ESTUDIO DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES DE COLOMBIA

JEFFERSON GONZALEZ LONDOÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUGA
2020

ESTUDIO DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES DE COLOMBIA

JEFFERSON GONZALEZ LONDOÑO

Monografía

Proyecto de grado para optar por el título de:
Especialista en seguridad informática

Asesor de proyecto: Yina Alexandra Gonzalez Sanabria

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUGA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

2020

DEDICATORIA

A mi familia, madre, padre, hermanas. Han sido un apoyo incondicional en cada uno de los proyectos que he emprendido y en lo cual he encontrado la fuerza necesaria para seguir adelante a pesar de los diferentes obstáculos presentados.

A mi esposa Alexandra que siempre me ha brindado su apoyo, su disposición y consejos en cada momento.

AGRADECIMIENTOS

Agradezco en primer lugar a la ingeniera Yina Gonzalez por su invaluable apoyo y consejos en el desarrollo de la presente investigación. También agradezco a la Universidad Nacional Abierta y a Distancia por que ha significado una gran oportunidad para mi desarrollo académico y profesional. Por último, agradezco a todos los tutores que han hecho parte del desarrollo de mis estudios con sus conocimientos y observaciones que me han permitido cumplir con mis objetivos y también crecer como persona.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

AMENAZA: Objeto o acción que puede impactar negativamente la seguridad informática.

CIBERATAQUE: Se denomina a toda acción ejecutada utilizando generalmente medios digitales como un computador y el internet para atentar o causar un perjuicio a otra persona o entidad.

CIBERDELITO: Es toda acción ejecutada usando como objeto o medio un sistema informático y que busca de forma fraudulenta acceder, modificar o destruir información para la cual no está autorizado, afectar un bien ajeno.

CIBERSEGURIDAD: Conjunto de medidas de tipo documentales, procedimentales o técnicas que permiten salvaguardar un activo en el ciberespacio.

CISO: Se denomina así al colaborador de una organización encargado de ajustar las posibles decisiones en materia de seguridad, políticas y programas, con los objetivos organizacionales.

CONFIDENCIALIDAD: Se define como la certeza de que la información solo se utilizará para los medios que fue autorizada y que ninguna persona no autorizada tendrá acceso a la misma.

DATACENTER: Termino común con el cual se refiere a los centros de procesamiento de datos. Se refiere a una ubicación física en la que se encuentra concentrado un conjunto de dispositivos informáticos que proveen un servicio a una organización.

DISPONIBILIDAD: Se denomina a la garantía que se da de que la información será accesible en todo momento.

DVWA: Se refiere a la aplicación “Damn Vulnerable Web Application” escrita en php y dispuesta para realizar pruebas de seguridad en aplicaciones web.

FIREWALL: Dispositivo o software que se encarga de monitorear el tráfico a través de una red y controlar los paquetes que pueden o no permitirse en la misma.

HACKER: Persona con avanzados conocimientos en el campo de la informática y en especial de la seguridad que se dedica a descubrir fallos en sistemas.

HACKING: Manipulación de un sistema informático para sacar provecho de un fallo de seguridad.

HARDWARE: Componentes físicos que hacen parte de un dispositivo electrónico.

HTML: Denominado lenguaje de marcado de Hipertextos es utilizado en el desarrollo de páginas web, permitiendo generar la estructura de estas.

HTTP: Protocolo utilizado en internet para la transferencia de los Hipertextos.

ICMP: El protocolo ICMP o “protocolo de control y notificación de errores a nivel de red” son paquetes enviados con el objetivo de encontrar las rutas más

adecuadas y notificar los posibles problemas en una determinada ruta. Esto es utilizado para la transmisión de paquetes o para cortar la comunicación debido a un problema de red.

IDS: Sistema de detección de intrusiones. Utilizado para monitorear el comportamiento de la red para detectar posibles comportamientos anómalos que indiquen un posible ataque.

INTEGRIDAD: Garantía que se brinda de que la información no ha sido alterada.

LICENCIA GNU: La licencia "General Public License" es utilizada de forma amplía en software libre y de código abierto. Este tipo de licenciamiento le brinda al usuario la posibilidad de utilizar el software, acceder al código, modificarlo y compartirlo garantizando que cualquier software derivado deberá tener este mismo tipo de licenciamiento.

MALWARE: Software malicioso que se escribe con el fin de generar alguna afectación en un sistema informático.

METODOLOGÍA: Conjunto de pasos que se ejecutan para desarrollar una determinada actividad. Como una investigación o el desarrollo de un proyecto.

PENTEST: Conjunto de pruebas que permiten determinar el nivel de exposición de un activo informático.

REDES: En informática son un conjunto de ordenadores interconectados y que les permite compartir diferentes tipos de recursos.

RIESGO: El riesgo es la posibilidad de materialización de una amenaza.

SEGURIDAD: Conjunto de garantías que se otorgan en la protección de un activo.

SOFTWARE: Es un conjunto de código que permite a un computador desarrollar determinadas tareas.

TCP: El protocolo de control de transmisión permite garantizar la correcta recepción de los paquetes de datos incluyendo un número secuencial que sirve para conservar el orden de transmisión y para ensamblar de la forma correcta los paquetes. Este protocolo requiere que la conexión entre los extremos haya sido establecida.

VPN: Red virtual privada que permite establecer conexión entre dos redes diferentes de forma segura.

VPS: Es un servidor virtual privado donde un mismo servidor físico es dividido en varios servidores virtuales.

VULNERABILIDAD: Toda aquella debilidad presente en un sistema informático que produce un riesgo para la seguridad de la información comprometiendo con esto la integridad.

WORDPRESS: Plataforma web de código abierto utilizada para desarrollar múltiples sitios web. Se estima que más del 36% de los sitios web de internet están creados utilizando WordPress.

XSS: Cross-site Scripting o XSS es una vulnerabilidad común en aplicaciones web que le permite a un atacante inyectar código en un sitio web que es de confianza para los usuarios, buscando suplantar la identidad del usuario.

RESUMEN

La creciente ola de información digital en la actualidad lleva a las organizaciones a concentrar su atención no solo en la mejora de procesos prácticos, livianos y de fácil manejo, si no que extiende su radio de acción hacía la protección de los datos producidos diariamente, pues estos toman hoy el peso de activo de gran importancia para los negocios.

Por ello es de gran interés ahondar en métodos que permitan evaluar periódicamente la protección de los datos y el sistema aplicado para salvaguardarlos. Garantizar la seguridad de esta y de la infraestructura sobre la cual se encuentra y se transporta es fundamental para el funcionamiento del negocio. De allí el interés del presente trabajo, el cual pretende generar un estudio del estado actual de la seguridad informática en las organizaciones de Colombia a través de un análisis de las vulnerabilidades a las que se expone una empresa en sus operaciones diarias donde constantemente se realiza intercambio de información para el cumplimiento de sus procesos internos y externos. Adicionalmente se presentará una serie de pruebas de penetración, que pueden ser aplicadas para identificar el posible nivel de exposición en el que se encuentra un sistema informático a un posible ataque por parte de ciberdelincuentes.

Basados en este análisis se podrán identificar los controles aplicados por las organizaciones que permitirían mitigar el riesgo.

De igual manera será realizado un análisis de las competencias aplicadas al perfil de los cargos de los profesionales que ejecutan labores en el área informática, específicamente en el campo de la seguridad, y así poder determinar el nivel de cualificación del recurso humano en las empresas.

Como resultado de los diferentes análisis realizados frente a controles, vulnerabilidades y perfiles, serán entregadas las recomendaciones que aplican para las entidades objeto de estudio mediante las cuales puedan las organizaciones tener un apoyo para mitigar los riesgos a los que se encuentran expuestas.

Palabras claves: Redes, Ciberseguridad, seguridad, Pentest.

ABSTRACT

The growing wave of information in the current technological world leads organizations to focus their attention not only on improving practical, light and easy-to-use processes, but extending their range of action towards the protection of daily produced data, as today they take the weight of assets of great importance for business.

Therefore, it is of great interest to delve into methods that allow periodically to evaluate the protection of the data and the system applied to safeguard them. Ensuring the safety of this and the infrastructure on which it is located and transported is essential for the operation of the business. Hence the interest of this work, which aims to generate a study of the current state of computer security in Colombian organizations through an analysis of the vulnerabilities to which a company is exposed in its daily operations where exchange is constantly carried out of information for the fulfillment of its internal and external processes. Additionally, a series of penetration tests will be presented, which can be applied to identify the possible level of exposure in which a computer system is located to a possible attack by cybercriminals.

Based on this analysis, the controls applied by the organizations that would mitigate the risk can be identified.

In the same way, an analysis of the competences applied to the profile of the positions of the professionals who perform tasks in the computer area, specifically in the field of security, will be carried out, and thus be able to determine the level of qualification of the human resource in the companies.

As a result of the different analyzes carried out against controls, vulnerabilities and profiles, the recommendations that apply to the entities under study will be delivered through which organizations can have support to mitigate the risks to which they are exposed.

Keywords: Networks, Cybersecurity, security, Pentest.

INTRODUCCIÓN

Esta monografía se desarrolla a partir de un estudio del estado en el que se encuentra actualmente la seguridad informática en Colombia, particularmente el sector empresarial. El desarrollo del primer objetivo documenta las principales debilidades que actualmente son explotadas por los ciberdelincuentes y los factores que contribuyen al éxito de estos atacantes. Se incluye también estadísticas de los ciberataques a los que se ve enfrentado el país. Una vez contextualizado el panorama, el desarrollo del segundo objetivo se enfoca en revisar algunas de las principales metodologías de hacking ético que están disponibles para implementar en busca de mejorar los niveles de seguridad y empezar a mitigar los riesgos que puedan generar un foco de inseguridad y permitir a un delincuente entrar en los sistemas informáticos y efectuar su ataque de forma exitosa. El objetivo tres se desarrolla ofreciendo al lector algunas pruebas de penetración sobre diferentes recursos con una red LAN en la identificación de equipos, puertos, servicios activos, aplicaciones web vulnerables y con esto entregar al lector herramientas que pueden ser implementadas para medir el nivel de eficiencia de sus controles y poder determinar las posibles mejoras que requiere.

Finalmente, en el desarrollo del objetivo 4 se consolida un conjunto de recomendaciones que se pueden aplicar en una organización para mitigar los riesgos y conseguir con esto un adecuado nivel de seguridad en sus procesos.

Una vez concluido el desarrollo de los objetivos de la monografía, se entregan las conclusiones que se pueden obtener a partir del desarrollo de la problemática y se emiten recomendaciones encaminadas a dar una solución a las mencionadas conclusiones.

Finalmente se entrega el apartado dedicado a la divulgación del documento donde se certifica que puede ser publicado sin ninguna restricción.

1. DESCRIPCIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La migración de los diferentes procesos al interior de las organizaciones empresariales en el país al campo digital, donde todas sus operaciones y la información depende del correcto funcionamiento de un software, hardware y demás componentes que conforman toda la infraestructura tecnológica, ha significado también una enorme preocupación y el crecimiento de blancos que son fijados por los criminales para sacar algún tipo de provecho, por lo general, económico. En el año 2019 se reportó un total de 42 billones de intentos de ataques por parte de ciber delincuentes en un espacio de tiempo igual a tres meses.[1] Estos estudios por parte de Fortinet también entregan a los Ransomware y el Phishing como los ataques más utilizados y que más perdidas han generado. En Colombia según el Informe de Tendencias del Cibercrimen 2019-2020 realizado en conjunto entre un equipo de investigadores particulares, un equipo de la Policía Nacional y empresas tecnológicas aliadas, reportaron un total de 15948 denuncias en 2019, siendo esto un 5.8% menos que el año 2018 que tuvo 22524,[2] estas cifras llevan a plantear si las medidas de seguridad adoptadas están siendo suficientes o el nivel de conciencia de la problemática aún no ha sido la adecuada.

1.2 PLANTEAMIENTO DEL PROBLEMA

Las organizaciones a nivel mundial se encuentran en continuo proceso de mejoramiento de la seguridad informática y de la información, entendiendo con esto la importancia y/o necesidad de garantizar que su activo se encuentre protegido conservando los pilares fundamentales de disponibilidad, privacidad e integridad. Sumado a lo anterior, la demanda de servicios multimedia por parte de los usuarios y organizaciones[3] ha propiciado la aparición de nuevas tecnologías y con ello también el nacimiento de nuevas amenazas para estas.

---

[1] DINERO. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. 2019. [En línea]. Disponible en https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

[2] CCIT. Informe de las tendencias del cibercrimen en Colombia 2019-2020. 2019. [En línea]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[3] AUSTIN, Robert y DARBY, Christopher. El mito de la seguridad informática. Ediciones Deusto – Planeta de Agostini Profesional y Formación S.L., 2004. 9 p. [En línea]. Disponible en https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3159136

La seguridad informática se puede analizar desde diferentes perspectivas como son la seguridad en red, seguridad de software y seguridad de hardware.

Estas tres perspectivas se ven involucradas directamente en el envío y recepción de información tanto al interior como fuera de las organizaciones y es por ello la importancia de abordar y aplicar controles en cada uno de ellos.

Para prevenir ataques se inicia con una detección oportuna de anomalías en el tráfico de información.[4] Por lo anterior, se hace necesario analizar y detectar todas aquellas anomalías que pueden ser corregidas con el tiempo adecuado. Desafortunadamente en Colombia aproximadamente un 80% de las empresas no han establecido ningún tipo de política o protocolo concerniente con la seguridad informática disponiendo un mínimo porcentaje de su presupuesto en la aplicación de controles, lo que resulta insuficiente para garantizar un nivel aceptable que permita garantizar la seguridad de su información y de su recurso tecnológico.

Según el balance entregado por la policía nacional de Colombia, en el año 2017 los delitos informáticos tuvieron un incremento del 28,3% con respecto al 2016, donde la suplantación de correos electrónicos corporativos generó una pérdida estimada en 380 millones de pesos como principales blancos altos cargos de diferentes empresas a nivel nacional. La baja implementación de programas de concientización a los funcionarios de las organizaciones contribuye con el ciberdelito teniendo en cuenta que el usuario del sistema es la primera barrera de seguridad que se debe fortalecer.

En la actualidad, si bien se empieza a encontrar perfiles laborales de personas en seguridad, aún es una disciplina altamente ignorada por los empresarios que no evalúan o prevén de forma clara el alto nivel de impacto que puede representar para su empresa enormes pérdidas.

[4] BARRIONUEVO, Mercedes, *et al*. Secure Computer Network: Strategies and Challengers in Big Data Era. Journal of Computer Science & Technology (JCS&T), 18(3), 248–257. 2018. [En línea]. Disponible en https://doi-org.bibliotecavirtual.unad.edu.co/10.24215/16666038.18.e28

1.3 FORMULACIÓN DEL PROBLEMA

¿Es evaluada de forma continua la seguridad de los sistemas informáticos en las organizaciones empresariales de Colombia?

2 JUSTIFICACIÓN

La seguridad informática se está convirtiendo en una urgencia para todos los países de Latinoamérica, zona del planeta donde durante el 2018 se alcanzó el máximo histórico en materia de vulnerabilidades. Uno de los mayores ataques que se puede destacar fue el generado por los denominados criptomineros, quienes realizaron la distribución de un malware que tiene como objetivo aprovechar los recursos de los equipos infectados en la minería de criptomonedas. Entre los países de Latinoamérica, el 5% de las detecciones de criptomineros fue realizada en Colombia.[5]

En el año 2019, la firma de seguridad Fortinet entregó un informe que permite detallar que Colombia es uno de los países Latinoamericanos que más intentos de ciberataques tiene diariamente, contabilizando en dicho informe un total de 42 billones de intentos de ataques en el primer trimestre del año, donde se destacan la distribución de malware a través de correos electrónicos. De acuerdo con este mismo estudio, las organizaciones financieras se muestran como los objetivos más frecuentes de estos intentos de intrusión.[6] La policía de Colombia reporto un total de 12014 denuncias de ciudadanos que fueron víctimas de ataques virtuales donde más del 50% de los casos se encuentra relacionado con fraudes financieros con saqueo de dineros a cuentas bancarias.[7]

Un estudio realizado por el ministerio de las TIC en Colombia determinó que una cifra superior al 60% de las empresas sufrió pérdidas económicas debido a la falta de controles de seguridad y luego de ser víctimas de ataques, los costos oscilaron entre un (1) millón los más bajos y un 5% de estas sufrieron pérdidas de un orden cercano a los cuatro (4) mil millones de pesos.[8]

Teniendo en cuenta la situación mencionada, el presente documento se realiza con el propósito de recoger evidencias que permitan dar una visión o panorama del estado actual de la seguridad informática en las empresas, las principales amenazas que las afectan actualmente generando conciencia en el lector y

[5] GUISTO BILIC, Denise. Las amenazas informáticas que más afectaron a los países de América Latina. 2019. [En línea] Disponible en https://www.welivesecurity.com/la-es/2019/01/10/amenazas-informaticas-mas-afectaron-paises-america-latina/

[6] DINERO. Op. Cit., En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. 2019. [En línea] Disponible en https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

[7] RAMÍREZ, María Carolina. El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia. 2019. [En línea] Disponible en https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067

[8] HEALTH ON LINE. 5% de las empresas colombianas han perdido hasta cuatro mil millones por ciberataques. 2019. [En línea] Disponible en https://www.heon.com.co/index.php/news/item/241-ataques-ciberneticos-colombia

generando como principal beneficio, un punto de partida en la aplicación de mejores prácticas de seguridad informática en sus organizaciones.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Presentar un análisis y detección de vulnerabilidades de seguridad informática para las organizaciones empresariales en Colombia que permita mitigar las principales debilidades que se presentan en la actualidad.

3.2 OBJETIVOS ESPECIFICOS

- Analizar el panorama actual de la seguridad informática de las organizaciones empresariales en Colombia.
- Analizar metodologías de hacking ético para la detección de vulnerabilidades en las organizaciones.
- Presentar un conjunto de pruebas de seguridad para detección de vulnerabilidades.
- Entregar recomendaciones fundamentales aplicables a las empresas para evaluar su seguridad.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Las organizaciones de Colombia no son ajenas al éxodo que se tiene hacía el mundo digital y la información resultante de sus procesos es un activo de gran valor que es necesario proteger y generar mecanismos que permitan garantizar los principios de confidencialidad, disponibilidad, integridad y no repudio, sin embargo, según los balances generados por empresas de seguridad como Fortinet, Colombia es uno de los países con mayor tasa de intentos de ataques cibernéticos del país, lo cual, no es sorpresa si se revisa el bajo porcentaje de empresas que invierte recursos en seguridad y en muchos casos, la inversión que se hace resulta ser infructuosa para enfrentar los desafíos actuales. La empresa Citrix para el año 2017 publicó un estudio que presenta cifras preocupantes sobre la implementación de mecanismos de seguridad en las compañias, donde en un total de 48% de las empresas encuestadas, no tienen desarrollado, ni en borrador, unas políticas de seguridad. Además, un 70% mencionó contar con herramientas de seguridad obsoletas y que no brindan el nivel requerido ante la amenaza actual.[9]

También es importante mencionar que de acuerdo con un estudio solicitado por la empresa CISCO hacía el año 2008 y realizado por Kaagan Reserch Associates, se calificó a Colombia como uno de los países más débiles en seguridad y propenso a ciberataques obteniendo una calificación de 62/100 puntos y con un panorama no muy diferente a otras investigaciones, ya que se encontró que más de un 65% no toman en cuenta la seguridad de su información como un proceso de importancia para la organización.[10] Lo anterior indica que en toda una década, la expansión de la tecnología y la expansión del cibercrimen han aumentado de forma constante y el interés de las empresas sigue siendo muy inferior a lo requerido.

Para conseguir un nivel aceptable de seguridad en nuestros sistemas informáticos es indispensable contar con un conjunto de procedimiento que permitan generar control en los diferentes procesos. La seguridad informática se divide en 3 tipo básicos que son la seguridad de red, la seguridad de hardware y la seguridad de software.

