TEST DE PENETRACION PENTESTING APLICADO EN LA EMPRESA MEGASEGURIDAD PARA EVALUAR VULNERABILIDADES Y FALLAS EN EL SISTEMA DE INFORMACIÓN.

JOSÉ LUIS GÓMEZ VILLAMIL.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA.

2.020.

TEST DE PENETRACION PENTESTING APLICADO EN LA EMPRESA MEGASEGURIDAD PARA EVALUAR VULNERABILIDADES Y FALLAS EN EL SISTEMA DE INFORMACIÓN.

JOSE LUIS GOMEZ VILLAMIL

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

INGENIERO MARTIN CAMILO CANCELALO RUIZ
Tutor de Curso.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA.
2.020.

ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Fecha sustentación (día, mes, año)

AGRADECIMIENTOS

Agradezco al ingeniero Martin Camilo Cancelalo Ruiz - UNAD, por aportarme conocimiento y motivación a la seguridad informática, y a la empresa Megaseguridad por permitirme aplicar los conocimientos adquiridos durante mi formación profesional.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

MEGASEGURIDAD, es una empresa con una infraestructura pequeña, pero que maneja procesos que requieren un buen soporte tecnológico que le garantice la continuidad de negocio, en esta época en la que la tecnología es el mejor aliado estratégico para cumplir las metas propuestas.

Con la propuesta del proyecto se evaluarán las fallas y vulnerabilidades por medio de la aplicación de pruebas de penetración Pentesting, como resultado se entregará a la Gerencia un diagnóstico real de las posibles vulnerabilidades y fallas a que está expuesta su red de información, así como las fortalezas que tiene que le servirán como base para la implementación de su Sistema de Gestión de la Seguridad de la información.

La información se ha convertido en un activo valioso para las empresas, garantizar su disponibilidad, integridad y confidencialidad debe ser uno de los objetivos de la Gerencia, es por esto que se hace necesario que se generen políticas y controles que garanticen el uso adecuado y la protección de la misma, el uso de herramientas que brinden un diagnóstico real de la situación actual de la información son necesarias para aplicar los correctivos necesarios y garantizar su seguridad.

La tecnología juega un papel importante en establecer mecanismos perimetrales de protección para detectar de manera temprana muchas de las amenazas cibernéticas a las que se ven expuestas las empresas, sin importar el escenario del ciberataque y la complejidad que esto signifique, éstas se deben preparar para gestionar un incidente cibernético.

Palabras claves; Pentesting, vulnerabilidad, sistema de información.

ABSTRACT

MEGASEGURIDAD is a company with a small infrastructure, but which manages processes that require good technological support that guarantees business continuity, in this era in which technology is the best strategic ally to meet the proposed goals.

With the project proposal, the failures and vulnerabilities will be evaluated through the application of Pentesting penetration tests, as a result a real diagnosis of the possible vulnerabilities and failures to which its information network is exposed, as well as the strengths that you have that will serve as a basis for the implementation of your Information Security Management System.

Information has become a valuable asset for companies, guaranteeing its availability, integrity and confidentiality must be one of Management's objectives, which is why it is necessary for policies and controls to be generated that guarantee the proper use and protection of the same, the use of tools that provide a real diagnosis of the current situation of the information are necessary to apply the necessary corrections and guarantee its security.

Technology plays an important role in establishing perimeter protection mechanisms to detect early on many of the cyber threats to which companies are exposed, regardless of the cyberattack scenario and the complexity that this implies, they must prepare to manage a cyberincident.

Keywords; Pentesting, vulnerability, information system.

INTRODUCCIÓN

La seguridad informática y/o la seguridad de la información va en auge y en todas las empresas u organizaciones que contengan algún sistema informático deben estar conscientes que las amenazas están por donde quiera y que la protección de su información debe ser prioridad para el cumplimiento de los objetivos de valor, recordemos que la seguridad cuenta con tres pilares fundamentales que son: la confidencialidad, la integridad y la disponibilidad[1].

Día a día las empresas están sometidas a vulnerabilidades que ponen en riesgo los tres pilares antes mencionados, estos riesgos pueden ser externos e inclusive aún más peligrosos, pueden ser internos. Salvaguardar la información debe ser prioridad, pero entonces como lograr esto, como enfrentar los riesgos a los cuales están expuestos las empresas, para ello han surgido varias normas, leyes e inclusive metodologías y prácticas para que las empresas puedan crear sus propias políticas, procesos y procedimientos, pero un buen comienzo es saber que tan expuesto se está pues es bien sabido que no hay seguridad 100 % completa y por lo general no se sabe cuándo se pueda llegar a tener uno de estos riesgos, simplemente cada empresa tendrá que estar preparada.

Las empresas deben conocer que impacto económico (aunque no solamente sería económico), generaría tener uno de estos riesgos informáticos tan de la mano, para ello podrían practicar ya sea de manera interna con el departamento de TI o el área encargada, unas serie de pruebas que deben hacerse a toda la infraestructura tecnológica y en general al entorno de TI, también podrían hacerse estas pruebas con empresas externas altamente calificadas y personal experto, con estas pruebas se busca que las empresas hagan una evaluación general y comiencen a priorizar sus objetivos de negocio, dicha evaluación se resume en encontrar las vulnerabilidades de riesgo bajo, alto y otras que puedan llevar a ser aprovechadas por algún atacante, ya sea externo o interno[2].

A esas pruebas realizadas sobre la infraestructura o sobre el entorno de TI se le conoce como pentesting o pruebas de penetración, donde se busca que las empresas sepan sus fallos de seguridad y las consecuencias que existen, además

---

[1] VANEGAS ROMERO, Alfonso Yucenid, autor [en línea]. Tesis pentesting, ¿Porque es importante para las empresas? Universidad Piloto de Colombia, 2020. [Consulta: 06 de junio de 2020]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1&isAllowed=y

[2] Ibíd, p.13.

gracias al pentesting las empresas sabrán como minimizar los riesgos, como priorizarlos y como tener los controles pertinentes[3].
La seguridad de la información un activo valioso para las organizaciones, cada vez son más frecuentes las amenazas que afectan el buen funcionamiento de la red de información como virus, ciberataques o malware, un ciberataque o un software malicioso altera el sistema de protección de la información accediendo a áreas restringidas y generando daños[4].

Es por esto que se hace necesario realizar un test de penetración o Pentesting que es la simulación de un ciberataque para comprometer el sistema e identificar fallos y vulnerabilidades, de esta forma se conocen brechas de seguridad con las cuales se puede prevenir ataques externos y determinar riegos.

El Pentesting o test de penetración es un hacking ético que cuenta con la autorización previa del dueño del equipo en el cual se realiza la prueba, los daños que se generan están controlados por el pentester, con los resultados obtenidos se establecen controles para proteger la confidencialidad, disponibilidad e integridad de la información.

Su importancia radica en que se ponen a prueba la fiabilidad y herramientas con que cuenta el sistema de información de la organización, así como la respuesta del sistema ante un ataque ciberataque real[5].

[3] Ibíd, p.13.

[4] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. [en línea]. Tesis Diagnóstico y viabilidad de implementación del modelo de seguridad informática para la empresa Megaseguridad. Universidad Nacional Abierta y a Distancia (UNAD), 2020. [Consulta: 06 de junio de 2020]. Tesis Diagnóstico y viabilidad de implementación del modelo de seguridad informática para la empresa Megaseguridad, pp. 9-30

[5] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Es importante conocer cómo está la situación en materia de seguridad en empresas de Latinoamérica, para esto ESET Latinoamérica publica anualmente un reporte de seguridad, según el Reporte de ESET para 2019 uno de sus principales datos es que 2 de cada 3 empresas sufrieron un incidente de seguridad en 2018 y el 40% sufrió una infección con códigos maliciosos siendo el incidente más recurrente, solo la mitad de las empresas encuestadas cuenta con 3 de los controles más básicos, antivirus, firewall y backup[6].

Las mayores preocupaciones se observan que giran en torno a los principios de seguridad de la información con el acceso indebido (61%), robo de información (58%) y la privacidad de la información 48%, esto se combina con la preocupación por códigos maliciosos (57%) que son las principales herramientas de los cibercriminales para poder hacerse de la información de las empresas[7].

Otro de los incidentes con altos niveles de ocurrencia en las empresas de Latinoamérica es la explotación de vulnerabilidades que afecto cerca del 10% de las empresas encuestadas y en algunos países como Perú (+7%), México (+3%) y Chile (+3%) se vio un incremento para el año anterior[8].

Para el caso de Colombia según el Informe de Tendencias Cibercrimen Colombia 2019-2020 de la CCIT el delito informático más denunciado es el hurto por medios informáticos con un total de 31.058 casos, en segundo lugar se encuentra la violación de datos personales con 8.037 casos, el tercer delito más denunciado es el acceso abusivo a sistemas informáticos con 7.994 casos, en el cuarto lugar con 3.425 casos se encuentra la transferencia no consentida de activos y finalmente en

---

[6] HARÁN, Juan Manuel, autor [en línea]. El 40% de las empresas de América Latina sufrió una infección con malware el último año, 2019. [Consulta: 06 de junio de 2020]. Disponible en:https://www.welivesecurity.com/la-es/2019/09/05/el-40-de-las-empresas-de-america-latina-sufrio-una-infeccion-con-malware-el-ultimo-ano/

[7] Ibíd, p.15.

[8] EXPERTS ON YOUR SIDE. [Sitio web]. Latinoamérica: ESET, Security Report. [Consulta: 12 de junio de 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

el quinto lugar se sitúa el delito de uso de software malicioso con 2.387 casos[9].

El principal interés de los cibercriminales en Colombia se basa en la motivación económica y la posterior monetización de las ganancias generadas en cada ciberataque[10].

1.2 FORMULACIÓN DEL PROBLEMA

MEGASEGURIDAD, no cuenta con un Sistema de Gestión de la Seguridad de la información, lo cual hace que su información sea vulnerable ante cualquier ataque cibernético, situación genera daños y perdida en la información, fallos en el sistema, intermitencia y caída de la red, situaciones que afectan el óptimo funcionamiento de la red y todos sus servicios[11].

Se puede mediante la implementación de pruebas de penetración “Pentesting” detectar fallos o vulnerabilidades en la red de información de la empresa MEGASEGURIDAD.

[9] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES (CCIT), Tendencias del cibercrimen en Colombia 2019-2020 [sitio web]. TicTac. [Consultado: 31 de mayo de 2021]. Disponible en: https://www.nist.gov/about-nist

[10] Ibíd, p.15.

[11] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

2 JUSTIFICACIÓN

La ejecución del proyecto le permitirá a MEGASEGURIDAD garantizar la confidencialidad, integridad y disponibilidad en su información y así garantizar que su red de información sea segura, con la aplicación de pruebas de penetración Pentesting se determinará el nivel de seguridad de la red a través de ataques informáticos simulados, sin poner en riesgo la información[12].

La prueba de penetración permitirá explorar la red, realizar análisis de seguridad y hacer auditorias de la red; una vez aplicada la prueba, se conocerán las debilidades del sistema, se identificarán los activos de mayor riesgo y las áreas que requieren mayor esfuerzo para la protección de datos.

El proyecto se desarrollará en cuatro etapas:

1. Recopilación de información: en la primera etapa o reconocimiento se recopilará la información necesaria para el desarrollo del proyecto, se delimitará la zona de aplicación de la prueba de penetración se realizará el análisis técnico con la herramienta Nmap (escaneo de puertos).
2. Análisis de vulnerabilidades: se descubrirán las fallas en el sistema que pueden ser aprovechadas por posibles atacantes, con la información recopilada y de acuerdo con los resultados obtenidos se buscan vulnerabilidades o brechas de seguridad.
3. Explotación de vulnerabilidades: se intentará sacar provecho de las vulnerabilidades para comprometer el sistema o las aplicaciones[13].
4. Elaboración del informe: se presentará el análisis de los resultados de la prueba y detalle de las vulnerabilidades encontradas, recomendaciones y medidas para solucionar los problemas detectados.

[12] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[13] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Implementar pruebas de penetración Pentesting para detectar fallas y/o vulnerabilidades en la red de información de la empresa MEGASEGURIDAD.

3.2 OBJETIVOS ESPECÍFICOS

1. Realizar un diagnóstico de seguridad informática en la cual se evidencie el estado actual de la compañía, nivel interno y externo.

2. Realizar pruebas de penetración Pentesting en la red de información para determinar qué tipo de vulnerabilidades presenta.

3. Identificar fallas y vulnerabilidades a que está expuesta la red de información.

4. Hacer recomendaciones para mitigar fallas y vulnerabilidades.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Existes muchos conceptos y términos en relación al campo de la seguridad de la información y la seguridad informática, es importante saber que, aunque estos términos no significan lo mismo, ambos buscan garantizar la seguridad de un bien común, LA INFORMACION, a continuación, se presentan algunos términos que son relevantes para el desarrollo del proyecto.

4.1.1 Seguridad informática

La informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar, almacenar y trasmitir la información, la principal tarea de la seguridad informática es la de minimizar los riesgos que pueden prevenir de muchas partes, pueden ser de la entrada de datos, del medio que la transporta, el hardware usado para transmitir y recibir, los mismos usuarios y hasta los mismos protocolos que se implementan, pero siempre la tarea principal es minimizar los riegos para obtener mejor y mayor seguridad[14].

La seguridad informática se puede clasificar en tres partes: los usuarios, la información y la infraestructura[15].

- Los usuarios son considerados como el punto más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información se deben proteger del mismo usuario[16].

- La información es considerada como el principal valor en la seguridad

[14] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[15] ROMERO CASTRO, Martha Irene, et al. Autor [en línea]. Tesis introducción a la seguridad informática y el análisis de vulnerabilidades. Universidad Estatal del sur de Manabí, 2018. [Consulta: 06 de junio de 2020]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[16] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

informática, es lo que se desea proteger y lo que tiene que estar a salvo es el principal activo.

- La infraestructura, es uno de los medios más controlado, pero esto no implica que sea el que corre menos riesgos, esto depende de los procesos que se manejen. Se deben considerar problemas complejos como un acceso no permitido, robo de identidad, hasta daños más comunes como el robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede afectar el material físico de la empresa.

4.1.2 Seguridad de la Información

Los pilares de la seguridad de la información se fundamentan en la necesidad que tienen todos de obtener la información, de su importancia, integridad y disponibilidad para sacarle el máximo de rendimiento con el mínimo riesgo.

La información es vital para la empresa, si cae en manos inapropiadas puede perder su valor, se perderá intimidad o capacidad de maniobra, además la reputación pude verse afectada sin contar con que la información puede ser accedida por cibercriminales y cualquier otra potencial fuente de riesgo.

- La confidencialidad consiste en asegurar que solo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas, para garantizar la confidencialidad se recurre principalmente a tres recursos: Autenticación de usuarios, Gestión de privilegios y cifrado de información[17].

- La integridad es asegurar que la información no se pierda ni se vea comprometida voluntaria o involuntariamente, para garantizar la integridad de la información se debe considerar lo siguiente. “1” Monitorear en tráfico de la red para descubrir posibles intrusiones. “2” Auditar los sistemas para implementar políticas de auditorías que registren quien hace que, cuando y con qué información. “3” Implementar sistemas de control de cambio. “4” Otro recurso serán las copias de seguridad, que permiten recuperar la información en su estado anterior[18].

- La disponibilidad La información para resultar útil y valiosa debe estar disponible para quien la necesita, se deben implementar las medidas necesarias para que

[17] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

[18] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

tanto la información como los servicios estén disponibles, para este propósito se implementa política de control como. “1” El acuerdo de nivel de servicio o (SLA). “2” Balanceadores de carga de tráfico para minimizar el impacto de DDos. “3” Copias de seguridad para restaurar la información perdida. “4” Disponer de recursos alternativos a los primarios[19].

4.1.3 Evaluación de riesgos, amenazas y vulnerabilidades

Cuando se plantea mejorar la seguridad de una empresa se debe tener en cuenta factores como recursos, amenazas, vulnerabilidades y riesgos.

Los recursos son los bienes tangibles e intangibles con los que se cuenta para hacer las tareas, la información de que se dispone es un bien intangible, los bienes tangibles son los recursos de que dispone en la empresa, servidores, equipos de red, computadoras, teléfonos[20]. El riesgo es la probabilidad de que algo negativo suceda dañando los bienes tangibles e intangibles de la empresa, las amenazas son esos sucesos que pueden dañar los procedimientos o recursos, mientras que las vulnerabilidades son los fallos de los sistemas de seguridad o en los que el usuario utiliza para desarrollar las actividades que permitirán que una amenaza tuviese éxito a la hora de generar un problema.

El principal trabajo de un responsable de la seguridad es la evaluación de los riesgos identificando las vulnerabilidades, amenazas y en base de esta información, evaluar los riesgos a que están sujetos las actividades y recursos. Se debe considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad.

Existen amenazas difíciles de controlar como los desastres naturales y los errores humanos, pero deben ser tenidas en cuenta a la hora de calcular los riesgos, una persona podría borrar accidentalmente información de un servidor o podría enviar un correo con información confidencial, del mismo modo el hardware de los recursos informáticos de la empresa puede verse dañados por el uso, por inundaciones, por fallas eléctricas, etc. Las amenazas voluntarias son aquellas que se derivan de ataques voluntarios ya sean de agentes internos o externos, los agentes internos pueden ser un ex empleado cuyas credenciales de acceso no han sido revocadas y los agentes externos pueden ser competencia desleal, terroristas, cibercriminales, etc.

---

[19] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

[20] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

Las vulnerabilidades son por lo general fallos de diseño de procedimientos o recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar un recurso, las vulnerabilidades son fallos en los sistemas, no son puertos abiertas diseñadas deliberadamente, sino errores de diseños, configuración o implementación que generan oportunidades de ataques, es decir que hace viable una amenaza.

Desde hace algunos años se viene reconociendo la información como uno de los principales recursos de las organizaciones, la cual debe ser administrada de forma clara, organizada, correcta y eficiente para optimizar su utilidad, los usos y/o procesos que se realizan con la información deben ser respaldados por el sistema de información SI, el cual realiza cuatro actividades básicas[21].

- Entrada de la Información (INPUT) Técnica mediante la cual el sistema obtiene los datos que necesita para el procesamiento de la información, por medio de teclados, códigos de barras, medios magnéticos, etc.[22].
- Almacenamiento de la información a través de esta tarea el sistema puede retomar la información empleada (modificada, eliminada, agregada, etc.)en procesos anteriores[23].
- Procesamiento de la información: Propiedad del sistema que facilita la transformación de la información para luego ser utilizada en la toma de decisiones para hacer más eficiente y productivo el negocio[24].
- Salida de la información (OUTPUT) Método con el cual se saca la información procesada mediante impresiones, medios magnéticos videos, etc.

El eficiente manejo del SI se ha convertido en un reto para las organizaciones ya que se ha logrado comprender que la información tiene un valor económico y que con su correcto uso logran mejoras que les permite ser más eficientes y competitivas.

El presente proyecto se base en la seguridad de la información o seguridad informática, es importante conocer algo de la historia de la tecnología, conocer como fue adquiriendo valor la información a través del tiempo, En la década de los 60's la empresa System Development Corporation (SDC). Elaboro un acuerdo para realizar estudios en diferentes áreas para romper sistemas de tiempo compartido, de allí surgieron los primeros equipos de penetradores que buscaban comprender las

[21] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

[22] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

[23] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

[24] ROMERO CASTRO, Martha Irene, et al. Op. Cit., p.19.

vulnerabilidades de los equipos militares y del gobierno, utilizaban la penetración de computadoras pentesting como medio para la seguridad del sistema en prueba[25].

