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

WILFREDO VALDERRAMA ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

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

WILFREDO VALDERRAMA ROJAS

JOHN FREDDY QUINTERO TAMAYO
Tutor de Seminario

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

Resumen

Durante la Etapa 5 del seminario especializado sobre Equipos Estratégicos en Ciberseguridad (Red Team & Blue Team), se exploraron las conclusiones y recomendaciones clave que orientan la inversión en ciberseguridad organizacional. Se resaltó la evolución constante de las amenazas cibernéticas y la necesidad de una inversión continua en tecnología y capacitación para proteger los activos digitales de una organización.

Se hizo hincapié en la importancia de la prevención de amenazas cibernéticas a través de soluciones proactivas, como firewalls avanzados y sistemas de detección de intrusiones, para evitar ataques antes de que ocurran. Además, se destacó la relevancia de la detección temprana y la respuesta rápida a incidentes como elementos cruciales para minimizar el impacto de los ataques.

La formación y concienciación de los empleados se identifican como aspectos críticos de la ciberseguridad, ya que muchos ataques se originan en prácticas de usuario descuidadas. También se subrayó la importancia del cumplimiento normativo para evitar sanciones financieras y daños a la reputación de la organización.

Por último, se resaltó que la alta dirección debe estar consciente de la importancia de la ciberseguridad y estar dispuesta a invertir en ella para respaldar las iniciativas de seguridad en toda la organización.

En conclusión, la Etapa 5 enfatizó la necesidad de una inversión estratégica en ciberseguridad, abordando la evolución de las amenazas, la prevención, la detección temprana, la formación, el cumplimiento normativo y la conciencia de la alta dirección como elementos clave en la protección de las organizaciones contra las amenazas cibernéticas en constante cambio.

Palabras claves: Evolución de amenazas, Prevención, Detección temprana, Respuesta a incidentes, Formación de empleados, Cumplimiento normativo, Alta dirección, Ciberseguridad.

ÍNDICE

Pág.

LISTA DE ILUSTRACIONES

Pág.

GLOSARIO

ATAQUE DE DDOS: Un ataque de denegación de servicio distribuido (DDoS) implica inundar un sistema o red con tráfico malicioso desde múltiples fuentes para sobrecargarlo y hacer que sea inaccesible.

AUTENTICACIÓN MULTIFACTORIAL: La autenticación multifactorial es un método de seguridad que requiere más de una forma de autenticación antes de permitir el acceso, como una contraseña y un código de verificación enviado al teléfono móvil del usuario.

CIFRADO: El cifrado es el proceso de codificar datos para que solo las partes autorizadas puedan leerlos. Se utiliza para proteger la confidencialidad de la información.

COPIAS DE SEGURIDAD (BACKUPS): Las copias de seguridad son duplicados de datos importantes que se almacenan fuera del sistema principal para su recuperación en caso de pérdida de datos debido a un ataque o un fallo del sistema.

DETECCIÓN DE INTRUSIONES: La detección de intrusiones implica monitorear y analizar el tráfico de red o los registros del sistema en busca de actividades sospechosas que puedan indicar un ataque.

FIREWALL: Un firewall es una barrera de seguridad que se utiliza para proteger una red de amenazas externas, controlando y filtrando el tráfico de datos.

INGENIERÍA SOCIAL: La ingeniería social es una técnica en la que los atacantes manipulan psicológicamente a las personas para que revelen información confidencial o realicen acciones específicas.

MALWARE: El malware es un término general para software malicioso, que incluye virus, gusanos, troyanos y otros programas diseñados para dañar o comprometer sistemas informáticos.

PARCHE DE SEGURIDAD: Un parche de seguridad es una actualización de software diseñada para corregir una vulnerabilidad o un fallo de seguridad en un programa o sistema operativo.

PHISHING: El phishing es una técnica de ingeniería social en la que los atacantes intentan engañar a las personas para que revelen información confidencial, como contraseñas o información financiera, haciéndose pasar por una entidad de confianza.

RANSOMWARE: El ransomware es un tipo de malware que cifra los archivos de una víctima y exige un rescate para descifrarlos y restaurar el acceso.

SEGURIDAD DE LA RED INALÁMBRICA (WI-FI): Se refiere a las medidas de seguridad implementadas para proteger las redes inalámbricas de accesos no autorizados, como el uso de contraseñas fuertes y cifrado.

VULNERABILIDAD: Una vulnerabilidad es una debilidad en un sistema informático que podría ser explotada por un atacante para comprometer la seguridad.

1. INTRODUCCIÓN

La creciente interconexión de sistemas y la dependencia de la tecnología en las organizaciones han abierto nuevas oportunidades, pero también han dado lugar a un aumento en las amenazas cibernéticas. La constante evolución de estas amenazas exige una inversión continua en tecnología y recursos humanos especializados para mantenerse al día y proteger los activos digitales de las organizaciones[1].

La ciberseguridad se ha convertido en una prioridad crítica para cualquier entidad que utilice sistemas de tecnologías de la información (TI) para operar y almacenar datos confidenciales. Los ataques cibernéticos pueden tener un impacto devastador en la integridad, disponibilidad y confidencialidad de la información, lo que puede resultar en pérdidas financieras significativas y daños a la reputación de la organización[2].

En este contexto, la prevención de amenazas cibernéticas se vuelve esencial. Para lograrlo, es necesario invertir en soluciones proactivas, como firewalls avanzados, sistemas de detección de intrusiones y programas de concienciación en seguridad, para evitar ataques antes de que ocurran. Además, la detección temprana y la respuesta rápida a incidentes son cruciales para minimizar el impacto de los ataques[3]

La formación y concienciación de los empleados son aspectos críticos de la ciberseguridad, ya que muchos ataques se originan a través de prácticas de usuario descuidadas. Por lo tanto, las organizaciones deben invertir en programas de formación para reducir el riesgo de ataques relacionados con el factor humano.

Además, la inversión en tecnologías avanzadas, como soluciones de Seguridad de la Información y Eventos de Seguridad (SIEM) y Detección y Respuesta Extendida (XDR), es esencial para mantenerse al día con las amenazas emergentes. Cumplir con las normativas y regulaciones de seguridad cibernética también se ha convertido en una inversión necesaria para evitar sanciones financieras y daños a la reputación[4].

Finalmente, la alta dirección debe estar consciente de la importancia crítica de la ciberseguridad y estar dispuesta a invertir en ella. Esta concienciación es esencial para respaldar y priorizar las inversiones necesarias en ciberseguridad en toda la organización. En este contexto, esta investigación se enfocará en abordar cómo la

---

[1] SANJUAN, L. Criptografía. Seminario – Seguridad en desarrollo del Software, 1-34. 2014. http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Crip?sequence=1

[2] ARROYO GUARDEÑO, D. GAYOSO MARTÍNEZ, V. & HERNÁNDEZ ENCINAS, L. Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. 2020. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

[3] EURPOL. Ciberseguridad: amenazas principales y emergentes. (27 de enero de 2022). https://www.europarl.europa.eu/news/es/headlines/society/20220120STO21428/ciberseguridad-amenanzas-principales-y-emergentes

[4] Microsoft. Definición de SIEM. 2023. https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

integración de equipos Blue Team, Red Team y Purple Team, junto con la formulación de políticas y recomendaciones adecuadas, puede respaldar la ciberseguridadnética y justificar la inversión necesaria en este campo en constante evolución[5].

[5] Marrero, Y. La Criptografía como elemento de la seguridad informática. ACIMED, 11(6). 2003. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012#:~:text=La%20Criptograf%C3%ADa%20es%20una%20disciplina,protecci%C3%B3n%20de%20sus%20documentos%20electr%C3%B3nicos.

2. OBJETIVOS

2.1. OBJETIVOS GENERAL

Formular estrategias efectivas de contención de amenazas cibernéticas mediante un análisis exhaustivo de los riesgos y vulnerabilidades presentes en la infraestructura de tecnologías de la información (TI) de la organización.

2.2. OBJETIVOS ESPECÍFICOS

- Analizar de qué manera la integración de equipos Blue Team, Red Team y Purple Team puede contribuir al fortalecimiento de la ciberseguridad en una organización.

- Diseñar políticas de seguridad y proporcionar recomendaciones detalladas para mejorar la ciberseguridad en entornos de tecnologías de la información (TI) en cualquier organización.

- Establecer conclusiones basadas en las etapas previas del seminario especializado, con el propósito de orientar aspectos fundamentales relacionados con la inversión en ciberseguridad dentro de las organizaciones.