[9] ANGULO, Susana. Empresas fallan en sus sistemas de seguridad informática. 2017. [En línea] Disponible en https://www.enter.co/especiales/empresas-del-futuro/segun-estudio-empresas-fallan-en-sus-sistemas-de-seguridad-informatica/

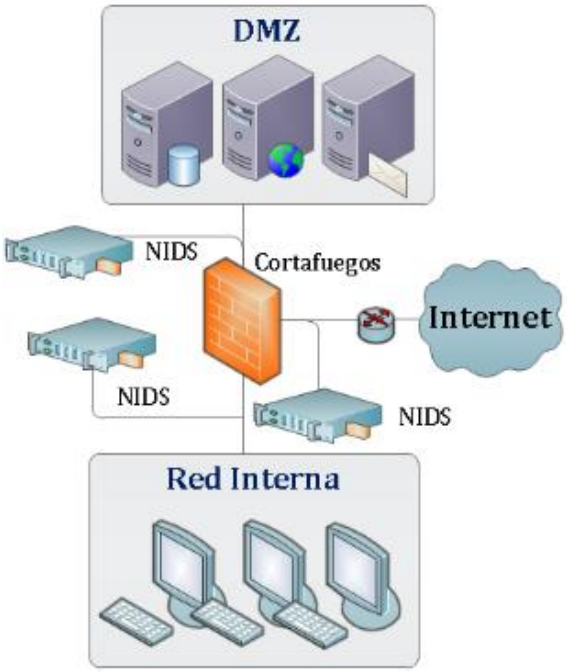
[10] DINERO. Empresas. Colombia, débil en seguridad informática. 2008. [En línea] Disponible en https://www.dinero.com/edicion-impresa/tendencias/articulo/empresas-colombia-debil-seguridad-informatica/66085

4.1.1 Seguridad De Red. Las redes de datos sirven de vehículo para el transporte de los datos de una organización, por lo tanto, es importante implementar controles de seguridad a nivel de red lo cuales van encaminados a impedir que las posibles amenazas puedan ingresar a los dispositivos y con ello infectar los sistemas informáticos de una organización.[11]

Son múltiples las amenazas que se pueden aprovechar de la ausencia de seguridad en la red para ingresar a los sistemas, estos pueden ser ataques de hacker, interceptación o escucha ilegal de información, la propagación de virus, software espía y robo de identidad.

Los controles efectivos de seguridad en la red son todos aquellos que agrupan un conjunto de soluciones entre software y hardware, entre los que se puede destacar el antivirus, firewall, un IDS o sistema de detección de intruso y el uso de redes VPN.

Ilustración 1. Controles de Seguridad en redes.



Fuente: RAMOS FRAILE, Alejandro. Lección 5: Seguridad Perimetral. [Imagen]. Intypedia. España. 2011. p. 3. [Consultado: 15 de noviembre de 2019]. Disponible en: http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

[11] UNIVERSIDAD INTERNACIONAL DE VALENCIA, VIU. Tres tipos de seguridad informática que debes conocer. 2018. [En línea] Disponible en https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/

4.1.2 Seguridad De Hardware. La seguridad de hardware se relaciona con todos los mecanismos utilizados para garantizar que los dispositivos físicos de un sistema informático se encuentran seguros ante las posibles amenazas. Este tipo de seguridad incluye áreas como el análisis de los equipos para detectar vulnerabilidades en los mismos, los denominados firewall de hardware.

La seguridad de hardware puede ser activa o pasiva, en la siguiente tabla se describe cada una:

Tabla 1. Seguridad Activa y Pasiva

Tipo Seguridad Hardware	Descripción
SEGURIDAD ACTIVA	La seguridad activa incluye todos aquellos mecanismos que se encuentran todo el tiempo en función de protección. Aquí se incluye las fuentes de voltaje ininterrumpidas.[12]
SEGURIDAD PASIVA	La seguridad pasiva son aquellos controles implementados para entrar a funcionar justo al momento que se presenta una amenaza para el sistema, es decir, si la seguridad pasiva se activa es porque la amenaza superó todos los controles activos.[13] En el proceso de seguridad del hardware también se puede incluir todas aquellas medidas aplicadas para proteger las partes físicas del dispositivo y el entorno. El control de acceso a un recinto en el que se encuentre un dispositivo, los sistemas de detección de incendio, la climatización de este, son medidas encaminadas a preservar el correcto funcionamiento de las partes del dispositivo.

[12] AGUILERA LÓPEZ, Purificación. Seguridad informática. 1ª ed.: Editex, 2010. 240 p. ISBN 978-84-9771-657-4

[13] NAKED SECURITY. Seguridad activa y seguridad pasiva en equipos informáticos. 2012 [En línea] Disponible en https://news.sophos.com/es-es/2012/09/14/seguridad-activa-y-seguridad-pasiva-en-equipos-informaticos/

4.1.3 Seguridad De Software. La seguridad de software es la encargada de proteger las aplicaciones instaladas en los diferentes dispositivos y que pueden ser blanco de ataques debido a las múltiples vulnerabilidades que usualmente presentan. Se debe tener en cuenta que el software es parte fundamental de cualquier organización en el cumplimiento de su propósito y se encarga de gestionar la información fruto de estos.

Los controles a nivel de software pasan por el antivirus, mantener actualizados los aplicativos en la última versión de los parches, las actualizaciones del sistema operativo y el control de cada uno de los nuevos programas que se deseen instalar.[14]

4.1.4 Mecanismos De Seguridad. Los mecanismos utilizados para la seguridad de un sistema informático y su información se pueden clasificar en dos clases principales que son la seguridad física y la seguridad lógica.[15]

Tabla 2. Mecanismos de Seguridad

Tipo de Mecanismo	Descripción
SEGURIDAD FÍSICA	Mecanismos de seguridad física son todos aquellos dispositivos implementados cuyo servicio permite otorgar seguridad a un sistema informático. Entre los diferentes dispositivos de seguridad física se pueden mencionar los siguientes: • SAI o Sistema de alimentación ininterrumpidas que permiten proteger los dispositivos ante fallas de carácter eléctrico. • Detectores de fuego y humo permiten proteger un espacio y brindar una alarma en caso de posible alza de temperatura en un recinto en el que se encuentren dispositivos. • Sistemas de control de acceso biométrico para evitar el acceso de personal no autorizado a los datacenter o recintos que alberguen dispositivos

[14] UNIVERSIDAD INTERNACIONAL DE VALENCIA, VIU. Op. Cit., Tres tipos de seguridad informática que debes conocer.
[15] AGUILERA LÓPEZ, Purificación. Op. cit., Seguridad informática.

	importantes para el funcionamiento de una organización.
SEGURIDAD LÓGICA	Mecanismos de seguridad lógico son aquellos destinados a la protección a nivel digital de los sistemas informáticos y la información. Como mecanismos de seguridad lógico se pueden mencionar:[16] • Software antivirus • Sistema de autenticación de usuarios • Firewall o cortafuegos • Encriptado de claves • Cifrado de datos

Fuente: El autor

Los mecanismos mencionados deben ser utilizados de forma combinada para poder afirmar que el nivel de seguridad cuenta con un nivel aceptable, ya que ningún mecanismo de seguridad implementado por sí solo podría brindar garantías.

Cuando se menciona mecanismos de seguridad dirigidos a la seguridad de la información, además de los mencionados, se deben incluir todos aquellos planes, procedimientos y políticas implementados en una organización, entre estos se puede mencionar:

- Plan de Backup.
- Políticas de seguridad de la información.
- Política de contraseñas.
- Plan de continuidad del negocio.
- Procedimiento de asignación de usuarios.
- Plan de recuperación de desastres.

[16] UNIVERSIDAD INTERNACIONAL DE VALENCIA, VIU. Conceptos sobre seguridad lógica informática. 2018. [En línea] Disponible en https://www.universidadviu.com/conceptos-seguridad-logica-informatica/

4.2 MARCO CONCEPTUAL

Para el desarrollo de este documento es fundamental apropiar un conjunto de conceptos básicos que permitirán comprender la información contenida en la investigación.

4.2.1 Seguridad De La Información. Se refiere al conjunto de métodos, procedimientos o técnicas implementadas con el fin de generar un nivel de seguridad para la información que se encuentra tanto en formato físico como en digital. La información se considera segura cuando su gestión se basa principalmente en 4 pilares fundamentales que son el de la confidencialidad que nos garantiza que la información sólo podrá ser consultada o accedida por las personas autorizadas, el segundo pilar es el de la integridad a través del cual se debe asegurar que la información almacenada o recibida en un intercambio de flujo de datos se trata de la original que fue enviada por el receptor autorizado. El tercer pilar es el de la disponibilidad con el que se busca garantizar que la información será accesible en cualquier momento y que se utilizan mecanismos que permiten garantizar que en caso de eventualidades que puedan afectar los sistemas informáticos, se cuenta con planes de contingencia que permita garantizar este acceso rápidamente. En la actualidad se menciona el "No repudio" como pilar de la seguridad donde se busca que se cuente con mecanismos que permitan demostrar o garantizar que el intercambio de la información los participantes fueron exactamente los autorizados y no se generó interceptación de un actor no autorizado.

4.2.1 Seguridad informática. Se refiere a los procedimientos implementados para fortalecer la seguridad de los recursos tanto físicos como lógicos de un sistema informático con el fin de evitar que se vea comprometido el principio de autentificación garantizando que quienes acceden a la información son realmente los autorizados para ello.[17] Entre estos se encuentran los servidores, equipos de cómputo, software, bases de datos y los entornos físicos donde se encuentran ubicados dichos elementos.

La seguridad informática tiene como objetivo garantizar los mencionados pilares para la seguridad de la información mediante la aplicación de un conjunto de

[17] CANDELARIO SAMPER, Juan José y RODRÍGUEZ BOLAÑO, Moisés. Seguridad informática en el Siglo xxi: Una perspectiva Jurídica Tecnológica Enfocada Hacia las Organizaciones Nacionales y Mundiales. Revista Especializada en Ingeniería, Universidad Nacional Abierta y a Distancia. 2012 [En línea] Disponible en http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1441/1760

controles que pueden ser físicos como los controles de acceso, cuartos de servidores. También se pueden generar controles a nivel lógico con la utilización de software y controles de acceso como claves de usuarios, biometría, etc.

Si bien es claro que la información se puede presentar en una gran variedad de formatos, destacan los físicos y en especial en la actualidad, el formato digital. Todo tipo de operaciones se realizan utilizando ordenadores y por lo general dichos ordenadores pertenecen a algún tipo de red. Estas redes pueden ser redes locales o redes LAN, estas a su vez pertenecer a una red con una extensión un poco más amplia que son denominadas redes de área metropolitana las cuales interconectan puntos alejados dentro de una misma área geográfica como ciudad o país y a su vez estas redes metropolitanas pertenecer a una red más amplia y gran cobertura a nivel global como son las redes de área extensa o redes WAN.

4.2.3 Redes WAN. Las redes de WAN o también llamadas redes de área extensa son aquellas que permiten la conexión de dispositivos ubicados a gran distancia a nivel geográfico, como países o incluso continentes. Algunas características de este tipo de red son la autonomía, confiabilidad, transparencia y capacidad de crecimiento.[18] un ejemplo de este tipo de red es la internet para el cual solo requiere de contar con un proveedor de conexión o ISP y el dispositivo con el cual conectarse y acceder a los datos de esta red a nivel mundial. [19]

Diariamente todos interactuamos al interior de una red WAN, desde nuestros teléfonos o tabletas móviles, ordenadores, relojes, lentes e incluso dispositivos del hogar con la incursión del IoT o “internet de las cosas” donde dichos dispositivos están continuamente conectados a internet.

4.2.4 Redes Man. Las redes de área metropolitana por sus siglas en inglés (Metropolitan área Networks) son aquellas utilizadas para brindar cobertura en un área geográfica especifica extensa, como ejemplo entre ciudades o al interior de un país, interconectados varias redes de tipo MAN se pueden conseguir grandes coberturas. Estas redes se caracterizan por tener bajas latencias y conseguir velocidades de transmisión del rango de 1 a 10 Gbps con fibra óptica.

Las redes de área metropolitanas son caracterizadas por tener una alta disponibilidad, fiabilidad y seguridad ya que cuentas con diferentes mecanismos que les permiten recuperar rápidamente su operación posterior a una falla, la

[18] BRICEÑO MARQUEZ, José E. Transmisión de Datos. 3a ed. 2005. Venezuela.: Departamento de Electrónica y Comunicaciones de la Escuela de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Los Andes. 564 p. [En línea]. Disponible en http://bdigital.ula.ve/storage/pdf/32381.pdf

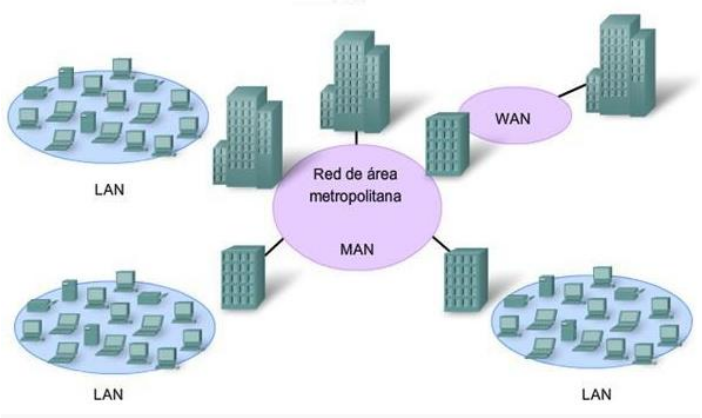
[19] RAFFINO, María Estela. Red WAN. Argentina. 2018. [En línea] Disponible en https://concepto.de/red-wan/

tasa de error en los paquetes transmitidos es baja y para acceder a los datos transmitidos sería necesario realizar la interrupción de forma física del enlace.

4.2.5 Redes LAN. Las redes de área local o redes LAN son todas aquellas redes que se encuentran en un único sitio cerrado, como una casa o un edificio de oficinas. Estas redes son muy comunes en las organizaciones y son las denominadas redes empresariales donde estas interconectan todos los equipos de la organización, pueden ser redes cableadas o redes wifi y permiten a unos equipos realizar intercambios de paquetes de datos con otros al interior de la organización sin que estos necesariamente tengas que salir a otros tipos de redes como la internet. Gracias a las redes LAN también se puede generar un sistema de impresión y digitalización centralizado en las organizaciones. Por todo lo anterior, las redes son un factor fundamental para tener en cuenta en el momento de aplicar controles que garanticen la seguridad de la información.[20]

La siguiente ilustración presenta un ejemplo de los tres tipos de redes mencionados anteriormente, LAN, MAN y WAN:

Ilustración 2. Redes LAN, MAN y WAN



Fuente: Ejemplo de Redes LAN, MAN, WAN. Disponible en: https://alexfcds.wordpress.com/mantenimiento-4/ejemplo-de-redes-lan-man-wam/

4.2.6 Prueba De Penetración. Se denomina prueba de penetración o pentesting a todas aquellas actividades o procesos ejecutado sobre un sistema informático con el fin de comprobar sus niveles de seguridad y detectar posibles falencias que hagan el sistema vulnerable. Estas se realizan mediante ambientes

[20] TANENBAUM, Andrew S., y WETHERALL, David J. Redes de computadoras. 5a ed. 2012. México.: Pearson Educación de México, S.A de C.V. 819 p. ISBN 978-607-32-0817-8

controlados simulando la actuación de un posible atacante para con ello analizar la forma en que reacciona el sistema y la efectividad de los controles.[21]

El uso de pruebas de penetración trae consigo los siguientes beneficios:

- Detectar las fortalezas
- Detectar las debilidades

Como consecuencia de estos, se obtiene un panorama claro que permite establecer medidas y priorizar de acuerdo con el impacto que pueden generar su explotación por parte de un delincuente.

Las pruebas de penetración como ya se mencionó, se realizan en ambientes controlados y con ello requiere que su ejecución no afecte la operación normal de los sistemas y pueda interrumpir la continuidad del negocio.

La ejecución de los pentesting de forma frecuente se considera una práctica adecuada ya que permite generar los informes al respecto de forma oportuna y así mismo tomar las medidas necesaria pudiendo determinar los aspectos que han mejorado y los que por el contrario han reducido su eficiencia comparado con las pruebas ejecutadas con anterioridad.[22]

4.2.7 OWASP Top 10 De 2017. El proyecto OWASP[23] dirigido a las mejores prácticas de seguridad en aplicaciones web publica un top de riesgos a los que se exponen las aplicaciones y que mayor impacto han generado. En su último top publicado en el año 2017, se publicaron 4 nuevos riesgos y se excluyeron 4 que se encontraban en el top del año 2013 y destaca la inyección como un riesgo que sigue siendo el número 1. El top 10 de OWASP 2017[24] es:

Tabla 3. Top 10 OWASP - 2017

Top	Riesgo	Descripción
1	Inyección	Hace referencia a los ataques como el SQL Inyección o NoSQL. Las aplicaciones con errores en el tratamiento de las cadenas de texto ingresadas en sus formularios pueden generar que un atacante logre inyectar código

[21] PINZÓN, Liliana Carolina, TALERO, MihdíBadí y BOHADA JAIME, John Alexander. Pruebas de intrusión y metodologías abiertas. Ciencia, innovación y tecnología, 1, 25-38. 2013. [En línea] Disponible en https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/120
[22] CASTRO VASQUEZ, Carlos Arturo. Pruebas de penetración e intrusión. 2019. Universidad Piloto de Colombia. [En línea] Disponible en http://35.227.45.16/handle/20.500.12277/6273
[23] OWASP. Who is the OWASP Foundation? [En línea] Disponible en https://owasp.org/
[24] OWASP. 2017 Top 10. [En línea] Disponible en https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_Top_10

		para extraer información o generar un daño al activo.
2	Perdida de Autenticación	Este riesgo se relaciona con la gestión inadecuada de la seguridad en las autenticaciones de los usuarios generando brechas que son aprovechadas para que un atacante suplante la identidad y pueda tomar el control total de los recursos bien sea de forma temporal o permanente.
3	Exposición de datos sensibles	La falta de controles adecuados en la protección de datos genera con frecuencia su exposición y acceso por personas no autorizadas. En este tipo de exposición se puede citar ejemplos como el acceso a un estado financiero mediante la navegación de directorios, una asignación incorrecta de permisos de acceso puede permitir que un atacante acceda a este tipo de datos.
4	Entidades externas XML	Este tipo de entidades externas unidas a un procesador XML mal configurado puede llevar a exponer archivos internos. Esto puede permitir generar ataques de denegación de servicio o realizar un escaneo de la red interna e identificar puertos y servicios activos.
5	Pérdida de control de acceso	Una gestión incorrecta de los permisos de acceso puede generar brechas aprovechadas por atacantes para acceder y modificar archivos obteniendo el control y permitiéndoles retirar los permisos de acceso a los usuarios y/o administradores legítimos.
6	Configuración de seguridad incorrecta	Este riesgo es muy frecuente y se puede presentar por la omisión en realizar una configuración de seguridad dejando los valores predeterminados o que la configuración realizada no cumpla completamente dejando brechas aprovechables.

7	Cross-Site Scripting o XSS	Este riesgo se presenta en las aplicaciones que no realizan de forma adecuada la validación de los comandos ingresados por el usuario y este puede llevar a la modificación no autorizada de la aplicación web en el lado del cliente o permitir que se realicen redirecciones a sitios maliciosos sin ningún control afectando a los usuarios legítimos.
8	Deserialización insegura	Este riesgo se refiere a la falta de controles en la recepción de archivos serializados provenientes de una fuente no confiable. Esto puede llevar a recibir código malicioso serializado que puede afectar la seguridad.
9	Uso de componentes con vulnerabilidades conocidas	La mayoría de las aplicaciones requieren de diferentes componentes para lograr sus funcionalidades completas, el uso de estos componentes sin los parches adecuados o que cuenten con vulnerabilidades sin corregir genera un riesgo a la seguridad de la aplicación.
10	Registro y monitoreo insuficiente	Un importante número de riesgos pueden ser descubiertos y mitigados de forma temprana gracias a un constante monitoreo y registro de los diferentes eventos que se presentan. Este riesgo se asocia a aquellas aplicaciones que no cuentan con este monitoreo y registro.