La metodología Pentesting en los años siguientes a su nacimiento se ha vuelto más sofisticada y compleja, actualmente constituye un conjunto de herramientas para la evaluación de la seguridad de sistemas o incluso servidores, hoy en día existe una gran variedad de metodologías de Pentesting cada uno con su grado de complejidad, las hay de origen militar como es Kill-Chain que se muestra por etapas y las aplicaciones están a criterio del pentester. Otra metodología no muy conocida pero la más completa es la OSSTMM (Open Sourse Security Testing Methodology Manual) está diseñada para ser coherente y repetible, permite al auditor de seguridad hacer pruebas más precisas y ejecutables[26].

Por otro lado, se encuentra OWASP que es una empresa enfocada a la seguridad web que cuenta con una guía de acceso libre para realizar pruebas a aplicaciones web, adicional está el sistema enfocado en la seguridad conocida como distribución para Pentesting (DISTRO), ayuda a detectar las vulnerabilidades de los sistemas informáticos o redes de computadoras. Se utiliza en las auditorias de seguridad con el apoyo de numerosas herramientas, la distribución más popular y usada por auditores de seguridad es Kali Linux[27].

Cada vez las organizaciones son más conscientes de realizar auditorías de seguridad de forma periódica, ya que las consecuencias derivadas de un ataque a sus sistemas a menudo se ven reflejadas en grandes pérdidas económicas y desconfianza por parte de sus clientes.

4.1.4. Que El Pentesting

Es una práctica o metodología realizada para descubrir vulnerabilidades y/o fallos de seguridad en un sistema informático, en una página web, en seguridad física o en cualquier entorno, para las empresas es de gran utilidad pues pueden comprobar hasta qué punto su red interna o algún sistema informático es seguro ante un ataque informático, está diseñado para clasificar y determinar los alcances y las repercusiones de los fallos de seguridad, dando resultados para las empresas en cuanto a poder identificar la información o entornos a los cuales se podrían alcanzar en un ataque, además de evaluar la eficiencia de la defensa con la que cuentan[28].

---

[25] MARTÍNEZ SÁNCHEZ, Patricia Alejandra. Op. Cit., p.23.

[26] MARTÍNEZ SÁNCHEZ, Patricia Alejandra. Op. Cit., p.23.

[27] MARTÍNEZ SÁNCHEZ, Patricia Alejandra. Op. Cit., p.23.

[28] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

4.1.4.1 Tipos de Pentesting

Dependen del tipo de información que se tenga sobre el sistema al que se quiere aplicar la prueba, esta puede ser:

a. Caja Blanca: Parte de un análisis integral, son las más fáciles de practicar pues la empresa suministra toda la información posible como por ejemplo cantidad de equipos, tipos de sistemas, estructura de la red, etc. Se usa la mayor cantidad de datos posibles para detectar puntos de fallo o vulnerabilidades potenciales en lo que su tiempo de ejecución es mayor en comparación con los otros tipos de pruebas[29].
b. Caja Negra: Es una prueba a ciegas, no se tiene información de los sistemas de infraestructura, redes, contraseñas, etc. Se acerca a la realidad de la empresa y sirve para reconocer que tan fuerte o frágiles se está[30].
c. Caja Gris: Es una mezcla de las anteriores, se usa cuando se quiere conocer vulnerabilidades en sectores determinados es muy rentable y proporciona información real de las amenazas[31].

4.1.4.2 Etapas del Pentesting

A continuación, se describen de las etapas en la aplicación de las pruebas de penetración Pentesting:

1. Reconocimiento y enumeración: En esta fase se recopila la información necesaria sobre el objetivo.
2. Análisis de Vulnerabilidades: Con la información recopilada y de acuerdo con los resultados obtenidos se busca vulnerabilidades o brechas de seguridad.
3. Explotación: Se saca provecho de las vulnerabilidades encontradas para intentar comprometer el sistema.
4. Informe: Presentación del informe con los resultados obtenidos durante las fases ejecutadas, en el cual se detallarán los riesgos de todas las vulnerabilidades encontradas.

---

[29] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[30] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[31] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

4.2 MARCO CONCEPTUAL

Activo, es todo elemento o material digital, físico o humano que puede ser afectado y que requiere protección.

Amenaza, es un evento que puede afectar los activos de la organización.

Armitage, es una herramienta instalada en Kali Linux, una distribución de GNU/Linux en formato Live CD diseñada para la realización de auditoria de seguridad.

Arp, protocolo de resolución de direcciones a nivel de capa de red responsable de encontrar la dirección MAC que corresponde.

Atacante, persona con conocimientos informáticos que está acechando un sistema.

Ataque, es un proceso dirigido por un atacante a través de un programa que intenta ingresar a un sistema.

Auditoria, es un estudio que se encarga de analizar e identificar vulnerabilidades.

Autenticación, es el proceso de establecimiento y verificación de la identidad para realizar una petición.

Blacktrack, distribución de Linux para realizar un ethical hacking, contiene varias herramientas de hacking.

Contraseña, es una clave para la autenticación que tiene información secreta para el acceso.

Cracker, persona con conocimiento de herramientas de hacking, pero con fines maliciosos.

Criptografía, proceso de transformar un test plano en un texto descifrado.

Denegación de servicios, es interrumpir el funcionamiento correcto de un servicio.

Exploits, consiste en aprovechar errores de programación en una aplicación con el objetivo de tomar el control de un sistema o realizar una escalada de privilegios.

Estimación del Riesgo, es el proceso que permite asignar valores para determinar la probabilidad y las consecuencias de un riesgo sobre un activo.

Identificación del Riesgo, es el proceso que permite encontrar, enumerar y caracterizar los activos del riesgo.

Impacto**,** es el efecto que puede generar la materialización de una amenaza sobre un activo.

Firewall, es un cortafuego/ software para controlar las comunicaciones denegando o permitiendo.

FTP, Protocolo de transferencia de archivos.

Hacker, individuo con conocimientos informáticos que no tiene intenciones maliciosas y es apasionado por la seguridad informática.

HTTP, protocolo perteneciente a la capa de aplicación usada para las trasferencias de los datos.

HTTPS**,** es un protocolo basado en http, asegurando la trasferencia de los datos.

IDS, sistema de detección de intrusos que detecta accesos no autorizados a una red a un sistema.

Ingeniería social, técnica que se aprovecha de la ingenuidad de las personas con el objeto de obtener información.

IPS, sistema de prevención de intrusos que previene accesos no autorizados.

IPSEC, protocolo seguro sobre el protocolo IP.

Nmap, herramienta para el escaneo de puertos.

Protocolo, conjunto de reglas que establecen la comunicación entre dos computadoras.

TCP, protocolo de control de trasmisión orientado a la conexión, ofreciendo mecanismos de seguridad en el proceso de comunicación.

TCP/IP, modelo de descripción de protocolos de red Telnet. Protocolo que permite la conexión desde un terminal remoto.

Test de Penetración, es un conjunto de metodologías y técnicas que permiten analizar debilidades de los sistemas informáticos.

Vulnerabilidad, es una debilidad presente en cualquier sistema pudiendo ser explotada.
Xploit, es un mecanismo que consiste en que la víctima recibe una postal falsa en su correo electrónico que contiene un link de una web falsa.

4.3 MARCO LEGAL.

De acuerdo con la actividad de cada empresa, se debe seguir la normatividad o leyes vigentes con el fin de no incurrir en multas por incumplimiento, existen varias normativas para la realización de “Pentesting”, cada empresa deberá seguir la reglamentación del país o según la metodología aplicada[32].

4.3.1 Normatividad Internacional

4.3.1.1 Estándar ISO/IEC 27001

Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI, documentado dentro del contexto de los riesgos globales del negocio de la organización.

Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a parte de ellas.

El SGSI está diseñado para asegurar controles de seguridad, suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas.

4.3.2 Normatividad Nacional

4.3.2.1. Ley 1273 de 2009 Delitos Informáticos

La normatividad colombiana está reglamentada por la ley 1273 de 2009 expedida por el congreso de la República de Colombia por la cual se modifica el Código Penal, se crea un nuevo bien jurídico titulado denominado De la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones la cual decreta[33].

Artículo 1, adicionase el Código penal con un Titulo VII BIS denominado de la

[32] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[33] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES [Sitio web]. Colombia: MINTIC, Ley 1273 de 2009. [Consulta: 20 de junio de 2020]. Disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Protección de la información y de los datos, en el siguiente tenor[34].

CAPITULO PRIMERO, de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos[35].

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMATICO, 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, incurrirá en una pena de prisión.

Artículo 269B. OSTACULIZACION ILEGITIMA DE SISTEMA INFORMATICO O RED DE TELECOMUNICACIONES, el que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión.

Artículo 269C. INTERCEPTACION DE DAÑOS INFORMATICOS, el que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o en las emisiones electromagnéticas provenientes de un sistema informático que los transporte que lo transporte incurrirá en pena de prisión.

Artículo 269D. DAÑO INFORMATICO, el que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión.

Artículo 269E. USO DE SOFTWARE MALICIOSO, el que, sin estar facultado para ello produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión.

Artículo 269F. VIOLACION 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, incurrirá en pena de prisión.

Artículo 269G. SUPLANTACION DE SITOS WEB PARA CAPTURAR DATOS PERSONALES, el que con objeto ilícito y sin estar facultado para ello, diseño,

[34] Ibíd, p.30.

[35] Ibíd, p.30.

desarrolle, trafique, venda, ejecute, programe, o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACION PUNITIVA, las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere.

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviera un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgos para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO SEGUNDO, de los atentados informáticos y otras infracciones.

Artículo 269I. HURTOS POR MEDIOS INFORMATICOS Y SEMEJANTES, el que superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este código[36].

Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS, el que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la trasferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión[37].

[36] Ibíd, p.30.

[37] Ibíd, p.30.

4.4 MARCO METODOLÓGICO

La metodología seleccionada para el proyecto es Penetration Testing Execution Stándard (PTES), apoyados también en la metodología Magerit, que se adapta al ámbito de aplicación, está orientada a niveles técnicos específicamente y permite una fácil comunicación con la empresa gracias a que maneja niveles de riesgo dirigidos a un lenguaje para negocio y una descripción cualitativa. Se divide en 7 fases, así[38]:

- Interacción previa: En esta fase se establecen las reglas sobre lo que se va a realizar, se establece el alcance, el objetivo y la infraestructura que ingresa en la prueba de penetración, se define el tiempo de ejecución de la prueba y se definen costos.
- Recolección de Información: El objetivo es recolectar la información necesaria para usarla en la evaluación de vulnerabilidades y la fase de explotación cuando se esté realizando la penetración al objetivo, se deben tener claras las reglas de recolección de información indicadas por la empresa y el objetivo planteado para evitar pérdida de tiempo y dinero examinado sistemas que estén fuera del alcance.
- Modelado de amenaza: No hay un modelo específico, se debe escoger un modelo de impacto para la empresa para tener una visión objetiva de los posibles escenarios donde se materialice una amenaza, esa fase permite priorizar los activos de la empresa y le da al Pentester una base para probar procesos, procedimientos y controles más destacados.
- Análisis de vulnerabilidades, en esta fase se detectan las vulnerabilidades del sistema o de las aplicaciones que un atacante puede usar para acceder. Esta fase se puede valorar en dos etapas activa y pasiva, la activa hace referencia a la interacción directa con el componente o servicio que se esté evaluando, la pasiva es la exploración de los metadatos en los archivos expuestos al público[39].
- Explotación, en esta fase se determina el acceso a un sistema, es necesario tener un buen análisis de vulnerabilidades para tener claro el punto de entrada y reconocer los activos de mayor valor, para que esta etapa sea exitosa se debe personalizar el ataque, el exploit se debe modificar de acuerdo a la tecnología e infraestructura propia de la empresa.
- Post-Explotación se valora la maquina comprometida de acuerdo con la información almacenada, privilegios que tenga, otras máquinas a las que pueda acceder o la utilidad para comprometer la red, es importante precisar con la empresa roles y responsabilidades establecidas en las primeras fases para protegerla, para realizar este tipo de pruebas se debe contar con el

[38] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[39] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

consentimiento de parte de la empresa y dejar claro que y como se va a hacer para evitar problemas legales al acceder a un sistema sin autorización.

- Informe, esta metodología tiene una guía del reporte técnico y ejecutivo que se debe presentar que incluye el contexto en el que se realizó la prueba, los lineamientos, objetivos alcanzados, informar los riesgos encontrados clasificados por su criticidad, presentar hallazgos encontrados y las recomendaciones o actividades que se deben realizar para resolver los riesgos encontrados.

Las herramientas de intrusión a utilizar en la aplicación de pruebas de penetración son Armitage y Nmap en Kali Linux una distribución GNU/Linux, están diseñadas para realizar auditorías de seguridad, escaneo de puertos, vulnerabilidades en redes de datos, así como también escaneo de vulnerabilidades de bases de datos, herramientas para auditoria, análisis forenses, es utilizada por los “Pentester” o hacker éticos en pruebas de penetración, para verificar si hay servicios no autorizados ejecutándose, o para descubrir posibles objetivos de ataque[40].

[40] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

5 DESARROLLO DE LOS OBJETIVOS

5.1 REALIZAR UN DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA EN LA CUAL SE EVIDENCIE EL ESTADO ACTUAL DE LA COMPAÑÍA, NIVEL INTERNO Y EXTERNO.

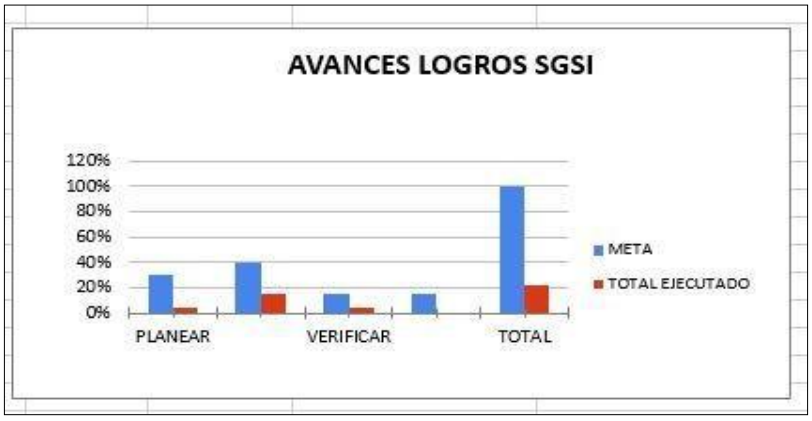
Para el diagnóstico de seguridad informática interno y externo de la empresa, se tomó como referencia la norma ISO 27001:2013, en su anexo "A", con el fin de tener un breve resumen del estado de implementación de los controles básicos de la dependencia a auditar[41].

Tabla 1. Análisis Logros por Fase.

	FASE	META	TOTAL EJECUTADO
LOGRO1	PLANEAR	30%	3,8%
LOGRO2	HACER	40%	14,6%
LOGRO3	VERIFICAR	15%	3,8%
	ACTUAR	15%	0,0%
	TOTAL	100%	22,2%

Fuente: "elaboración propia"

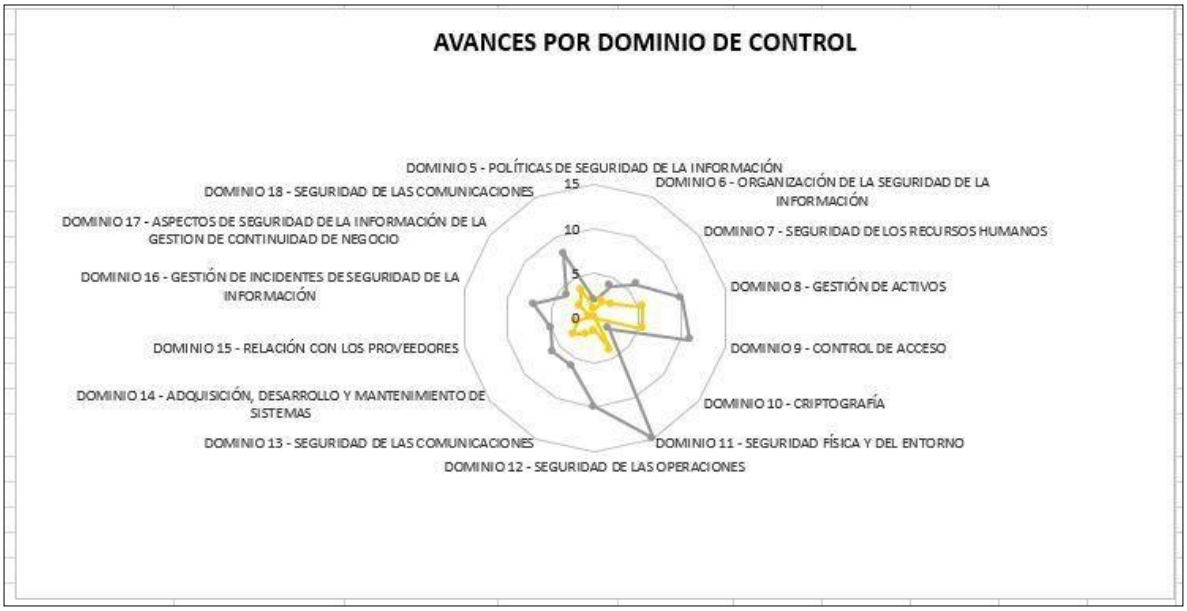
Figura 1. Avance Logro SGSI.



Fuente: "elaboración propia"

[41] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

Figura 2. Estado de implementación por Dominio ISO 2700:2013.



Fuente: “elaboración propia”

Cuadro 1. Consolidado de Implementación ISO 27001:2013

POR DOMINIO DE CONTROL						
NOMBRE DOMINIOS DE CONTROL	CONTROLES QUE APLICAN	PESO CONTROLES IMPLEMENTADOS Y PARCIALMENTE IMPLEMENTADOS	IMPLEMENTADOS	PARCIALMENTE	NO CUMPLE	NO APLICA
DOMINIO 5 - POLÍTICAS DE SEGURIDAD DE LA	2	1	0	2	0	0
DOMINIO 6 - ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	4	2	0	4	0	3
DOMINIO 7 - SEGURIDAD DE LOS RECURSOS HUMANOS	6	2,5	0	5	1	0
DOMINIO 8 - GESTIÓN DE ACTIVOS	10	5,5	1	9	0	0
DOMINIO 9 - CONTROL DE ACCESO	11	5,5	0	11	0	3
DOMINIO 10 - CRIPTOGRAFÍA	2	0	0	0	2	0
DOMINIO 11 - SEGURIDAD FÍSICA Y DEL ENTORNO	15	4	0	8	7	0
DOMINIO 12 - SEGURIDAD DE LAS OPERACIONES	10	1,5	0	3	7	4
DOMINIO 13 - SEGURIDAD DE LAS COMUNICACIONES	6	2	0	4	2	1
DOMINIO 14 - ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	6	3	0	6	0	7
DOMINIO 15 - RELACIÓN CON LOS PROVEEDORES	5	2	0	4	1	0
DOMINIO 16 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	0,5	0	1	6	0
DOMINIO 17 - ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO	4	2	0	4	0	0
DOMINIO 18 - SEGURIDAD DE LAS COMUNICACIONES	8	3,5	1	5	2	0

Fuente: “elaboración propia”

Como análisis del diagnóstico de seguridad de la información a la dirección de Talento humano de la empresa Megaseguridad, se puede evidenciar que el total

de implementación es del 22% como se describe en la ilustración 4-1 Análisis de logros por fases, evidenciando grandes falencias de implementación de seguridad en relación al anexo. “A” de la norma ISO 27001:2013[42].

Tabla 2. Valor Cualitativo Activos de Información.