3. DESARROLLO

3.1. INFORME TÉCNICO

3.2. ETAPA 1: CONCEPTOS EQUIPOS DE SEGURIDAD

Para asegurar la protección de la información y la privacidad de una organización, es fundamental para que un profesional en seguridad informática implemente estrategias de ciberseguridad efectivas y éticas. Estas estrategias se desglosan en las siguientes etapas:

Comprensión de Conceptos Clave de Ciberseguridad: Como profesionales de seguridad de la información, es crucial adquirir un conocimiento sólido de los principios fundamentales de la ciberseguridad. Esto facilita la identificación de posibles amenazas y vulnerabilidades en los sistemas de información, lo que a su vez permite la adopción de medidas preventivas y correctivas adecuadas para minimizar los riesgos de seguridad. Además, comprender la ciberseguridad es esencial para el cumplimiento de las normativas de seguridad de la información y para mantener la confianza de clientes y socios comerciales[6].

Para asegurar la protección de la información y la privacidad de una organización, es fundamental para que un profesional en seguridad informática implemente estrategias de ciberseguridad efectivas y éticas. Estas estrategias se desglosan en las siguientes etapas:

Comprensión de Conceptos Clave de Ciberseguridad: Como profesionales de seguridad de la información, es crucial adquirir un conocimiento sólido de los principios fundamentales de la ciberseguridad. Esto facilita la identificación de posibles amenazas y vulnerabilidades en los sistemas de información, lo que a su vez permite la adopción de medidas preventivas y correctivas adecuadas para minimizar los riesgos de seguridad. Además, comprender la ciberseguridad es esencial para el cumplimiento de las normativas de seguridad de la información y para mantener la confianza de clientes y socios comerciales.

Equipos de Seguridad Clave:

- **Equipo Rojo:** Este equipo simula ataques adversos con el propósito de identificar vulnerabilidades y fortalecer las defensas de una organización.
- **Blue Team:** Su función es proteger sistemas y organizaciones contra ataques reales, enfocándose en la detección, respuesta y mitigación de amenazas.
- **Firewall:** Un software o hardware que guarda las redes informáticas al controlar el tráfico de acuerdo con políticas de seguridad predefinidas.
- **Escaneo (Scanning):** El proceso de exploración de sistemas en busca de debilidades que puedan ser explotadas por atacantes.

[6] ISECOM. Open-Source Security Testing Methodology Manual (OSSTMM) Versión 3.0. 2008. https://www.isecom.org/OSSTMM.3.pdf

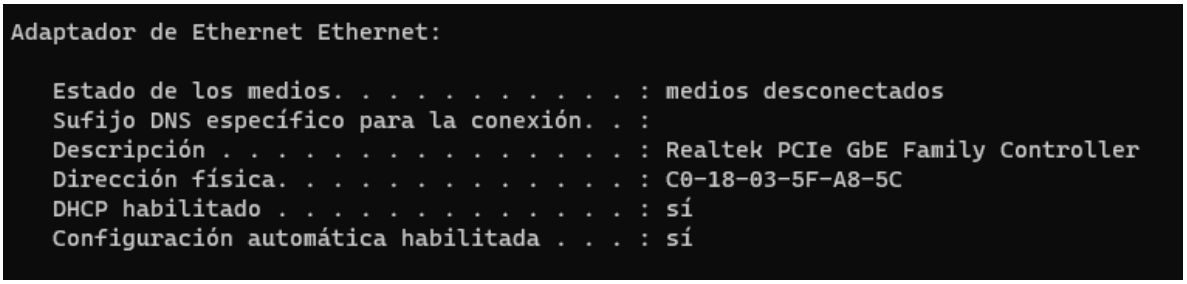
- **Vulnerabilidad:** Una debilidad o falla en sistemas o aplicaciones que podrían ser explotadas por atacantes para acceder o dañar información.
- **Pruebas de Penetración (Penetration Testing):** Simulan ataques de ciberseguridad para descubrir vulnerabilidades.
- **Descubrimiento:** Identificar dispositivos y sistemas en una red.
- Enumeración: Identificar usuarios, cuentas, recursos y servicios en una red o sistema.
- **Mapeo de Seguridad (Security Mapping):** Comprender la arquitectura y topología de un sistema o red para evaluar vulnerabilidades.
- **Valoración de Riesgos:** Asignar prioridad a las vulnerabilidades según su probabilidad e impacto.
- **Reporte (Reporting):** Documentar y comunicar resultados de evaluaciones de seguridad.
- **Phishing:** Un tipo de ataque que intenta engañar a personas para obtener información confidencial.
- **Exploit:** Código o técnica utilizada para aprovechar una vulnerabilidad.
- **Botnet:** Red de computadoras comprometidas para actividades maliciosas.
- **Metasploit:** Herramienta de pruebas de penetración de código abierto para identificar y explotar vulnerabilidades.
- **OpenVAS:** Escáner de vulnerabilidades de código abierto para detectar vulnerabilidades en sistemas y aplicaciones[7].

Estos conceptos y equipos desempeñan un papel crucial en la protección efectiva de la información y los sistemas de una organización en el ámbito de la ciberseguridad.

Para personalizar eficazmente estas herramientas, los equipos de trabajo pueden optar por crear entornos virtuales utilizando máquinas virtuales, como se lleva a cabo en la Etapa 2 que se describirá a continuación:

Sintaxis de la estructura básica de las dos Máquinas, Kali Linux (máquina atacante) y la Máquina Windows 10 (máquina víctima).

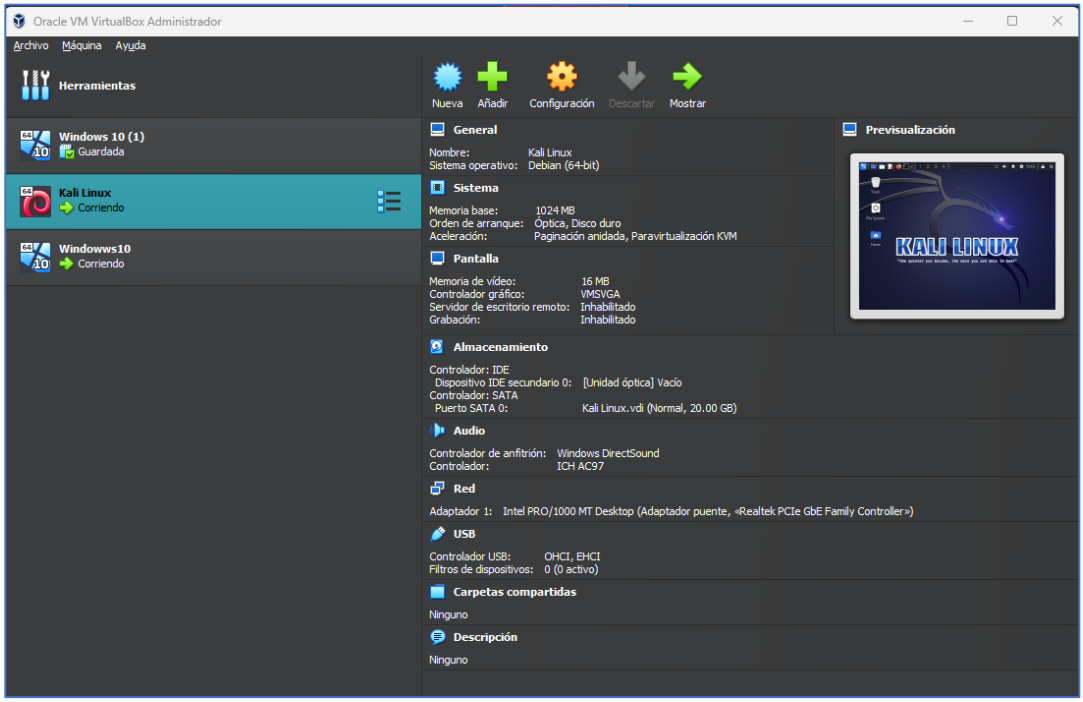
lustración 1 Adaptador de Red Física.



Fuente: elaboración propia.

[7] ISECOM. Open-Source Security Testing Methodology Manual (OSSTMM) Versión 3.0. 2019. https://www.openvas.org/

Ilustración 2 Maquina Atácate modo bridge.



Fuente: elaboración propia.

3.3. ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL:

Es esencial comprender las acciones de los equipos Red Team y Blue Team en una organización, especialmente dentro del alcance de los criterios éticos y legales. En Colombia, existen las siguientes normativas de ciberseguridad clave, que incluyen:

Ley 1266 de 2008: Esta ley establece el régimen de Habeas Data en Colombia y tiene como objetivo proteger los datos personales de las personas[8].

Ley 527 de 1999: Regula el uso de mensajes de datos y firmas digitales, obligando a las empresas a garantizar la autenticidad, integridad y confidencialidad de los mensajes de datos enviados por medios electrónicos[9].

Ley 1273 de 2009: Definir los delitos informáticos y sus sanciones, imponiendo penas de prisión a quienes realicen actividades ilegales a través de medios electrónicos[10].

---

[8] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1266 de 2008. https://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[9] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 527 de 1999. 1999. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5376

[10] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Decreto 1078 de 2015: Regula la seguridad de la información en el sector público, requiriendo que las entidades del Estado implementen medidas de seguridad para proteger la información que manejan.

