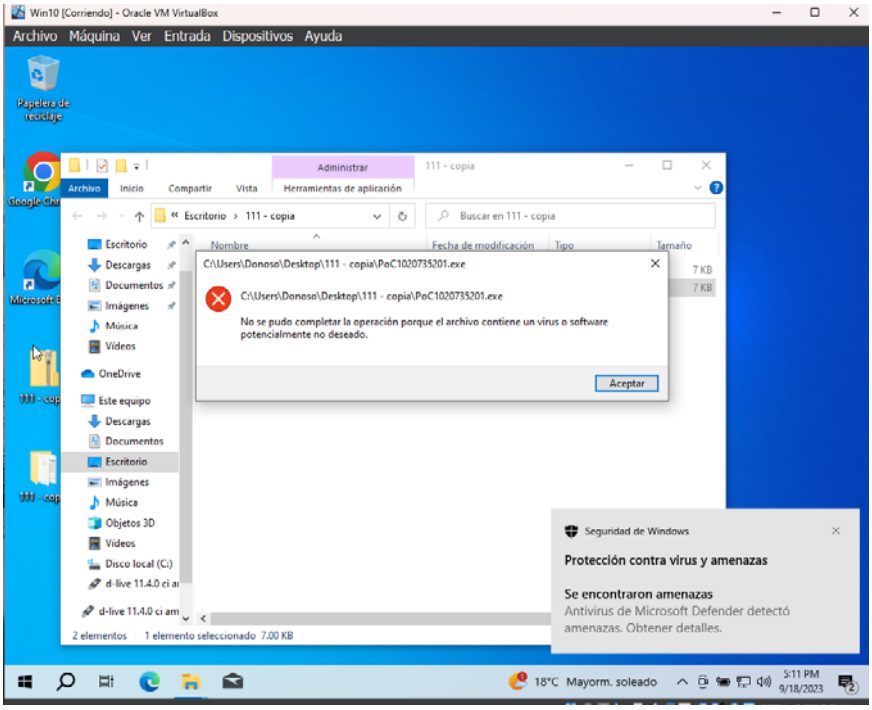



Fuente: Elaboración propia

Paso numero 5: Una vez realizada la verificación que todos los mecanismos de defensa se encuentran activos, procedemos a realizar un intento de ejecución del archivo .exe que fue creado desde Kali Linux para determinar si el antivirus es capaz de detectarlo e inhabilitarlo, Como recomendaciones generales se puede realizar una refinación de roles y permisos, para eliminar la posibilidad que un usuario estándar pueda ejecutar

programas .exe dentro de los equipos de la compañía, lo mismo que realizar el control de las descargas que se realicen de internet. Esto ayuda a aumentar la seguridad del dispositivo, es recomendable mantener un control en la red de los equipos que se encuentren conectados: Network Access Control (NAC), en español control de acceso a la red, para que solo aquellos usuarios y equipos autenticados mediante el dominio de red puedan acceder a la red corporativa, esto nos ayuda a eliminar la posibilidad de recibir ataques desde la misma red. De igual manera es recomendable realizar la implementación de un IDS (sistema de detección de intrusos), para detectar conexiones sospechosas y realizar el bloqueo antes que puedan acceder a algún equipo de la red.

*Figura 11 Bloqueo del archivo malicioso*




Fuente: Elaboración propia

## 2.2 ¿DE QUÉ MANERA PUEDEN APORTAR EN EL CAMPO DE LA CIBERSEGURIDAD LA INTEGRACIÓN DE EQUIPOS BLUE TEAM, RED TEAM Y PURPLE TEAM AL MISMO TIEMPO DENTRO DE UNA ORGANIZACIÓN?

Purple Team[7] es una filosofía que busca la colaboración y aprendizaje continuo entre los equipos RedTeam y BlueTeam, su enfoque está basado en la transparencia y la mejora continua de las prácticas de seguridad. Esta integración fomenta la colaboración, el intercambio de conocimiento y la alineación de objetivos, para la integración exitosa de Purple Team es requerido una comunicación abierta, una estructura organizativa adecuada y una revisión constante de los resultados, por ellos, las reuniones regulares de revisión y la documentación son esenciales.