Valores			
Mínimo	Máximo	Ponderación	Valor
>190.000		Muy - alto	M.A.
90.000	<180.000	Alto	A.
40.000	<80.000	Medio	M.
15.000	<35.000	Bajo	B.
	10.000	Muy-bajo	M.B.

Fuente: “elaboración propia”

Tabla 3. Probabilidad de Ocurrencia.

Valor sobre dia (Frecuencia)				
Año	Descripción	Siglas	Dias	Valor
1	Extremadamente - Frecuente	E.F.	1	1
1	Muy- frecuente	M.F.	20	0,05
1	Frecuente	F.	80	0,0125
1	Poco - Frecuente	P.F.	182	0,00549451
1	Muy - poco - Frecuente	M.P.F.	366	0,00273224

Fuente: “elaboración propia”

Relación de Impacto, desde el valor cualitativo hasta el cualitativo[43].

[42] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[43] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

Tabla 4. Relación Impacto.

Cuantitativo		
Descripción	Siglas	Valor
Critico	C.	(85% - 100%]
Alto	A.	(65% - 84%]
Medio	M.	(35% - 64%]
Bajo	B.	[4% - 34%]

Fuente: “elaboración propia”

Análisis de activos.

Tabla 5. Análisis de Activo – Magerit.

Activo	Código #	Activo	Cuantitativo	Cualitativo
APP	A001	Siasoft_SIIGO	$ 40.000.000	A.
Físico_F	F001	Lector biométrico	$ 60.000.000	M.A.
	F002	Circuito cerrado de televisión	$ 80.000.000	M.A.
Hardware_H	H001	Server 2012r2 Archivos	$ 30.000.000	A.
	H002	Computadores	$ 20.000.000	A.
Servicio_SE	SE001	Proveedor de datos	$ 12.000.000	M.A.
	SE002	Firewall	$ 6.000.000	B.
	SE003	Cpanel de dominio	$ 9.000.000	B.
	SE004	Printer	$ 7.000.000	B.
	SE005	Active Directory	$ 20.000.000	A.
Software_SO	SO001	Sistema operativo Wind10	$ 7.000.000	B.
	SO002	Ofimática Off2010	$ 7.000.000	B.

Fuente: “elaboración propia”

Análisis de Amenazas.

Tabla 6. Análisis de Amenazas Primera Parte.

Codigo#	Activo	Amenaza =A	Cualitativo	Cuantitativo	A.	C.	I.	D.	T.	Impacto Potencial
A001	APP	A_Fuego	M.P.F.	0,003				85%		$ 128.894
		A_Daños_por_agua	M.P.F.	0,003				75%		$ 146.080
		A_Otros_desastres_Naturales	M.P.F.	0,003				75%		$ 146.080
		A_Fuego	M.P.F.	0,003				85%		$ 128.894
		A_Daños_por_agua	M.P.F.	0,003				75%		$ 146.080
		A_Contaminacion_Mecanica	M.P.F.	0,003				65%		$ 168.554
		A_Contaminación_electromagnética	M.P.F.	0,003				45%		$ 243.467
		A_Avería_de_origen_fisico/lógico	M.P.F.	0,003				55%		$ 199.200
		A_Corte_del_suministro_eléctrico	M.P.F.	0,003				55%		$ 199.200
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$ 199.200
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$ 243.467
		A_Errores_del_administrador	M.P.F.	0,003		55%	55%	55%		$ 66.400
		A_Errores_de_mantenimiento/actualización_de_equipos_(hardware)	F.	0,017				55%		$ 1.212.073
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$ 291.435
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$ 145.717
		A_Abuso_de_privilegios_de_acceso	P.F.	0,005		75%	55%	65%		$ 112.090
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$ 66.400
		A_Acceso_no_autorizado	M.P.F.	0,003		75%	55%			$ 84.277
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$ 168.554
		A_Manipulación_de_los_equipos	P.F.	0,005		55%		55%		$ 198.703
		A_Denegación_de_servicio	M.P.F.	0,003				65%		$ 168.554
		A_Robo	P.F.	0,005		75%		75%		$ 145.717
		A_Ataque_destructivo	M.P.F.	0,003				75%		$ 146.080
F001	Fisico_F	A_Fuego	M.P.F.	0,003				85%		$ 193.341
		A_Daños_por_agua	M.P.F.	0,003				75%		$ 219.120
		A_Otros_desastres_Naturales	M.P.F.	0,003				75%		$ 219.120
		A_Fuego	M.P.F.	0,003				85%		$ 193.341
		A_Daños_por_agua	M.P.F.	0,003				75%		$ 219.120
		A_Contaminacion_Mecanica	M.P.F.	0,003				65%		$ 252.831
		A_Contaminación_electromagnética	M.P.F.	0,003				45%		$ 365.200
		A_Avería_de_origen_fisico/lógico	M.P.F.	0,003				55%		$ 298.800
		A_Corte_del_suministro_eléctrico	M.P.F.	0,003				55%		$ 298.800
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$ 298.800
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$ 365.200
		A_Errores_del_administrador	M.P.F.	0,003		55%	55%	55%		$ 99.600
		A_Errores_de_mantenimiento/actualización_de_equipos_(hardware)	F.	0,017				55%		$ 1.818.109
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$ 437.152
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$ 218.576
		A_Abuso_de_privilegios_de_acceso	P.F.	0,005		75%	55%	65%		$ 168.133
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$ 99.600
		A_Acceso_no_autorizado	M.P.F.	0,003		75%	55%			$ 126.415
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$ 252.831
		A_Manipulación_de_los_equipos	P.F.	0,005		55%		55%		$ 298.058
		A_Denegación_de_servicio	M.P.F.	0,003				65%		$ 252.831
		A_Robo	P.F.	0,005		75%		75%		$ 218.576
		A_Ataque_destructivo	M.P.F.	0,003				75%		$ 219.120

Fuente: “elaboración propia”

Tabla 7. Análisis de Amenazas Segunda Parte.

					Impacto					
Código#	Activo	Amenaza =A	Cualitativo	Cuantitativo	A.	C.	I.	D.	T.	Impacto Potencial
F002	Físico_F	A_Fuego	M.P.F.	0,003				85%		$257.788
		A_Daños por agua	M.P.F.	0,003				75%		$292.160
		A_Otros desastres_Naturales	M.P.F.	0,003				75%		$292.160
		A_Fuego	M.P.F.	0,003				85%		$257.788
		A_Daños por agua	M.P.F.	0,003				75%		$292.160
		A_Contaminacion_Mecanica	M.P.F.	0,003				85%		$337.108
		A_Contaminación_electromagnética	M.P.F.	0,003				45%		$486.933
		A_Avería_de_origen_físico/lógico	M.P.F.	0,003				55%		$398.400
		A_Corte_del_suministro_eléctrico	M.P.F.	0,003				55%		$398.400
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$398.400
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$486.933
		A_Errores_del_administrador	M.P.F.	0,003		55%	55%	55%		$132.800
		A_Errores_de_mantenimiento/actualización_de_equipos_(hardware)	F.	0,017				55%		$2.424.143
		A_Caída_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$582.869
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$291.435
		A_Abuso_de_privilegios_de_acceso	P.F.	0,005		75%	55%	65%		$224.181
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$132.800
		A_Acceso_no_autorizado	M.P.F.	0,003		75%	55%			$168.554
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$337.108
		A_Manipulación_de_los_equipos	P.F.	0,005		55%		55%		$397.411
		A_Denegación_de_servicio	M.P.F.	0,003				65%		$337.108
		A_Robo	P.F.	0,005		75%		75%		$291.435
		A_Ataque_destructivo	M.P.F.	0,003				75%		$292.160
H001	Hardware_H	A_Fuego	M.P.F.	0,003				85%		$96.671
		A_Daños por agua	M.P.F.	0,003				75%		$109.560
		A_Otros desastres_Naturales	M.P.F.	0,003				75%		$109.560
		A_Fuego	M.P.F.	0,003				85%		$96.671
		A_Daños por agua	M.P.F.	0,003				75%		$109.560
		A_Contaminacion_Mecanica	M.P.F.	0,003				85%		$126.413
		A_Contaminación_electromagnética	M.P.F.	0,003				45%		$182.600
		A_Avería_de_origen_físico/lógico	M.P.F.	0,003				55%		$149.400
		A_Corte_del_suministro_eléctrico	M.P.F.	0,003				55%		$149.400
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$149.400
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$182.600
		A_Errores_del_administrador	M.P.F.	0,003		55%	55%	55%		$49.800
		A_Errores_de_mantenimiento/actualización_de_equipos_(hardware)	F.	0,017				55%		$909.053
		A_Caída_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$218.576
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$109.288
		A_Abuso_de_privilegios_de_acceso	P.F.	0,005		75%	55%	65%		$84.068
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$49.800
		A_Acceso_no_autorizado	M.P.F.	0,003		75%	55%			$63.208
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$126.413
		A_Manipulación_de_los_equipos	P.F.	0,005		55%		55%		$149.029
		A_Denegación_de_servicio	M.P.F.	0,003				65%		$126.413
		A_Robo	P.F.	0,005		75%		75%		$109.288
		A_Ataque_destructivo	M.P.F.	0,003				75%		$109.560

Fuente: “elaboración propia”

Tabla 8. Análisis de Amenazas Tercer Parte.

					Impacto					
Código#	Activo	Amenaza =A	Cualitativo	Cuantitativo	A.	C.	I.	D.	T.	Impacto Potencial
		A_Fuego	M.P.F.	0,003				85%		$64.447
		A_Daños_por_agua	M.P.F.	0,003				75%		$73.040
		A_Otros_desastres_Naturales	M.P.F.	0,003				75%		$73.040
		A_Fuego	M.P.F.	0,003				85%		$64.447
		A_Daños_por_agua	M.P.F.	0,003				75%		$73.040
		A_Contaminacion_Mecanica	M.P.F.	0,003				65%		$84.277
		A_Contaminación_electromagnética	M.P.F.	0,003				45%		$121.733
		A_Averia_de_origen_fisicológico	M.P.F.	0,003				55%		$99.600
		A_Corte_del_suministro_eléctrico	M.P.F.	0,003				55%		$99.600
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$99.600
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$121.733
		A_Errores_del_administrador	M.P.F.	0,003		55%	55%	55%		$33.200
H002	Hardware_H	A_Errores_de_mantenimiento/actualización_de_equipos_(hardware)	F.	0,017				55%		$606.036
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$145.717
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$72.859
		A_Abuso_de_privilegios_de_acceso	P.F.	0,005		75%	55%	65%		$56.043
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$33.200
		A_Acceso_no_autorizado	M.P.F.	0,003		75%	55%			$42.138
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$84.277
		A_Manipulación_de_los_equipos	P.F.	0,005		55%		55%		$99.353
		A_Denegación_de_servicio	M.P.F.	0,003				65%		$84.277
		A_Robo	P.F.	0,005		75%		75%		$72.859
		A_Ataque_destructivo	M.P.F.	0,003				75%		$73.040
		A_Fuego	M.P.F.	0,003				85%		$38.668
		A_Daños_por_agua	M.P.F.	0,003				75%		$43.824
		A_Otros_desastres_Naturales	M.P.F.	0,003				75%		$43.824
		A_Fuego	M.P.F.	0,003				85%		$38.668
		A_Daños_por_agua	M.P.F.	0,003				75%		$43.824
		A_Contaminacion_Mecanica	M.P.F.	0,003				65%		$50.566
		A_Contaminación_electromagnética	M.P.F.	0,003				45%		$73.040
		A_Averia_de_origen_fisicológico	M.P.F.	0,003				55%		$59.760
		A_Corte_del_suministro_eléctrico	M.P.F.	0,003				55%		$59.760
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$59.760
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$73.040
		A_Errores_del_administrador	M.P.F.	0,003		55%	55%	55%		$19.920
SE001	Servicio_SE	A_Errores_de_mantenimiento/actualización_de_equipos_(hardware)	F.	0,017				55%		$363.622
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$87.430
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$43.715
		A_Abuso_de_privilegios_de_acceso	P.F.	0,005		75%	55%	65%		$33.627
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$19.920
		A_Acceso_no_autorizado	M.P.F.	0,003		75%	55%			$25.283
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$50.566
		A_Manipulación_de_los_equipos	P.F.	0,005		55%		55%		$59.612
		A_Denegación_de_servicio	M.P.F.	0,003				65%		$50.566
		A_Robo	P.F.	0,005		75%		75%		$43.715
		A_Ataque_destructivo	M.P.F.	0,003				75%		$43.824

Fuente: “elaboración propia”

Tabla 9. Análisis de Amenazas Cuarta Parte.

					Impacto					
Código#	Activo	Amenaza =A	Cualitativo	Cuantitativo	A.	C.	I.	D.	T.	Impacto Potencial
		A_Fuego	M.P.F.	0,003				85%		$ 19.334
		A_Daños por agua	M.P.F.	0,003				75%		$ 21.912
		A_Otros desastres Naturales	M.P.F.	0,003				75%		$ 21.912
		A_Fuego	M.P.F.	0,003				85%		$ 19.334
		A_Daños por agua	M.P.F.	0,003				75%		$ 21.912
		A_Contaminacion Mecanica	M.P.F.	0,003				65%		$ 25.283
		A_Contaminación electromagnética	M.P.F.	0,003				45%		$ 36.520
		A_Avería de origen físico/lógico	M.P.F.	0,003				55%		$ 29.880
		A_Corte del suministro eléctrico	M.P.F.	0,003				55%		$ 29.880
		A_Condiciones_inadecuadas_de_temperatura_o humedad	M.P.F.	0,003				55%		$ 29.880
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$ 36.520
		A_Errores del administrador	M.P.F.	0,003		55%	55%	55%		$ 9.960
SE002	Servicio_SE	A_Errores_de_mantenimiento/actualización de equipos (hardware)	F.	0,017				55%		$ 181.811
		A_Caída_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$ 43.713
		A_Pérdida de equipos	P.F.	0,005		75%		75%		$ 21.858
		A_Abuso de privilegios de acceso	P.F.	0,005		75%	55%	65%		$ 16.814
		A_Uso no previsto	M.P.F.	0,003		55%	55%	55%		$ 9.960
		A_Acceso no autorizado	M.P.F.	0,003		75%	55%			$ 12.642
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$ 25.283
		A_Manipulación de los equipos	P.F.	0,005		55%		55%		$ 29.806
		A_Denegación de servicio	M.P.F.	0,003				65%		$ 25.283
		A_Robo	P.F.	0,005		75%		75%		$ 21.858
		A_Ataque destructivo	M.P.F.	0,003				75%		$ 21.912
		A_Fuego	M.P.F.	0,003				85%		$ 29.001
		A_Daños por agua	M.P.F.	0,003				75%		$ 32.868
		A_Otros desastres Naturales	M.P.F.	0,003				75%		$ 32.868
		A_Fuego	M.P.F.	0,003				85%		$ 29.001
		A_Daños por agua	M.P.F.	0,003				75%		$ 32.868
		A_Contaminacion Mecanica	M.P.F.	0,003				65%		$ 37.925
		A_Contaminación electromagnética	M.P.F.	0,003				45%		$ 54.780
		A_Avería de origen físico/lógico	M.P.F.	0,003				55%		$ 44.820
		A_Corte del suministro eléctrico	M.P.F.	0,003				55%		$ 44.820
		A_Condiciones_inadecuadas_de_temperatura_o humedad	M.P.F.	0,003				55%		$ 44.820
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$ 54.780
		A_Errores del administrador	M.P.F.	0,003		55%	55%	55%		$ 14.940
SE003	Servicio_SE	A_Errores_de_mantenimiento/actualización de equipos (hardware)	F.	0,017				55%		$ 272.716
		A_Caída_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$ 65.573
		A_Pérdida de equipos	P.F.	0,005		75%		75%		$ 32.786
		A_Abuso de privilegios de acceso	P.F.	0,005		75%	55%	65%		$ 25.220
		A_Uso no previsto	M.P.F.	0,003		55%	55%	55%		$ 14.940
		A_Acceso no autorizado	M.P.F.	0,003		75%	55%			$ 18.962
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$ 37.925
		A_Manipulación de los equipos	P.F.	0,005		55%		55%		$ 44.709
		A_Denegación de servicio	M.P.F.	0,003				65%		$ 37.925
		A_Robo	P.F.	0,005		75%		75%		$ 32.786
		A_Ataque destructivo	M.P.F.	0,003				75%		$ 32.868

Fuente: “elaboración propia”

Tabla 10. Análisis de Amenazas Quinta Parte.

					Impacto					
Codigo#	Activo	Amenaza =A	Cualitativo	Cuantitativo	A.	C.	I.	D.	T.	Impacto Potencial
SE004	Servicio_SE	A_Fuego	M.P.F.	0,003				85%		$22.556
		A_Daños por agua	M.P.F.	0,003				75%		$25.564
		A_Otros desastres Naturales	M.P.F.	0,003				75%		$25.564
		A_Fuego	M.P.F.	0,003				85%		$22.556
		A_Daños por agua	M.P.F.	0,003				75%		$25.564
		A_Contaminacion Mecanica	M.P.F.	0,003				65%		$29.497
		A_Contaminación electromagnética	M.P.F.	0,003				45%		$42.607
		A_Avería de origen físico/lógico	M.P.F.	0,003				55%		$34.860
		A_Corte del suministro eléctrico	M.P.F.	0,003				55%		$34.860
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$34.860
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$42.607
		A_Errores del_administrador	M.P.F.	0,003		55%	55%	55%		$11.620
		A_Errores_de_mantenimiento/actualización de equipos (hardware)	F.	0,017				55%		$212.113
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$51.001
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$25.501
		A_Abuso de privilegios de acceso	P.F.	0,005		75%	55%	65%		$19.616
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$11.620
		A_Acceso no autorizado	M.P.F.	0,003		75%	55%			$14.748
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$29.497
		A_Manipulación de los equipos	P.F.	0,005		55%		55%		$34.773
		A_Denegación de servicio	M.P.F.	0,003				65%		$29.497
		A_Robo	P.F.	0,005		75%		75%		$25.501
		A_Ataque destructivo	M.P.F.	0,003				75%		$25.564
SE005	Servicio_SE	A_Fuego	M.P.F.	0,003				85%		$64.447
		A_Daños por agua	M.P.F.	0,003				75%		$73.040
		A_Otros desastres Naturales	M.P.F.	0,003				75%		$73.040
		A_Fuego	M.P.F.	0,003				85%		$64.447
		A_Daños por agua	M.P.F.	0,003				75%		$73.040
		A_Contaminacion_Mecanica	M.P.F.	0,003				65%		$84.277
		A_Contaminación electromagnética	M.P.F.	0,003				45%		$121.733
		A_Avería_de_origen_físico/lógico	M.P.F.	0,003				55%		$99.600
		A_Corte del suministro eléctrico	M.P.F.	0,003				55%		$99.600
		A_Condiciones_inadecuadas_de_temperatura_o_humedad	M.P.F.	0,003				55%		$99.600
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$121.733
		A_Errores del_administrador	M.P.F.	0,003		55%	55%	55%		$33.200
		A_Errores_de_mantenimiento/actualización de equipos (hardware)	F.	0,017				55%		$606.036
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$145.717
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$72.859
		A_Abuso de privilegios de acceso	P.F.	0,005		75%	55%	65%		$56.045
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$33.200
		A_Acceso no autorizado	M.P.F.	0,003		75%	55%			$42.138
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$84.277
		A_Manipulación de los equipos	P.F.	0,005		55%		55%		$99.353
		A_Denegación de servicio	M.P.F.	0,003				65%		$84.277
		A_Robo	P.F.	0,005		75%		75%		$72.859
		A_Ataque destructivo	M.P.F.	0,003				75%		$73.040

Fuente: “elaboración propia”

Tabla 11. Análisis de Amenazas Sexta Parte.