Fuente: El autor

4.3 ANTECEDENTES

El desarrollo de la investigación toma como referentes 5 investigaciones realizadas con anterioridad y de las cuales se detallan sus principales objetivos en la tabla 1.

Tabla 4. Antecedentes de Investigaciones

Título	Autores	Año	País

El Riesgo Y La Falta De Políticas De Seguridad Informática Una Amenaza En Las Empresas Certificadas BASC.	Diego Felipe Gonzalez Agudelo	2014	Colombia

RESUMEN

Este documento visualiza la gran importancia que tiene la correcta implementación de medidas de seguridad para la protección de la información y de los datos, se aborda la utilidad de los procedimientos, políticas de seguridad informática y demás actividades que, de ser mal aplicados, generan graves consecuencias para cualquier entidad.[25]

Título	Autores	Año	País
Diseño De Manual De Diagnóstico Y prevención De Vulnerabilidades En Redes De Datos Para Pymes	Julian Hernan Barreto Cuitiva	2018	Colombia

RESUMEN

Esta investigación fue entregada a la Universidad Nacional Abierta y a Distancia y el objetivo realizado entregó como resultado un manual de detección de vulnerabilidades aplicable a pequeñas y medianas empresas. En el desarrollo del documento, se realizó entrevistas a diferentes empresas donde se concluyó que si bien, entienden el riesgo que implica la falta de controles, también expresan su poco interés en la implementación de estos y en cualquier inversión relacionada.[26]

Título	Autores	Año	País

[25] GONZALEZ AGUDELO, Daniel Felipe. El Riesgo Y La Falta De Políticas De Seguridad Informática Una Amenaza En Las Empresas Certificadas Basc. Ensayo para Administrador en Seguridad y Salud Ocupacional. Bogotá D.C.: Universidad Militar Nueva Granada. Facultad de Relaciones Internacionales, Estrategia y Seguridad. 2014. 24 p. [En línea] Disponible en https://repository.unimilitar.edu.co/bitstream/handle/10654/12251/ENSAYO%20FINAL.pdf?sequence=1

[26] BARRETO CUITIVA, Julian Hernán. Diseño De Manual De Diagnostico Y Prevención De Vulnerabilidades En Redes De Datos Para Pymes. Proyecto de Grado Especialista en Seguridad Informática. Bogotá D.C.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2018. 45 p. [En línea] Disponible en https://repository.unad.edu.co/bitstream/handle/10596/15026/80225921.pdf?sequence=1&isAllowed=y

Análisis E Identificación Del Estado Actual De La Seguridad Informática, Dirigido A Las Organizaciones En Colombia, Que Brinde Un Diagnóstico General Sobre La Importancia Y Medidas Necesarias Para Proteger El Activo De La Información	Yiny Dayan Peñuela Vasquez	2018	Colombia

RESUMEN

Este documento fue entregado a la Universidad Nacional Abierta y a Distancia y se trata de una investigación dedicada al análisis de la situación actual de la seguridad en las organizaciones donde se recolectó información sobre la problemática en informes entregados por parte de las grandes industrias del software de seguridad, donde se evidencia que los ataques cibernéticos cada vez aumentan y se realizan con mayor técnica y organización lo que hace que se genere un mayor sentido de urgencia en la concientización de toda la ciudadanía y que la seguridad no sea vista como un gasto sino más bien como lo que realmente es, una inversión.[27]

Título	Autores	Año	País
Riesgos de Ciberseguridad en las Empresas	Enrique Javier Santiago, Jesús Sanchez Allende	2017	España

RESUMEN

Esta investigación aborda los conceptos de riesgos, amenazas y todo aquello que implica un problema de ciberseguridad para empresas de diferentes sectores. El documento se presenta estructurado por secciones empezando con una presentación o introducción a los diferentes riesgos que se presentan a las empresas. La sección 2 se enfoca en generar conciencia hacia la ciberseguridad a través de la justificación de la importancia que tiene la

[27] PEÑUELA VASQUEZ, YINY DAYAN. Análisis E Identificación Del Estado Actual De La Seguridad Informática, Dirigido A Las Organizaciones En Colombia, Que Brinde Un Diagnóstico General Sobre La Importancia Y Medidas Necesarias Para Proteger El Activo De La Información. Proyecto de Grado Especialista en Seguridad Informática. Fusagasuga.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2018. 60 p. [En línea] Disponible en https://repository.unad.edu.co/bitstream/handle/10596/17260/35254395.pdf?sequence=1&isAllowed=y

información como activo. En la sección 3 se presentan los riesgos resultantes de la dependencia que cada día se genera hacía la tecnología. La sección 4 estudia los diferentes riesgos expuestos y la probabilidad de que estos se materialicen afectando así los procesos. En la sección 4 se describen los principales ciberataques del que se puede ser blanco y que afectan la triada de la seguridad de la información.[28]

Título	Autores	Año	País
Estado Actual Del Cibercrimen En Colombia Con Respecto A Latinoamérica	Luis Fernanda Acuña Lopez, Sandra Milena Villa Motato	2018	Colombia

RESUMEN

Esta investigación presentada a la Universidad Nacional abierta y a distancia presenta una comparativa del estado del cibercrimen en Colombia con respecto a diferentes países de Latinoamérica, estudiando la legislación colombiana vs la legislación de dichos países. También el documento aborda como se encuentran catalogados los cibercrímenes que mayor afectación ha causado a las empresas.[29]

Fuente: El autor

4.4 MARCO TECNOLOGICO

Se desarrollaron varias pruebas para el desarrollo del objetivo 3.

Para el desarrollo de las pruebas se utilizó un computador portátil con sistema operativo Windows 10 en el que se configuran 2 máquinas virtuales utilizando VirtualBox. Las herramientas utilizadas se describen en la siguiente tabla:

[28] SANTIAGO, Enrique Javier y SÁNCHEZ ALLENDE, Jesús. Riesgos de ciberseguridad en las empresas. España. 2017. [En línea] Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=6670303

[29] ACUÑA LOPEZ, Luisa Fernanda y VILLA MOTATO, Sandra Milena. Estado Actual Del Cibercrimen En Colombia Con Respecto A Latinoamérica. Proyecto de Grado Especialista en Seguridad Informática. Pereira, Colombia.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2018. 104 p. [En línea] Disponible en https://repository.unad.edu.co/bitstream/handle/10596/25619/%20%09lfacunal.pdf?sequence=1

Tabla 5. Detalle Herramientas Utilizadas

Nombre de Recurso	Descripción
Virtual Box	Software de virtualización desarrollado por Oracle. Se utilizará para crear las máquinas virtuales de Kali Linux y Ubuntu para las pruebas.
Kali Linux	Sistema operativo desarrollado por la organización Offensive Security y especializado en seguridad informática. Uso Libre.
Ubuntu	Sistema operativo basado en Debian, libre y de código abierto.
Retire.js	Complemento disponible en varios navegadores que permite escanear sitios web y detectar el uso de componentes con vulnerabilidades conocidas. Uso Libre.
OWASP Dirbuster	Aplicación desarrollada para listar los nombres de los directorios y archivos de un sitio web a través de fuerza bruta.[30] Uso Libre.
WPHunter	Escáner de vulnerabilidades de aplicaciones desarrolladas sobre WordPress. Permite determinar si un sitio web tiene vulnerabilidades de acuerdo con su versión, complementos y temas instalados. Uso Libre.
WireShark	Analizador de protocolos de red, permite detectar todo el

[30] MUNDO HACKER. OWASP – DIRBUSTER. [En línea]. Disponible en https://mundo-hackers.weebly.com/dirbuster.html

	comportamiento y tráfico de una red de datos. Es de uso libre.
nMap	Esta herramienta permite realizar escaneo de redes detectando equipos, puertos y servicios activos.
OpenVas	Escáner de vulnerabilidades con licenciamiento GNU que permite realizar múltiples pruebas, sus principales características son: • Pruebas no autenticadas • Pruebas autenticadas • Diversos protocolos industriales • Mejoramiento del funcionamiento para procesos a gran escala.

Fuente: El autor

4.5 MARCO LEGAL

El desarrollo de esta monografía contiene menciones de delitos informáticos en Colombia y que se encuentran tipificados en la Ley 1273 de 2009:

Ley 1273 de 2009, a través de la cual se adiciona al código penal un nuevo bien jurídico denominado “De la protección de la información y de los datos”. Delitos informáticos. [31] Esta ley está compuesta por dos capítulos y diez artículos que se describen en la siguiente tabla:

Tabla 6. Ley 1273 de 2009

Capitulo	Articulo	Descripción
1. De los atentados contra la confidencialidad,	269A. Acceso Abusivo a un Sistema Informático	Acceder total o parcialmente a un sistema informático sin autorización, aunque este

[31] CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. [En línea]. Disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

la integridad y la disponibilidad de los datos y de los sistemas informáticos[32]		cuente o no con medidas de seguridad.
	269B: Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación	Este delito aplica a toda persona que genere un obstáculo para el acceso normal a un sistema información.
	269C: Interceptación de Datos Informáticos	Aplica a cualquier interceptación de datos informático incluyendo interceptaciones a emisiones electromagnéticas.
	269D: Daño Informático	Aplica a la persona que destruya sin autorización datos informáticos.
	269E: Uso de Software Malicioso	Aplica a cualquier actividad relacionada con el uso de software malicioso, esto incluye actividades como el desarrollo o distribución.
	269F: Violación de Datos Personales	Cualquier actividad que implique la obtención sin autorización de datos personales con beneficio sea propia o de un tercero.
	269G: Suplantación de Sitios WEB para Capturar Datos	Aplica a cualquier actividad con la suplantación y engaño de personas con el fin de obtener información.
	269H: Circunstancias de Agravación Punitiva	Menciona algunas causales de agravación de las penas, dependiendo la actividad final

[32] Ibid.

		realizada o la propiedad del bien afectado.
2. De los Atentados informáticos y otras infracciones[33]	269I: Hurto por Medios Informáticos y Semejantes	Toda actividad en la que se supere cualquier medida de seguridad bien sea manipulando un sistema de seguridad o suplantando a una persona.
	269J: Transferencia No Consentida de Activos	Realizar la manipulación y/o transferencia no autorizada de un activo y que esto sea en perjuicio de un tercero.

Fuente: El autor.

5 METODOLOGIA

Para el desarrollo de la presente monografía se utilizó una metodología basada en el ciclo PHVA (Planea, Hacer, Verificar, Actuar) de Deming, la cuál es planteada como una herramienta para generar un mejoramiento continuo a través de una serie de actividades que van desde el estudio y reconocimiento de una situación actual reuniendo datos que permitan generar un plan de mejora, su ejecución, la verificación de las medidas ejecutas y finalmente la corrección o mejora de todos aquellos aspectos que generaron alguna no conformidad.[34]

En la siguiente ilustración se puede detallas el proceso del Ciclo PHVA[35].

[33] Ibid. P. 2

[34] COLORADO, Francisco. El Ciclo PHVA de Deming y el Proceso Administrativo de Fayol. 2009. [En línea]. Disponible en https://www.academia.edu/5110051/3_Articulo_El_Ciclo_PHVA_de_Deming_y_al_Proceso_Administrativo_de_Fayol

[35] SAFETYA. PHVA: Procedimiento lógico y por etapas para la mejora continua. 2016. [En línea] Disponible en https://safetya.co/phva-procedimiento-logico-y-por-etapas/

Ilustración 3. Ciclo PHVA.

Fuente: SAFETYA. PHVA: Procedimiento lógico y por etapas para la mejora continua. 2016. [En línea] Disponible en https://safetya.co/phva-procedimiento-logico-y-por-etapas/

En el desarrollo de la investigación se desarrollan los capítulos basados en las fases del ciclo PHVA.

Tabla 7. Fases PHVA

Fase	Descripción
PLANEAR	En el desarrollo del objetivo principal del presente documento, se inicia con el análisis de las diferentes variantes que nos presenta la ciberseguridad a nivel global y específicamente en Colombia, esta información hace parte de la planeación del desarrollo del objetivo general ya que para establecer procedimientos que permitan mejorar la seguridad requiere que se conozca los principales factores de riesgo.
HACER	En esta etapa del desarrollo del trabajo se empiezan a analizar alternativas que existen con el fin de contribuir o mitigar los riesgos que se expusieron en la etapa de planeación.

VERIFICAR	En esta etapa del desarrollo de los objetivos, se implementan metodologías presentadas en el capítulo anterior con el fin de generar un conjunto de pruebas y visualizar su utilidad en el mejoramiento del estado de la seguridad.
ACTUAR	En esta etapa se efectúa el desarrollo de las recomendaciones que deben ser aplicadas y con las que se complementa el desarrollo del objetivo principal de la monografía que es presentar un conjunto de lineamientos que permita a las organizaciones empresariales realizar un análisis de su nivel de riesgo o vulnerabilidades de sus sistemas informáticos.

Fuente: El autor

6 DESARROLLO DE LA METODOLOGÍA

6.1 PLANEAR - ANALIZAR EL PANORAMA ACTUAL DE LA SEGURIDAD INFORMÁTICA DE LAS ORGANIZACIONES EMPRESARIALES EN COLOMBIA

Como primer objetivo, se realiza un análisis de las vulnerabilidades que se encuentran con mayor frecuencia en las empresas. realizando una introducción con los ataques que más han afectado este sector y posteriormente indicando los procedimientos que nos permiten detectar vulnerabilidades en una empresa.

El sector empresarial en Colombia con frecuencia reporta pérdidas económicas por cuenta de ciberataques que afectan de diferentes maneras su proceso productivo y que ponen en evidencia la falta de compromiso por parte de las organizaciones en el desarrollo de estrategias claras y efectivas que permitan mitigar este problema.

Según un estudio presentado por la policía en los primeros meses del año 2019, las organizaciones en Colombia han sufrido más de 28000 ciberataques generado pérdidas que se encuentran en el rango de $500 Millones de pesos y hasta $5.000 Millones de pesos cada uno.[36] Estudios realizados destacan que el principal interés de los atacantes es el de obtener beneficios económicos.

Los ataques más comunes que se efectúan contra las empresas en Colombia permiten identificar cuáles son los mayores focos de exposición en este aspecto. Para el año 2019 el Ransomware, sigue siendo el ataque que más han sufrido las empresas, seguido del phishing o suplantación de identidad y la difusión de malware.[37]

Colombia no es el único país que sufre las consecuencias del crecimiento del cibercrimen, también a nivel internacional muchas empresas de diferentes países son víctimas a diario de ciber ataques que van evolucionando con el tiempo y también aumentando en número. La empresa de seguridad Sophos en su informe para el año 2019, publicó algunas cifras donde se evidencia los ataques mediante Ransomware como los principales implicados también a nivel mundial, destacando que los atacantes han migrado sus técnicas a los ataques

[36] RED+. En 2019 se han registrado más de 28 mil ciberataques a las empresas. 2019. [En línea] Disponible en http://www.redmas.com.co/tecnologia/mas-de-28-mil-ciberataques-al-sector-empresarial-se-han-registrado-en-lo-corrido-de-2019/

[37] EL TIEMPO. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. 2019. [En línea] Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

manuales ya que los automatizados han sido predecibles y fácilmente fracasan en sus intentos. [38]

6.1.1 Ransomware. El Ransomware es un tipo de malware que al infectar las computadoras, toma el control de la información aplicando un cifrado por contraseña y desplegando mensajes a los usuarios exigiendo sumas económicas a cambio de liberar dicha información.[39] En el año 2017 se generó la mayor cantidad de ataques de este tipo y apareció una de las variaciones del mismo denominado WannaCry, el cual ataca a las computadoras con sistemas operativos Windows a través de las redes usando SMBv1, protocolo que utilizan los equipos para realizar comunicación con impresoras, dejando a su paso gran cantidad de afectaciones a sistemas. Si bien, Microsoft liberó los parches necesarios para corregir esta vulnerabilidad, muchos dispositivos con sistemas operativos sin soporte se vieron expuestos al ataque, dejando una cifra estimada en 230.000 dispositivos infectados alrededor del mundo, principalmente de entidades gubernamentales y hospitales, según informó la empresa de seguridad AVAST.[40]

El Ransomware en la actualidad es controlado por un gran número de software de seguridad, sin embargo, aún es la amenaza a la cual le temen las organizaciones y el ataque más ejecutado. Una vez se infecta un sistema, las ventanas desplegadas pueden ser como las de la siguiente ilustración:

Ilustración 4. Ransomware - Solicitud de rescate

Fuente: AVAST. WannaCry. 2019. [En línea] Disponible en https://www.avast.com/es-es/c-wannacry

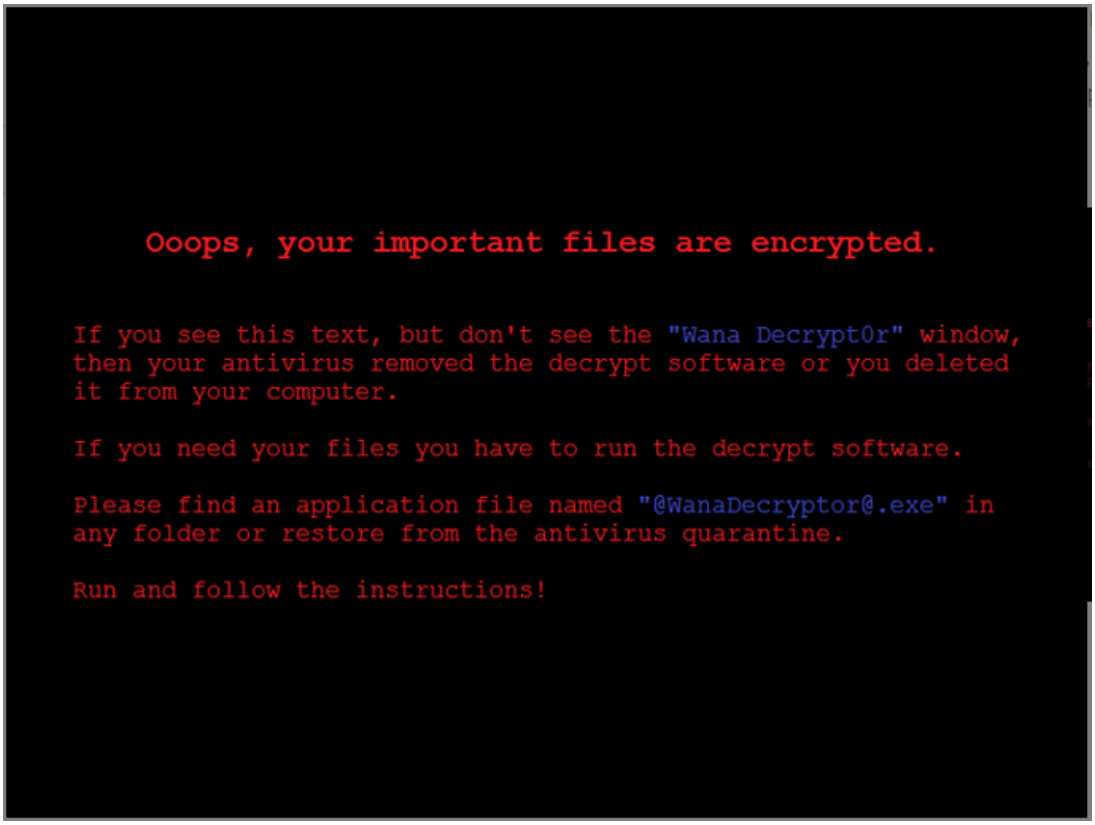
[38] SOPHOS. Informe de amenazas 2019 de SOPHOSLABS. 2020 [En línea] Disponible en https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

[39] KASPERSKY. ¿Qué es el Ransomware? 2019. [En línea] Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

[40] AVAST. WannaCry. 2019. [En línea] Disponible en https://www.avast.com/es-es/c-wannacry

Es posible eliminar esta amenaza usando software antivirus, sin embargo, esto no elimina el cifrado en la información y es por ello por lo que, en muchos casos, recuperar la información es casi imposible, salvo aquellos Ransomware para los cuales ya ha sido publicada su clave de descifrado.