Los beneficios que son ofrecidos al integrar los equipos son:

- Postura de seguridad mejorada
- Rutas de ataque cerradas
- Respuesta eficaz a incidentes
- Gestión de riesgos mejorados
- Inteligencia de amenazas mejorada

Tabla 1 Función de Equipos

| EQUIPO | FUNCION |
|---|---|
| Blue Team | Centrado en la defensa y seguridad de una organización, su objetivo principal es proteger los sistemas, redes y datos de ataques informáticos. Trabajan en diseño implementación y mantenimiento de medidas de seguridad, entre ellas |

[7] (esecurityplanet, 2023)

| | |
|---|---|
| | encontramos firewalls, sistemas de detección de intrusos y políticas de seguridad. |
| Red Team | Cuentan con un enfoque ofensivo, el objetivo es simular ataques cibernéticos y evaluar la actividad de las defensas de seguridad, los Red Teamers se encargan de identificar vulnerabilidades y debilidades en los sistemas. |
| Purple Team | Es una combinación de Blue Team y Red Team, en donde el objetivo es facilitar la colaboración entre ambos equipos, forman un equipo en donde evalúan la seguridad de la organización, el Purple Team coordina ejercicios de seguridad, comparte información y mejora la capacidad de respuesta. |

En la implementación de un equipo de Purple Team[8] lograremos realizar las siguientes actividades:

- Realizar ataques de ingeniería social
- Lanzamiento de malware y ataques de errores contra sistemas críticos
- Intento en la explotación de vulnerabilidades
- Pruebas de penetración del sistema
- Auditorias de seguridad de sistemas y redes
- Desarrollo e implementación de plan de seguridad integral
- Análisis regulares de vulnerabilidades
- Cifrar datos en reposo y transito
- Restricción de acceso a datos y sistemas confidenciales
- Monitoreo tráfico de red, verificando actividades sospechosas
- Implementación de sistemas de detección, prevención de intrusos

[8] (coursera, 2023)

Como se observa cada una de estas actividades se ven reflejadas en las actividades de los equipos RedTeam y BlueTeam, que al juntarse los profesionales de cada área entran en un enfoque colaborativo para la mejora en la ciberseguridad.

## 2.3 PLANTEE POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES PARA MEJORAR LOS ASPECTOS DE CIBERSEGURIDAD EN CUALQUIER ORGANIZACIÓN EN SUS ENTORNOS T.I

De acuerdo a lo visto en el transcurso del seminario se pueden plantear las siguientes políticas de ciberseguridad[9], las cuales permiten tomar medidas a la seguridad de sus sistemas informáticos, esto implica capacitar a todo el personal sobre la ciberseguridad y procediendo con simulaciones de ataques a la organización. Entre las políticas podemos incluir:

- Políticas de acceso[10]:

  Se deben establecer para limitar el acceso a sistemas y datos solo a personas autorizadas, implementando autenticación de doble factor y controles de acceso basados en roles
- Gestión de parches y actualizaciones[11]:

[9] (WATCH&ACT, 2023) WATCH&ACT [En línea] // POLÍTICAS DE CIBERSEGURIDAD EN LAS EMPRESAS: CÓMO IMPLEMENTARLAS. - 25 de 09 de 2023. - https://watchandact.eu/politicas-de-ciberseguridad/#:~:text=Las%20pol%C3%ADticas%20de%20ciberseguridad%20son,riesgos%20que%20amenazan%20a%20estas..

[10] (ibm, 2022) ibm [En línea] // Políticas de control de acceso. - 07 de 12 de 2022. - https://www.ibm.com/docs/es/sva/10.0.5?topic=administration-access-control-policies.

[11] (IBM, 2023) ibm [En línea] // ¿Qué es la gestión de parches?. - 25 de 09 de 2023. - https://www.ibm.com/es-es/topics/patch-management.

La gestión de parches y actualizaciones es crucial para abordar vulnerabilidades conocidas, estableciendo procesos para la aplicación oportuna de parches de seguridad tanto para los firmwares como software.