					Impacto					
Codigo#	Activo	Amenaza =A	Cualitativo	Cuantitativo	A.	C.	I.	D.	T.	Impacto Potencial
		A_Fuego	M.P.F.	0,003				85%		$22.556
		A_Daños por agua	M.P.F.	0,003				75%		$25.564
		A_Otros desastres Naturales	M.P.F.	0,003				75%		$25.564
		A_Fuego	M.P.F.	0,003				85%		$22.556
		A_Daños por agua	M.P.F.	0,003				75%		$25.564
		A_Contaminacion Mecanica	M.P.F.	0,003				65%		$29.497
		A_Contaminación electromagnética	M.P.F.	0,003				45%		$42.607
		A_Avería de origen fisicológico	M.P.F.	0,003				55%		$34.860
		A_Corte del suministro eléctrico	M.P.F.	0,003				55%		$34.860
		A_Condiciones_inadecuadas_de_temperatura o humedad	M.P.F.	0,003				55%		$34.860
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$42.607
		A_Errores del administrador	M.P.F.	0,003		55%	55%	55%		$11.620
SO001	Servicio_SO	A_Errores_de_mantenimiento/actualización de equipos (hardware)	F.	0,017				55%		$212.113
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$51.001
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$25.501
		A_Abuso de privilegios de acceso	P.F.	0,005		75%	55%	65%		$19.616
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$11.620
		A_Acceso no autorizado	M.P.F.	0,003		75%	55%			$14.748
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$29.497
		A_Manipulación de los equipos	P.F.	0,005		55%		55%		$34.773
		A_Denegación de servicio	M.P.F.	0,003				65%		$29.497
		A_Robo	P.F.	0,005		75%		75%		$25.501
		A_Ataque destructivo	M.P.F.	0,003				75%		$25.564
		A_Fuego	M.P.F.	0,003				85%		$22.556
		A_Daños por agua	M.P.F.	0,003				75%		$25.564
		A_Otros desastres Naturales	M.P.F.	0,003				75%		$25.564
		A_Fuego	M.P.F.	0,003				85%		$22.556
		A_Daños por agua	M.P.F.	0,003				75%		$25.564
		A_Contaminacion Mecanica	M.P.F.	0,003				65%		$29.497
		A_Contaminación electromagnética	M.P.F.	0,003				45%		$42.607
		A_Avería de origen fisicológico	M.P.F.	0,003				55%		$34.860
		A_Corte del suministro eléctrico	M.P.F.	0,003				55%		$34.860
		A_Condiciones_inadecuadas_de_temperatura o humedad	M.P.F.	0,003				55%		$34.860
		A_Emanaciones_electromagnéticas	M.P.F.	0,003				45%		$42.607
		A_Errores del administrador	M.P.F.	0,003		55%	55%	55%		$11.620
SO002	Servicio_SO	A_Errores_de_mantenimiento/actualización de equipos (hardware)	F.	0,017				55%		$212.113
		A_Caida_del_sistema_por_agotamiento_de_recursos	P.F.	0,005				75%		$51.001
		A_Pérdida_de_equipos	P.F.	0,005		75%		75%		$25.501
		A_Abuso de privilegios de acceso	P.F.	0,005		75%	55%	65%		$19.616
		A_Uso_no_previsto	M.P.F.	0,003		55%	55%	55%		$11.620
		A_Acceso no autorizado	M.P.F.	0,003		75%	55%			$14.748
		A_Modificación_deliberada_de_la_información	M.P.F.	0,003			65%			$29.497
		A_Manipulación de los equipos	P.F.	0,005		55%		55%		$34.773
		A_Denegación de servicio	M.P.F.	0,003				65%		$29.497
		A_Robo	P.F.	0,005		75%		75%		$25.501
		A_Ataque destructivo	M.P.F.	0,003				75%		$25.564

Fuente: “elaboración propia”

El modelo de seguridad de la información que se toma como guía para la elaboración del presente trabajo, se tiene como referencia el Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea – (MSPI)[44].

[44] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

1. **Fase Diagnostico:** En esta fase se identifica el estado actual de la dependencia a verificar.

2. **Fase Planificación (Planear),** se establecen los objetivos a alcanzar y las tareas que se deben mejorar, así mismos indicadores que sean medibles para controlar y cuantificar los objetivos.

3. **Fase Implementación (Hacer),** en esta fase se efectúa el plan establecido para la ejecutar acciones de las mejoras establecidas.

4. **Fase Evaluación de desempeño (Verificar**), una vez determinada las acciones de mejora, se establece el tiempo para su implementación.

5. **Fase Mejora Continua (Actuar):** Se examinan los resultados de las acciones de mejora determinadas, con el fin de analizar su efectividad y eficacia.

Marco de Referencia de Seguridad Informática.

Para el desarrollo del presente trabajo se tomó como marco normativo la norma ISO 27001:2013, que sirve como guía para evaluar y determinar posibles riesgos, brindando estrategias y controles eficaces para mitigar la pérdida o fuga de información, alineado al modelo MSPI[45].

Cuadro 2. MSPI vs ISO 27001:2013.

FASE	ANEXO "A" ISO 27001:2013
Diagnóstico	4. Contexto de la Organización
Planificación	5. Liderazgo 6. Planificación
Implementación	7. Soporte 8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

Fuente: "elaboración propia"

[45] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

Fase diagnóstica.

Capítulo 4 - Contexto de la organización: En la norma ISO 27001:2013, se trata del punto de partida para desarrollar el SGSI y consiste en determinar o identificar los problemas internos y externos a los que se enfrenta la organización (ISO 27001 n.d.).

Fase planeación.

Capítulo 5 – Liderazgo: En la norma ISO 27001:2013, se requiere de una participación activa y comprometida de la alta dirección de la organización evitando situaciones como las que hemos vivido hasta ahora donde la dirección aparece ocasionalmente en la reunión de revisión (ISO 27001 n.d.).

Capítulo 6 – Planeación: En la norma ISO 27001:2013, la identificación de los riesgos y oportunidades que afectan al contexto de la organización lo hemos visto en el apartado correspondiente de la norma[46].
Sección 4 el contexto de la organización donde se determinan en base a las necesidades y expectativas de las partes interesadas en relación a la seguridad de la información (ISO 27001 n.d.).

Capítulo 7 – Soporte: En la norma ISO 27001:2013, La implementación de un SGSI es necesariamente disponer de los recursos necesarios para que el sistema de gestión pueda llevarse a cabo según lo planeado (ISO 27001 n.d).

Fase implementación.

Capítulo 8 – Operación: En la norma ISO 27001:2013, se presentan una serie de requisitos para controlar que estamos tomando las medidas adecuadas para lograr los objetivos de la Seguridad de la Información (ISO 27001 n.d.)[47].

Fase evaluación del desempeño.

[46] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[47] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

Capítulo 9 - Evaluación del desempeño: En la norma ISO 27001:2013, Necesitamos evaluar para medir el rendimiento del SGSI. Se trata de determinar que debemos medir y controlar, cuándo, quién y cómo (ISO 27001 n.d.)[48].

Fase mejora continua.

Capítulo 10 – Mejora: En la norma ISO 27001:2013, enfoque basado en el riesgo, el papel de las acciones preventivas como tal deja su lugar a las conclusiones del análisis de riesgos (ISO 27001 n.d.).

Fase I. Diagnóstico - etapas previas a la implementación.
En esta fase se identifica el estado actual de la organización en relación al modelo de seguridad y privacidad de la información (MinTIC 2015:22)[49].

Figura 3. Etapa previa a la Implementación.

Fuente: Documento Modelo de Seguridad y Privacidad de la Información (MinTIC 2015:22).

Fase II. Planificación – fase de planificación.

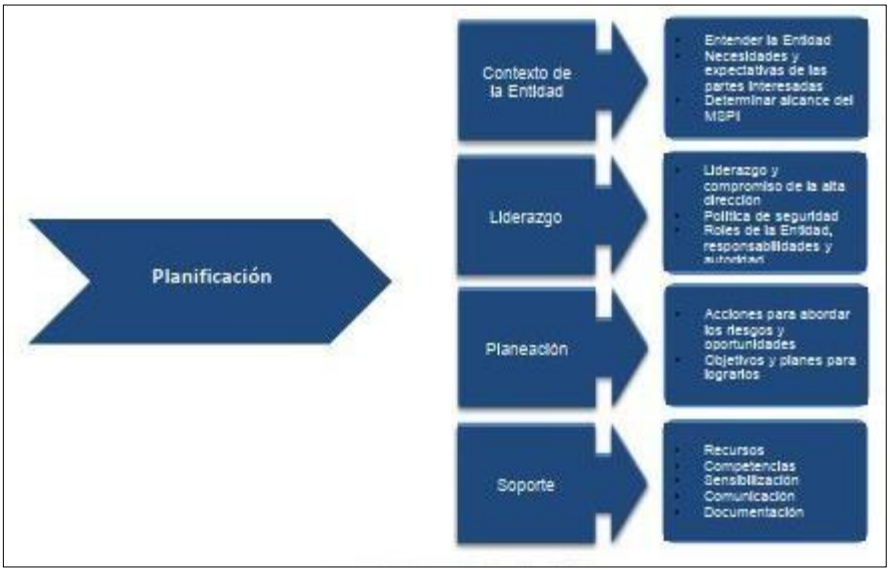
Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de

[48] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[49] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

la información, a través de una metodología de gestión del riesgo (MinTIC 2015:23).

Figura 4. Fase de Planificación.

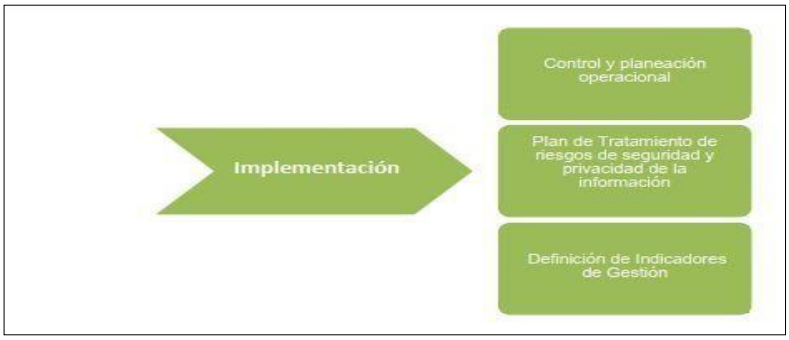


Fuente: Documento Modelo de Seguridad y Privacidad de la Información (MinTIC 2015:24).

Fase III. Implementación.

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI (MinTIC 2015:28).

Figura 5. Fase de Implementación.



Fuente: Documento Modelo de Seguridad y Privacidad de la Información (MinTIC 2015:29)[50].

[50] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

Fase IV. Evaluación de desempeño.

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información, propuesta para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas (MinTIC 2015:31)[51].
Figura 6. Fase de Evaluación de Desempeño.

Fuente: Documento Modelo de Seguridad y Privacidad de la Información (MinTIC 2015:32)[52].

Fase VI. Mejora continua.

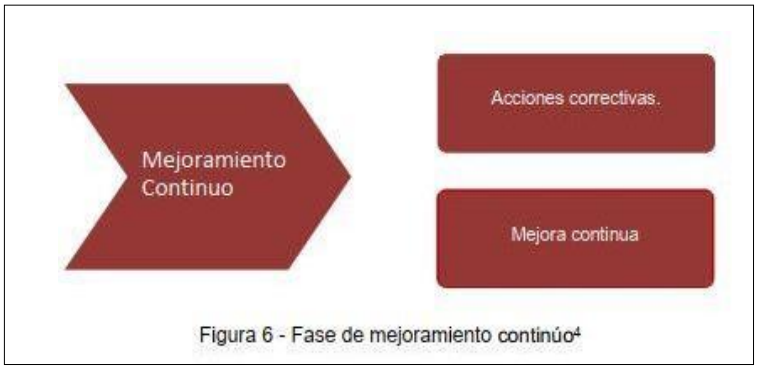
Se consolida los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información (MinTIC 2015:34)[53].

[51] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[52] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[53] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

Figura 7. Fase de Mejoramiento Continuo.

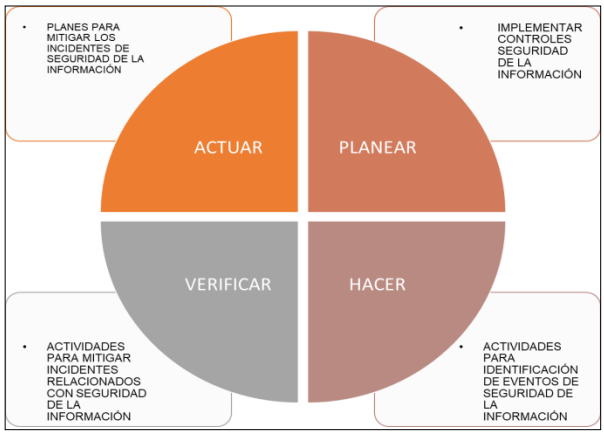


Fuente, Documento Modelo de Seguridad y Privacidad de la Información (MinTIC 2015:34)[54].

Mejora continua, modelo de seguridad Megaseguridad.

Para la mejora continua del modelo de seguridad de la información para la empresa Megaseguridad, se debe tener en cuenta el ciclo PHVA, para implementar y fortalecer las buenas prácticas de seguridad de la información al interior de la organización[55].

Figura 8. Mejora Continua.



Fuente, Documento Modelo de Seguridad y Privacidad de la Información (MinTIC 2015:34).

[54] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

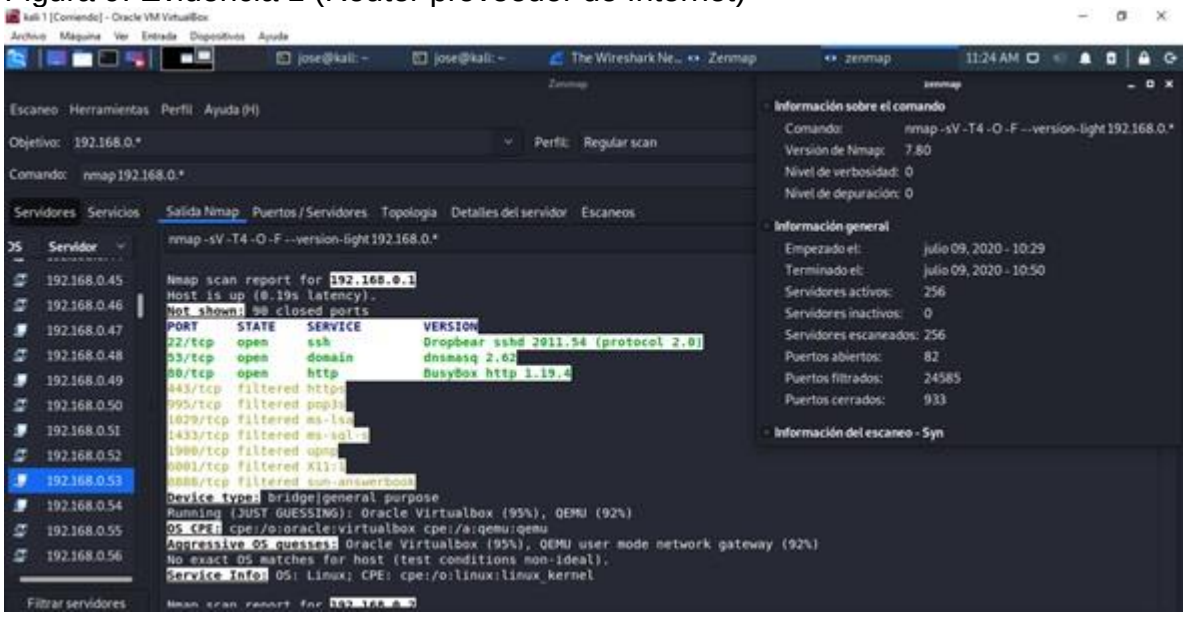
[55] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

5.2 REALIZAR PRUEBAS DE PENETRACIÓN PENTESTING EN LA RED DE INFORMACIÓN PARA DETERMINAR QUÉ TIPO DE VULNERABILIDADES PRESENTA.

Estas pruebas se va a llevar a cabo desde la distribución de Linux Kali Linux 2020 2, y desde las herramientas Nmap, Zenmap, Armitage y Metasploit Framework.

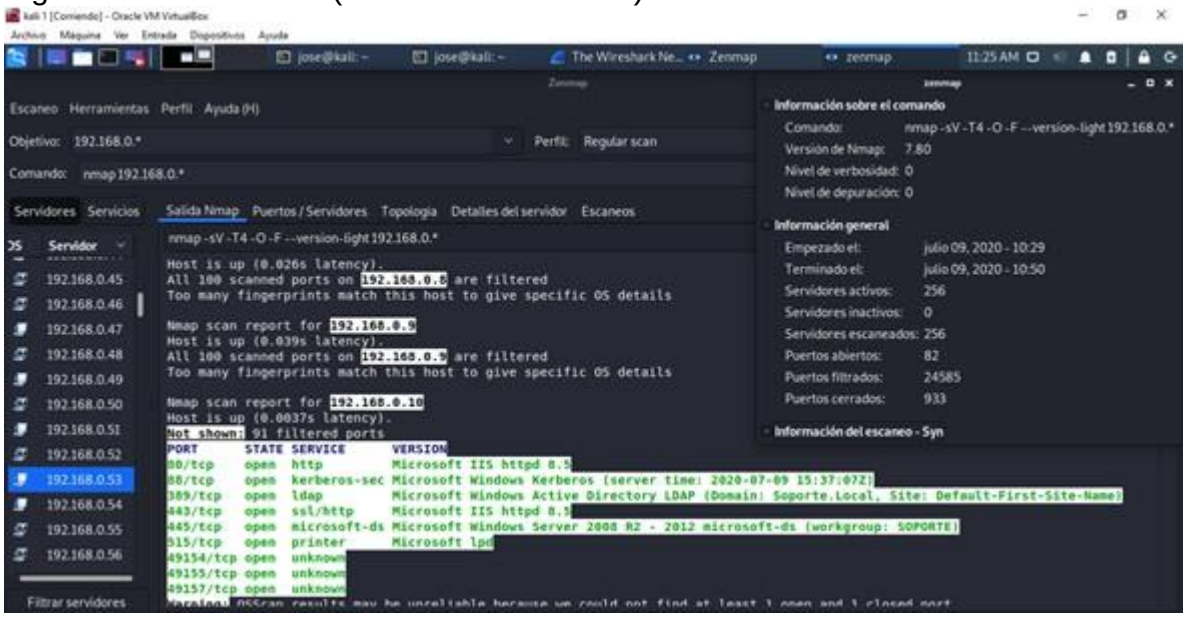
Desde Kali Linux con la Zenmap se hizo un escaneo completo al rango de la IP (192.168.0.), interna de la compañía, identificando algunas vulnerabilidades como puertos expuestos, información de sistemas operativos y ninguna restricción en la red para conectar o correr herramientas como esta (Zenmap), se toma como evidencia 01 equipo router, 01 equipo servidor de archivos (Server 2012r2), 05 equipos usuarios (Windows).