Por ejemplo, si una empresa incumple con estos protocolos, culpando a sus empleados, explotándolos y exponiendo información sensible, estaría violando estas normativas de ciberseguridad. Esto podría resultar en sanciones y multas por parte de las autoridades competentes.

Además, llevar a cabo actividades de Red Team o Blue Team sin el consentimiento adecuado puede considerar una violación de la privacidad y seguridad de la organización objetivo, lo que podría dar lugar a responsabilidades legales y sanciones. En Colombia, la Ley 1273 de 2009 regula esta situación, estableciendo la prohibición de acceder a sistemas informáticos, bases de datos o redes de computadoras sin autorización o excediendo la autorización otorgada.

Adicional a lo anterior, se considera que el Marco Normativo para la Seguridad y Privacidad de la Información (Resolución 20002688 de 2019) establece que todas las actividades de seguridad informática deben realizarse dentro de un marco legal y regulatorio, y con el consentimiento adecuado de los propietarios de la información. De lo contrario, podrían enfrentar sanciones por parte de la Superintendencia de Industria y Comercio[11].

ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y HACKERHOUSE

4. CONSIDERACIONES

1. Que la información compartida en virtud del presente acuerdo pertenece a HackerHouse**,** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal*.*

2. Que la información de propiedad de HackerHouse ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o

[11] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. (2015). Decreto 1078 de 2015. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201078%20DEL%2026%20DE%20MAYO

proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal*, nombre estudiante* que, para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de HackerHouse*.*

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de HackerHouse no podrán ser divulgados.

La ley 842 de 2003 en su capítulo II Articulo 31 Deberes generales de los profesionales en el literal "e y f" habla de : e)" Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones"[1]; y, f) "Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder"[2]; así mismo en el artículo 32 PROHIBICIONES GENERALES A LOS PROFESIONALES en su literal "b" menciona: b) "Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley"[3].

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

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".

   Es importante tener en cuenta que al ser información obtenida de forma abusiva y sin autorización estaría incurriendo en faltas contempladas en la ley 1273 artículo 269ª: Artículo 269A: "Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo"[4].

   parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal,

[1] *http://www.secretariasenado.gov.co/senado/basedoc/ley_0842_2003.html*
[2] *id*
[3] *id*

visual o materialmente, por escrito en los documentos, medios electrónicos.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma HackerHouse**,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

   Se estaría incurriendo en la actividad ilícita tipificada en la ley 1273 de 2009 en el "Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes"[5].

[4] *http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html*

[5] *Id*

4. Responder por el mal uso que le den sus representantes a la **información confidencial.**

5. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

   Sería ilegal siempre que no se demuestre que la forma en la que esta persona adquirió dicha información es procedente de una conducta tipificada; en ese caso se daría aplicación a las sanciones estipuladas en la ley 1273 de 2009 por violación de datos personales articulo 269F.

6. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial o ilegal** sin el previo consentimiento por escritopor parte de HackerHouse**.**

   En lo que refiere a la información confidencial, es de anotar que esta no debe ser suministrada sin autorización escrita por parte de la organización siempre y cuando esta no sea requerida por un ente judicial con losrequisitos de ley correspondientes. Ley de protección de datos, 1581 de 2012, Artículo 10. "Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial"[6].

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto

[6] *https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981*

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse.

En la medida en que se encuentre en manos de la parte receptora la información obtenida de forma ilegal, es este el que debe responder ante las autoridades por dicha conducta ilícita y las sanciones correspondientes conforme se establece enla ley 1273 de 2009. Así mismo, si dicha información se adquirió por orden directade HackerHouse Y EXISTE MATERIAL PROBATORIO DEL MISMO, la sanción será para las dos partes.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Punto 3. El sueldo para los puestos de Red tema y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría el contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo

que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente:

Ante esta situación se debe tener en cuenta que la ética reúne los valores, deberes y responsabilidades que debemos tener en la sociedad. Dentro de los valores debemos destacar la honestidad, ya que, al revisar el acuerdo de confidencialidad, se evidencian varias situaciones ilegales que se deben cumplir al aceptarlo; por lo tanto, no se debe acordar.

La COPNIA establece Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, que en su artículo 32 PROHIBICIONES GENERALES A LOS PROFESIONALES en su literal “b” menciona: b) “Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley”[7], ya que, al aceptar el acuerdo de confidencialidad, se permite que esta empresa continue realizando las actividades ilícitas señalas; de otro lado el ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD literal “a” “Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación”[8]; lo que significa que se aceptaría un trabajo a sabiendas de que existen irregularidades en su contexto que están por fuera de la Ley.

Punto 4. Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

[7] *http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html*
[8] *http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html*

A mediados del mes de diciembre de 2022 las Empresas Públicas de Medellín, EPM, sufrió un hackeo a sus sistemas informáticos. Este hecho dejó "varias consecuencias para la compañía, proveedores y usuarios de los servicios públicos que presta la compañía en departamentos como Antioquia (y su área metropolitana), Santander y parte de la región Atlántica"[9].

"En el reporte se evidencia que el impacto del ataque fue importante al punto de perder el control de la plataforma, respaldos e información clave.

Pero también se sabe que hay información secuestrada por medio de códigos a los que no tiene acceso la compañía, además de pérdidas de respaldos e información.

Reportes por confirmar aseguran que el servidor llamado Consorcio 20 fue que inició con el virus y lo esparció por todos los equipos de la compañía: "un usuario de ese servidor fue el que le dio clic al enlace o descargó el archivo prohibido que infectó todo".

Según reportes de El Colombiano, el ataque cibernético contra EPM desde el 12 de diciembre lo perpetuó Blackcat, lo que sería un grupo de ciberdelincuentes especializado en este tipo de ataques y en, posteriormente, cobrar recompensas o rescates para evitar la filtración de información sensible de una empresa, persona u organización"[10].

Este delito constituye una violación a la LEY 1273 DE 2009 en los siguientes artículos:

Artículo 269A: Acceso abusivo a un sistema informático

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación

Artículo 269C: Interceptación de datos informáticos

---

[9] *VALORA Analitik, Ciberataque a EPM: ¿Qué ha pasado con las investigaciones y soluciones?,Colombia,2022, https://www.valoraanalitik.com/2022/12/21/ciberataque-a-epm-que-ha-pasado-con-las-investigaciones-y-soluciones/*

[10] *id*

Artículo 269D: Daño Informático

Artículo 269E: Uso de software malicioso

Artículo 269F: Violación de datos personales

De igual manera atenta contra la Ley Estatutaria 1581 de 2012.

El ciberdelito se ha incrementado en los últimos años, debido a que la mayoría de información que se maneja en la actualidad reposa en plataformas informáticas; lo que hace posible interceptarla.

En conclusión, es fundamental que las organizaciones cumplan con las actividades normativas de ciberseguridad y obtengan el consentimiento adecuado al llevar a cabo a cabo de ciberseguridad, ya sea Red Team o Blue Team, para evitar consecuencias legales adversas.

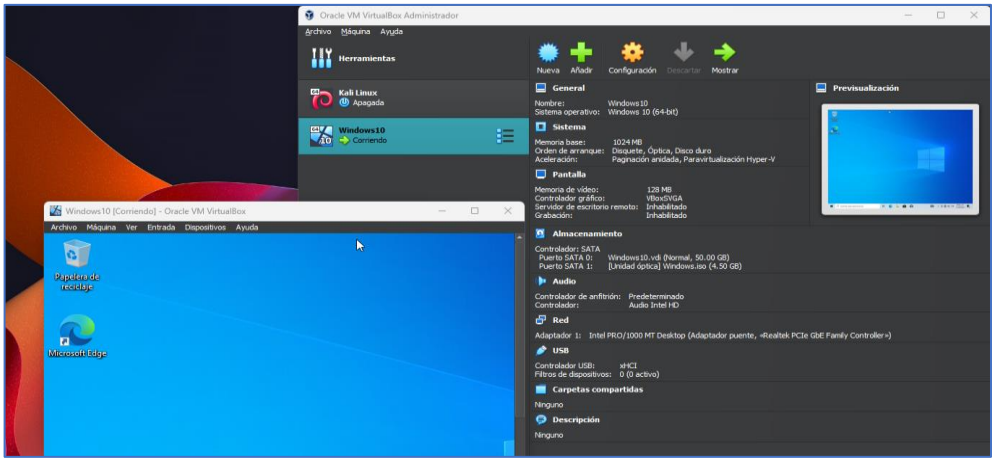
4.1. ETAPA 3: EJECUCIÓN PRUEBAS DE INTRUSIÓN:

Se requiere evidenciar las vulnerabilidades de un sistema informático mediante la aplicación de metodologías y tácticas de intrusión. Las pruebas de intrusión representan un proceso proactivo en el que un equipo de seguridad se esfuerza por identificar y explotar las debilidades en un sistema o red con el propósito de evaluar su nivel de seguridad. El objetivo fundamental de estas pruebas es detectar las falencias antes de que un atacante las descubra y aproveche en su propio beneficio.