Ilustración 5. Ransomware eliminado por antivirus



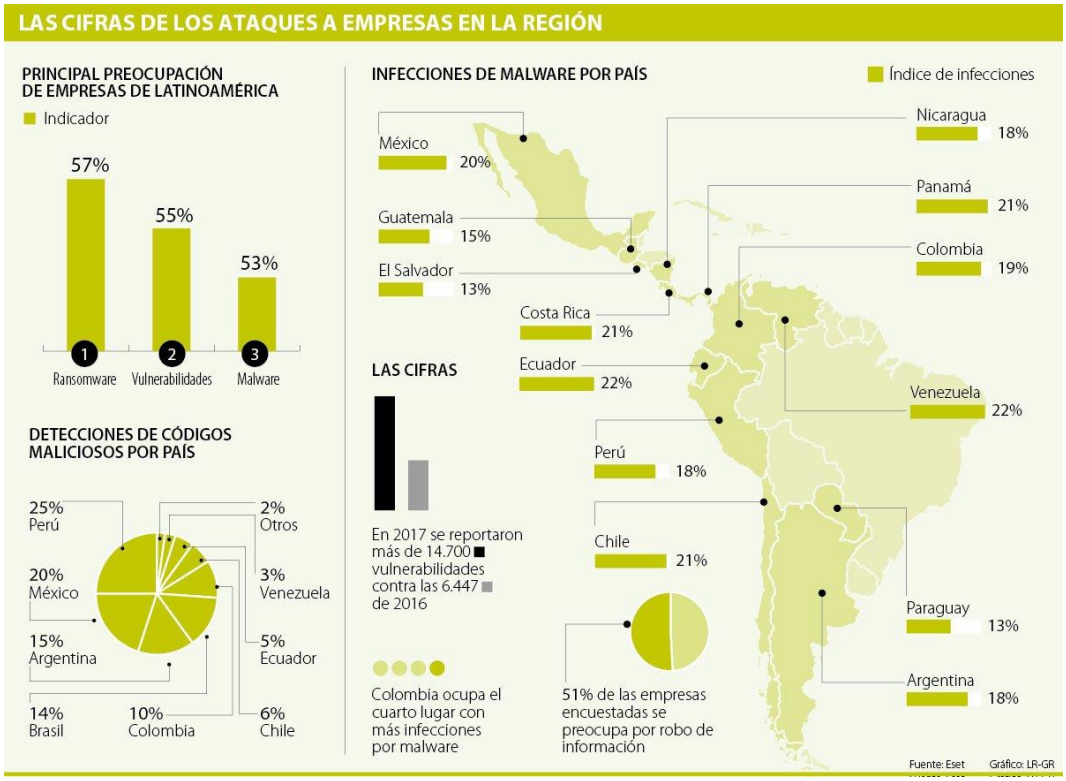
Fuente: AVAST. WannaCry. 2019. [En línea] Disponible en https://www.avast.com/es-es/c-wannacry

La empresa de seguridad ESET presentó un informe con cifras producto de una encuesta a más de 4.500 ejecutivos de Latinoamérica, donde se evidencia el Ransomware como la mayor preocupación para las organizaciones. Sin embargo, en la gráfica se puede evidenciar las diferentes infecciones comunes por país y nos permite identificar el porcentaje de compromiso de cada uno de estos.

Las infecciones por Malware en Colombia corresponden a un 19% de todos los países de Latinoamérica, adicional, la cantidad de vulnerabilidades detectadas fue el doble que las del año inmediatamente anterior confirmando su incremento con el paso de tiempo y también la ausencia del crecimiento continuo de controles.

Los códigos maliciosos en Colombia significo el 10% del total de todos los países. [41]

Ilustración 6. Cifras de ataques en Latinoamérica



Fuente: VENEGAS LOAIZA, Andrés. Colombia, entre los países de la región en donde las compañías más sufren malware. 2018. [En línea] Disponible en https://www.larepublica.co/internet-economy/colombia-esta-entre-los-paises-en-donde-las-companias-mas-sufren-de-malware-2746737

En la ilustración 6 se presentan las cifras de los ataques que han sufrido las empresas en los países latinoamericanos, donde Colombia ocupa la cuarta posición en la escala de los países con mayor cantidad de infecciones por Malware con una cifra del 19% superado en el tercer lugar por México con el 20%, Panamá, Costa Rica y Chile comparten el segundo lugar con 21%, Venezuela y Ecuador en el primer lugar con 22%.[42]

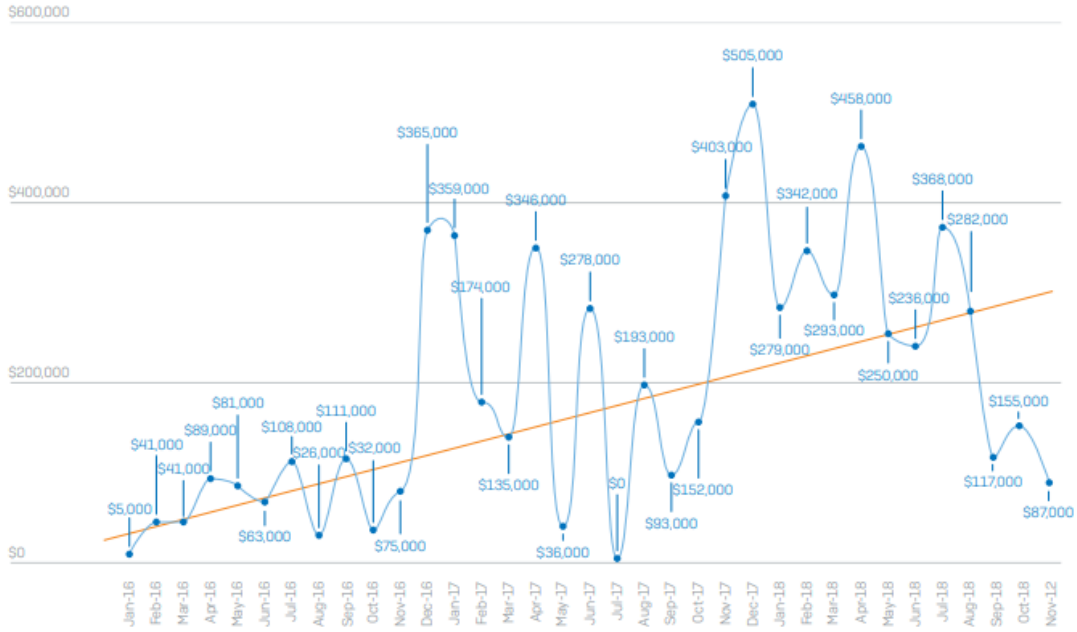
El Ransomware WannaCry no ha sido el único en generar incertidumbre en las organizaciones, también Sophos menciona en su informe el Ransomware llamado SamSam, el cual, según el mencionado informe, desde su descubrimiento hasta hoy, ha generado el pago de más de 6 Millones de dólares

[41] VENEGAS LOAIZA, Andrés. Colombia, entre los países de la región en donde las compañías más sufren malware. 2018. [En línea] Disponible en https://www.larepublica.co/internet-economy/colombia-esta-entre-los-paises-en-donde-las-companias-mas-sufren-de-malware-2746737

[42] Ibid.

en rescates. La siguiente ilustración presenta la gráfica de los rescates pagados por SamSam[43]

Ilustración 7. Pagos de Rescate SamSam



Fuente: SOPHOS., Informe de amenazas 2019 de SOPHOSLABS. p. 7. Disponible en: https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

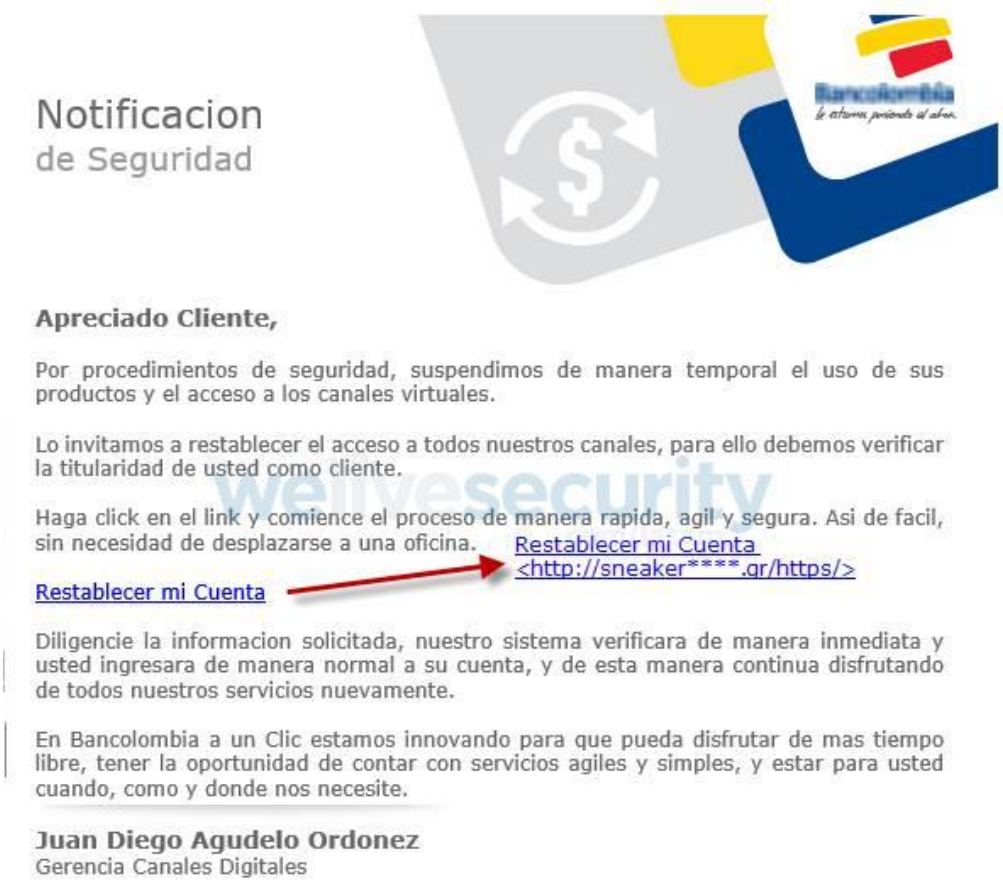
6.1.2 PHISHING. Si bien el Ransomware es la mayor preocupación de los empresarios en Colombia y Latinoamérica en general, el Phishing o también denominado suplantación de identidad, tiene un porcentaje alto de incidencia diaria sobre los procesos de las organizaciones. Este tipo de ataque busca recopilar información personal a través de engaños donde se benefician de personas incautas. Los ataques de suplantación de identidad pueden ser de diferentes tipos entre los que se destaca la suplantación mediante correo electrónico.[44]

Este ataque se aprovecha de la ingeniería social, manipulando a los usuarios. En Colombia las organizaciones reciben de forma frecuente correos electrónicos informando sobre facturas, pagos pendientes, citaciones judiciales, archivos compartidos, aparentemente de una fuente confiable, pero en realidad muchos de estos casos son suplantaciones que buscan engañar al usuario y llevarlo por medio de enlaces a compartir información o instalar Malware en los computadores logrando con esto acceder a la red de la organización.

[43] SOPHOS. Op. ci., Informe de amenazas 2019 de SOPHOSLABS. p. 7.
[44] LUBECK, Luis. Phishing suplanta identidad de reconocido banco de Colombia y busca robar información financiera. 2019. [En línea] Disponible en https://www.welivesecurity.com/la-es/2019/06/05/phishing-activo-reconocido-banco-colombia/

Los casos de Phishing a organizaciones colombianas son muy comunes, quizás uno de los casos más conocidos fue el que sufrieron los usuarios de una entidad bancaria de alto reconocimiento nacional, quienes recibieron un correo con una supuesta notificación del banco donde le indicaban el bloqueo de sus productos y les pedían acceder a un enlace para actualizar sus datos.[45]

Ilustración 8. Email Phishing



Fuente: DINERO. ¡Cuidado! Están suplantando a Bancolombia para estafar a miles de clientes. 2017. [En línea] Disponible en https://www.dinero.com/empresas/articulo/campana-de-phishing-afecta-a-miles-de-clientes-de-bancolombia/242871

Tanto el Malware como el Phishing son ataques que una alta frecuencia sufren las organizaciones, pero estos son efectivos en la medida de que existan las vulnerabilidades necesarias que así lo permitan. En el último año, muchas empresas han empezado a optar por evaluar de forma periódica sus sistemas informáticos con firmas especializadas en seguridad informática, donde se realizan los denominados pentesting o pruebas de penetración en busca de

[45] DINERO. ¡Cuidado! Están suplantando a Bancolombia para estafar a miles de clientes. 2017. [En línea] Disponible en https://www.dinero.com/empresas/articulo/campana-de-phishing-afecta-a-miles-de-clientes-de-bancolombia/242871

vulnerabilidades. Las pruebas de penetración pueden ser de tres tipos, de caja blanca, de caja gris o de caja negra.

6.1.3 Relación Entre Competencias De Los Profesionales Y El Estado De La Seguridad En La Actualidad. El ya mencionado aumento exponencial de los ataques cibernéticos alrededor del mundo ha generado también una creciente demanda de profesionales del campo, a nivel mundial. Al respecto, Cybersecurity Ventures publicó en noviembre de 2019 un informe en el que se evidencia que entre el año 2013 para el año 2021 la oferta laboral relacionada con la ciberseguridad tendrá un incremento de un 350%. Se debe mencionar la preocupación que se tiene debido a la gran brecha que se tiene en las habilidades de estos profesionales, llevando a muchos CISOS al temor de no contar con este recurso que llevaría a empeorar la situación actual. Según el MIT Technology Review, incluso menos de uno de cada cuatro que se presentan a las vacantes disponibles, cuentan con las habilidades requeridas.[46]

En el foro económico Mundial (WEF) se publicó un artículo en el que se menciona que en ningún campo la brecha de habilidades es tan amplia como en el de la ciberseguridad, señalando para la fecha de publicación y de acuerdo con una publicación de Forbes, un total de 1,4 millones de vacantes no cubiertas.[47]

Teniendo en cuenta las cifras mencionadas anteriormente y las brechas existentes, Juan Manual Harán en una publicación para el portal de seguridad de ESET, WeLiveSecurity, entrevistó a algunos especialistas en seguridad acerca de la formación recibida y la oferta existente en instituciones de educación, en las que si bien ha ido en aumento el número de acuerdo con la demanda, aún no es una carrera que sea común en las diferentes instituciones educativas y muchos de las grandes personalidades de la rama, han adquirido sus conocimientos de forma autodidacta o a través de cursos informales.[48]

Estas cifras a nivel mundial reflejan una realidad que para Colombia no es indiferente, la oferta académica en seguridad informática no es común, aún existen muchas universidades o instituciones de educación que no tienen esta rama en sus ofertas habituales.

6.1.4 Factores Que Exponen La Seguridad Informática De Las Empresas. Existen muchos factores que contribuyen directa o indirectamente la seguridad informática en las empresas, sin embargo, uno de los que mayor impacto y

[46] MORGAN, Steve. Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. 2019 [En línea] Disponible en https://cybersecurityventures.com/jobs/

[47] WORLD ECONOMIC FORUM. This is what the future of cybersecurity will look like. 2017. [En línea] Disponible en https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-against-cyber-attacks-but-the-security-industry-faces-a-huge-challenge

[48] HARÁN, Juan Manuel. Profesionales en seguridad informática: entre la formación académica y la autodidacta. 2019. [En línea] Disponible en https://www.welivesecurity.com/la-es/2019/11/11/profesionales-en-seguridad-informatica-entre-la-formacion-academica-y-la-autodidacta/

frecuencia tienen es el factor humano. Muchos empleados en las empresas no cuentan con hábitos de trabajo que contribuyan positivamente a la ciberseguridad. En un artículo publicado en foro económico mundial por S. Nadal.[49], menciona la importancia de los empleados en el fortalecimiento de la ciberseguridad y como las empresas suelen olvidar este aspecto.

La mayoría de los ciberataques a nivel mundial tienen una implicación directa del factor humano como se vio con el Ransomware WannaCry, mencionado al inicio del capítulo, estos errores hacen que la tarea para el ciberdelincuente se vea facilitada, un ejemplo es el constante uso de contraseñas débiles, como el 123456 que ha sido la contraseña más usada a nivel mundial[50] , seguida de "password", "12345678" y "qwerty". Sin embargo, aunque no tan frecuente, siguen apareciendo contraseñas con el "1234".

Los malos hábitos más frecuentes entre los empleados son:

6.1.4.1 Claves Inseguras. Una gran cantidad de personas opta por asignar claves débiles, obvias y por ende inseguras en sus diferentes plataformas con el miedo de extraviarlas, llevando a un segundo plano la seguridad de la información.

6.1.4.2 Conexiones a Redes Públicas. Es muy frecuente que los empleados en especial aquellos que realizan labores fuera de las empresas, se conecten a redes públicas como los aeropuertos, parques, centros comerciales, donde no se tiene control de quienes se conectan y pueden ser fácil blanco de ciberdelincuentes de diversas maneras. Según una publicación realizada por Bancolombia[51], el "68% de los ataques informáticos se realizan desde conexiones públicas o no seguras".

6.1.4.3 No Aplicar con Frecuencia las Actualizaciones. Es frecuente que los usuarios decidan posponer las actualizaciones argumentando los tiempos que puede tomar su instalación, estas actualizaciones pueden ser de sistema operativo, aplicaciones de la empresa, ofimática o antivirus. No tener la base de datos del antivirus actualizada o el sistema operativo con los parches actualizados son causa frecuente de ataques.

---

[49] S., NADAL, M., Victoria. Los malos hábitos de los empleados son una amenaza para la ciberseguridad. 2018. [En línea]. Disponible en https://es.weforum.org/agenda/2018/01/los-malos-habitos-de-los-empleados-son-una-amenaza-para-la-ciberseguridad?utm_content=buffer99fec&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

[50] ARNAL MARTÍN, Andrea. La contraseña más popular del mundo sigue siendo '123456'. 2016. [En línea]. Disponible en https://elpais.com/tecnologia/2016/01/20/actualidad/1453281839_103381.html

[51] GRUPO BANCOLOMBIA. Ciberseguridad: Malos hábitos vs buenas prácticas de las startups. [En línea]. Disponible en https://www.grupobancolombia.com/wps/portal/innovacion/tecnologias-disruptivas/malos-habitos-vs-buenas-practicas-de-las-startups

6.1.4.4 Visitas a Sitios Web no Confiables. Los empleados en muchas ocasiones visitan páginas no confiables, según la publicación de Grupo Bancolombia[52] cerca del 47% de los malware en las empresas, provienen de descargas de este tipo de sitios y el 57% de los empleados los visitan.

6.1.4.5 Educación o Conciencia en Ciberseguridad. Muchas empresas que no han desarrollado plena conciencia en ciberseguridad no cuentan con un plan de educación o generación de conciencia en sus empleados y esto a su vez impacta y genera como resultado muchos de los malos hábitos que adquieren.[53]

[52] Ibid.
[53] TOUS-MULKAY, Abelardo. ¿Cómo deberían afrontar las pymes los riesgos de ciberseguridad? [En línea] Disponible en https://www.finanzaspersonales.co/columnistas/articulo/principales-riesgos-de-ciberseguridad-en-las-pymes/79732

6.2 HACER - ANALIZAR METODOLOGÍAS DE HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES EN LAS ORGANIZACIONES EMPRESARIALES

El segundo objetivo se enfoca en analizar metodologías de hacking ético que permiten detectar vulnerabilidades en las organizaciones mediante la ejecución de pruebas sobre los sistemas tanto internos como externos permitiendo así evaluar las fortalezas y debilidades presentes en el mismo.