Figura 9. Evidencia 1 (Router proveedor de Internet)



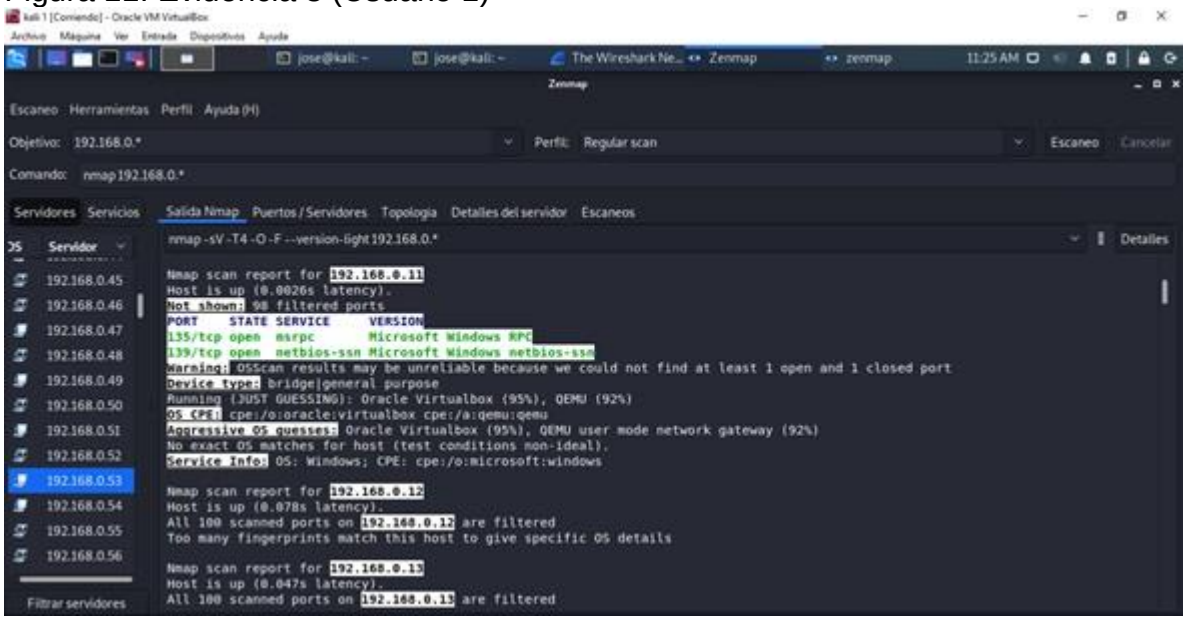
Fuente: “elaboración propia”

Figura 10. Evidencia 2 (Servidor de archivos)



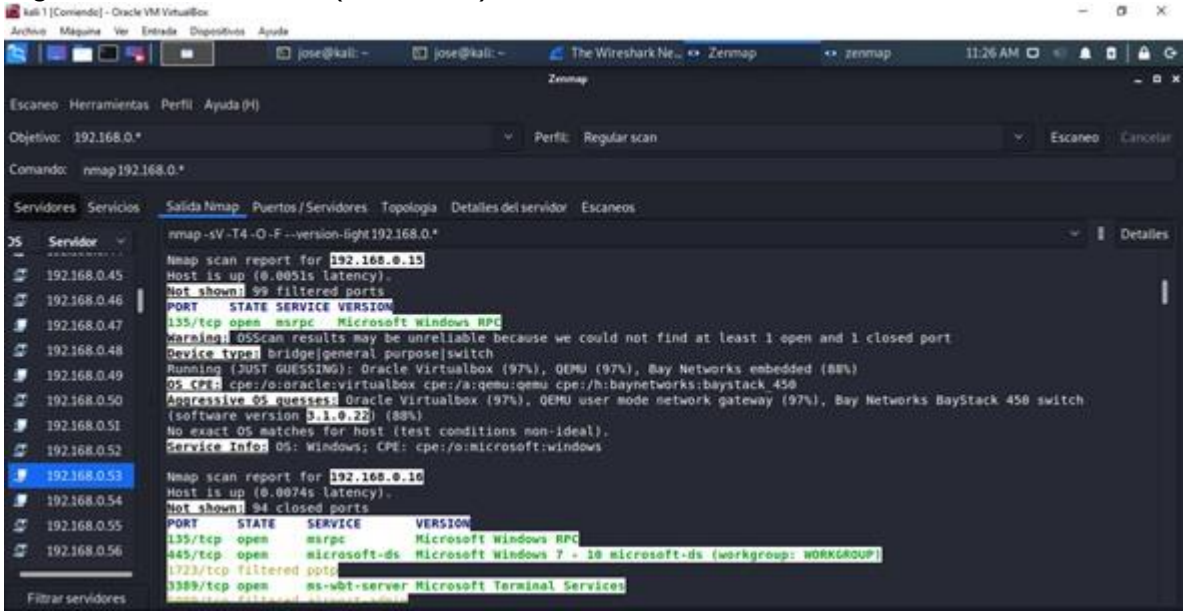
Fuente: “elaboración propia”

Figura 11. Evidencia 3 (Usuario 1)



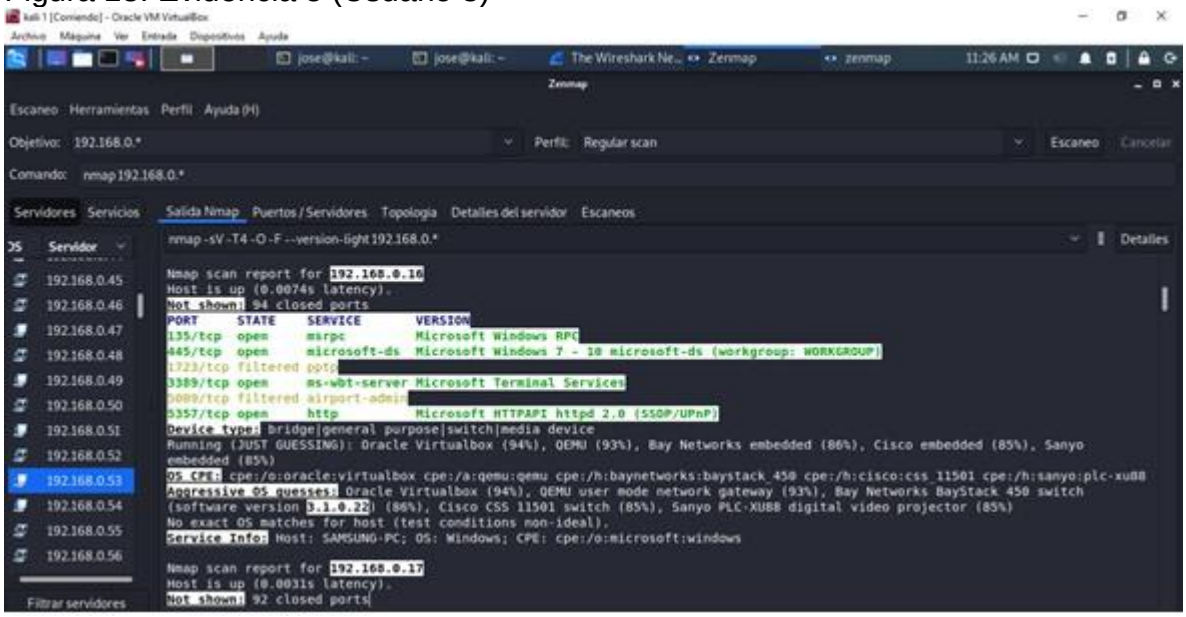
Fuente: “elaboración propia”

Figura 12. Evidencia 4 (Usuario 2)



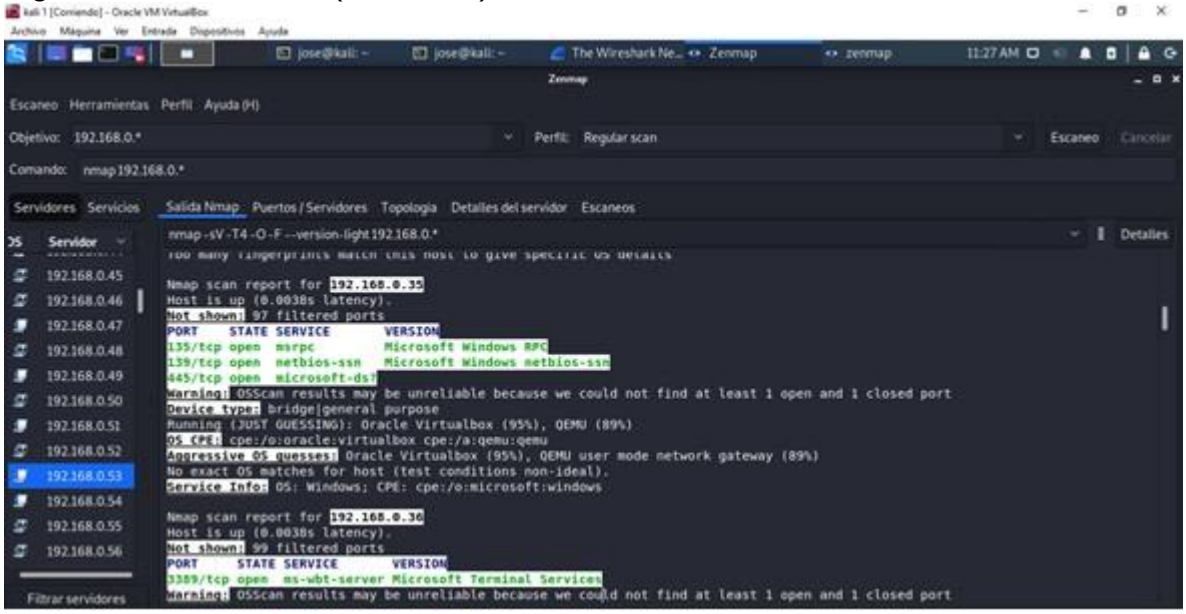
Fuente: “elaboración propia”

Figura 13. Evidencia 5 (Usuario 3)



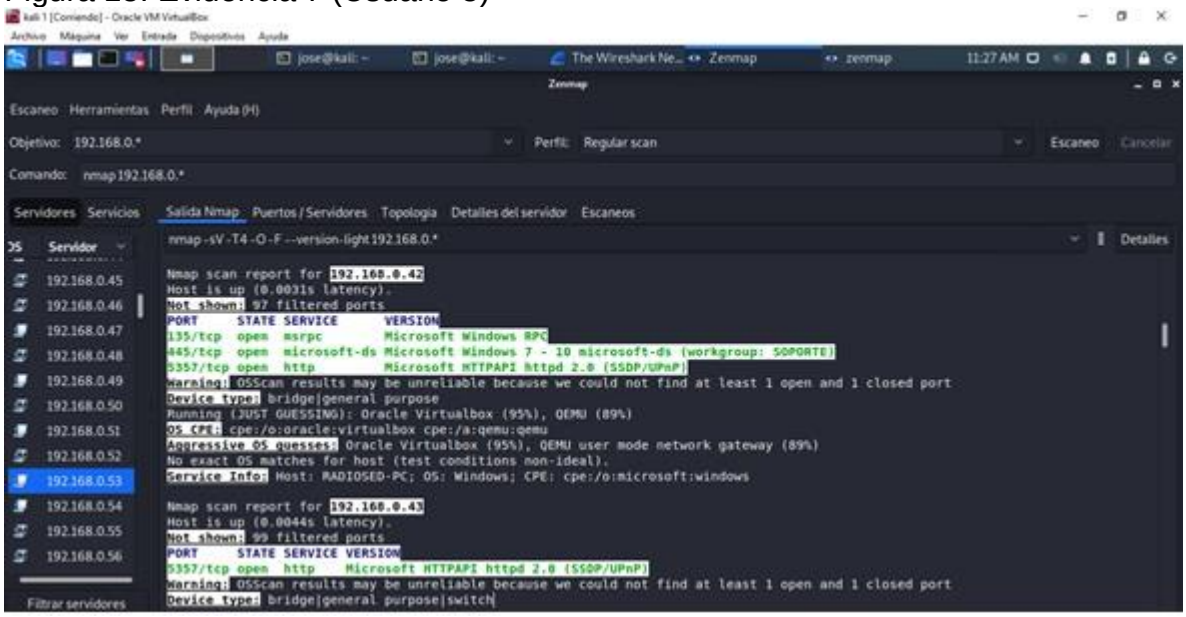
Fuente: “elaboración propia”

Figura 14. Evidencia 6 (Usuario 4)



Fuente: “elaboración propia”

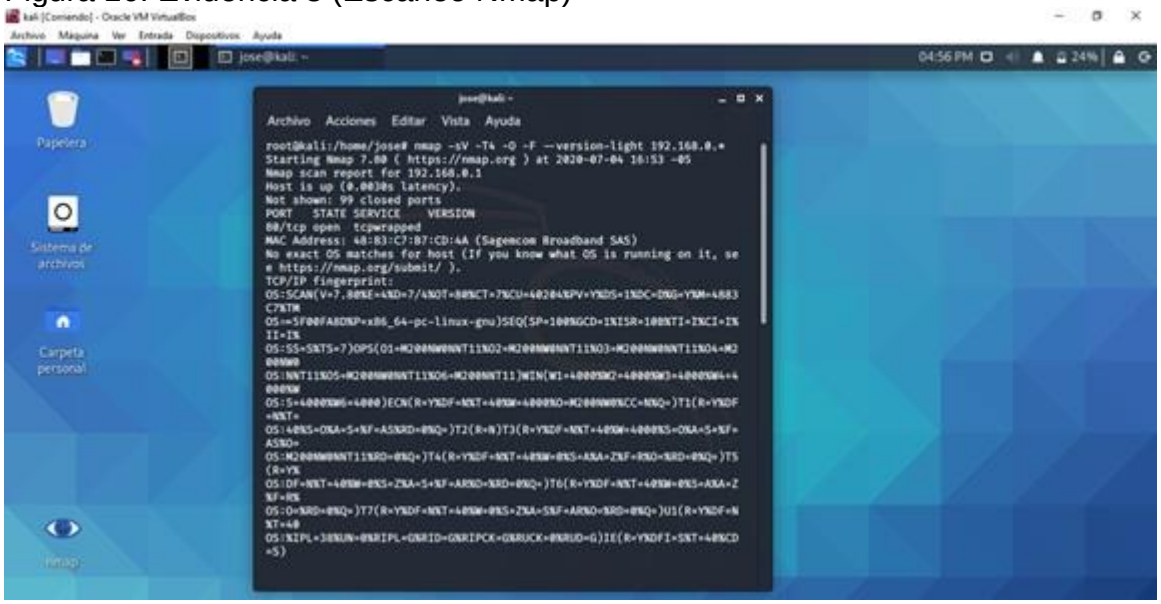
Figura 15. Evidencia 7 (Usuario 5)



Fuente: “elaboración propia”

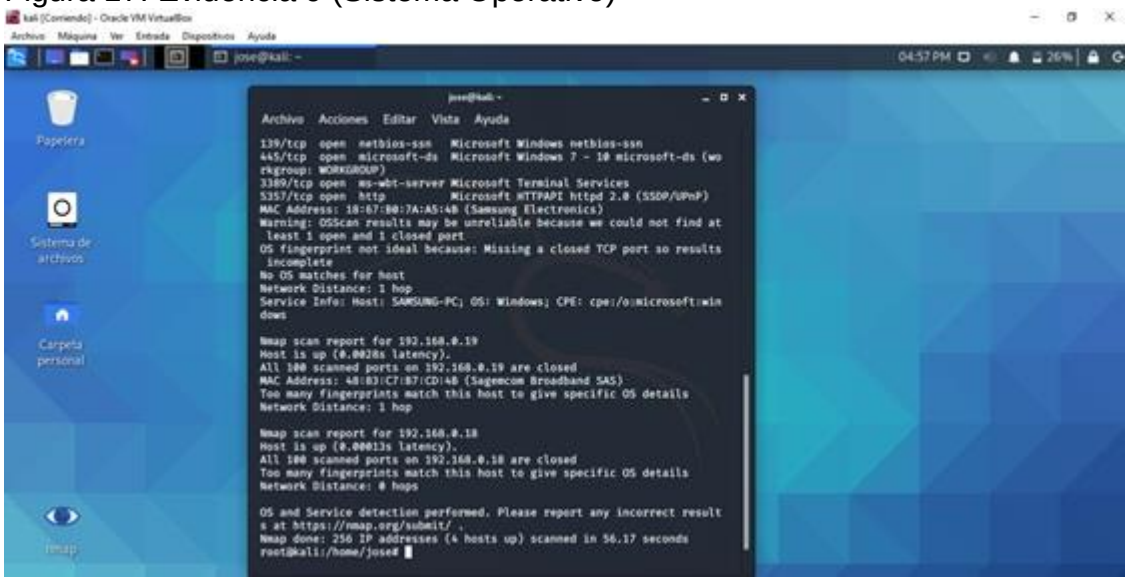
Desde Kali Linux con la herramienta Nmap, se escanean puertos y sistemas operativos, disponibles.

Figura 16. Evidencia 8 (Escaneo Nmap)



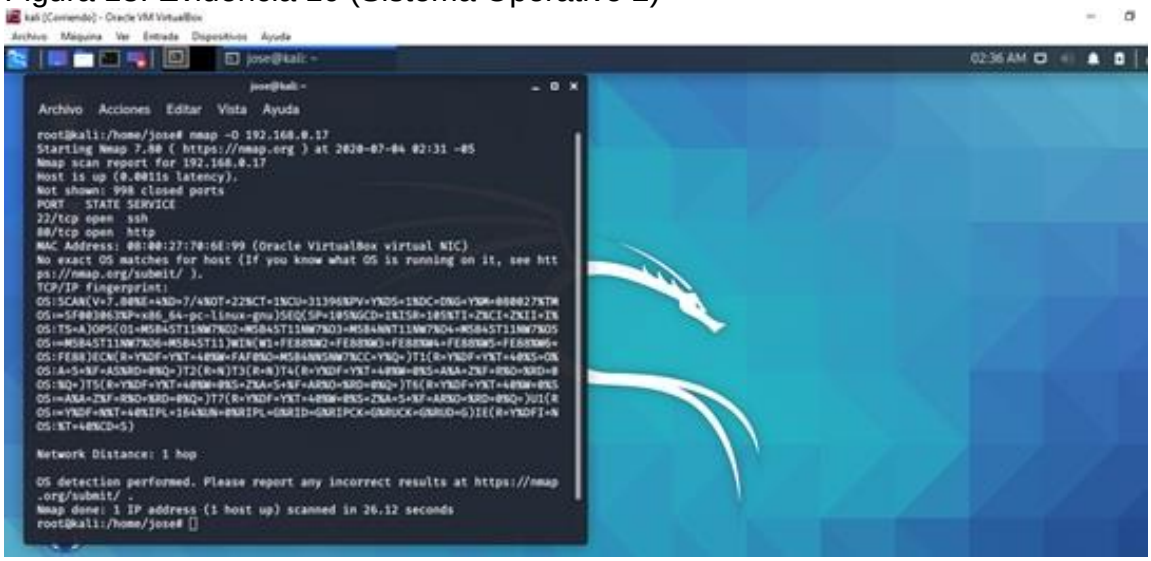
Fuente: “elaboración propia”

Figura 17. Evidencia 9 (Sistema Operativo)