Para llevar a cabo las pruebas de intrusión, se emplean diversas herramientas y estrategias, que incluyen actividades como la exploración de puertos, la identificación de servicios en ejecución, la explotación de vulnerabilidades, la elevación de privilegios y la obtención de acceso remoto. Además, estas pruebas pueden abordar la ingeniería social, que implica influir en los usuarios para que divulguen información confidencial o realicen acciones que comprometan la seguridad.

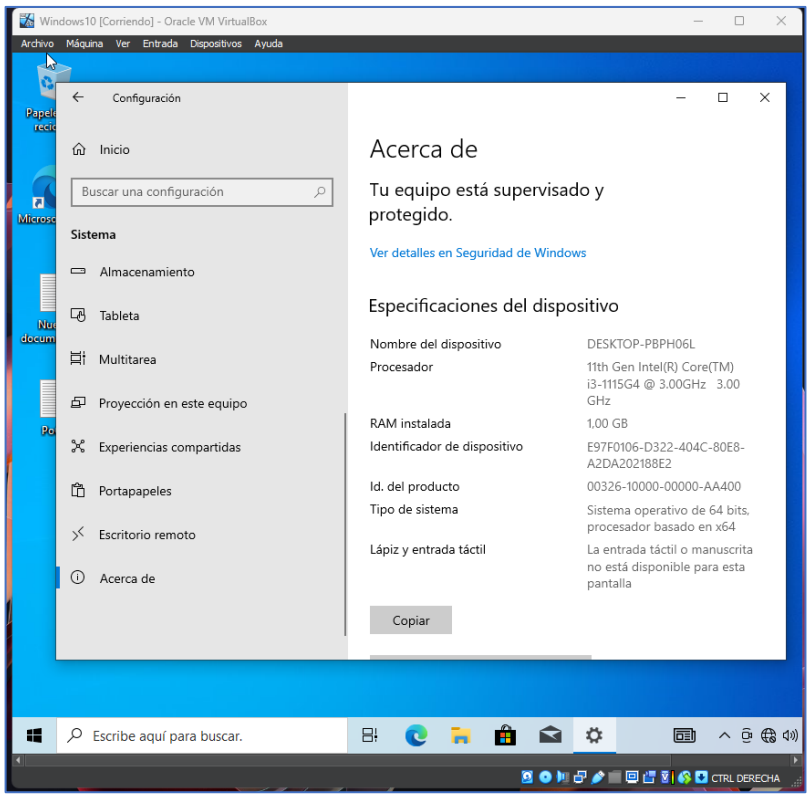
Es crucial recordar que la realización de pruebas de intrusión debe estar a cargo de profesionales debidamente capacitados y éticos, dado que involucra actividades que podrían ser consideradas ilegales si se llevan a cabo sin el consentimiento expreso del propietario del sistema o la red. El proceso de ejecución de una prueba de intrusión por lo general sigue estos pasos:

Ilustración 3 Maquina Victima modo bridge.



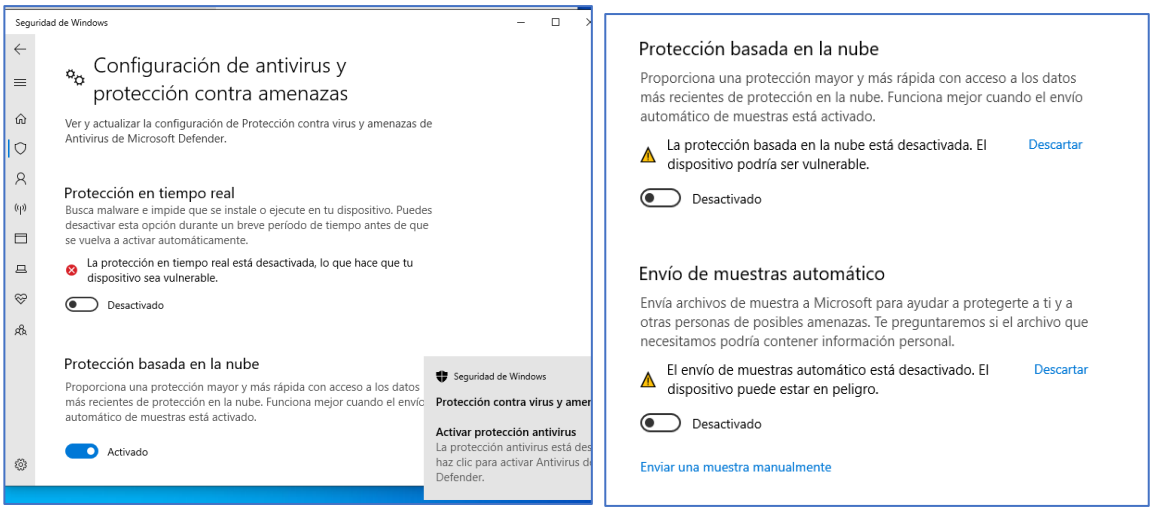
Fuente: elaboración propia.

Ilustración 4 Sistema Operativo de la Maquina Victima



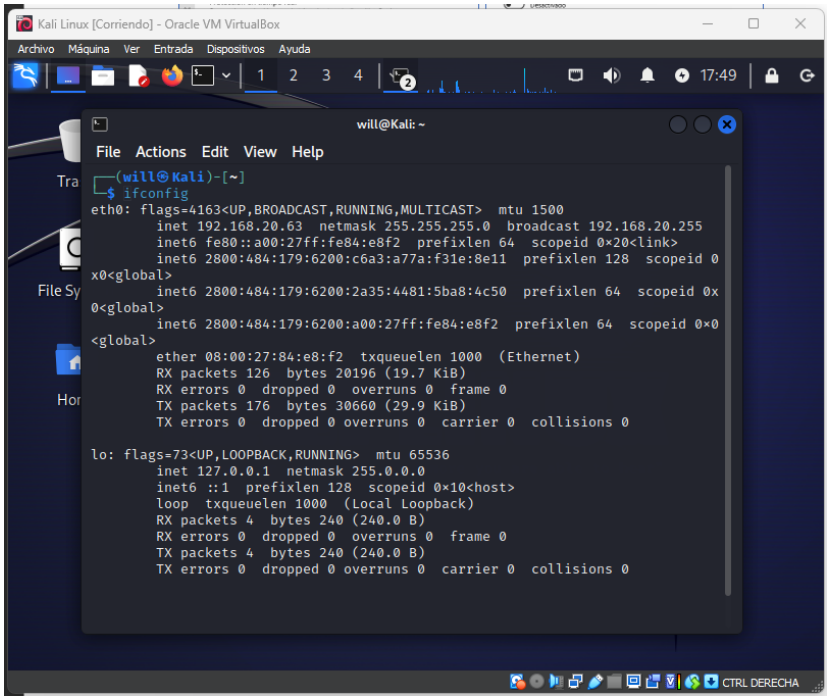
Fuente: elaboración propia.

Ilustración 5 Desactivar Windows Defender y Firewall de Windows.



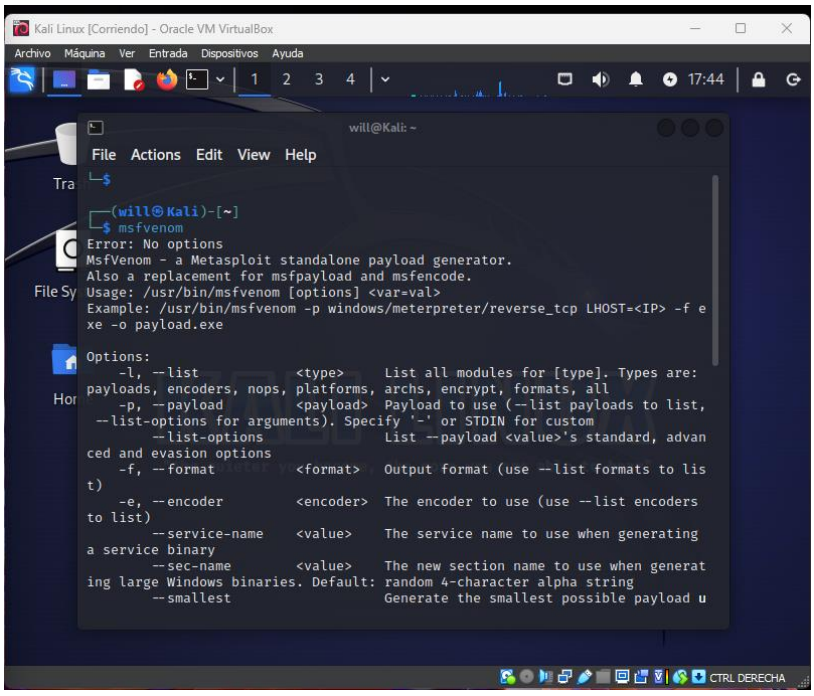
Fuente: elaboración propia.