- Evaluación de riesgos y plan de continuidad[12]:

  La organización debe llevar periódicamente evaluaciones de riesgo con el fin de identificar y mitigar posibles amenazas, lo que significa la identificación de otras preocupaciones para la organización relacionadas con sus activos de información críticos, debe contar con un plan de continuidad de negocio para mantener la operación en caso de algún evento de ciberseguridad

- Concientización y capacitación en seguridad[13]:

  La concientización y capacitación en seguridad son esenciales para involucrar a todo el personal en las mejores prácticas de ciberseguridad, enfatizando en la prevención de ataques de ingeniería social los cuales ocurren con frecuencia y por la cual las organizaciones se ven más vulnerables en la protección de sus sistemas informáticos. Estas se definen en una serie de prácticas y estrategias causando un impacto positivo a la organización.

- Herramientas de monitoreo y detección:

  La implementación de herramientas de monitoreo y detección de amenazas permite una respuesta más rápida a los incidentes de seguridad. Encontramos variedad en herramientas para la implementación de ataques informáticos, como Suricata[14], fail2ban[15], etc.

- Plan de respuesta a incidentes:

[12] (welivesecurity, 2022) welivesecurity Miguel Angel Mendoza [En línea] // 8 pasos para la evaluación de riesgos de ciberseguridad de una empresa (parte II). - 13 de 12 de 2022. - https://www.welivesecurity.com/la-es/2022/12/13/8-pasos-evaluacion-de-riesgos-2/.

[13] (Protect, 2023) Jorge Garcia Martinez [En línea] // Plan de concientización en ciberseguridad: Importancia y buenas prácticas. - 11 de 09 de 2023. - https://www.deltaprotect.com/blog/concientizacion-ciberseguridad.

[14] (SURICATA, 2023) SURICATA [En línea] // Observar, proteger, adaptar. - 09 de 10 de 2023. - https://suricata.io/.

[15] (fail2ban, 2023) fail2ban.org [En línea]. - 19 de 10 de 2023. - https://www.fail2ban.org/wiki/index.php/Main_Page.

Contar con un plan de respuesta a incidentes bien definido y probado es crucial, esto permite una acción coordinada en caso de ataques cibernéticos.

# 3. CONCLUSIONES

La inversión en la ciberseguridad es un aspecto crítico para garantizar la protección de los activos, datos y la continuidad de las operaciones de una organización. Basándonos en las etapas ejecutadas a lo largo del seminario, podemos extraer las siguientes conclusiones que orientan aspectos importantes en cuanto a la necesidad de inversión en ciberseguridad:

- Riesgos cibernéticos en constante evolución, dentro del ejercicio evaluado para este seminario, se destaco la naturaleza en constante evolución de las amenazas cibernéticas, visualizando la rápida adaptación de los atacantes a nuevas técnicas y vulnerabilidades, en donde se subraya la necesidad de contar con recursos y tecnologías actualizadas para enfrentar las amenazas.
- Valor de la evaluación proactiva, la implementación en estrategias RedTeam & BlueTeam demostró la importancia de una evaluación proactiva de la seguridad, la capacidad de identificar y mitigar vulnerabilidades antes de que sean explotadas.
- Integración de equipos para una defensa más robusta, la integración de equipos en un enfoque Purple Team se evidencia en un enfoque efectivo para mejorar la colaboración y capacidad de respuesta ante ataques cibernéticos. Esto resalta la necesidad de invertir en la capacidad y desarrollo de habilidades de los equipos de seguridad.
- Políticas y procedimientos sólidos, las políticas de seguridad implementadas en conjunto con los procedimientos bien definidos son el cimiento de una ciberseguridad efectiva.
- Educación y concientización continua, la capacitación del personal en seguridad cibernética son aspectos primordiales para prevenir amenazas internas, como se observo en el ejercicio, la inversión en programas de formación y en la promoción

de una cultura de seguridad pueden llegar a reducir y mitigar el riesgo de incidentes.

- Herramientas y tecnologías de monitore, al implementar herramientas de monitoreo y detección de amenazas nos demuestra un resultado esencial para identificar y responder rápidamente a incidentes. Esta inversión a soluciones de seguridad avanzada es fundamental para mitigar daños en la continuidad de la organización y cumplimiento en la seguridad de datos evitando posibles sanciones y multas legales.