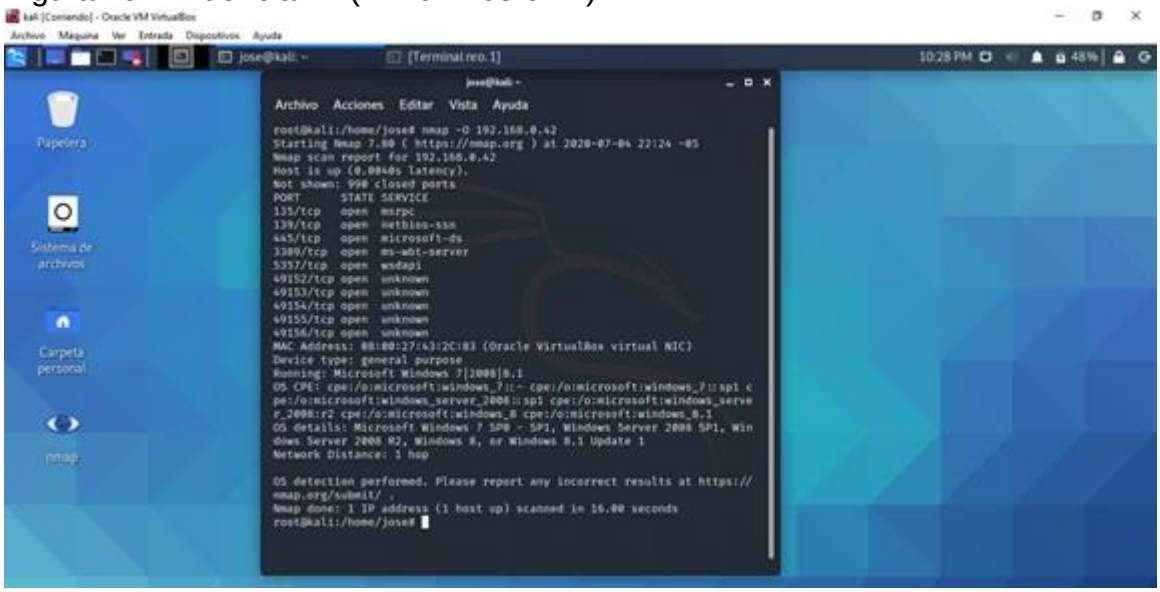
Fuente: “elaboración propia”

Figura 18. Evidencia 10 (Sistema Operativo 2)



Fuente: “elaboración propia”

Figura 19. Evidencia 11 (IP 192.168.0.42)



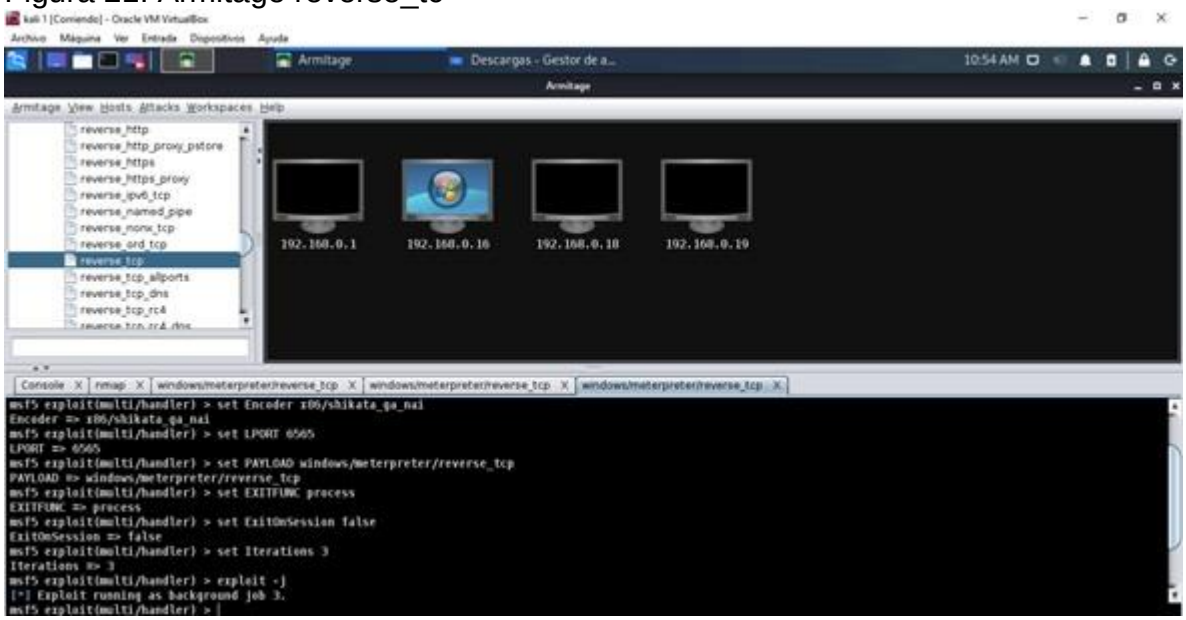
Fuente: “elaboración propia”

Con Armitage se escanean puertos desde Quick scan, y desde reverse_tcp se crea un ejecutable .exe con el nombre de trojan, que comunique la maquina atacante (192.168.0.18), con la maquina conectada a la red, esta prueba es fallida ya que el antivirus 360 Total Security lo identifica y elimina.

Figura 20. Armitage Scan.

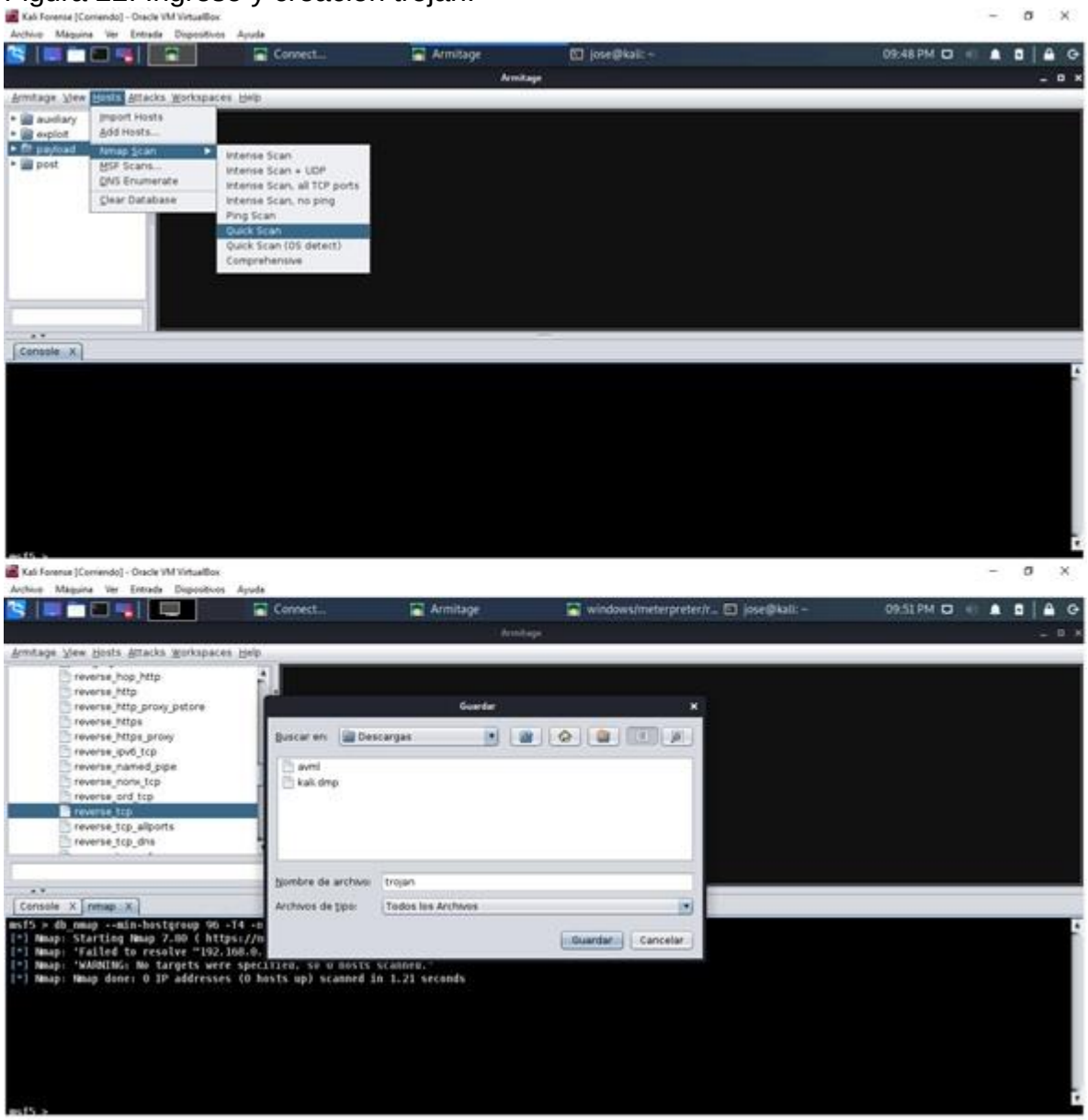
Fuente: “elaboración propia”

Figura 21. Armitage reverse_tc



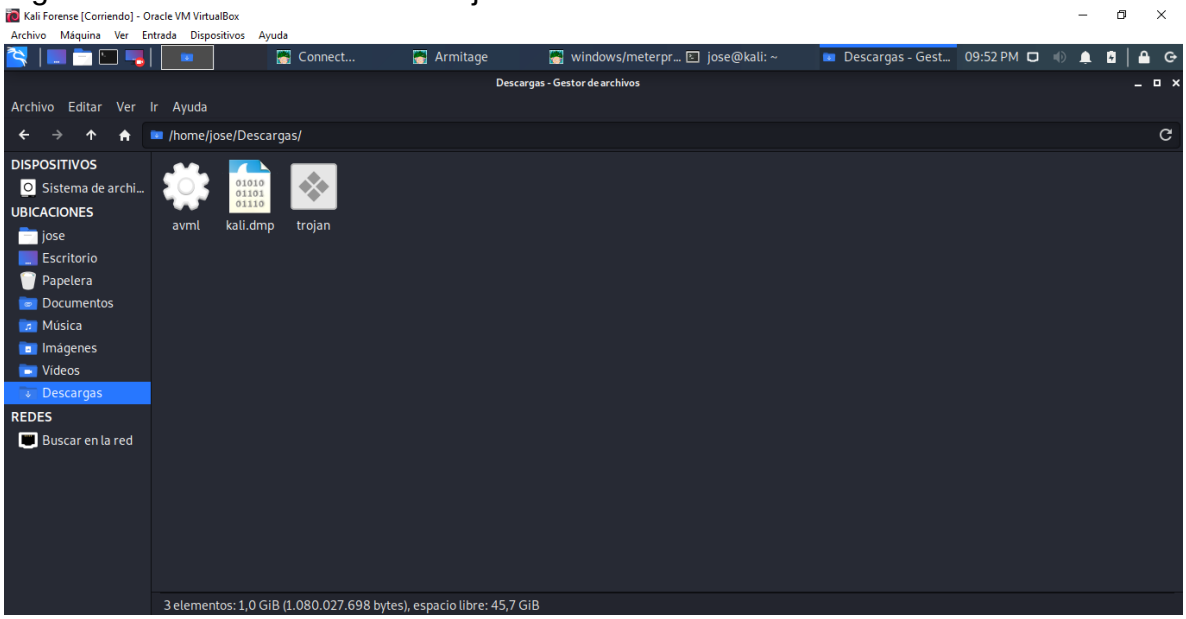
Fuente: “elaboración propia”

Figura 22. Ingreso y creación trojan.



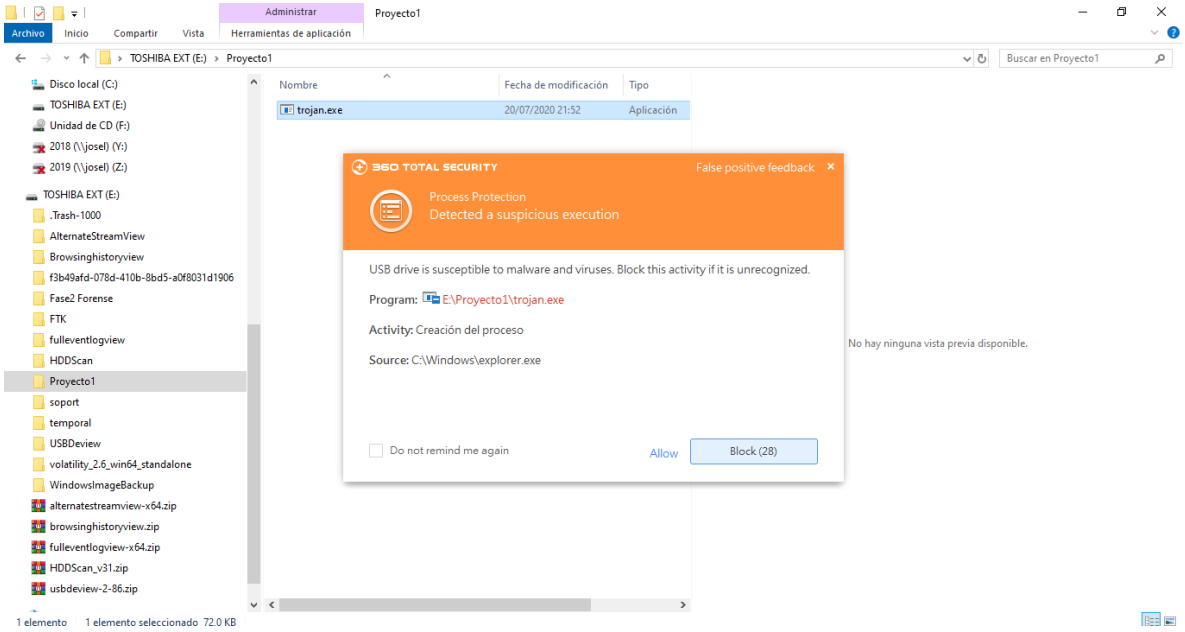
Fuente: “elaboración propia”

Figura 23. Evidencia creación trojan.



Fuente: “elaboración propia”

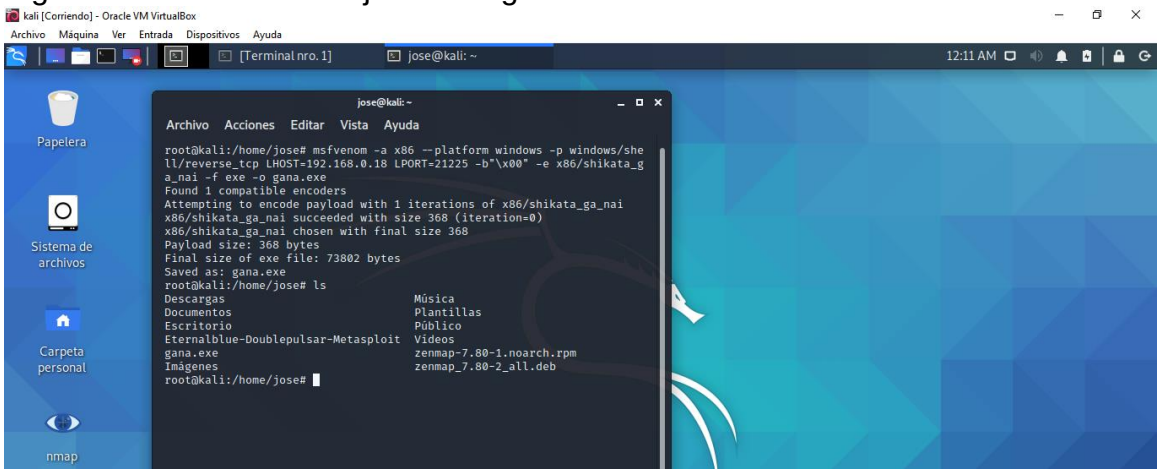
Figura 24. Identificación y eliminación de trojan máquina de prueba en la red.



Fuente: “elaboración propia”

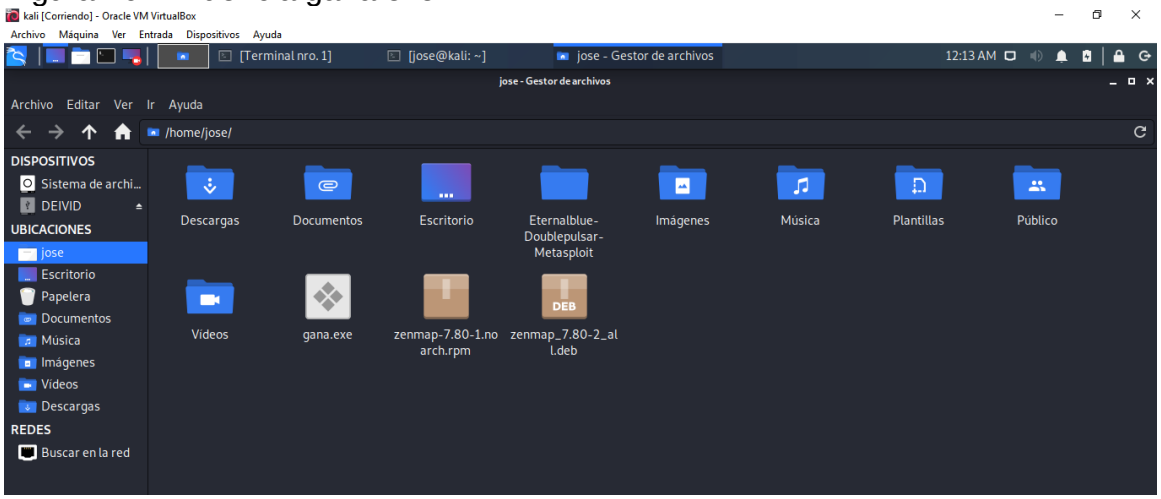
También se hacen pruebas con Metasploit Framework creando un ejecutable con el nombre de gana, intentando tomar control de una maquina victima y que comunique a la atacante (192.168.0.18), se logra ingresar a la maquina y se reinicia desde la terminal.

Figura 25. Creación del ejecutable gana.



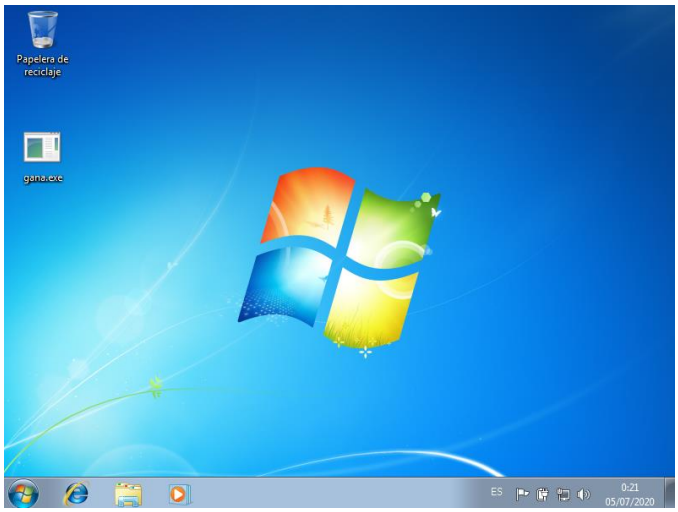
Fuente: “elaboración propia”

Figura 26. Evidencia gana.exe.



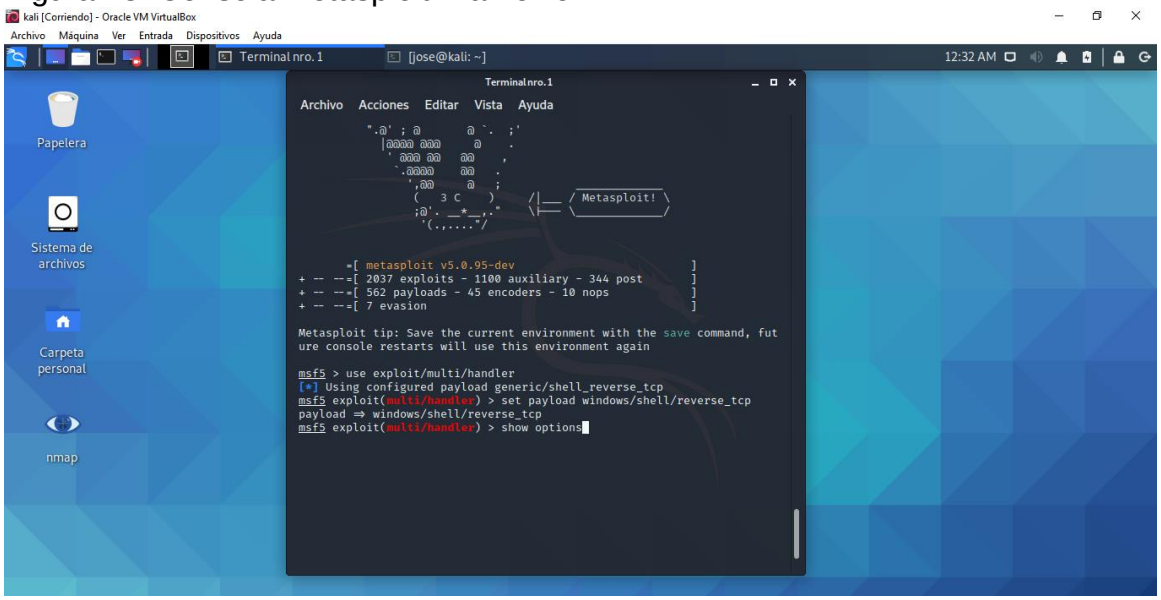
Fuente: “elaboración propia”

Figura 27. Ejecutable maquina atacada.