Ilustración 6 IP Maquina Atacante



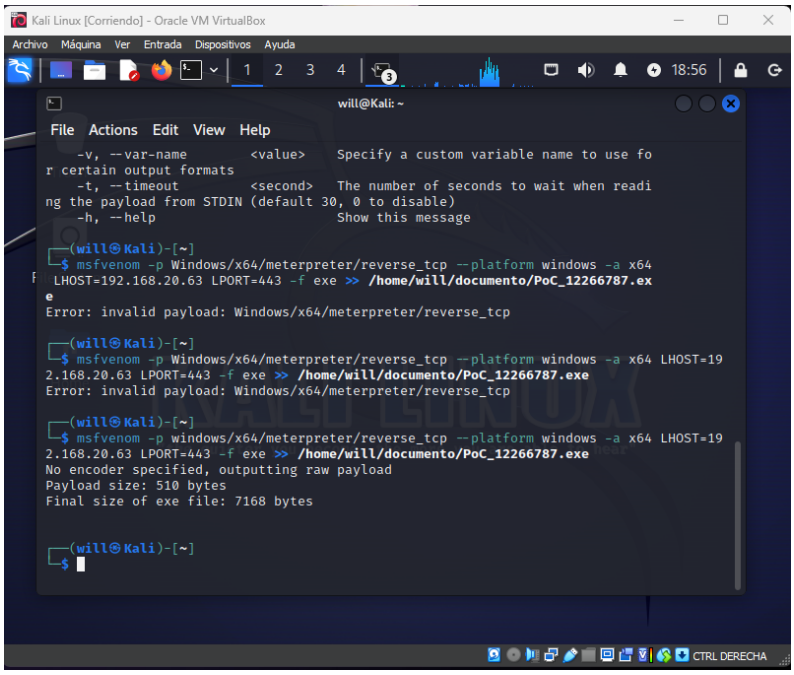
Fuente: elaboración propia.

Ilustración 7 Comando msfvenom en maquina Atacante.



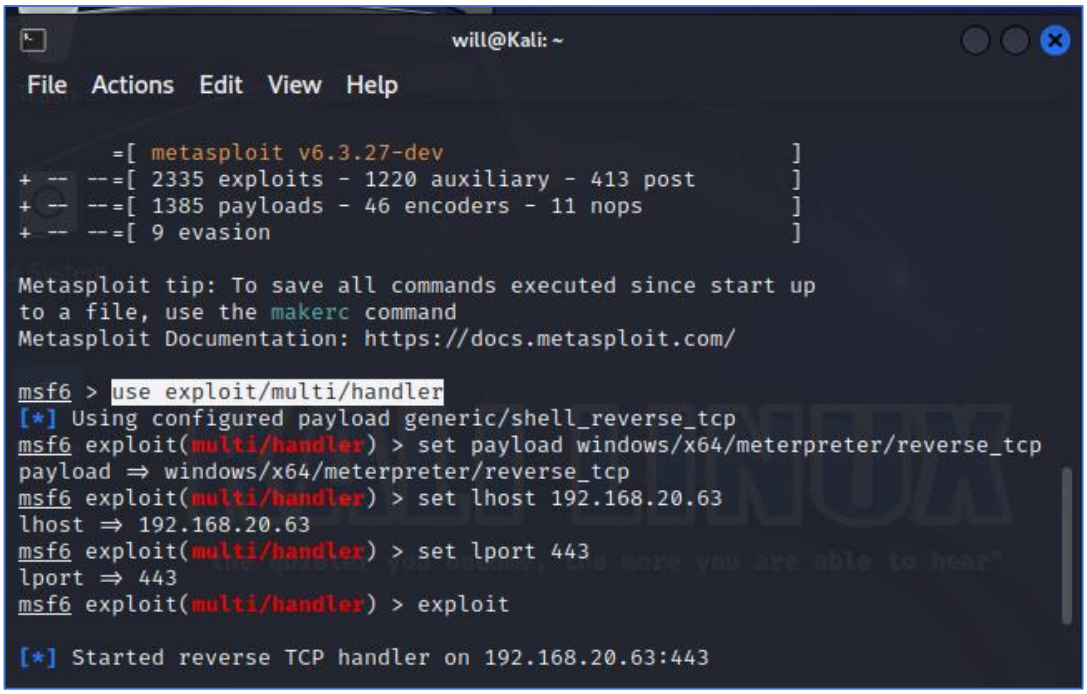
Fuente: elaboración propia.

Ilustración 8 . Creación de carga útil msfvenom.



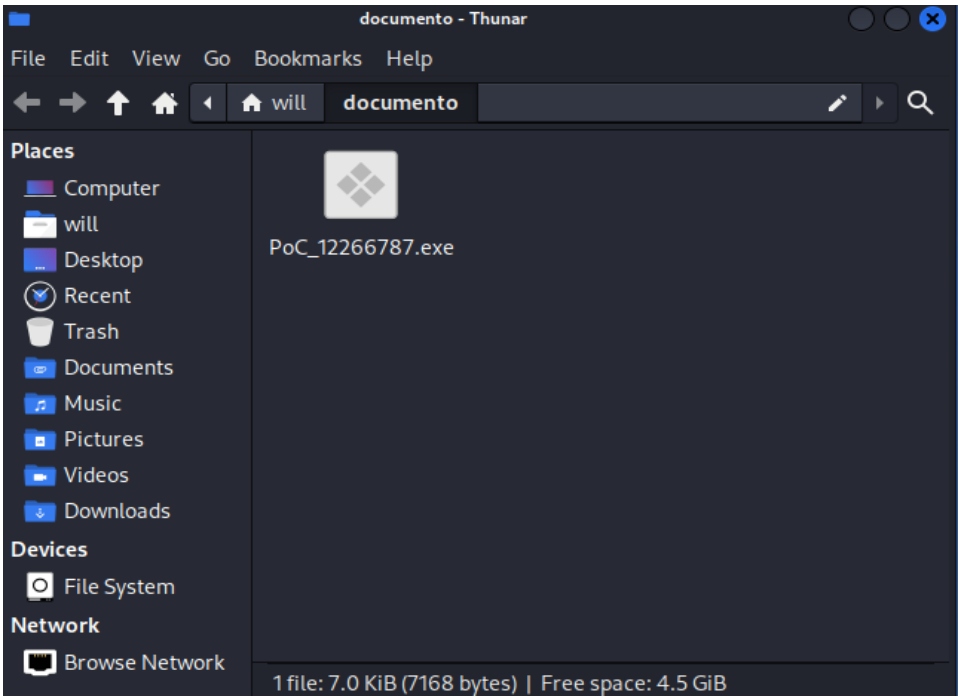
Fuente: elaboración propia.

Ilustración 9 . Ejecución exploit y .exe en windows 10 x64



Fuente: elaboración propia.

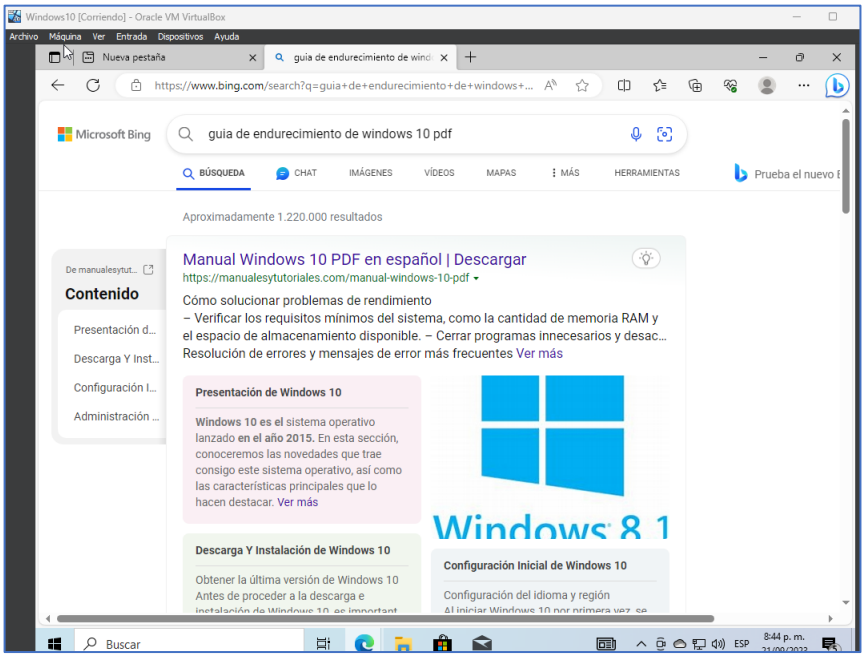
Ilustración 10 Documento creado



Fuente: elaboración propia.