Antes de analizar las diferentes metodologías, es importante destacar la importancia que tiene el hacking ético para las organizaciones empresariales de los diferentes sectores en Colombia. El hacking ético es realizado por los denominados hackers de sombrero blanco o individuos con grandes conocimientos de seguridad informática que focalizan sus conocimientos en realizar actividades de detección de debilidades en seguridad y notificar las mismas para que las personas u organizaciones afectadas puedan tomar medidas antes de que un atacante pueda sacar provecho de ello afectando el proceso productivo.[54]

6.2.1 OSSTM – Open Source Security Testing Methodology. La primera metodología en ser analizada será la OSSTM de sus siglas en inglés “Open Source Security Testing Methodology Manual” o en español “Manual de la Metodología Abierta de Testeo de Seguridad” es un estándar publicado en el año 2010 y considerado como uno de los más completos y con un amplio rango de cobertura y uso en procesos de auditoría de seguridad.[55]

Esta metodología se considera completa dado que abarca todos los aspectos de mayor importancia en el campo de los sistemas de información, tomando como referencia el documento oficial de OSSTM, se presentan las definiciones de las pruebas, así:

Tabla 8. Tipos de Pruebas - OSSTM

Tipo de Prueba	Descripción
Pruebas de seguridad humana	Esta sección permite realizar estudios acera de la relación humana con los sistemas informáticos, identificar sus habilidades y el nivel

[54] ENTER.CO. El hacking ético y su importancia para las empresas. 2014. [En línea] Disponible en https://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

[55] OSSTMM. OSSTM 3 – The Open Source Security Testing Methodology Manual. 2010.

	de conciencia que tienen los usuarios hacia la seguridad y determinar las brechas existentes entre la realidad y el estándar requerido según el área de trabajo.
Pruebas de seguridad física	Esta sección permite obtener una guía de pruebas para determinar el nivel de seguridad de las barreras físicas y comparar con el estándar requerido como se describe en la política de seguridad de la organización. En esta categoría se evalúan factures como los controles de acceso, el perímetro, el monitoreo que se realiza de las ubicaciones físicas, la respuesta de los sistemas de alarmas y el entorno en general.
Pruebas de seguridad inalámbricas	Las pruebas de seguridad inalámbricas tienen como objetivo verificar que todas las comunicaciones realizadas a través de medios inalámbricos como el bluetooth, redes wifi, RFid y demás comunicaciones que se efectúan por este medio, cuenten con las medidas de seguridad necesarias que eviten que estas sean interceptadas de forma irregular por personal no autorizado.
Pruebas de seguridad de telecomunicaciones	Esta sección busca brindar la oportunidad de determinar la seguridad de las comunicaciones por medios alámbricos.

Pruebas de seguridad de redes de datos	Estas pruebas comúnmente denominadas “pruebas de penetración” buscan detectar las brechas de seguridad en todas las redes de datos y los componentes incluidos en ella permitiendo determinar las diferencias entre los objetivos trazados de seguridad y el estado actual del sistema.

Fuente: El autor

Como se puede apreciar en los diferentes enfoques que tiene la metodología, la ejecución de las pruebas documentadas permiten a la organización generar un contexto importante del estado actual de seguridad informática y tomar acciones de mejora de gran impacto para sus procesos.

6.2.2 OWASP – Open Web Application Security. La siguiente metodología es la **OWASP** o “Open Web Application Security Project” que se enfoca en pruebas de seguridad para aplicaciones web, cuenta con un amplio reconocimiento entre los desarrolladores de software, los testers de software y los especialistas en ciberseguridad. OWASP cuenta con diferentes proyectos, algunos de tipo documental entre los que se puede mencionar los siguientes[56]:

- OWASP FAQ
- OWASP Development
- OWASP Testing Guide
- OWASP Code Review
- OWASP TOP 10
- OWASP mobile Security

Adicional a los proyectos documentales, también cuenta con proyectos de Software como el OWASP Live CD y el OWASP WAF.

OWASP cuenta con un grupo de pruebas que deben ser ejecutadas cuando se utiliza dicha metodología, estas se dividen por categorías así:

- Recopilar información
- Gestión de la configuración
- Autenticación
- Autorización

[56] SALAZAR D., Edgar D. Pruebas de Seguridad en aplicaciones web segun OWASP. 2016. [En línea] Disponible en https://www.owasp.org/images/2/2f/OWASP_SUSCERTE.pdf

- Gestión de sesiones
- Validación de datos
- Denegación de servicio
- Servicios Web
- Ajax

Las metodologías de hacking ético se basan principalmente en 5 factores fundamentales:

- Recolección de información

De acuerdo con el tipo de hacking, este se puede realizar de diferentes maneras, en el denominado hacking de caja blanca, la información es suministrada por la organización objeto de estudio, en el hacking de caja gris, la empresa suministra solo de forma parcial la información y finalmente el hacking de caja negra consiste en la obtención de la información desde el exterior, la organización no aporta ninguna información.

Una forma de recolectar información es a través de internet, el plugin Retire.js para el navegador Google Chrome me permite conocer si una aplicación web tiene vulnerabilidades como complementos deshabilitados.

- Descubrimiento

Esta etapa permite a un atacante profundizar en la información recolectada, buscando obtener información de los diferentes activos que se pueden encontrar en una organización y que contengan vulnerabilidades que puedan ser aprovechadas. En esta etapa se puede llegar a obtener:

- Rangos de IP
- Nombres de servidores
- Puertos activos
- Servicios activos sobre los puertos
- Dispositivos presentes en la red

Como se puede apreciar, en esta fase se empieza a generar un banco importante de información sobre la victima obteniendo datos de alta importancia.

- Enumeración de usuarios

La enumeración de usuarios comprende la consecución de los nombres de usuarios en las aplicaciones web de la organización, es una vulnerabilidad muy conocida y de alto impacto, muchas aplicaciones utilizan WordPress y está por defecto hace fácil la enumeración de usuarios. Una vez el atacante consigue los nombres de usuario, por medio de un ataque de diccionario o fuera bruta podría llegar a conseguir el acceso al sistema.

Kali Linux cuenta con un gran número de herramientas para diferentes aplicaciones en seguridad informática entre las que se encuentran varias herramientas de automatización del proceso de enumeración de usuarios.

6.2.3 Offensive Security. Esta metodología fue desarrollada por una organización con el mismo nombre y creadora del sistema operativo por excelencia en pruebas de seguridad como lo es el Kali Linux y se basa en la ejecución constante de pruebas de seguridad como estrategia de mitigación de vulnerabilidades.[57]

Las pruebas efectuadas bajo este marco metodológico tienen un nivel de intrusión bastante elevado dado que se procura recrear el escenario igual al que tendría un delincuente cuando efectúa el ataque, además de este, se deben destacar los enfoques en ejecución de pruebas en entornos reales y el soporte que se sustenta sobre evidencias obtenidas que sean claramente visibles y no contempla la toma de decisiones basándose en estadísticas.[58]

La implementación de esta metodología de pruebas de penetración requiere el cumplimiento de una serie de fases que al igual que las metodologías mencionadas anteriormente, pueden ser ejecutadas como pruebas de penetración de caja negra, caja gris o caja blanca. En la siguiente tabla se describen las diferentes fases:

Tabla 9. Fases de OFFENSIVE SECURITY

Fase	Descripción
Recolección de información	Fase en la que se adquiere la mayor cantidad de información de la víctima, teniendo en cuenta si se decide realizar con información previamente conocida o sin conocimiento alguno sobre el objetivo. La información que se busca son enrutamientos IP internos, ip pública, proveedores de internet, nombres de servidores, la existencia o no de firewall,

[57] OFFENSIVE SECURITY. Why OffSec? [En línea] Disponible en https://www.offensive-security.com/why-offsec/

[58] CUZME RODRÍGUEZ, Fabián, et al. Administration and Management Platform of Electricity Consumption for Home Appliances Based on IoT. 2020. Ecuador.: Ingeniería en Telecomunicaciones, Universidad Técnica del Norte. [En línea] Disponible en https://www.researchgate.net/publication/328367829_Offensive_Security_Ethical_Hacking_Methodology_on_the_Web

	servicios en ejecución en equipos de la red como servidores web, etc.[59]
Análisis de Vulnerabilidades	La organización Offensive Security cuenta con un gran número de pruebas diseñada para realizar análisis de vulnerabilidades, este, se realiza utilizando la información adquirida en la etapa anterior con el uso de herramientas especializadas entre las que se encuentra el nMap para escanear las redes, el sistema operativo Kali Linux, Nessus, entre otros.[60]
Definición de Objetivos Secundarios	Teniendo en cuenta la información obtenida del análisis de vulnerabilidades, se realiza la selección de los posibles objetivos que, según los resultados, nos ofrecen un mayor porcentaje de éxito en el ataque. A estos objetivos se les llama objetivos primarios, pero es recomendable siempre seleccionar un grupo de objetivos secundarios, teniendo en cuenta la posibilidad de fallo al atacar alguno de los primarios.[61]
Ataque	Fase de ataque a los objetivos seleccionados, en esta etapa se logra determinar con exactitud el nivel de exposición y posibilidad real de explotación de las vulnerabilidades halladas en la fase 2.

[59] LEÓN GUDIÑO, Marcelo Wladimir. Auditoría De Seguridad Informática En La Red Interna De La Univeridad Técnica Del Norte Según La Metodología Offensive Security Professional Training And Tools For Security Specialists Y Planteamiento De Políticas De Seguridad Basadasen La Norma Iso/Iec 27001. Trabajo de Grado Ingeniero en Electrónica y Redes de Comunicación. Ecuador.: Facultad de Ingeniería en Ciencias Aplicadas. Universidad Técnica del Norte. 2017. 261 p. [En línea]. Disponible en http://repositorio.utn.edu.ec/handle/123456789/6975

[60] VELOZ, Jorge, et al. Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informaticos mediante la herramienta KALI-LINUX. Revista de Tecnologías de la Informática y las Comunicaciones. V1. Nº 1. Año 1. 2017. [En línea] Disponible en https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/view/194/156

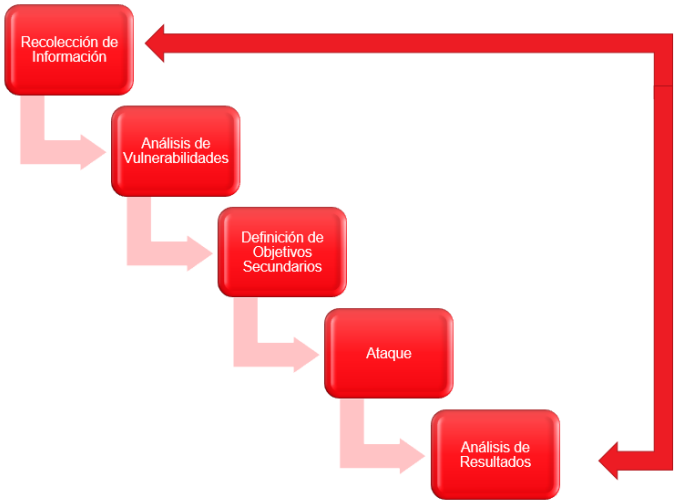
[61] CUZME RODRÍGUEZ, Fabián, et al. Op. ci. Administration and Management Platform of Electricity Consumption for Home Appliances Based on IoT. 2020

Análisis de resultados	El análisis de los resultados obtenido de cada uno de los ataques efectuados supone la última etapa del marco metodológico, sin embargo, también refiere el retorno a la fase inicial donde se verificarán la eficacia de las acciones ejecutadas. Sólo se detiene este ciclo una vez se compruebe que las pruebas ya han sido terminadas y se realiza la documentación total de todos los pasos ejecutados, hallazgos y medidas de corrección o mejora generas.

Fuente: El autor.

La ilustración 9 presenta el ciclo de vida del marco metodológico de la seguridad ofensiva.

Ilustración 9. Fases Offensive Security



Fuente: El autor

6.2.4 ISSAF – Information Systems Security Assessment Framework. El marco metodológico ISSAF, es ampliamente utilizado en las organizaciones como herramienta para el testeo de su seguridad interna y cumplir así los requisitos exigidos en materia de seguridad.[62] Esta metodología se basa en un

[62] VALENCIA BLANCO, Leidi Stefani. Metodologías Ethical Hacking. Bolivia. 2017. [En línea] Disponible en http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a12.pdf

conjunto de criterios de evaluación que han sido desarrollado de forma colaborativa por expertos alrededor del mundo.[63]

Esta metodología está compuesta por tres fases que se describen en la siguiente tabla:

Tabla 10. Fases ISSAF

Fase	Descripción
Planificación y Preparación	En esta primera fase se define el alcance de las pruebas a ejecutar, se establecen funciones y responsabilidades de los diferentes actores involucrados y la metodología de trabajo. [64]
Evaluación	La segunda fase es la evaluación. Aquí se realiza la identificación de los posibles riesgos asociados a los activos, y se evalúa la eficacia de los controles implantados hasta el momento.
Informe y Eliminación de Residuos	En esta fase los responsables de la auditoría realizan los informes con los hallazgos, emiten las recomendaciones de mejora y eliminan todos los posibles rastros generados en los procesos después de la ejecución de las diferentes pruebas.

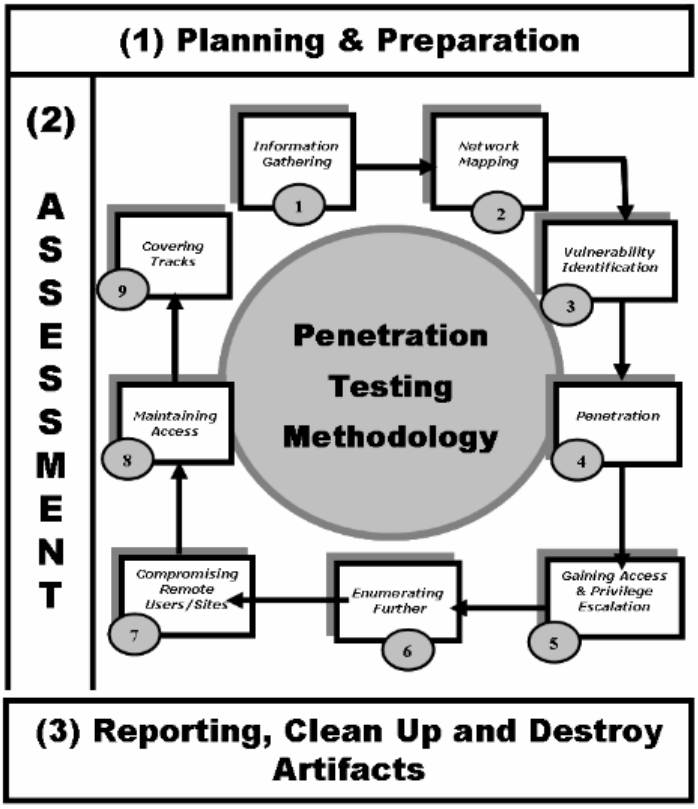
Fuente: El autor

[63] ALVAREZ INTRIAGO, Vilma Karina. Propuesta De Una Metodología De Pruebas De Penetración Orientada A Riesgos. Tesis Magister en Auditoría en Tecnología de Información. 2018. Ecuador.: Universidad Espíritu Santo. 26 p. [En línea] Disponible en https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

[64] FLOREZ ROJANO, Jorge Alonso. Metodología Para Realizar Hacking Ético En Bases De Datos Para Positiva Compañía De Seguros S.A En La Ciudad De Bogotá. Proyecto de Grado Especialista en Seguridad Informática. 2017. Bogotá D.C.: Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad Nacional Abierta y a Distancia. 70 p. [En línea] Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17375/1/19418118.pdf

En la siguiente ilustración se puede apreciar las fases de la metodología[65]

Ilustración 10. ISSAF



Fuente: ARAOZ, Israel. Metodología de test de intrusión ISSAF. 2009. [En línea] Disponible en http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html

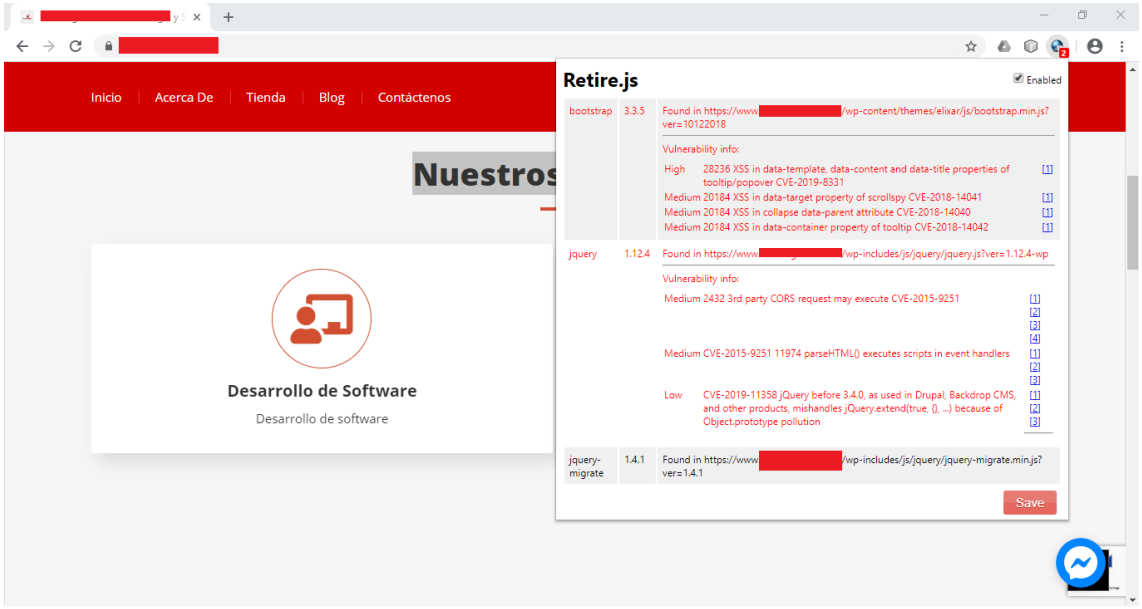
[65] ARAOZ, Israel. Metodología de test de intrusión ISSAF. 2009. [En línea] Disponible en http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html

6.3 VERIFICAR - PRESENTAR UN CONJUNTO DE PRUEBAS DE SEGURIDAD PARA DETECCIÓN DE VULNERABILIDADES

El desarrollo de este objetivo se centra en la presentación de diferentes pruebas utilizando herramientas de libre acceso que permiten obtener información acerca de las vulnerabilidades existentes en un sistema informático y con ello poder generar un plan de acción que permita corregir las debilidades.

6.3.1 Recolección de Información. Una de las principales fuentes de recolección de información es el internet a través del cual se puede realizar consultas buscando información sobre la víctima. Las páginas web generalmente son de acceso público por lo que se convierten en una fuente importante de información. En la primera prueba ejecutada para recolección de información se instala el complemento Retire.js al navegador web y se accede a la página web de la víctima, el complemento inmediatamente genera una notificación en la que se puede apreciar las vulnerabilidades existentes en la página web y los complementos que usa, además brinda acceso a enlaces que permiten obtener más información sobre cada una y las indicaciones para corregirlas.

Ilustración 11. Retire.js



Fuente: El autor

Como se puede apreciar en la ilustración anterior, la página en mención tiene vulnerabilidades relacionadas con la versión de Jquery y Bootstrap. (Se protege la dirección web de la página por confidencialidad)

Cada uno de los hallazgos se debe documentar indicando los detalles de la vulnerabilidad, el impacto y la solución. Se desarrolla un formato basado en la documentación del OWASP Top10 2017. En la siguiente ilustración se puede ver la vulnerabilidad de Bootstrap documentada.

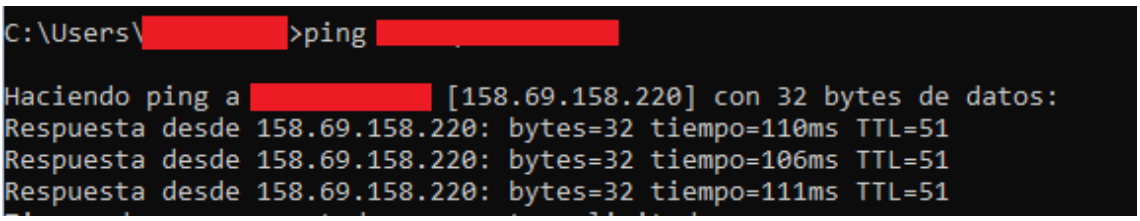
Ilustración 12. Vulnerabilidad 001 OWASP

Nº 001	**Bootstrap Vulnerable**				Fecha:
Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específica de la aplicación	2	3	2	2	No aplica
La página web utiliza una versión de Jquery que tiene vulnerabilidades conocidas relacionadas con el Cross Site Scripting. La versión actual es 3.3.5					
Impacto					
Se podría inyectar código XSS en la página principal.					
Solución					
Actualizar la versión a la 3.4.1 donde se corrigió la vulnerabilidad					

Fuente: El autor

Una vez se identifica la página web, se puede conseguir la dirección ip pública del servidor en el que se encuentra hospedada la aplicación web. Para esto, se realizó un ping a la página web. En la siguiente ilustración se evidencia la respuesta obtenida por el servidor y la ip pública correspondiente al servidor.