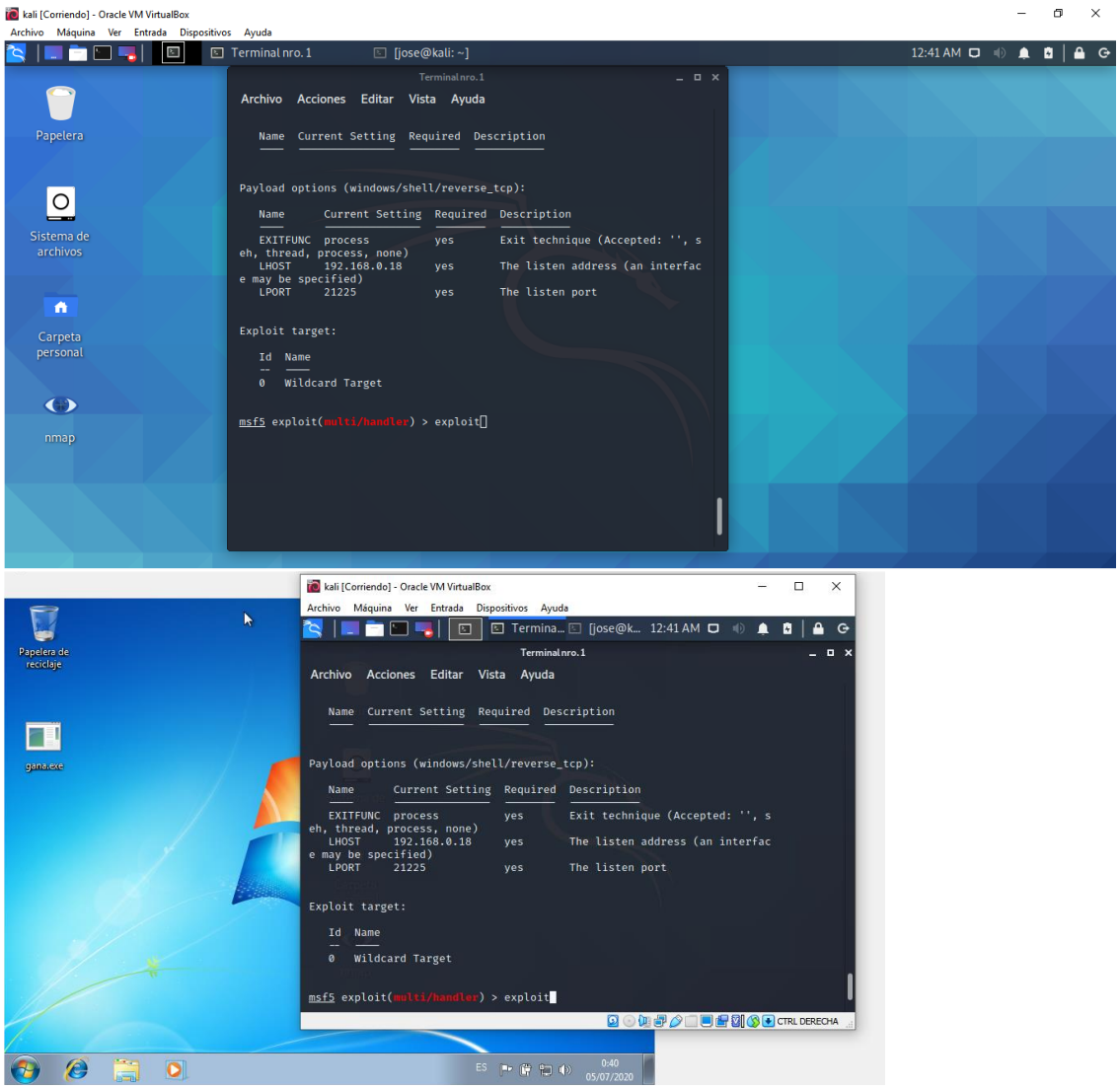
Fuente: “elaboración propia”

Figura 28. Consola Metasploit Framework.



Fuente: “elaboración propia”

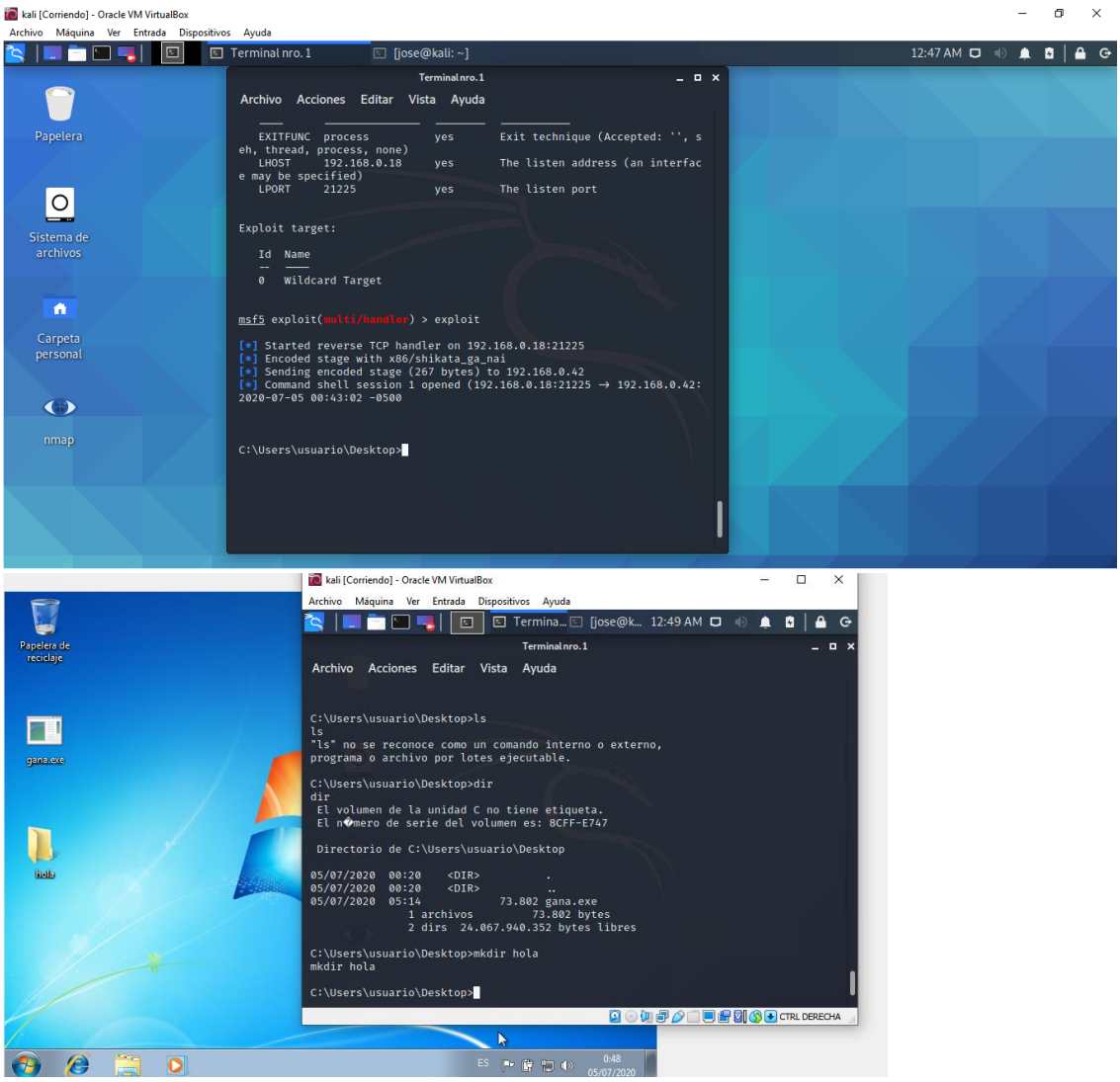
Figura 29. Ingreso a la máquina.



Fuente: “elaboración propia”

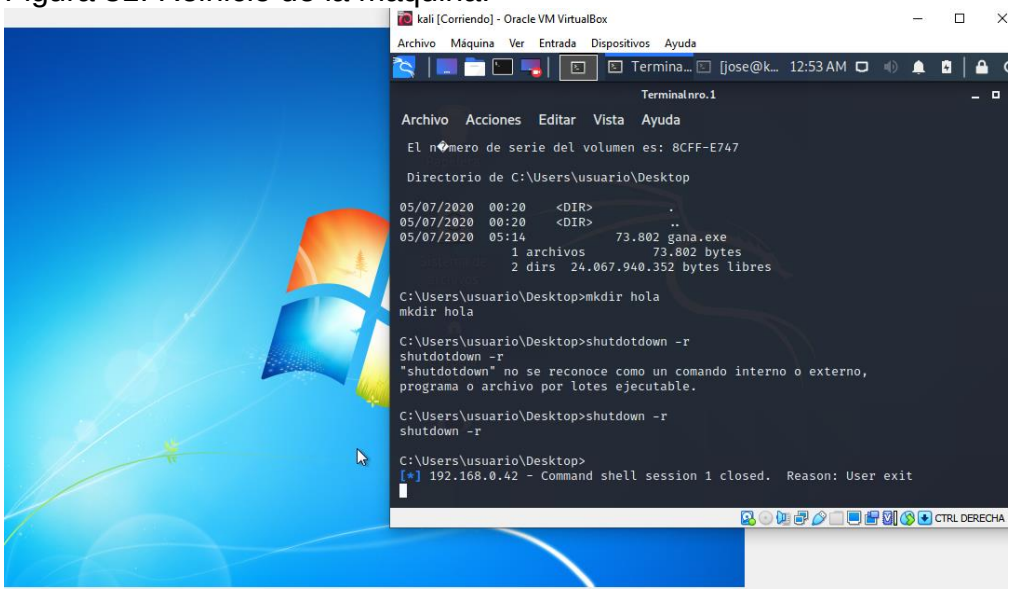
.

Figura 30. Control de la máquina.



Fuente: “elaboración propia”

Figura 31. Reinicio de la máquina.



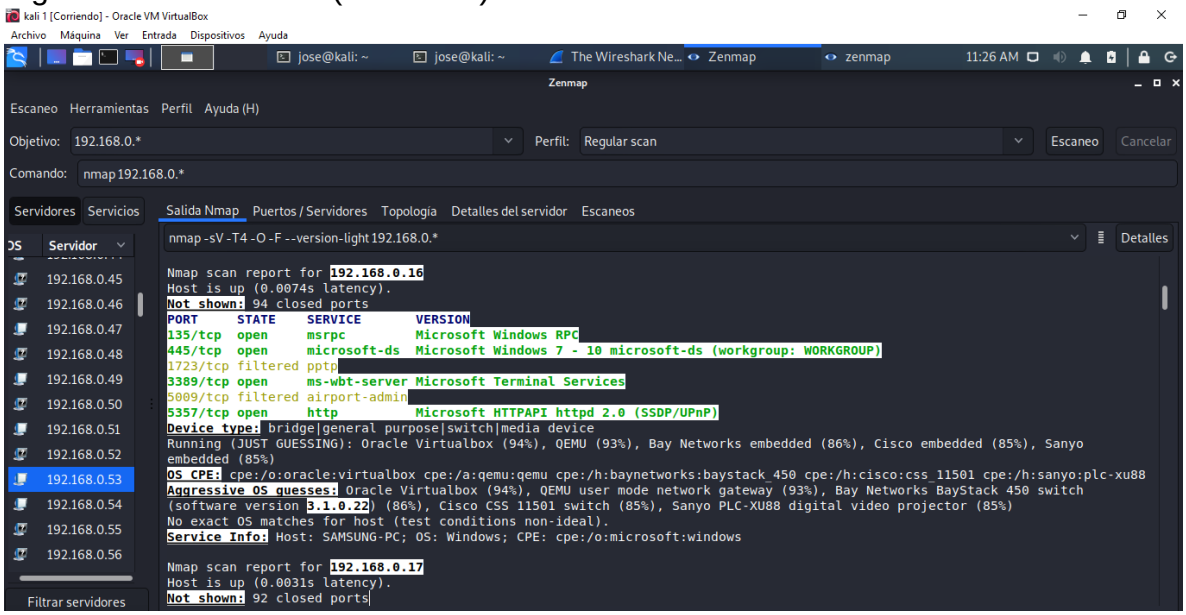
Fuente: “elaboración propia”

5.3 IDENTIFICAR FALLAS Y VULNERABILIDADES A QUE ESTÁ EXPUESTA LA RED DE INFORMACIÓN.

Desde Kali Linux con la Zenmap se hizo un escaneo completo al rango de la IP (192.168.0.), interna de la compañía, identificando algunas vulnerabilidades como información de sistemas operativos y ninguna restricción en la red para conectar o correr herramientas como esta (Zenmap), se toma como evidencia, sistema operativo Windows 7 sin actualizaciones.

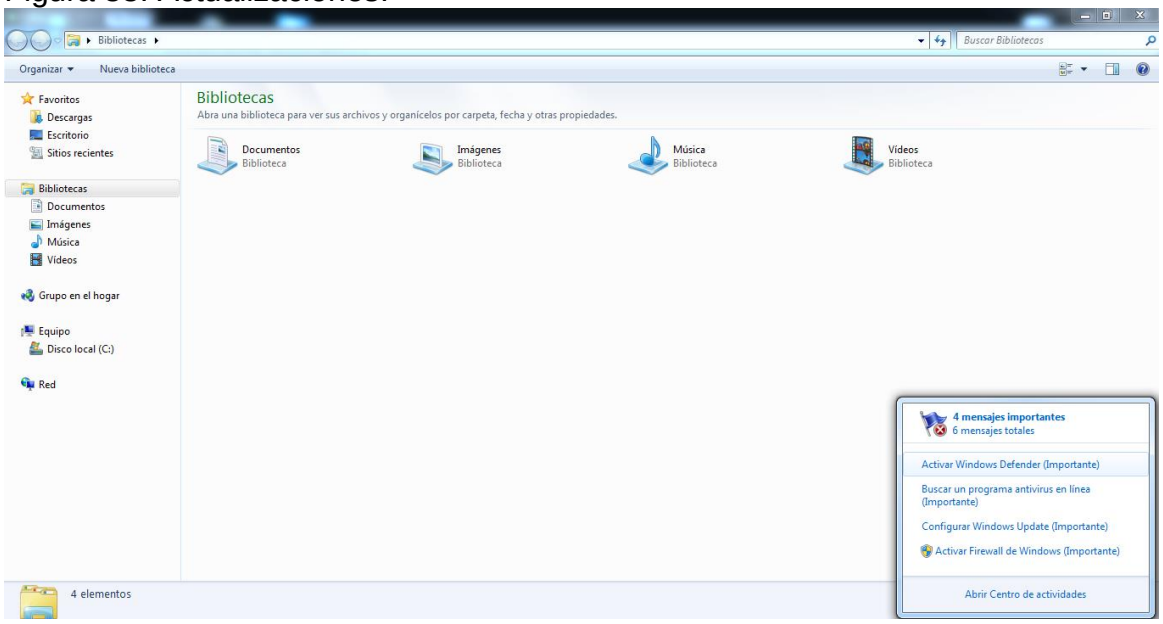
Sistemas operativos desactualizados.

Figura 32. Evidencia 5 (Usuario 3)



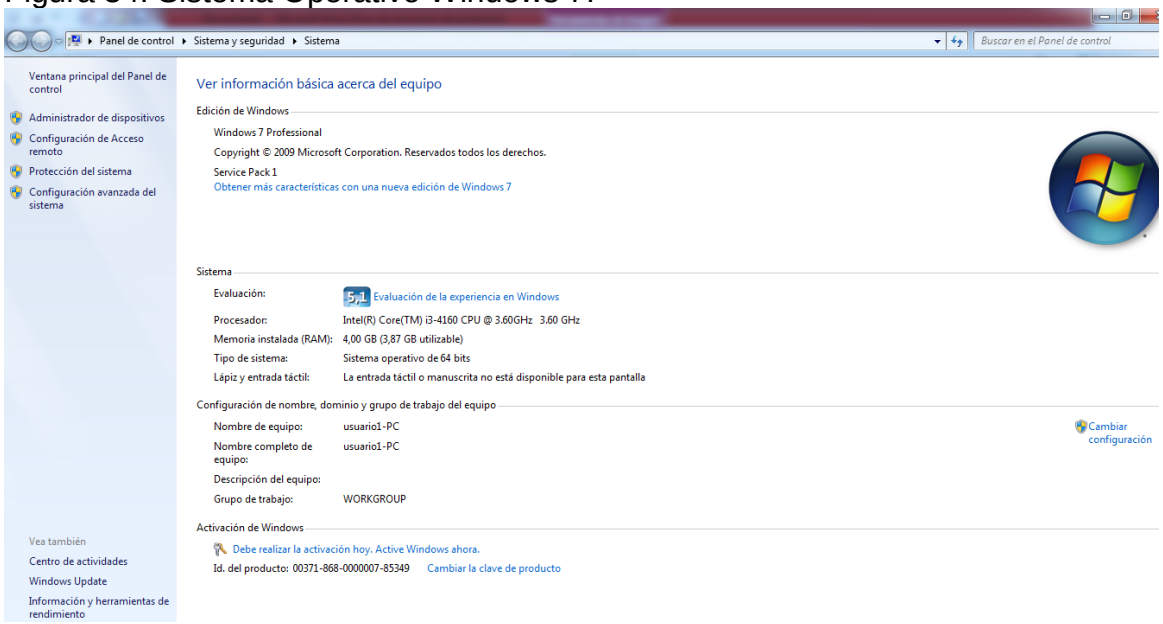
Fuente: “elaboración propia”

Figura 33. Actualizaciones.