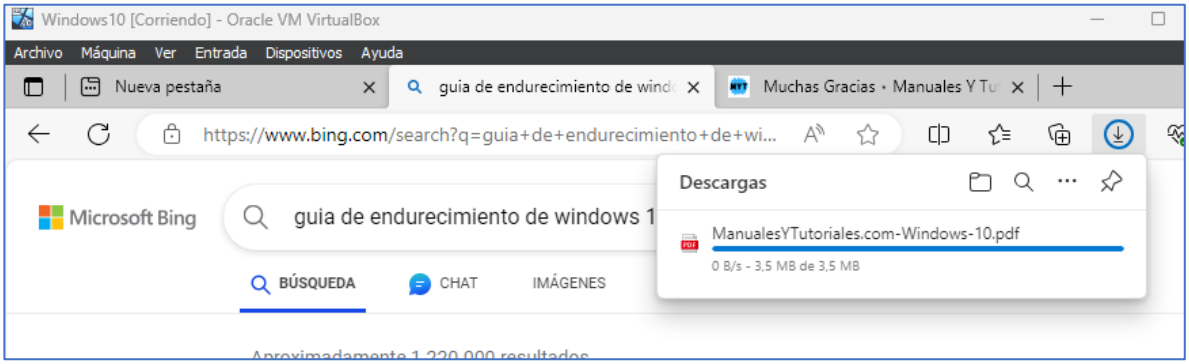
4.2. ETAPA 4: CONTENCIÓN DE ATAQUES INFORMÁTICO

Ilustración 11 Búsqueda de la Guía.



Fuente: elaboración propia.

Ilustración 12 Evidencia de descarga de la Guía.



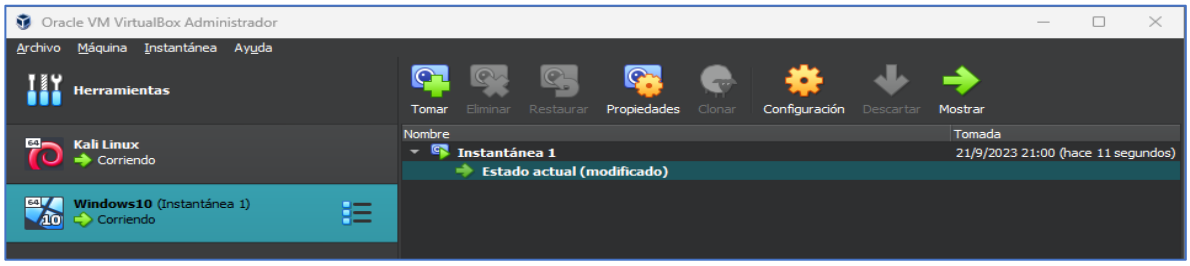
Fuente: elaboración propia.

Asegure la máquina que fue afectada con el Payload

Ilustración 13 Detener la máquina virtual.

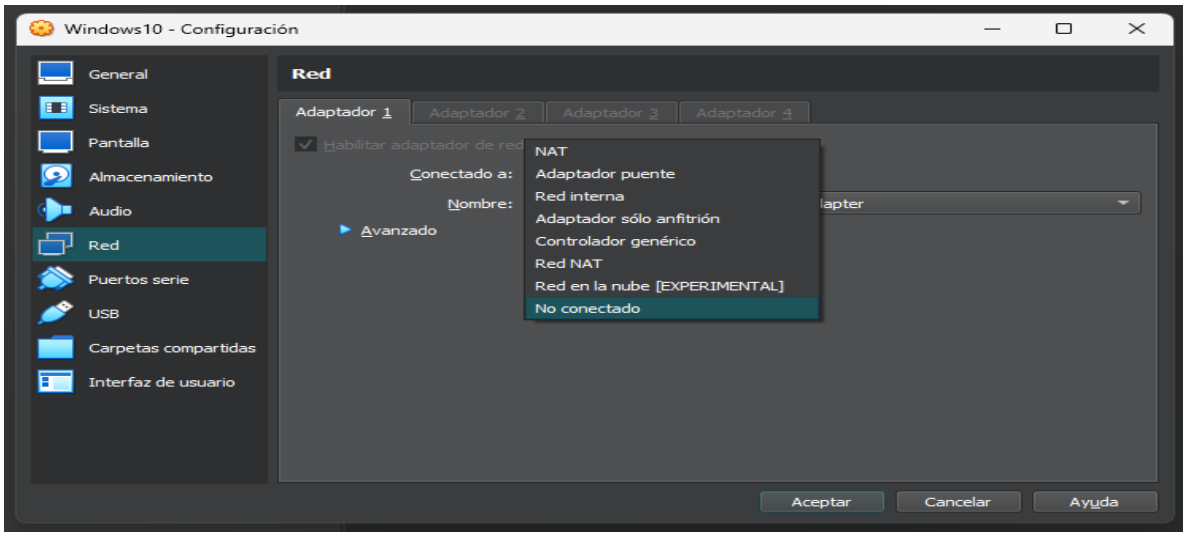
Fuente: elaboración propia.

Ilustración 14 Tomar una instantánea.



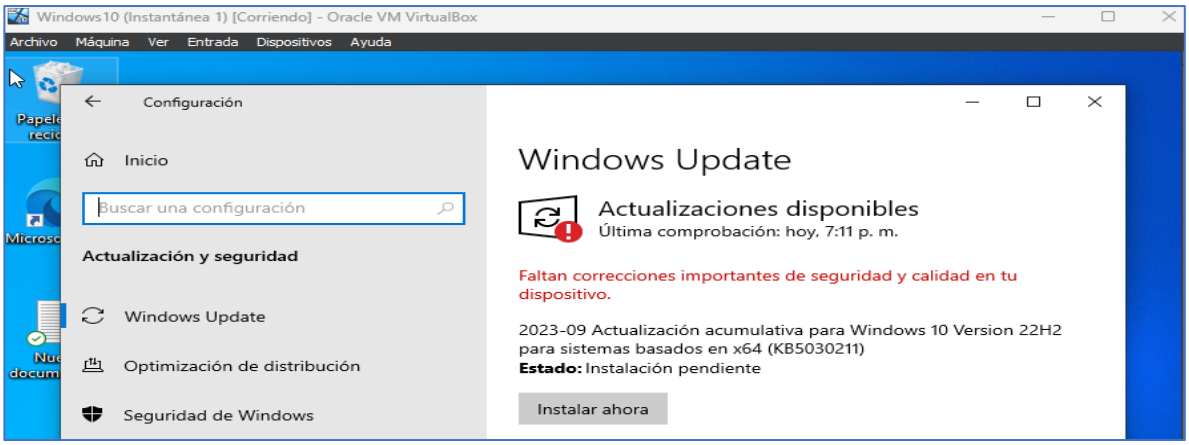
Fuente: elaboración propia.

Ilustración 15 Desactivar adaptador de red.



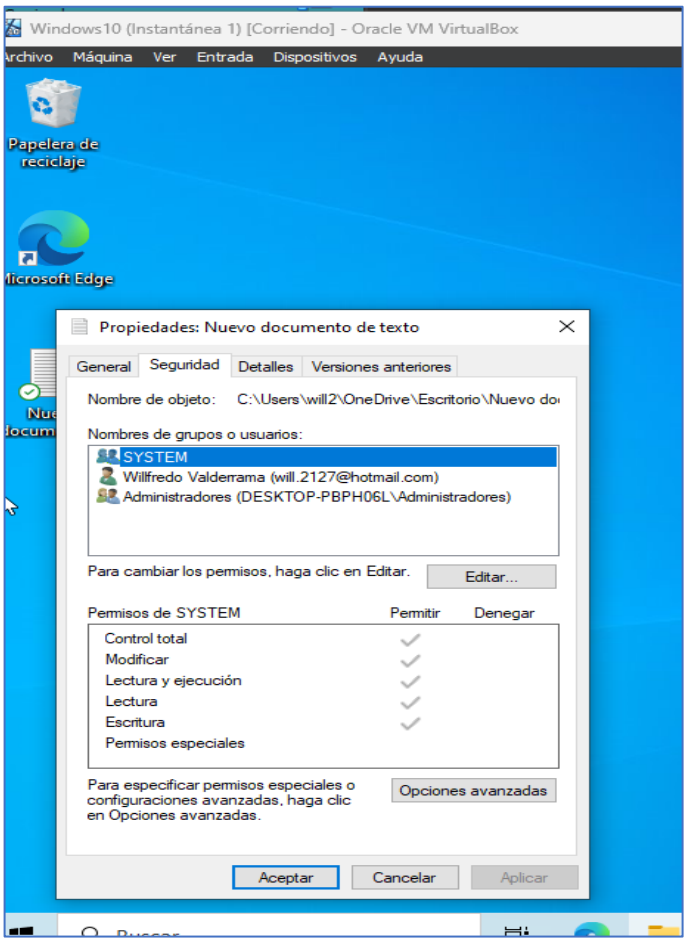
Fuente: elaboración propia.

Ilustración 16 Actualizar Windows 10.



Fuente: elaboración propia.

Ilustración 17 Restringir los permisos.