Concluyendo la inversión a la ciberseguridad es fundamental para mantener la competitividad y la integración de una organización en un entorno digital seguro, el cual está en constante evolución, tanto en herramientas efectivas como en cibercrímenes.

# 4. RECOMENDACIONES

Para finalizar este informe se realizan las siguientes recomendaciones:

- Promover una cultura de seguridad en toda la organización
- Mantener al día con las tendencias y amenazas cibernéticas
- Evaluar y mejorar continuamente las políticas y procedimientos de seguridad
- Asignar recursos adecuados para la ciberseguridad
- Fomentar la colaboración y la comunicación entre equipos de seguridad, RedTeam, BlueTeam, Purple Team y Equipos de respuesta a incidentes.

## BIBLIOGRAFÍA

**coursera** coursera [En línea] // What Is the Purpose of the Purple Team?. - 22 de 09 de 2023. - https://www.coursera.org/articles/purple-team.

**esecurityplanet** Kaye Timonero [En línea] // Red Team vs Blue Team vs Purple Team: Differences Explained. - 22 de 02 de 2023. - https://www.esecurityplanet.com/networks/red-team-vs-blue-team-vs-purple-team/#:~:text=Simulation%20(BAS)%20Vendors-,6%20Benefits%20of%20Using%20Red%2C%20Blue%2C%20and%20Purple%20Teams,scanning%20and%20testing%20for%20vulnerabilities..

**fail2ban** fail2ban.org [En línea]. - 19 de 10 de 2023. - https://www.fail2ban.org/wiki/index.php/Main_Page.

**ibm** ibm [En línea] // Políticas de control de acceso. - 07 de 12 de 2022. - https://www.ibm.com/docs/es/sva/10.0.5?topic=administration-access-control-policies.

**IBM** ibm [En línea] // ¿Qué es la gestión de parches?. - 25 de 09 de 2023. - https://www.ibm.com/es-es/topics/patch-management.

**KALI LINUX** KALI LINUX [En línea] // | Penetration Testing and Ethical Hacking Linux Distribution. - 28 de 08 de 2023. - https://www.kali.org/.

**LEGION** KALI LINUX [En línea] // Kali Linux Tools. - 10 de 09 de 2023. - https://www.kali.org/tools/legion.

**METASPLOIT** METASPLOIT [En línea] // Penetration Testing Software, Pen Testing Security. - 2 de 09 de 2023. - https://www.metasploit.com.

**ORACLE VM** ORACLE VM [En línea] // Hipervisor VirtualBox. - 05 de 09 de 2023. - https://www.virtualbox.org/.

**Protect Delta** Jorge Garcia Martinez [En línea] // Plan de concientización en ciberseguridad: Importancia y buenas prácticas. - 11 de 09 de 2023. - https://www.deltaprotect.com/blog/concientizacion-ciberseguridad.

**Publica Funcion** Ley 1581 de 2012 [En línea] // Funcion Publica. - 18 de 10 de 2012. - https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

**senado Secretaria de** Ley 1273 de 2009 [En línea] // secretaria de senado. - 2023 de 08 de 04. - http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

**SURICATA** SURICATA [En línea] // Observar, proteger, adaptar. - 09 de 10 de 2023. - https://suricata.io/.

**WATCH&ACT** WATCH&ACT [En línea] // POLÍTICAS DE CIBERSEGURIDAD EN LAS EMPRESAS: CÓMO IMPLEMENTARLAS. - 25 de 09 de 2023. - https://watchandact.eu/politicas-de-ciberseguridad/#:~:text=Las%20pol%C3%ADticas%20de%20ciberseguridad%20son,riesgos%20que%20amenazan%20a%20estas..

**welivesecurity** Miguel Angel Mendoza [En línea] // 8 pasos para la evaluación de riesgos de ciberseguridad de una empresa (parte II). - 13 de 12 de 2022. - https://www.welivesecurity.com/la-es/2022/12/13/8-pasos-evaluacion-de-riesgos-2/.