Ilustración 13. Ping hacia IP pública

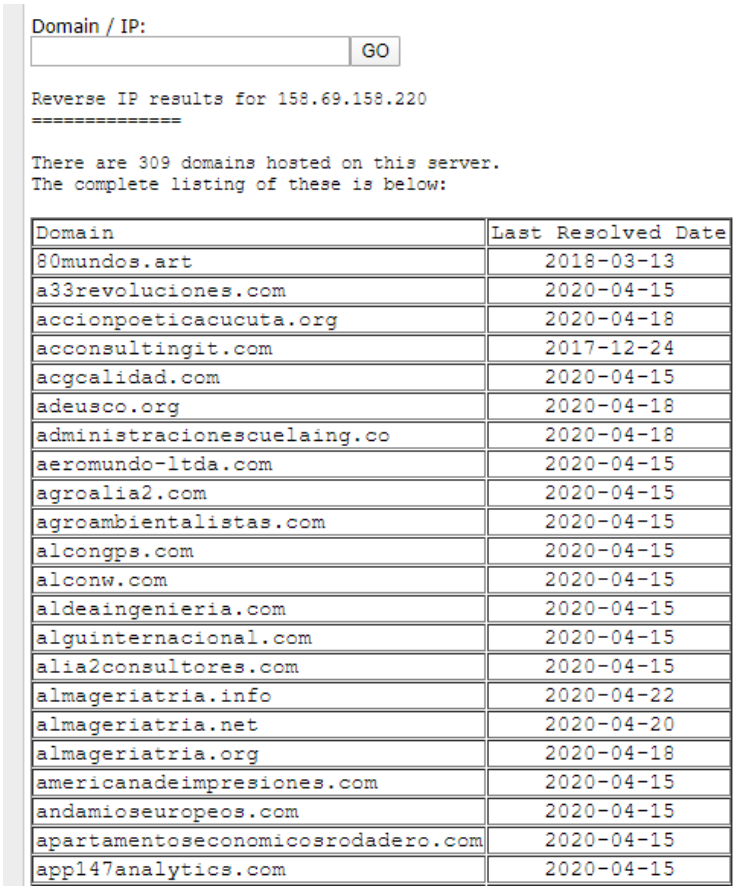


Fuente: El autor

6.3.2 Detección de Vulnerabilidades. Una vez identificada la dirección ip publica es posible realizar un escaneo al servidor y validar si este tiene más aplicaciones web.

En la siguiente ilustración se puede observar el resultado obtenido del sitio web https://viewdns.info/reverseip/, donde se introduce la ip pública y se detecta que en este destino se tienen más de 309 dominios adicionales, indicando que funciona como un VPS o servidor virtual compartido, este tipo de sitios se consideran vulnerables ya que no se puede garantizar las medidas de seguridad implementadas en cada una de las aplicaciones hospedadas. A través de un sitio vulnerable que se logre romper por parte de los delincuentes, se podría acceder a los demás.

Ilustración 14. VPS



Domain / IP:

GO

Reverse IP results for 158.69.158.220

==========

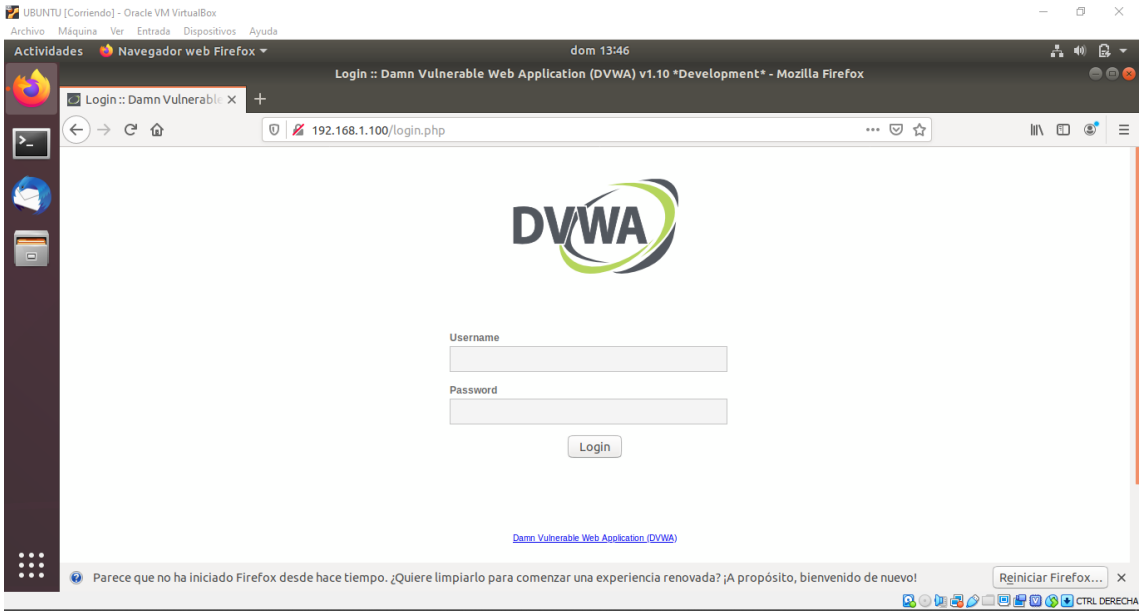
There are 309 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
80mundos.art	2018-03-13
a33revoluciones.com	2020-04-15
accionpoeticacucuta.org	2020-04-18
acconsultingit.com	2017-12-24
acgcalidad.com	2020-04-15
adeusco.org	2020-04-18
administracionescuelaing.co	2020-04-18
aeromundo-ltda.com	2020-04-15
agroalia2.com	2020-04-15
agroambientalistas.com	2020-04-15
alcongps.com	2020-04-15
alconw.com	2020-04-15
aldeaingenieria.com	2020-04-15
alguinternacional.com	2020-04-15
alia2consultores.com	2020-04-15
almageriatria.info	2020-04-22
almageriatria.net	2020-04-20
almageriatria.org	2020-04-18
americanadeimpresiones.com	2020-04-15
andamioseuropeos.com	2020-04-15
apartamentoseconomicosrodadero.com	2020-04-15
app147analytics.com	2020-04-15

Fuente: El autor

6.3.3 Listando directorios. A través del listado de directorios es posible obtener la estructura de carpetas y archivos de una aplicación web. La siguiente prueba se realiza utilizando la herramienta “OWASP Dirbuster” disponible en Kali Linux y que permite listar los directorios de un sitio web. La victima utilizada para la prueba es la aplicación DVWA funcionando en una máquina virtual.

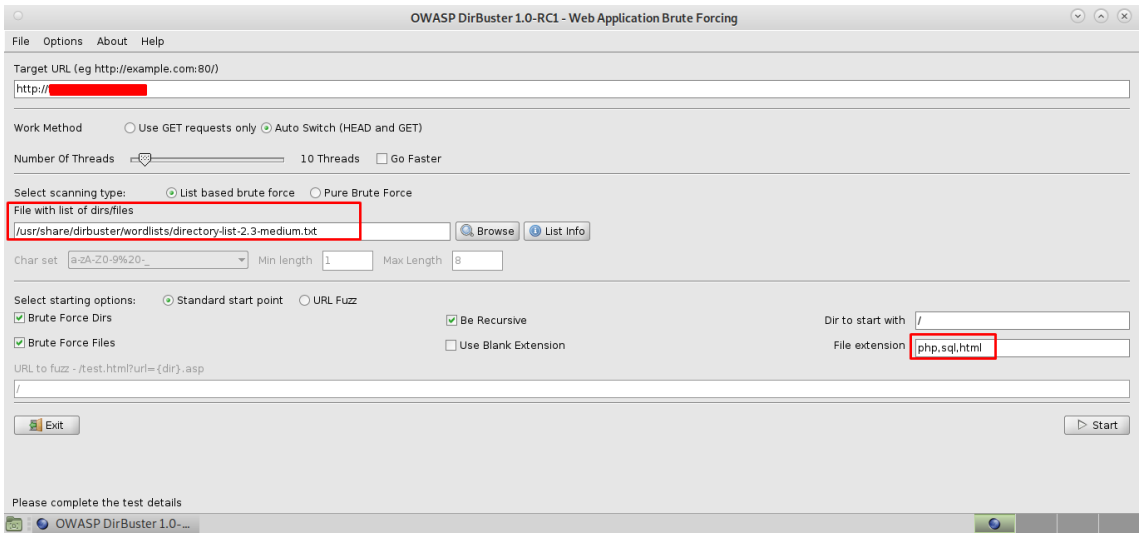
Ilustración 15. Máquina virtual Ubuntu con DVWA



Fuente: El autor

Una vez se ejecuta la aplicación se debe configurar el tipo de ataque que se utilizará, el objetivo, directorios a utilizar y extensiones de archivos que se desean listar. La configuración utilizada es:

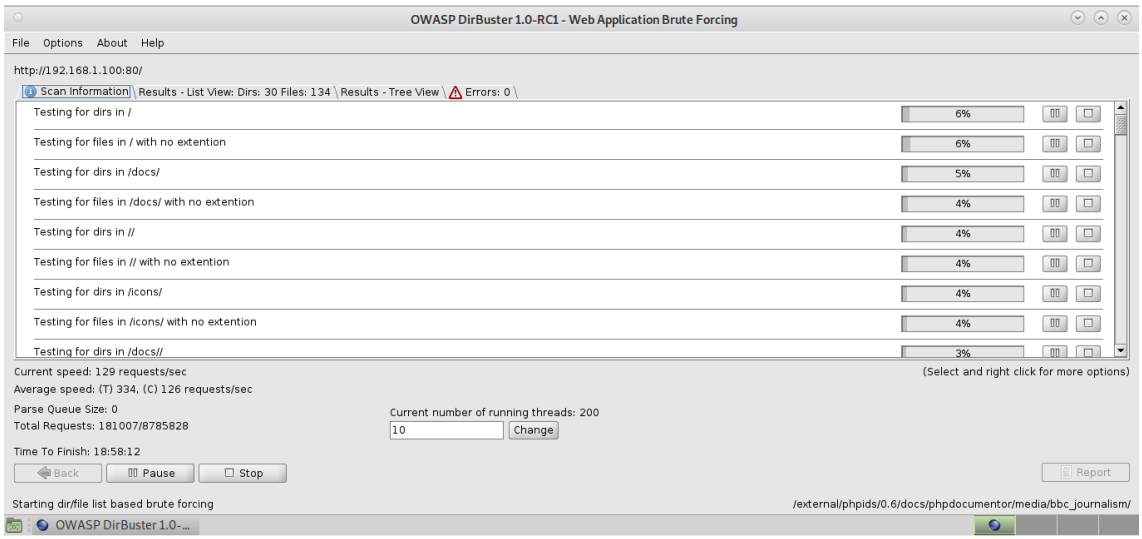
Ilustración 16. Configuración OWASP-Dirbuster



Fuente: El autor

Una vez se configuran todas las opciones del escaneo, se inicia. El tiempo de duración del proceso es variable.

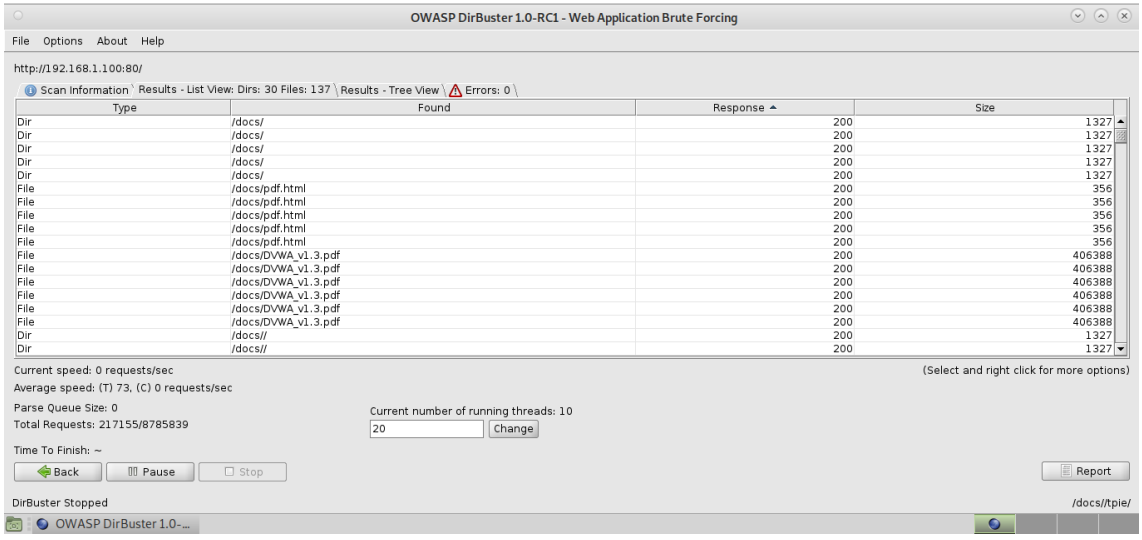
Ilustración 17. Escáner - OWASP-Dirbuster



Fuente: El autor.

Una vez finalizado el proceso se puede obtener el listado de directorio y archivos completo que coincidieron con el diccionario de búsqueda seleccionado. En la siguiente ilustración se evidencia la estructura de la página.

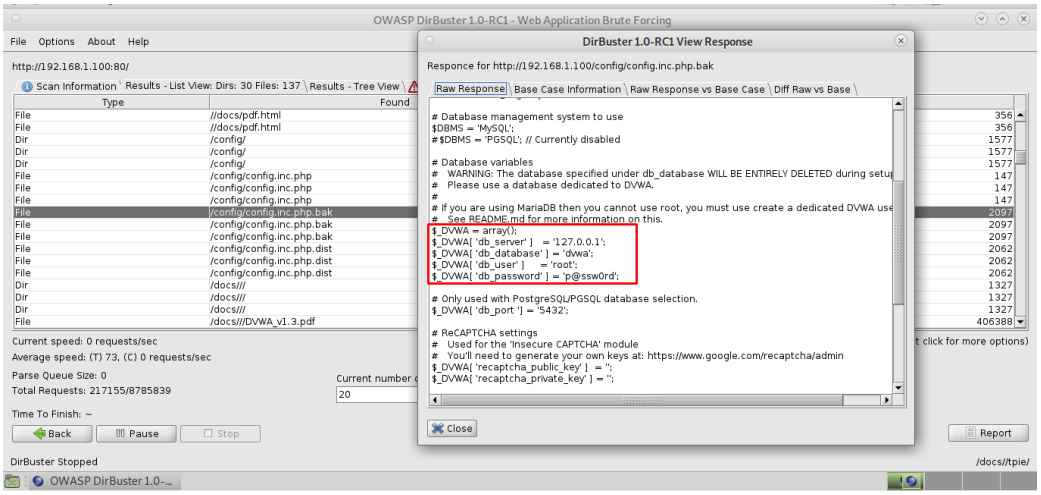
Ilustración 18. Listado de Directorios y archivos



Fuente: El autor

Esta prueba permite verificar si la aplicación web tiene directorios o archivos expuestos sin ser requerido. En la prueba se puede identificar archivos .bak con la configuración de la aplicación.

Ilustración 19. Configuración seguridad DVWA



Fuente: El autor

6.3.4 Enumeración de Usuarios. La enumeración de usuarios permite escanear una página y probar si es posible acceder a los nombres de usuarios que tiene creados la página. Para esta prueba existen muchas herramientas. WPHunter permite realizar esta prueba para sitios creados con WordPress. En la siguiente ilustración se puede apreciar que la página utilizada de prueba no cuenta con esta vulnerabilidad y no permite listar los usuarios

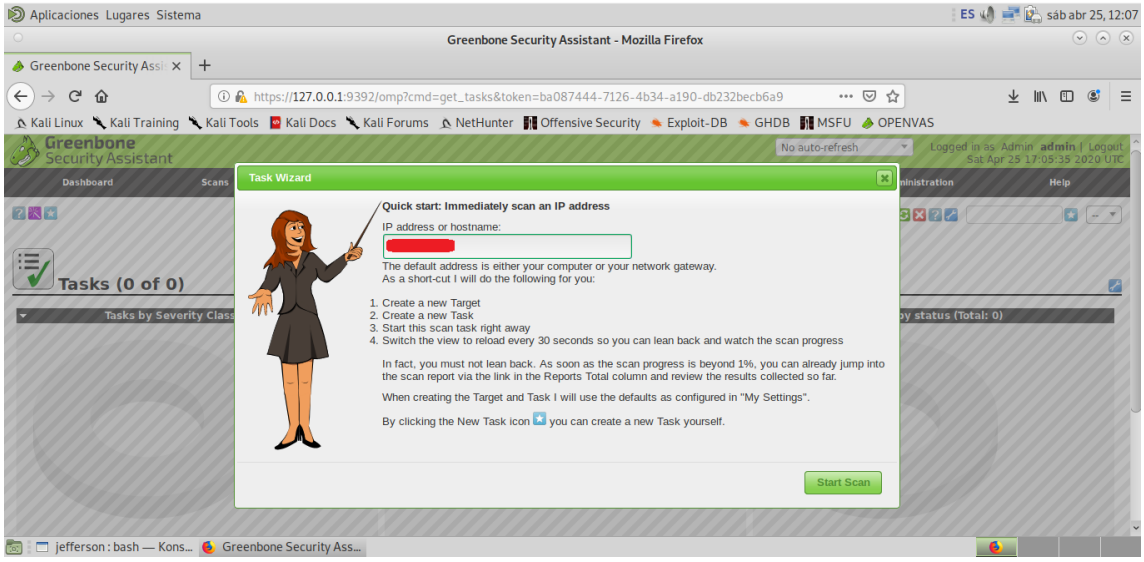
Ilustración 20. Enumeración de usuario 1

Fuente: El autor

6.3.5 Escáner Vulnerabilidades Equipos en Red. Es posible realizar un escaneo masivo de vulnerabilidades en equipos que se encuentren en una red determinada. Para la siguiente prueba se utilizó la herramienta OpenVas y se ejecutó sobre todo un rango de ip. El software detecta los equipos presentes en la red al momento de su ejecución y determinada para cada uno, las vulnerabilidades que tienen.

Una vez se ejecuta el software, en el apartado “tareas/Asistente de tareas” se genera la nueva tarea adicionando la ip o el rango de ip que se desea escanear. En la siguiente ilustración se evidencia la creación de la tarea.

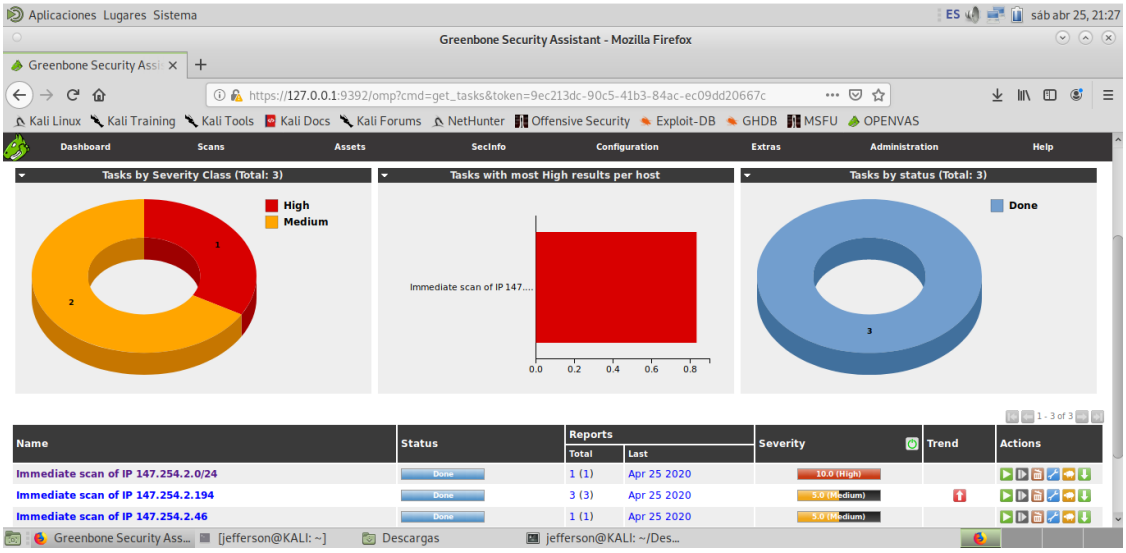
Ilustración 21. Creación de tarea en OpenVas



Fuente: El autor.