Fuente: elaboración propia.

4.3. ETAPA 5: SOCIALIZACIÓN DE INFORME TÉCNICO

4.3.1. Integración de Equipos Blue, Red y Purple Team en Ciberseguridad.

La integración de equipos Blue Team, Red Team y Purple Team dentro de una organización puede tener un impacto significativo en el fortalecimiento de la ciberseguridad y la protección de los activos digitales. A continuación, se destacan varias formas en que estos equipos pueden contribuir en el campo de la ciberseguridad cuando trabajan juntos[12]:

Mejora de las Defensas: El equipo Blue Team se enfoca en defender y proteger activamente los sistemas y redes. Al colaborar con el Purple Team, pueden utilizar los conocimientos adquiridos de los ejercicios de Red Team para identificar debilidades y vulnerabilidades en sus defensas. Esto permite una mejora continua de las medidas de seguridad[13].

Pruebas de Resiliencia: El equipo Red Team realiza pruebas de penetración simuladas para evaluar la resistencia de las defensas de la organización. La colaboración con el Purple Team ayuda a entender los métodos y las tácticas utilizadas por los atacantes reales, lo que a su vez permite al Blue Team fortalecer sus defensas contra amenazas conocidas[14].

Aprendizaje Continuo: El Equipo Púrpura actúa como un puente de conocimiento entre los equipos Azul y Rojo. Facilita la comunicación y el intercambio de información. Esto crea un ambiente de aprendizaje continuo donde se comparten las mejores prácticas, se analizan los incidentes simulados y se desarrollan estrategias más efectivas.

Detección Temprana de Amenazas: La colaboración entre los equipos puede llevar a una detección más temprana de amenazas. El Red Team puede proporcionar información sobre las tácticas actuales utilizadas por los atacantes, lo que permite al Blue Team ajustar sus sistemas de monitoreo y detección para identificar señales de ataques en una etapa inicial[15].

---

[12] UNIR-Revista. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? 07 de enero de 2020. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

[13] OSTEC. Purple Team: en medio del Red y el Blue Team. 24 de octubre de 2022. https://ostec.blog/es/aprendizaje-descubrimiento/purple-team-en-medio-del-red-y-el-blue-team/

[14] ALCALDÍA DE BOGOTÁ. Guardianes de la información Penetration Testing. Alcaldía de Bogotá. 2018. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

[15] CRANFORD. RED TEAM VS BLUE TEAM IN CYBERSECURITY. abril de 2023. https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

Mejora de la Respuesta a Incidentes: En el caso de que ocurra un incidente real, la colaboración entre los equipos permite una respuesta más efectiva. El Equipo Púrpura puede desempeñar un papel fundamental al coordinar los esfuerzos de los equipos Azul y Rojo para mitigar la amenaza de manera rápida y eficiente.

Cambio de Cultura de Seguridad: La presencia de los equipos Blue, Red y Purple fomenta una cultura de seguridad sólida dentro de la organización. Todos los empleados se vuelven más conscientes de la importancia de la ciberseguridad y de su papel en la protección de los activos de la empresa[16].

Adaptación a Amenazas Emergentes: Los equipos pueden anticipar amenazas emergentes y desarrollar contramedidas antes de que se conviertan en ataques reales. Esto proporciona una ventaja estratégica en la lucha contra las amenazas cibernéticas en constante evolución[17].

Concluyendo de este modo que, la integración de equipos Blue Team, Red Team y Purple Team promueve una ciberseguridad más sólida y adaptativa en una organización, facilitando de este modo el aprendizaje continuo, la identificación proactiva de amenazas y una respuesta más efectiva ante incidentes de seguridad.

4.3.2. Políticas de Seguridad y Recomendaciones para Mejorar la Ciberseguridad en una Organización.

En un mundo cada vez más digitalizado, la seguridad cibernética se ha convertido en un aspecto crítico para cualquier organización. En este contexto, a continuación, se presentan políticas y recomendaciones diseñadas para fortalecer la ciberseguridad en su organización. Estas son medidas esenciales para proteger los sistemas y datos de posibles amenazas cibernéticas[18]. (Shea, 2023)

Política 1: Gestión de Contraseñas Fuertes
Todos los empleados deben utilizar contraseñas fuertes y únicas para acceder a sistemas y aplicaciones. Las contraseñas deben contener al menos 12 caracteres, incluyendo letras mayúsculas, minúsculas, números y caracteres especiales.

---

[16] REEGÅRD, K., & BLACKETT, C. (septiembre de 2019). The Concept of Cybersecurity Culture. https://www.researchgate.net/publication/336149766_The_Concept_of_Cybersecurity_Culture

[17] PARIDA, B. Red Team vs Blue Team: An In-depth Analysis of Cybersecurity Operations. (19 de junio de 2023). https://www.wevolver.com/article/red-team-vs-blue-team-an-in-depth-analysis-of-cybersecurity-operations

[18] SHEA, S. What is cybersecurity? Junio de 2023. https://www.techtarget.com/searchsecurity/definition/cybersecurity

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

- Implementar la autenticación de dos factores siempre que sea posible.
- Educar a los empleados sobre las buenas prácticas de creación y gestión de contraseñas.
- Utilizar un sistema de gestión de contraseñas para almacenar y proteger contraseñas.

Política 2: Actualización y parcheo de software
Todos los sistemas y aplicaciones deben mantenerse actualizados con los últimos parches de seguridad. Se debe establecer un programa de parcheo regular[19]**.**

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

- Implementar un sistema de gestión de parches automatizado.
- Realizar auditorías regulares para identificar sistemas no parcheados.

Política 3: Seguridad de Red y Firewall
Configurar un firewall para restringir el tráfico no autorizado. Prohibir el uso de redes Wi-Fi públicas no seguras para acceder a recursos internos.

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

- Establecer reglas de firewall que permitan solo el tráfico necesario.
- Utilizar VPN para conexiones remotas a la red de la empresa.

Política 4: Control de Acceso y Privacidad de Datos
Limitar el acceso a los datos confidenciales y garantizar que solo las personas autorizadas puedan acceder a ellos[20].

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

---

[19] NATIONAL CYBER SECURITY CENTRE. Device Security Guidance. Guidance for organisations on how to choose, configure and use devices securely: (29 de junio de 2021). https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date

[20] ISO 27001. Anexo A.9: Control de acceso. (octubre de 2022). https://www.isms.online/iso-27001/annex-a-9-access-control/

- Implementar políticas de mínimo privilegio.
- Realizar auditorías de acceso para identificar actividad sospechosa.

Política 5: Concientización y Formación en Seguridad
Proporcionar formación y concienciación en seguridad cibernética a todos los empleados.

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

- Realizar sesiones de formación periódicas sobre seguridad informática.
- Fomentar la denuncia de incidentes de seguridad por parte de los empleados.

Política 6: Respuesta a Incidentes
Establecer un plan de respuesta a incidentes que incluya la identificación, notificación, mitigación y recuperación de incidentes de seguridad[21].

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

- Designar un equipo de respuesta a incidentes y definir roles y responsabilidades.
- Probar regularmente el plan de respuesta a incidentes a través de ejercicios y simulacros.

Política 7: Copias de Seguridad y Recuperación de Datos
Realizar copias de seguridad regulares de datos críticos y mantener un plan de recuperación de desastres.

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

- Almacenar copias de seguridad en ubicaciones seguras y fuera del sitio.
- Probar la restauración de datos de forma periódica.

Política 8: Evaluación de Riesgos y Auditorías
Realizar evaluaciones de riesgos regulares para identificar posibles amenazas y vulnerabilidades. Realizar auditorías de seguridad de manera periódica.

Esta política es posible lograr si el usuario tiene en cuenta las siguientes recomendaciones:

---

[21] ELLIS, D. 6 Phases in the Incident Response Plan. 2023. https://www.securitymetrics.com/blog/6-phases-incident-response-plan

- Contratar a profesionales de seguridad para realizar auditorías independientes.
- Implementar medidas correctivas basadas en los resultados de las auditorías.

Cabe destacar que estas políticas y recomendaciones son fundamentales para mejorar la ciberseguridad en cualquier organización y ayudar a proteger sus activos de posibles amenazas cibernéticas. Es esencial que estas políticas se revisen y actualicen de forma periódicamente para adaptarse a las amenazas cambiantes y las nuevas tecnologías.

4.3.3. CONCLUSIONES ESTRATÉGICAS PARA LA INVERSIÓN EN CIBERSEGURIDAD ORGANIZACIONAL.

Basándome en las etapas y conceptos discutidos a lo largo del seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, a continuación, presentó conclusiones que pueden orientar aspectos importantes en cuanto a la inversión de ciberseguridad dentro de las organizaciones.