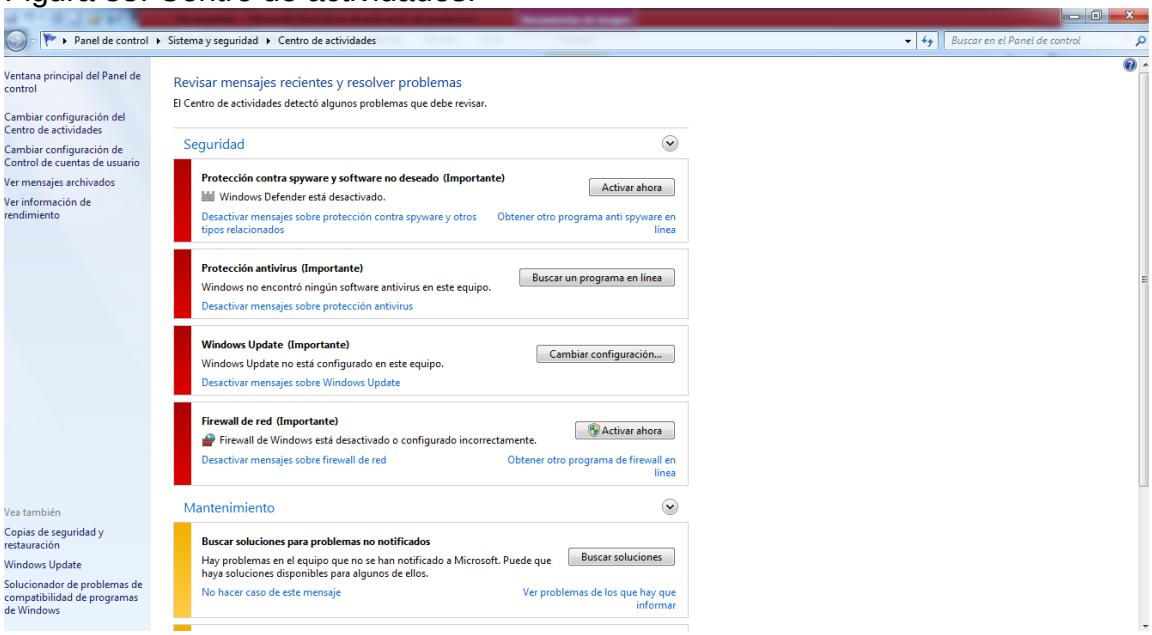
Fuente: “elaboración propia”

Figura 34. Sistema Operativo Windows 7.



Fuente: “elaboración propia”

Figura 35. Centro de actividades.



Fuente: “elaboración propia”

5.4 HACER RECOMENDACIONES PARA MITIGAR FALLAS Y VULNERABILIDADES.

En cuanto a este aspecto de seguridad, las medidas prácticas de prevención se enfocan en.

- ✓ Nunca descargar actualizaciones desde sitios web desconocidos.
- ✓ Realice la descarga de las actualizaciones a través de los procedimientos brindados por el fabricante o programador.
- ✓ En los entornos empresariales, y sin importar la plataforma del sistema operativo, se aconseja mantener las actualizaciones activas tanto de los sistemas operativos como de las aplicaciones.

Es muy importante la configuración del sistema operativo para hacerlo más seguro; buenas prácticas que se deben tener en cuenta[56].

- ✓ Deshabilitar las carpetas compartidas, para evitar la propagación de gusanos o troyanos que aprovechan cualquier vulnerabilidad.
- ✓ Utilizar contraseñas fuertes para el ingreso al sistema operativo, porque el uso de contraseñas débiles permite que se penetren fácilmente.
- ✓ Crear o configurar un perfil de usuario con privilegios restringidos.
- ✓ Deshabilitar la ejecución automática de dispositivos de almacenamiento USB.
- ✓ Usar sistemas operativos modernos y de última generación, los sistemas operativos obsoletos no cuentan con soporte técnico[57].
- ✓ Configurar la visualización de archivos ocultos, dado que los virus se esconden en el sistema con este tipo de atributos[58].

[56] Ibíd, p.69.

[57] Ibíd, p.69.

[58] Ibíd, p.69.

- ✓ El encargado del proceso debe garantizar la renovación de las contraseñas cada cierto tiempo dependiendo la criticidad de la información transmitida, la cual se determina un periodo no mayor a 7 días para información crítica, de 30 días para información Media y de 90 días para información de categoría baja[59].

- ✓ El área que necesite transmitir información deberá colocar un requerimiento indicando el tipo de información que se desea enviar, con el fin de poder determinar la criticidad de la misma y así poder asignarle un método de transmisión de la información.

- ✓ En el momento de adquirir o implementar herramientas de terceros que basen sus servicios en nube, la administración debe propender por usar aquellas que tengan inmersas en su arquitectura un mecanismo de cifrado de datos que se base en las mejores prácticas del mercado e implementar controles para verificar que la información esta protegida adecuadamente.

- ✓ Cualquier comunicación que se transmita a través de correo electrónico y que contenga información sensible sobre los clientes, colaboradores o accionistas de la organización debe viajar cifrada usando la herramienta proporcionada por el servicio de correo electrónico, adicionalmente los documentos anexos deben estar protegidos con una contraseña fuerte de al menos 10 caracteres y con una combinación de mayúsculas, minúsculas, números y símbolos[60].

- ✓ Dentro del ciclo de desarrollo seguro de software se debe garantizar que las aplicaciones y servicios que requieran el uso de una combinación de login y password incluyan cifrado de las credenciales y que dentro del código no se pueda visualizar en claro ninguna contraseña, es responsabilidad del equipo de Seguridad de la Información implementar un control para garantizar el cumplimiento de esta directriz.

- ✓ Los sitios web corporativos deben estar protegidos con certificados de seguridad expedidos por entidades reconocidas con el objeto de prevenir la interceptación de los datos ingresados por clientes o colaboradores; el equipo de Seguridad de la Información debe implementar un control sobre

[59] Ibíd, p.69.

[60] Ibíd, p.69.

los vencimientos de estos certificados para garantizar continuidad en el servicio[61].

- ✓ Los discos duros de los equipos de usuario final deben cifrarse utilizando las herramientas propias del sistema operativo o soluciones adquiridas y administradas por el equipo de Tecnología y verificadas por el equipo de Seguridad de la Información; de igual forma se debe realizar cifrado de los discos y memorias USB corporativas[62].

[61] Ibíd, p.69.

[62] Ibíd, p.69.

6 CONCLUSIONES

Por medio del diagnóstico basado en la norma ISO 27001:2013 en su anexo “A”, y la herramienta de análisis Magerit, se logró obtener un breve resumen del estado actual de la compañía, con sus controles y clasificación de activos a nivel interno y externo[63].

Con el manejo de la tecnología y sobre todo el trabajo en red tanto para equipos conectados al WIFI como a la LAN deja una brecha abierta a un activo bien importante como lo es la información digital de la compañía.

Las pruebas de penetración “pentesting”, buscan identificar las vulnerabilidades a las que están expuestas la información de la empresa Megaseguridad la proveedora Ltda., como:

Sistemas operativos
Rangos de IP
Puertos abiertos
Pruebas de firewall

Por medio de simulaciones y ataques autorizados con las herramientas Nmap, Zenmap, Armitage y Metasploit Framework, se logro identificar algunas vulnerabilidades a las que esta expuesta la red, y asi poder exponer por medio de este proyecto los soportes y recomendaciones.

Se encuentran sistemas operativos (Windows7), sin actualizaciones, deshabilitadas la seguridad de firewall, update, y protección de antivirus, se hace recomendaciones como actualización de software y compra de licencias para mitigar fallas y vulnerabilidades a las que está expuesta la seguridad informática y/o la seguridad de la información[64].

[63] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

[64] TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. Op. Cit., p.14.

RECOMENDACIONES

- Mantener los sistemas operativos debidamente actualizados y licenciados.
- El uso de un buen antivirus, con restricciones de uso para el usuario.
- Administración de directivas desde el equipo servidor, y desarrollo de políticas de descargas y ejecución de archivos.
- Creación de un dominio debidamente administrador por personal idóneo, interno o externo de la compañía.
- Actualización de herramientas ofimáticas y software internos y externos de la compañía.
- Administración de directivas desde el equipo servidor, y desarrollo de políticas de autorización de manejo del firewall.

BIBLIOGRAFÍA

ANDALUCÍA ES DIGITAL. [Sitio web]. Bogotá: ANDALUCÍA ES DIGITAL, qué es pentesting y por qué es importante en una estrategia de seguridad. [Consulta: 07 de junio de 2020]. Disponible en: https://www.blog.andaluciaesdigital.es/pentesting-que-es/

AVENÍA DELGADO, Carlos Arturo, autor [en línea]. Tesis fundamentos de seguridad informática. Fundación Universidad del área Andina, 2017. [Consulta: 06 de junio de 2020]. Disponible en: https://digitk.areandina.edu.co/bitstream/handle/areandina/1367/Fundamentos%20de%20seguridad%20inform%C3%A1tica.pdf?sequence=1&isAllowed=y

BUCKER, Caleb, autor [en línea]. Tesis Pen-Tester – Ethical Hacker – Security Researcher. Seguridad informática, 2012. [Consulta: 10 de junio de 2020]. Disponible en: https://www.exploit-db.com/docs/spanish/22954-[spanish]-penetration-testing---analisis-web---evaluacion-de-vulnerabilidades---explotacion.pdf

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. [Sitio web]. Colombia: CCIT, tendencias cibercrimen Colombia 2019 – 2020. [Consulta: 12 de junio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CAMPUS INTERNACIONAL CIBERSEGURIDAD. [Sitio web]. Bogotá: ¿Qué es el pentesting? [Consulta: 07 de junio de 2020]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

CASTRO, Carlos, autor [en línea]. Tesis pruebas de penetración e intrusión. Universidad Piloto de Colombia, 2019. [Consulta: 06 de junio de 2020]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y

CASTRO, Duvan; ROJAS, Ángela ROMERO, autor [en línea]. Tesis Trabajo de grado para optar al título de Ingeniero de Sistemas. Universidad Católica de Colombia, 2013. [Consulta: 06 de junio de 2020]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZ

AS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf

DIGITAL GUIDE IONOS. [Sitio web]. España: IONOS, DDoS y DoS: así puedes proteger a tu equipo de estos ataques. [Consulta: 10 de junio de 2020]. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/dos-y-ddos-un-vistazo-a-ambos-patrones-de-ataque/

DONGEE. [Sitio web]. Bogotá: DONGEE, tipos de Vulnerabilidades que se pueden encontrar aplicando pentesting. [Consulta: 10 de junio de 2020]. Disponible en: https://blog.dongee.com/tipos-de-vulnerabilidades-que-se-pueden-encontrar-aplicacando-pen-testing-59ccc9c12cc0

DRAGONJAR. [Sitio web]. Bogotá: DRAGONJAR, ¿Cómo se realiza un Pentest? [Consulta: 10 de junio de 2020]. Disponible en: https://www.dragonjar.org/como-realizar-un-pentest.xhtml

EXPERTS ON YOUR SIDE. [Sitio web]. Latinoamérica: ESET, Security Report. [Consulta: 12 de junio de 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

FAQ. [Sitio web]. (US): FAQ, Penetration Testing Execution Standard - the FAQ. [Consulta: 07 de junio de 2020]. Disponible en: http://www.pentest-standard.org/index.php/FAQ#Q:_Who_is_involved_with_this_standard.3F

GUILLÉN ZAFRA, José Luis, autor [en línea]. Tesis introducción al pentesting. Universidad de Barcelona, 2017. [Consulta: 08 de junio de 2020]. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf

HARÁN, Juan Manuel, autor [en línea]. El 40% de las empresas de América Latina sufrió una infección con malware el último año, 2019. [Consulta: 06 de junio de 2020]. Disponible en:https://www.welivesecurity.com/la-es/2019/09/05/el-40-de-las-empresas-de-america-latina-sufrio-una-infeccion-con-malware-el-ultimo-ano/

HIBERUS TECNOLOGÍA. [Sitio web]. Bogotá: HIBERUS, Qué es pentesting y cómo detectar y prevenir ciberataques. [Consulta: 07 de junio de 2020]. Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/

INFOSECINSTITUTE. [Sitio web]. (US): INFOSECINSTITUTE, Top 7 Web Application Penetration Testing Tools. [Consulta: 10 de junio de 2020]. Disponible

en: https://resources.infosecinstitute.com/top-7-web-application-penetration-testing-tools/#gref

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. España: INCIBE, ¿Qué es pentesting? Auditando la seguridad de tus sistemas. [Consulta: 10 de junio de 2020]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (NIST), Sobre NIST [sitio web]. Gaithersburg, Maryland [Consultado: 1 de sept. de 2020]. Disponible en: https://www.nist.gov/about-nist

ISO 27001. [Sitio web]. España: ISO 27001: Fase 2 análisis del contexto de la organización y determinación del alcance. [Consulta: 26 de junio de 2020]. Disponible en: https://normaiso27001.es/fase-2-analisis- del-contexto-de-la-organización-y-determinación-del-alcance/).

JIMÉNEZ, CRISTIAN, autor [en línea]. Tesis seguridad en redes y sistemas, técnicas y conceptos sobre hacking y pentesting. Universidad Oberta de Catalunya, 2016. [Consulta: 10 de junio de 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/52944/9/cjmenezTFG0616memoria.pdf

LINKEDIN. [Sitio web]. Bogotá: LINKEDI, Metodologías para la auditoria de la seguridad. [Consulta: 06 de junio de 2020]. Disponible en: https://www.linkedin.com/pulse/metodolog%C3%ADas-para-la-auditoria-de-seguridad-kevin-rodriguez-lago

MACHACA TOLA, Álvaro, autor [en línea]. Tesis análisis de riesgos aplicando la metodología OWASP, 2017. [Consulta: 08 de junio de 2020]. Disponible en: https://owasp.org/www-pdf-archive/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

MARTÍNEZ SÁNCHEZ, Patricia Alejandra, autor [en línea]. Tesis implementación de pentesting para encontrar vulnerabilidades en el sistema utilizado en la compañía “DIRSA” aplicando metodología de OWASP. Universidad autónoma de baja california sur, 2018. [Consulta: 06 de junio de 2020]. Disponible en: http://biblio.uabcs.mx/tesis/te4095.pdf

MEGASEGURIDAD. [Sitio web]. Bogotá: MEGASEGURIDAD. [Consulta: 06 de junio de 2014]. Disponible en: https://www.megaseguridad.co/
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE. [Sitio web]. España: PNTIC, vulnerabilidades de un sistema informático. [Consulta: 07 de junio de 2020]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES [Sitio web]. Colombia: MINTIC, Ley 1273 de 2009. [Consulta: 20 de junio de 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES [Sitio web]. Colombia: MINTIC, Ley 1273 de 2009. [Consulta: 20 de junio de 2020]. Disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MinTIC. 2015. “Modelo de Seguridad y Privacidad de La Información.” 1–32. SIIGO. n.d. “Siigo Contador, El Modelo de Software Contable En Colombia.”
NORMA TÉCNICA COLOMBIANA [Sitio web]. Colombia: NTC-ISO/IEC, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (sgsi). Requisitos. [Consulta: 20 de junio de 2020]. Disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

OPENWEBINARS. [Sitio web]. España: OPENWEBINARS, ¿Que es un Pantesting? [Consulta: 10 de junio de 2020]. Disponible en: https://openwebinars.net/blog/que-es-el-pentesting/
OSTEC SEGURANCA DIGITAL DE RESULTADOS. [Sitio web]. Brasil: OSTEC, 07 Jun Pentest: ¿qué es y cuáles son los principales tipos? [Consulta: 10 de junio de 2020]. Disponible en: https://ostec.blog/es/seguridad-perimetral/pentest-concepto-tipos

OWASP. [Sitio web]. Bogotá: OWASP, Los diez riesgos más críticos en Aplicaciones Web. [Consulta: 07 de junio de 2020]. Disponible en: https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf
PÁEZ PIRAZAN, Miguel Camilo, autor [en línea]. Tesis Especialización en Seguridad Informática. Universidad Piloto de Colombia, 2014. [Consulta: 12 de junio de 2020]. Disponible en:

http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2942/00002027.pdf?sequence=1
PORTANTIER, Fabián, autor [en línea]. Tesis seguridad informática. Red User, 2013. [Consulta: 07 de junio de 2020]. Disponible en: http://biblioteca.utsem-morelos.edu.mx/files/tic/14octubre2013/red/Seguridad%20Informatica.PDF

PULIDO, Andrea; RINCON, Paulo y VELASQUEZ, Oscar, autor [en línea]. Tesis ingeniería de sistemas. Universidad san Buenaventura, 2011. [Consulta: 06 de junio de 2020]. Disponible en: http://biblioteca.usbbog.edu.co:8080/Biblioteca/BDigital/66035.pdf

ROMERO CASTRO, Martha Irene, et al. Autor [en línea]. Tesis introducción a la seguridad informática y el análisis de vulnerabilidades. Universidad Estatal del sur de Manabí, 2018. [Consulta: 06 de junio de 2020]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

SOFTWARE LAB. [Sitio web]. España: SOFTWARE LAB, ¿Qué es una vulnerabilidad informática? [Consulta: 07 de junio de 2020]. Disponible en: https://softwarelab.org/es/que-es-una-vulnerabilidad-informatica/
TECHTARGET. [Sitio web]. Bogotá: TECHTARGET, Pentesting e ingeniería social, ¿sí o no? [Consulta: 10 de junio de 2020]. Disponible en: https://searchdatacenter.techtarget.com/es/opinion/Pen-testing-e-ingenieria-social-si-o-no

TECNOLOGÍA INFORMÁTICA. [Sitio web]. (US): TECNOLOGÍA INFORMÁTICA, vulnerabilidades informáticas. [Consulta: 10 de junio de 2020]. Disponible en: https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/

TOVAR, Álvaro; GOMEZ, José, M., & Jaime, J. A. B. [en línea]. Tesis Diagnóstico y viabilidad de implementación del modelo de seguridad informática para la empresa Megaseguridad. Universidad Nacional Abierta y a Distancia (UNAD), 2020. [Consulta: 06 de junio de 2020]. Tesis Diagnóstico y viabilidad de implementación del modelo de seguridad informática para la empresa Megaseguridad, pp. 9-30

UNIR REVISTA. [Sitio web]. Bogotá: UNIR, 07 Jun Pentest: Pentest: test de seguridad para prevenir ciberataques. [Consulta: 10 de junio de 2020]. Disponible en: https://www.unir.net/ingenieria/revista/noticias/pentest/549204824885/

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. [Sitio web]. México: UNAM, pruebas de penetración para principiantes: 5 herramientas para empezar. [Consulta: 10 de junio de 2020]. Disponible en: https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

VANEGAS ROMERO, Alfonso Yucenid, autor [en línea]. Tesis pentesting, ¿Porque es importante para las empresas? Universidad Piloto de Colombia, 2020. [Consulta: 06 de junio de 2020]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1&isAllowed=y

VINCENSINI, Pierre. Organización Internacional para la Normalización, Qué es la ISO [sitio web]. Cointrin, Ginebra [Consultado: 1 de sept. de 2020]. Disponible en: https://www.ioe-emp.org/es/organizaciones-internacionales/organizacion-internacional-para-la-normalizacion

ANEXOS

Anexo A. Acuerdo de confidencialidad.

MEGASEGURIDAD
DESDE 1979

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 *(JOSE LUIS GOMEZ VILLAMIL* – MEGASEGURIDAD LA PROVEEDORA LTDA.*)* 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 de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las cláusulas del presente acuerdo de confidencialidad por parte de *JOSE LUIS GOMEZ VILLAMIL*

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.

Firman en Bogotá D.C., a los (13) días del mes de julio de 2020

Como Parte Receptora:	Por la parte reveladora:
José Luis Gómez Villamil	Claudia Palacino Lemus
C.C. 80.199.947 de Bogotá	C.C. 39.546.081 de
Estudiante de la UNAD	Megaseguridad La Proveedora Ltda.

VIGILADO Superintendencia R 2013120033397 del 25-06-2013

TELÉFONOS: +(57) 482 1200 | +(57) 321 2133356
E-MAIL: correspondencia@megaseguridad.co
DIRECCIÓN: Calle 98 N° 20 - 45, Bogotá, Colombia

MEGASEGURIDAD.co

Fuente: “elaboración propia”

Anexo B. Autorización.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por **MEGASEGURIDAD LA PROVEEDORA LTDA.**
- La empresa **MEGASEGURIDAD LA PROVEEDORA LTDA.** deberá establecer qué tipo de información es privada y cuál es pública para delimitar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.

Firman en Bogotá D.C., a los 13 días del mes de julio de 2020

Cordialmente,

JOSE LUIS GOMEZ VILLAMIL
Estudiante UNAD.

CLAUDIA PALACINO LEMUS
Gerente Talento Humano

Fuente: "elaboración propia"