Una vez creada la tarea, esta se ejecuta de forma automática. La duración depende de la cantidad de equipos. En la siguiente ilustración se puede evidenciar el listado de tareas, la severidad más importante en cada una y el número de ejecución que se tiene.

Ilustración 22. Estadísticas de tareas OpenVas



Fuente: El autor.

Una vez finalizada la ejecución de las tareas, presionando clic en el nombre de la tarea se puede ingresar al reporte general. Para la práctica se accede a la tarea ejecutada sobre el rango completo que evidencia vulnerabilidades de alta severidad. En la siguiente ilustración se puede apreciar el listado completo de vulnerabilidades halladas, la severidad y el equipo afectado.

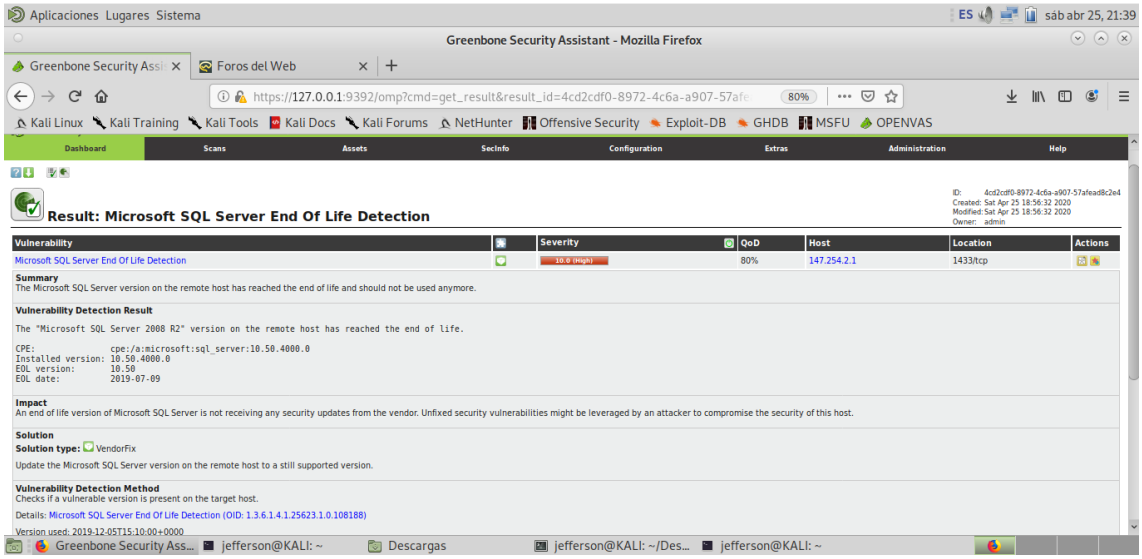
Ilustración 23. Listado de Vulnerabilidades OpenVas

Fuente: El autor.

Seleccionando cada una de las vulnerabilidades se puede obtener un detalle de esta, el impacto que genera, método de mitigación, método utilizado para la

detección y enlaces a páginas relacionadas que permiten ampliar información. En la siguiente ilustración se puede apreciar el detalle de la primera vulnerabilidad.

Ilustración 24. Detalle de Vulnerabilidad OpenVas



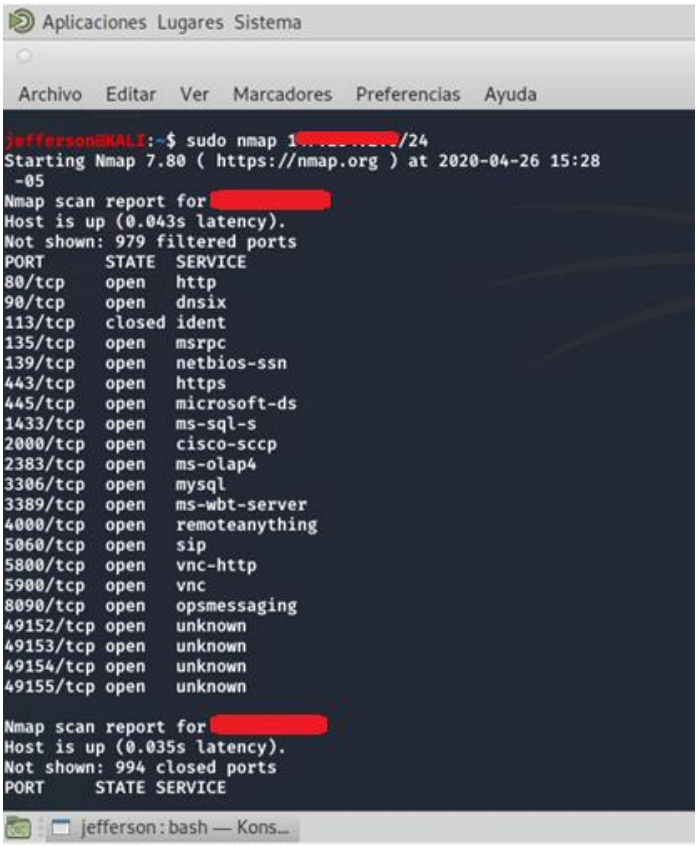
Fuente: El autor.

El informe general de todas las vulnerabilidades puede ser exportado en diferentes formatos como HTML, pdf, etc.

6.3.6 Descubriendo equipos en la red. Es posible identificar los equipos que se encuentran conectados a una red. Existe una gran variedad de herramientas que permite obtener esta información. Para la siguiente prueba se utiliza la herramienta nMap incluida en Kali Linux.

En la siguiente ilustración se puede apreciar el resultado de la ejecución de la prueba, se encuentran 60 equipos activos en la red y se evidencia el detalle de los equipos. El primer equipo tiene servicios activos en el puerto 80 http, se identifica también un servidor de base de datos mysql en el puerto 3306.

Ilustración 25. nMap



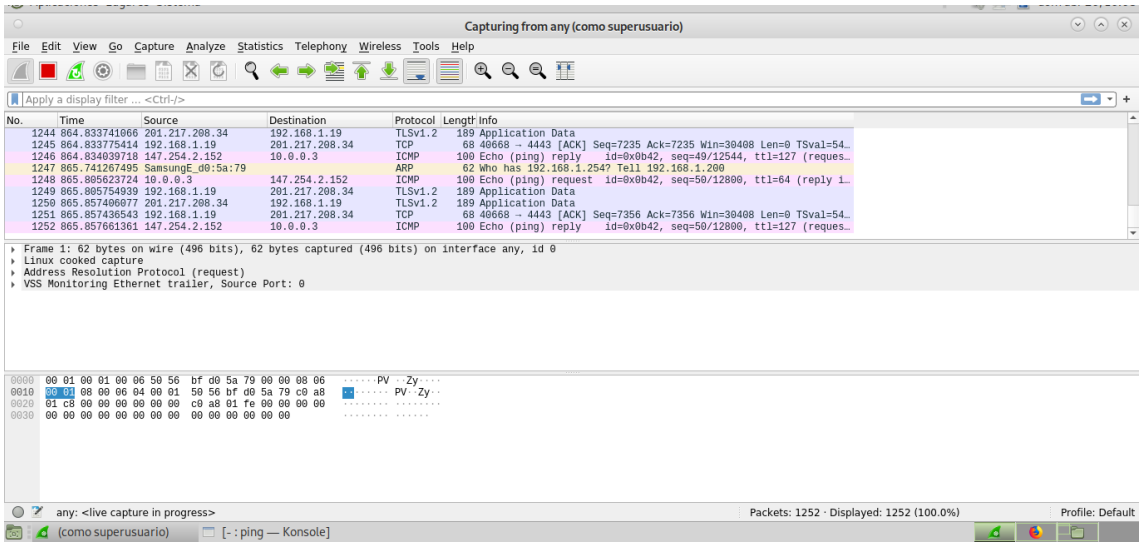
Fuente: El autor

Como se puede apreciar en la anterior ilustración, se puede detectar información relevante de cada equipo, esta información va desde el nombre del dispositivo en la red, los puertos y el tipo de servicios que tiene activos en cada uno, suponiendo con esto alternativas para explorar posibles vulnerabilidades y explotarlas.

6.3.7 Análisis de Red con Wireshark. El análisis de las redes puede ayudar a detectar posibles intentos de intrusión de forma anticipada. La herramienta Wireshark permite visualizar cada detalle de los paquetes intercambiados en la red, presentando la fuente del paquete, el destino, protocolo y puertos.

En la siguiente ilustración se puede apreciar el comportamiento de la red cuando se realiza un ping con destino a un equipo de la red. Esto se puede apreciar por los paquetes ICMP intercambiados.

Ilustración 26. Wireshark ping



Fuente: El autor

Comportamientos inusuales como los presentados en la siguiente ilustración, pueden brindar indicios sobre la posibilidad de ser víctimas de un ataque.

Ilustración 27. Tráfico inusual WireShark

No.	Time	Source	Destination	Protocol	Length	Info
11131	85.207044	192.168.1.230	192.168.1.231	TCP	60	36539 → 50475 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11132	85.210529	192.168.1.231	192.168.1.230	TCP	54	50475 → 36539 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11133	85.217864	192.168.1.230	192.168.1.231	TCP	60	36539 → 44362 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11134	85.221390	192.168.1.231	192.168.1.230	TCP	54	44362 → 36539 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11135	85.267197	192.168.1.230	192.168.1.231	TCP	60	36543 → 9051 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11136	85.270376	192.168.1.231	192.168.1.230	TCP	54	9051 → 36543 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11137	85.278106	192.168.1.230	192.168.1.231	TCP	60	36540 → 13004 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11138	85.288733	192.168.1.230	192.168.1.231	TCP	60	36540 → 51335 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11139	85.295642	192.168.1.231	192.168.1.230	TCP	54	13004 → 36540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11140	85.296256	192.168.1.231	192.168.1.230	TCP	54	51335 → 36540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11141	85.298713	192.168.1.230	192.168.1.231	TCP	60	36540 → 60336 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11142	85.305936	192.168.1.231	192.168.1.230	TCP	54	60336 → 36540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11143	85.308911	192.168.1.230	192.168.1.231	TCP	60	36540 → 50475 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11144	85.313731	192.168.1.231	192.168.1.230	TCP	54	50475 → 36540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11145	85.318807	192.168.1.230	192.168.1.231	TCP	60	36540 → 44362 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11146	85.322731	192.168.1.231	192.168.1.230	TCP	54	44362 → 36540 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11147	85.367288	192.168.1.230	192.168.1.231	TCP	60	36544 → 9051 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11148	85.370631	192.168.1.231	192.168.1.230	TCP	54	9051 → 36544 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11149	85.377917	192.168.1.230	192.168.1.231	TCP	60	36539 → 15517 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11150	85.380802	192.168.1.231	192.168.1.230	TCP	54	15517 → 36539 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11151	85.388748	192.168.1.230	192.168.1.231	TCP	60	36539 → 47495 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11152	85.392661	192.168.1.231	192.168.1.230	TCP	54	47495 → 36539 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11153	85.399737	192.168.1.230	192.168.1.231	TCP	60	36539 → 4012 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11154	85.407613	192.168.1.231	192.168.1.230	TCP	54	4012 → 36539 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11155	85.409813	192.168.1.230	192.168.1.231	TCP	60	36539 → 51414 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11156	85.413472	192.168.1.231	192.168.1.230	TCP	54	51414 → 36539 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11157	85.420155	192.168.1.230	192.168.1.231	TCP	60	36539 → 10811 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Fuente: El autor

Se aprecia un envío y recepción constante de paquetes a diferentes puertos entre los mismos dispositivos, este comportamiento no es común y nos puede dar señales de que un ataque se está presentando. Al igual que los paquetes ICMP cuando se realiza un ping. Un atacante antes de ejecutar su ataque

primero realiza ping para verificar si tiene o no comunicación con el dispositivo víctima.

6.4 ACTUAR - ENTREGAR RECOMENDACIONES FUNDAMENTALES APLICABLES A LAS ORGANIZACIONES EMPRESARIALES PARA EVALUAR SU SEGURIDAD

El desarrollo de los objetivos anteriores ha permitido recopilar información acerca de las debilidades que se encuentran actualmente a nivel de seguridad informática y las principales estrategias utilizadas por los criminales. También se han presentado algunas alternativas que se tienen disponibles y que con un correcto uso y/o implementación permitirán mitigar muchas de estas amenazas.

Tabla 11. Recomendaciones de Seguridad

CATEGORIA	RECOMENDACIÓN
Seguridad de la información	• Establecer un conjunto de políticas de seguridad de la información, las cuales deben ser aprobadas por la alta dirección y aplicadas por todo el personal. Dichas políticas deben ser revisadas y actualizadas de forma constante. Adicional, estás deben contemplar escenarios como el teletrabajo o el uso de dispositivos móviles para procesar cualquier información laboral. • Establecer políticas para creación, modificación y eliminación de usuarios en los diferentes sistemas informáticos. • Clasificar la información con criterios como su valor, la criticidad, requisitos legales.

	• Implementar políticas para la gestión de unidades o medios extraíbles.
Pruebas de penetración	Se recomienda al menos 1 vez al año realizar un estudio de vulnerabilidades de todos los sistemas informáticos. Estas pruebas deben incluir: • Análisis de tráfico en las redes. • Detección de dispositivos presentes en la red para detectar posibles equipos intrusos o no autorizados. • Verificación de aplicaciones web, estas deben cumplir con certificado SSL. • Uso de captchas en formularios de Login. • Probar fortaleza de las claves de usuario. • Escanear vulnerabilidades en todos los equipos de la red. • Fortaleza de cables de redes Wifi. • Prueba de penetración externas que permitan verificar la efectividad de firewall y la seguridad perimetral en general. • Ejecución de campaña de phishing para detectar posibles vulnerabilidades del factor humano.
Seguridad de Red	• Segmentación de direccionamientos ip

	• Wifi para visitantes exclusivo y sin ningún tipo de comunicación con los segmentos ip de los equipos internos de la organización. • En caso de contar con servidores físicos, estos deben tener un direccionamiento ip diferente al utilizado por el general de los equipos de la organización, las reglas de intercambio de paquetes deben ser exclusivo de aquellos para los que esté dispuesto. • Uso de Firewall o cortafuegos.
Seguridad de Hardware	• Mantener un inventario de los diferentes activos informáticos, sus responsables y los riesgos presentes para cada uno de ellos. • Aplicaciones Antivirus instaladas y actualizadas.
Recursos Humanos	El phishing en uno de los ataques más comunes y desafortunadamente más efectivos, ya que se aprovecha de la ingeniería social o del factor humano para cometer el crimen. Es por ello por lo que se recomienda: • Establecer un plan de capacitación y sensibilización constante a los colaboradores donde se aborden temas como las modalidades más utilizadas en

	ingeniería social, identificación de sitios web y de remitentes de correo.
Controles de acceso	• Establecer políticas para asignación de roles. • Establecer una política de control de acceso y controles que permitan que el acceso de usuarios a la red y servicios sea de forma controlada. • Las áreas o cuartos físicos donde se alberguen equipos de procesamiento de información como cuartos de servidores o cuartos de redes deben contar con controles de acceso para evitar el ingreso de personal no autorizado. Adicional se debe generar una bitácora de ingresos que permita llevar una trazabilidad de los ingresos y las razones o labores realizadas al interior.
Control de autenticación	• Garantizar la restricción de acceso a la información, solo puede acceder a ella quien tenga realmente el permiso y necesidad de hacerlo. El mínimo privilegio. • Las aplicaciones o software utilizados deben contar con control de autenticación. • La instalación de nuevo software se debe ejecutar de forma controlada por personal autorizado y validado que provenga de fuentes confiables y firmados digitalmente.

Cifrado	• Las bases de datos deben estar cifradas. • Los discos duros de los equipos y unidades extraíbles deben estar cifrados. • Sistemas operativos y aplicaciones deben tener el 100% de las actualizaciones o parches publicados.

Fuente: El autor

7 CONCLUSIONES

- Establecer un programa de seguridad informática en las empresas a través de metodologías conocidas que permiten combinar factores tanto físicos como lógicos, contribuye a un proceso de ciberseguridad efectivo.
- La seguridad informática en Colombia ha empezado a tener relevancia y esto se puede apreciar por el crecimiento de la oferta tanto laboral como académica en esta especialidad en particular buscando fortalecer el recurso humano cualificado que pueda enfrentar las diferentes modalidades del cibercrimen.
- Existen diferentes metodologías que pueden ser adaptadas por cualquier empresa para establecer mecanismos de defensa y control en ciberseguridad.
- La ejecución de pruebas de seguridad sobre un sistema informático permite de forma temprana detectar y corregir fallos que puedan ser aprovechados por cibercriminales.
- La aplicación de estrategias de seguridad combinadas puede dificultar en gran medida la tarea a un delincuente haciendo los sistemas informáticos cada vez más seguros.

8 RECOMENDACIONES

- Teniendo en cuenta el crecimiento tanto de las aplicaciones de las nuevas tecnologías en los procesos y el crecimiento del cibercrimen ser recomienda establecer medidas de control y seguimiento de procesos que permitan mitigar las amenazas a las que se pueda encontrar expuesto.

- La formación en ciberseguridad tiene gran importancia y es por ello por lo que se recomienda que sea depositada esta responsabilidad en un profesional formado en ciberseguridad.

- Seleccionar una metodología de hacking ético a través de la cual se puedan aplicar las pruebas de forma periódica a los sistemas informáticos y evaluar su nivel de exposición.

- Generar un plan de concientización para los empleados en temas de ciberseguridad a través de capacitaciones, talleres y demás actividades que permitan una correcta apropiación del conocimiento.

- Establecer un plan de detección y respuesta ante ataques informáticos.

9 DIVULGACIÓN

La divulgación del presente proyecto no posee ninguna restricción, pues la información desarrollada es completamente pública y orientadora. Por esto la divulgación se realizar en el repositorio de la UNAD, para que éste pueda ser consultado por los estudiantes de la UNAD y el resto de los usuarios que ingresen a dicho repositorio.

BIBLIOGRAFÍA COMPLEMENTARIA

BALUJA GARCÍA, Walter y ANÍAS CALDERÓN, Caridad. Amenazas y defensas de seguridad en las redes de próxima generación. Ingeniería y Competitividad, 8(2), 7–16. 2006. [En línea]. Disponible en https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=a9h&AN=23820951&lang=es&site=ehost-live

CORTÉS CAMACHO, Jesús Germán. Auditoria a la seguridad de la red de datos de la empresa Panavias S.A. Trabajo de Grado Especialista en Seguridad Informática. 2016. San Juan de Pasto. Colombia.: Escuela de Ciencias Básicas, Tecnologías e Ingeniería. Universidad Nacional Abierta y a Distancia. 307 p. [En línea]. Disponible en https://repository.unad.edu.co/handle/10596/12014

ESCRIVÁ GASCÓ, Gema, *et al*. Seguridad informática. Macmillan Iberia, S.A. 2013. 218 p. ISBN 9788415991410. [En línea]. Disponible en https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3217398

FRANCO, David A., PEREA, Jorge L. y PUELLO, Plinio. Metodología para la Detección de Vulnerabilidades en Redes de Datos / Methodology for Detecting Vulnerabilities in Data Networks. Información Tecnológica, 23(3), 113. [En línea]. Disponible en https://doi-org.bibliotecavirtual.unad.edu.co/10.4067/S0718-07642012000300014

GARCÍA GUACANEME, Raúl. Análisis de seguridad a la red de datos de la empresa Asistir Computadores de la ciudad de Bogotá. Trabajo de Grado de Especialista en Seguridad Informática. 2017. Bogotá D.C.: Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad Nacional Abierta y a Distancia. 80p. [En línea]. Disponible en https://repository.unad.edu.co/handle/10596/12926

GIL VERA, Víctor Daniel y GIL VERA, Juan Carlos. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et Technica, 22(2), 193–197. 2017. [En línea]. Disponible en https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=a9h&AN=129781870&lang=es&site=ehost-live

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000. 4ed. Geneva.