Las siguientes conclusiones pueden utilizarse para respaldar la necesidad de inversión en ciberseguridad ante la alta gerencia:

La Evolución de las Amenazas Cibernéticas: Es fundamental reconocer que las amenazas cibernéticas evolucionan constantemente. Los ataques se vuelven más atractivos y dirigidos. Por lo tanto, es necesario que las organizaciones estén preparadas para enfrentar amenazas en cambio constante y que esto requiere inversión continua en tecnología y recursos humanos especializados[22].

Importancia de la Prevención: El seminario destacó la importancia de la prevención de amenazas cibernéticas. Invertir en soluciones de seguridad proactivas, como firewalls avanzados, sistemas de detección de intrusiones y programas de concienciación en seguridad, puede ayudar a prevenir ataques antes de que ocurran.

Detección Temprana y Respuesta Rápida: A pesar de los esfuerzos de prevención, los ataques pueden ocurrir. La capacidad de detectar amenazas temprano y responder rápidamente es esencial. Las organizaciones deben invertir en sistemas de monitorización avanzados, herramientas de análisis de seguridad y equipos de respuesta a incidentes para minimizar el impacto de los ataques.

Formación y Concienciación: La formación y la concienciación de los empleados son componentes cruciales de la ciberseguridad. Invertir en programas de formación que eduquen a los empleados sobre las mejores prácticas de seguridad cibernética puede reducir significativamente el riesgo de ataques relacionados con el factor humano.

Evaluación y Mejora Continua: Las evaluaciones regulares de seguridad, como pruebas de penetración y análisis de vulnerabilidades, son esenciales para identificar debilidades en la infraestructura. Las organizaciones deben invertir en

[22] QUINTERO, H. Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. 2023. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.unad.edu.co/bitstream/handle/10596/57180/hquinterom.pdf?sequence=1&isAllowed=y

estas evaluaciones y, más importante aún, en la corrección de las vulnerabilidades identificadas[23].

Cumplimiento y Normativas: Cumplir con las normativas y regulaciones de seguridad cibernética es una inversión necesaria. No cumplir con estas regulaciones puede resultar en sanciones financieras y daños a la reputación. Por lo tanto, las organizaciones deben invertir en la implementación y el mantenimiento de prácticas de seguridad que cumplan con los estándares aplicables.

Herramientas y Tecnología Avanzada: La inversión en herramientas de seguridad avanzadas, como soluciones SIEM, XDR y antivirus de última generación, es esencial para mantenerse al día con las amenazas emergentes. La actualización constante de estas tecnologías es un imperativo.

Planificación de Continuidad del Negocio: La ciberseguridad no solo se trata de evitar ataques, sino también de prepararse para recuperarse de ellos. Las organizaciones deben invertir en planes de continuidad del negocio y en soluciones de copia de seguridad y recuperación de desastres.

Gestión de Identidad y Acceso: Invertir en soluciones de gestión de identidad y acceso es fundamental para garantizar que solo las personas autorizadas tengan acceso a sistemas y datos críticos. La autenticación multifactorial es una clave de inversión en este sentido.

Conciencia de la Alta Gerencia: Finalmente, es crucial que la alta gerencia esté consciente de la importancia de la ciberseguridad y esté dispuesta a invertir en ella. La educación de la alta dirección sobre los riesgos y las implicaciones financieras de los ataques cibernéticos puede respaldar la toma de decisiones de inversión adecuadas.

Con base en lo anterior, se concluye que, la inversión en ciberseguridad es una necesidad crítica en el entorno actual de amenazas cibernéticas en constante evolución. Las organizaciones que comprenden la importancia de la inversión en prevención, detección, respuesta y formación estarán mejor preparadas para proteger sus activos y mantener la continuidad de sus operaciones.

[23] ALVAREZ, V. Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). 2018. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

5. CONCLUSIONES

La constante evolución de las amenazas cibernéticas exige una inversión continua en tecnología y recursos humanos especializados para mantenerse al día y proteger los activos digitales de la organización.

La prevención de amenazas cibernéticas es fundamental, y se debe invertir en soluciones proactivas, como firewalls avanzados y sistemas de detección de intrusiones, para evitar ataques antes de que ocurran.

La inversión en soluciones proactivas, como firewalls avanzados y sistemas de detección de intrusiones, es fundamental para evitar ataques cibernéticos antes de que ocurran.

La detección temprana y la respuesta rápida a incidentes son cruciales para minimizar el impacto de los ataques, lo que requiere inversiones en sistemas de monitoreo avanzados y equipos de respuesta a incidentes.

La formación y concienciación de los empleados son aspectos críticos de la ciberseguridad, y las organizaciones deben invertir en programas de formación para reducir el riesgo de ataques relacionados con el factor humano.

Cumplir con las normativas y regulaciones de seguridad cibernética es una inversión necesaria para evitar sanciones financieras y daños a la reputación.

La alta dirección debe estar consciente de la importancia de la ciberseguridad y estar dispuesta a invertir en ella para respaldar las iniciativas de seguridad en toda la organización.

6. RECOMENDACIONES

- Establecer políticas de gestión de contraseñas fuertes y promover la autenticación multifactorial.
- Implementar un programa de actualización y parcheo de software regular.
- Configurar firewalls y restringir el uso de redes Wi-Fi públicas no seguras.
- Limitar el acceso a datos confidenciales y aplicar políticas de mínimo privilegio.
- Proporcionar formación y concienciación en seguridad cibernética a todos los empleados.
- Desarrollar un plan de respuesta a incidentes y realizar ejercicios de simulacro periódicos.
- Realizar copias de seguridad regulares y establezca un plan de recuperación de desastres.
- Realizar evaluaciones de riesgos y auditorías de seguridad de manera periódica.
- Invertir en herramientas de seguridad avanzadas y actualizadas.
- Implementar soluciones de gestión de identidad y acceso.
- Educación continua de la alta dirección sobre los riesgos cibernéticos y las implicaciones financieras de los ataques.

7. BIBLIOGRAFÍA

Alcaldía de Bogotá. Guardianes de la información Penetration Testing.

Alcaldía de Bogotá. 2018. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

Álvarez, V. Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). 2018. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020) Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. 2020. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

Congreso de La República de Colombia. Ley 1266 de 2008. https://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congreso De La República De Colombia. Ley 1273 de 2009. https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso De La República De Colombia. Ley 527 de 1999. 1999. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5376

Cranford. (abril de 2023). RED TEAM VS BLUE TEAM IN CYBERSECURITY. https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

Ellis, D. (2023). 6 Phases in the Incident Response Plan. Obtenido de https://www.securitymetrics.com/blog/6-phases-incident-response-plan

EURPOL. (27 de enero de 2022). Ciberseguridad: amenanzas principales y emergentes.
https://www.europarl.europa.eu/news/es/headlines/society/20220120STO21428/ciberseguridad-amenanzas-principales-y-emergentes

ISECOM. Open-Source Security Testing Methodology Manual (OSSTMM) Versión 3.0. 2019. https://www.openvas.org/

ISECOM. Open-Source Security Testing Methodology Manual (OSSTMM) Versión 3.0. 2008. https://www.isecom.org/OSSTMM.3.pdf

ISO 27001. (octubre de 2022). Anexo A.9: Control de acceso. Obtenido de https://www.isms.online/iso-27001/annex-a-9-access-control/
Marrero, Y. (2003). La Criptografía como elemento de la seguridad informática.

ACIMED, 11(6). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012#:~:text=La%20Criptograf%C3%ADa%20es%20una%20disciplina,protecci%C3%B3n%20de%20sus%20documentos%20electr%C3%B3nicos.

Microsoft. (2023). Definición de SIEM. Obtenido de https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

National Cyber Security Centre. (29 de Junio de 2021). Device Security Guidance. Guidance for organisations on how to choose, configure and use devices securely: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date.

OSTEC. (24 de octubre de 2022). Purple Team: en medio del Red y el Blue Team. https://ostec.blog/es/aprendizaje-descubrimiento/purple-team-en-medio-del-red-y-el-blue-team/

Parida, B. (19 de junio de 2023). Red Team vs Blue Team: An In-depth Analysis of Cybersecurity Operations https://www.wevolver.com/article/red-team-vs-blue-team-an-in-depth-analysis-of-cybersecurity-operations

Presidencia De La República De Colombia. (2015). Decreto 1078 de 2015. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201078%20DEL%2026%20DE%20MAYO

Quintero, H. (2023). Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.unad.edu.co/bitstream/handle/10596/57180/hquinterom.pdf?sequence=1&isAllowed=y

Reegård, K., & Blackett, C. (septiembre de 2019). The Concept of Cybersecurity Culture. https://www.researchgate.net/publication/336149766_The_Concept_of_Cybersecurity_Culture

Sanjuan, L. (2014). Criptografía. Seminario – Seguridad en desarrollo del Software, 1-34. http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Crip?sequence=1

Shea, S. (junio de 2023). What is cybersecurity? https://www.techtarget.com/searchsecurity/definition/cybersecurity

UNIR-Revista. (07 de enero de 2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

UNIR-Revista. Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? 07 de enero de 2020. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

ANEXOS

Link del video

Reporte Turnitin