ORTIZ ARISTIZÁBAL, Diego Fernando. Desarrollo De Metodología Para Hallazgos De Vulnerabilidades En Redes Corporativas E Intrusiones Controladas. Trabajo de Grado de Ingeniero Electrónico. 2015. Bogotá D.C.: Facultad de Ingenierías. Fundación Universitaria los Libertadores. 141 p. [En

línea]. Disponible en https://repository.libertadores.edu.co/bitstream/handle/11371/342/DiegoFernandoOrtizAristizabal.pdf?sequence=2&isAllowed=y

PAZMIÑO CALUÑA, Andrés Alejandro. (2011). Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas WiFi. Tesis de Grado de Ingeniero en Electrónica, Telecomunicaciones y Redes. 2011. Riobamba, Ecuador.: Facultad de Informática y Electrónica. Escuela Superior Politécnica de Chimborazo. 201 p. [En línea]. Disponible en http://dspace.espoch.edu.ec/handle/123456789/1726

POLICIA NACIONAL DE COLOMBIA. Balance de cibercrimen en Colombia. 2017. [En línea]. Disponible en https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

RAMOS FRAILE, Alejandro. Seguridad perimetral. 2011. [En línea]. Disponible en http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

REMACHE RUBIO, Eduardo Marcelo. Modelo para la mitigación de vulnerabilidades informáticas en los servicios web de la Pontificia Universidad Católica del Ecuador Ambato. Tesis de Magister en Gerencia Informática. 2018. Ambato, Ecuador.: Pontificia Universidad Católica del Ecuador. 139 p. [En línea]. Disponible en https://repositorio.pucesa.edu.ec/handle/123456789/2474

RESTREPO ZULUAGA, Arley Guillermo. Vulnerabilidades en redes de internet alámbricas e inalámbricas. Trabajo de grado de Especialista en Seguridad Informática. 2018. Pereira, Colombia.: Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad Nacional Abierta y a Distancia. 117 p. [En línea]. Disponible en https://repository.unad.edu.co/handle/10596/27729

ROSERO ALMEIDA, Diego Fernando y MESÍAS NARVÁEZ, Javier Orlando. Auditoría a la seguridad de la red de datos del Instituto Departamental de Salud de Nariño. Trabajo de grado de Especialista en Seguridad Informática. 2016. Pasto, Colombia.: Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad Nacional Abierta y a Distancia. 176 p. [En línea]. Disponible en https://repository.unad.edu.co/handle/10596/11986

UNILIBRE. Crecen los ataques de Phishing en Colombia. 2019. [En línea]. Disponible en http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia

VALDERRAMA GUARDIA, Jhon Edinson. Pentesting “prueba de penetración” para la identificación de vulnerabilidades en la red de computadoras en la Alcaldía del municipio de Cantón del San Pablo, departamento del Chocó. Trabajo de grado de Especialista en Seguridad Informática. 2017. Quibdó, Colombia.: Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad

Nacional Abierta y a Distancia. 79 p. [En línea]. Disponible en https://repository.unad.edu.co/handle/10596/18049

VIVER RAMIREZ, Aydee Mercedes. Identificación de vulnerabilidades de la red LAN del Buque Oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de Pentesting. Trabajo de grado de Especialista en Seguridad Informática. 2016. Cali, Colombia.: Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad Nacional Abierta y a Distancia. 84 p. [En línea]. Disponible en https://repository.unad.edu.co/handle/10596/12425

REFERENCIAS

ACUÑA LOPEZ, Luisa Fernanda y VILLA MOTATO, Sandra Milena. Estado Actual Del Cibercrimen En Colombia Con Respecto A Latinoamérica. Proyecto de Grado Especialista en Seguridad Informática. Pereira, Colombia.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2018. 104 p. [En línea] Disponible en https://repository.unad.edu.co/bitstream/handle/10596/25619/%20%09lfacunal.pdf?sequence=1

AGUILERA LÓPEZ, Purificación. Seguridad informática. 1a ed.: Editex, 2010. 240 p. ISBN 978-84-9771-657-4.

ALVAREZ INTRIAGO, Vilma Karina. Propuesta De Una Metodología De Pruebas De Penetración Orientada A Riesgos. Tesis Magister en Auditoría en Tecnología de Información. 2018. Ecuador.: Universidad Espíritu Santo. 26 p. [En línea] Disponible en https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

ANGULO, Susana. Empresas fallan en sus sistemas de seguridad informática. 2017. [En línea] Disponible en https://www.enter.co/especiales/empresas-del-futuro/segun-estudio-empresas-fallan-en-sus-sistemas-de-seguridad-informatica/

ARAOZ, Israel. Metodología de test de intrusión ISSAF. 2009. [En línea] Disponible en http://insecuredata.blogspot.com/2009/04/metodologia-de-test-de-intrusion-issaf.html

ARNAL MARTÍN, Andrea. La contraseña más popular del mundo sigue siendo '123456'. 2016. [En línea]. Disponible en https://elpais.com/tecnologia/2016/01/20/actualidad/1453281839_103381.html

AUSTIN, Robert y DARBY, Christopher. El mito de la seguridad informática. Ediciones Deusto – Planeta de Agostini Profesional y Formación S.L., 2004. 9 p. 2019. [En línea]. Disponible en https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3159136

AVAST. WannaCry. 2019. [En línea] Disponible en https://www.avast.com/es-es/c-wannacry

BARRETO CUITIVA, Julian Hernán. Diseño De Manual De Diagnostico Y Prevención De Vulnerabilidades En Redes De Datos Para Pymes. Proyecto de Grado Especialista en Seguridad Informática. Bogotá D.C.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2018. 45 p. [En línea] Disponible en

https://repository.unad.edu.co/bitstream/handle/10596/15026/80225921.pdf?sequence=1&isAllowed=y

BARRIONUEVO, Mercedes, *et al*. Secure Computer Network: Strategies and Challengers in Big Data Era. Journal of Computer Science & Technology (JCS&T), 18(3), 248–257. 2018. [En línea]. Disponible en https://doi-org.bibliotecavirtual.unad.edu.co/10.24215/16666038.18.e28

BRICEÑO MARQUEZ, José E. Transmisión de Datos. 3ª ed. 2005. Venezuela.: Departamento de Electrónica y Comunicaciones de la Escuela de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Los Andes. 564 p. [En línea]. Disponible en http://bdigital.ula.ve/storage/pdf/32381.pdf

CANDELARIO SAMPER, Juan José y RODRÍGUEZ BOLAÑO, Moisés. Seguridad informática en el Siglo xxi: Una perspectiva Jurídica Tecnológica Enfocada Hacia las Organizaciones Nacionales y Mundiales. Revista Especializada en Ingeniería, Universidad Nacional Abierta y a Distancia. 2012 [En línea] Disponible en http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1441/1760

CASTRO VASQUEZ, Carlos Arturo. Pruebas de penetración e intrusión. 2019. Universidad Piloto de Colombia. [En línea] Disponible en http://35.227.45.16/handle/20.500.12277/6273

CCIT. Informe de las tendencias del cibercrimen en Colombia 2019-2020. 2019. [En línea]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

COLORADO, Francisco. El Ciclo PHVA de Deming y el Proceso Administrativo de Fayol. 2009. [En línea]. Disponible en https://www.academia.edu/5110051/3_Articulo_El_Ciclo_PHVA_de_Deming_y_al_Proceso_Administrativo_de_Fayol

CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley 1273 de 2009. [En línea]. Disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

CUZME RODRÍGUEZ, Fabián, *et al*. Administration and Management Platform of Electricity Consumption for Home Appliances Based on IoT. 2020. Ecuador.: Ingeniería en Telecomunicaciones, Universidad Técnica del Norte. [En línea] Disponible en https://www.researchgate.net/publication/328367829_Offensive_Security_Ethical_Hacking_Methodology_on_the_Web

DINERO. ¡Cuidado! Están suplantando a Bancolombia para estafar a miles de clientes. 2017. [En línea] Disponible en https://www.dinero.com/empresas/articulo/campana-de-phishing-afecta-a-miles-de-clientes-de-bancolombia/242871

DINERO. Empresas. Colombia, débil en seguridad informática. 2008. [En línea] Disponible en https://www.dinero.com/edicion-impresa/tendencias/articulo/empresas-colombia-debil-seguridad-informatica/66085

DINERO. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. 2019 [En línea]. Disponible en https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

EL TIEMPO. En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. 2019. [En línea] Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

ENTER.CO. El hacking ético y su importancia para las empresas. 2014. [En línea] Disponible en https://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

FLOREZ ROJANO, Jorge Alonso. Metodología Para Realizar Hacking Ético En Bases De Datos Para Positiva Compañía De Seguros S.A En La Ciudad De Bogotá. Proyecto de Grado Especialista en Seguridad Informática. 2017. Bogotá D.C.: Escuela de Ciencias Básicas, Tecnología e Ingeniería. Universidad Nacional Abierta y a Distancia. 70 p. [En línea] Disponible en https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17375/1/19418118.pdf

GONZALEZ AGUDELO, Daniel Felipe. EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INFORMÁTICA UNA AMENAZA EN LAS EMPRESAS CERTIFICADAS BASC. Ensayo para Administrador en Seguridad y Salud Ocupacional. Bogotá D.C.: Universidad Militar Nueva Granada. Facultad de Relaciones Internacionales, Estrategia y Seguridad. 2014. 24 p. [En línea] Disponible en https://repository.unimilitar.edu.co/bitstream/handle/10654/12251/ENSAYO%20FINAL.pdf?sequence=1

GRUPO BANCOLOMBIA. Ciberseguridad: Malos hábitos vs buenas prácticas de las startups. [En línea]. Disponible en https://www.grupobancolombia.com/wps/portal/innovacion/tecnologias-disruptivas/malos-habitos-vs-buenas-practicas-de-las-startups

GUISTO BILIC, Denise. Las amenazas informáticas que más afectaron a los países de América Latina. 2019. [En línea] Disponible en https://www.welivesecurity.com/la-es/2019/01/10/amenazas-informaticas-mas-afectaron-paises-america-latina/

HARÁN, Juan Manuel. Profesionales en seguridad informática: entre la formación académica y la autodidacta. 2019. [En línea] Disponible en

https://www.welivesecurity.com/la-es/2019/11/11/profesionales-en-seguridad-informatica-entre-la-formacion-academica-y-la-autodidacta/

HEALTH ON LINE. 5% de las empresas colombianas han perdido hasta cuatro mil millones por ciberataques. 2019. [En línea] Disponible en https://www.heon.com.co/index.php/news/item/241-ataques-ciberneticos-colombia

KASPERSKY. ¿Qué es el Ransomware? 2019. [En línea] Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

LEÓN GUDIÑO, Marcelo Wladimir. Auditoría De Seguridad Informática En La Red Interna De La Univeridad Técnica Del Norte Según La Metodología Offensive Security Professional Training And Tools For Security Specialists Y Planteamiento De Políticas De Seguridad Basadasen La Norma Iso/Iec 27001. Trabajo de Grado Ingeniero en Electrónica y Redes de Comunicación. Ecuador.: Facultad de Ingeniería en Ciencias Aplicadas. Universidad Técnica del Norte. 2017. 261 p. [En línea]. Disponible en http://repositorio.utn.edu.ec/handle/123456789/6975

LUBECK, Luis. Phishing suplanta identidad de reconocido banco de Colombia y busca robar información financiera. 2019. [En línea] Disponible en https://www.welivesecurity.com/la-es/2019/06/05/phishing-activo-reconocido-banco-colombia/

MORGAN, Steve. Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. 2019 [En línea] Disponible en https://cybersecurityventures.com/jobs/

MUNDO HACKER. OWASP – DIRBUSTER. [En línea]. Disponible en https://mundo-hackers.weebly.com/dirbuster.html

NAKED SECURITY. Seguridad activa y seguridad pasiva en equipos informáticos. 2012 [En línea] Disponible en https://news.sophos.com/es-es/2012/09/14/seguridad-activa-y-seguridad-pasiva-en-equipos-informaticos/

OFFENSIVE SECURITY. Why OffSec? [En línea] Disponible en https://www.offensive-security.com/why-offsec/

OSSTMM. OSSTM 3 – The Open Source Security Testing Methodology Manual. 2010.

OWASP. 2017 Top 10. [En línea] Disponible en https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_Top_10

OWASP. Who is the OWASP Foundation? [En línea] Disponible en https://owasp.org/

PEÑUELA VASQUEZ, YINY DAYAN. Análisis E Identificación Del Estado Actual De La Seguridad Informática, Dirigido A Las Organizaciones En Colombia, Que

Brinde Un Diagnóstico General Sobre La Importancia Y Medidas Necesarias Para Proteger El Activo De La Información. Proyecto de Grado Especialista en Seguridad Informática. Fusagasuga.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería. 2018. 60 p. [En línea] Disponible en https://repository.unad.edu.co/bitstream/handle/10596/17260/35254395.pdf?sequence=1&isAllowed=y

PINZÓN, Liliana Carolina, TALERO, MihdíBadí y BOHADA JAIME, John Alexander. Pruebas de intrusión y metodologías abiertas. Ciencia, innovación y tecnología, 1, 25-38. 2013. [En línea] Disponible en https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/120

RAFFINO, María Estela. Red WAN. Argentina. 2018. [En línea] Disponible en https://concepto.de/red-wan/

RAMÍREZ, María Carolina. El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia. 2019. [En línea] Disponible en https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067

RED+. En 2019 se han registrado más de 28 mil ciberataques a las empresas. 2019. [En línea] Disponible en http://www.redmas.com.co/tecnologia/mas-de-28-mil-ciberataques-al-sector-empresarial-se-han-registrado-en-lo-corrido-de-2019/

S., NADAL, M., Victoria. Los malos hábitos de los empleados son una amenaza para la ciberseguridad. 2018. [En línea]. Disponible en https://es.weforum.org/agenda/2018/01/los-malos-habitos-de-los-empleados-son-una-amenaza-para-la-ciberseguridad?utm_content=buffer99fec&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

SAFETYA. PHVA: Procedimiento lógico y por etapas para la mejora continua. 2016. [En línea] Disponible en https://safetya.co/phva-procedimiento-logico-y-por-etapas/

SALAZAR D., Edgar D. Pruebas de Seguridad en aplicaciones web segun OWASP. 2016. [En línea] Disponible en https://www.owasp.org/images/2/2f/OWASP_SUSCERTE.pdf

SANTIAGO, Enrique Javier y SÁNCHEZ ALLENDE, Jesús. Riesgos de ciberseguridad en las empresas. España. 2017. [En línea] Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=6670303

SOPHOS. Informe de amenazas 2019 de SOPHOSLABS. 2020 [En línea] Disponible en https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

TANENBAUM, Andrew S., y WETHERALL, David J. Redes de computadoras. 5ª ed. 2012. México.: Pearson Educación de México, S.A de C.V. 819 p. ISBN 978-607-32-0817-8

TOUS-MULKAY, Abelardo. ¿Cómo deberían afrontar las pymes los riesgos de ciberseguridad? [En línea] Disponible en https://www.finanzaspersonales.co/columnistas/articulo/principales-riesgos-de-ciberseguridad-en-las-pymes/79732

UNIVERSIDAD INTERNACIONAL DE VALENCIA, VIU. Conceptos sobre seguridad lógica informática. 2018. [En línea] Disponible en https://www.universidadviu.com/conceptos-seguridad-logica-informatica/

UNIVERSIDAD INTERNACIONAL DE VALENCIA, VIU. Tres tipos de seguridad informática que debes conocer. 2018. [En línea] Disponible en https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/

VALENCIA BLANCO, Leidi Stefani. Metodologías Ethical Hacking. Bolivia. 2017. [En línea] Disponible en http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a12.pdf

VELOZ, Jorge, *et al*. Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informaticos mediante la herramienta KALI-LINUX. Revista de Tecnologías de la Informática y las Comunicaciones. V1. Nº 1. Año 1. 2017. [En línea] Disponible en https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/view/194/156

VENEGAS LOAIZA, Andrés. Colombia, entre los países de la región en donde las compañías más sufren malware. 2018. [En línea] Disponible en https://www.larepublica.co/internet-economy/colombia-esta-entre-los-paises-en-donde-las-companias-mas-sufren-de-malware-2746737

WORLD ECONOMIC FORUM. This is what the future of cybersecurity will look like. 2017. [En línea] Disponible en https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-against-cyber-attacks-but-the-security-industry-faces-a-huge-challenge

RESUMEN ANALÍTICO ESPECIALIZADO

Fecha de Realización:	22/05/2020
Programa:	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Línea de Investigación:	INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD EN REDES
Título:	ESTUDIO DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES DE COLOMBIA
Autor(es):	GONZALEZ LONDOÑO JEFFERSON
Palabras Claves:	Redes, Ciberseguridad, seguridad, Pentest
Descripción:	La presente monografía brinda al lector un panorama general sobre la situación actual en materia de ciberseguridad en las empresas de Colombia, los principales cibercrímenes que las afectan y los hábitos que de forma negativa contribuyen a la expansión de este tipo de actividades. A partir del panorama entregado como primer objetivo, se entrega al lector una descripción de las principales metodologías de hacking ético y que siendo implementadas pueden contribuir a mitigar muchas de las brechas de seguridad. El desarrollo del tercer objetivo se centra en la presentación de pruebas de análisis de vulnerabilidades aplicables a través de la cual se pueden establecer controles de mejora de los diferentes componentes de un sistema de información.

Fuentes bibliográficas destacadas:

CCIT. Informe de las tendencias del cibercrimen en Colombia 2019-2020. 2019. [En línea]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

GUISTO BILIC, Denise. Las amenazas informáticas que más afectaron a los países de América Latina. 2019. [En línea] Disponible en https://www.welivesecurity.com/la-es/2019/01/10/amenazas-informaticas-mas-afectaron-paises-america-latina/

MORGAN, Steve. Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. 2019 [En línea] Disponible en https://cybersecurityventures.com/jobs/

S., NADAL, M., Victoria. Los malos hábitos de los empleados son una amenaza para la ciberseguridad. 2018. [En línea]. Disponible en https://es.weforum.org/agenda/2018/01/los-malos-habitos-de-los-empleados-son-una-amenaza-para-la-

ciberseguridad?utm_content=buffer99fec&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
SOPHOS. Informe de amenazas 2019 de SOPHOSLABS. 2020 [En línea] Disponible en https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf
VELOZ, Jorge, et al. Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informaticos mediante la herramienta KALI-LINUX. Revista de Tecnologías de la Informática y las Comunicaciones. V1. Nº 1. Año 1. 2017. [En línea] Disponible en https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/view/194/156

Contenido del documento:	

Conceptos adquiridos:	El desarrollo de la monografía permitió adquirir o reforzar los conceptos relacionados con el cibercrimen en especial lo relacionado con el impacto que este genera en los diferentes países del mundo y en mayor detalle, en Colombia. Las pérdidas económicas que estas actividades generan ascienden a cientos de millones y la lucha por su contención aumenta cada día. El entorno también permitió reforzar los conceptos de pentesting en un entorno LAN con diversos dispositivos y servicios activos, permitiendo realizar un análisis y evidenciar posibles mejoras que contribuyan a cerrar brechas.
Conclusiones:	Las tecnologías de información y su constante expansión han permitido a los criminales tener un mayor número de posibles objetivos. Las empresas en Colombia son blanco frecuente de este tipo de delincuentes, siendo el factor humano, uno de los más determinantes y más aprovechado por los cibercriminales para cumplir con su objetivo. Teniendo en cuenta que no se puede garantizar la seguridad de un sistema en un 100%, se pueden implementar mecanismos que permitan detectar de forma temprana brechas que pongan en riesgo un sistema informático.