ANÁLISIS DE METODOLOGÍAS DE ETHICAL HACKING PARA LA DETECCIÓN DE VULNERABILIDADES EN LAS PYMES

CRISTIAN CAMILO PENAGOS MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD.
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA.
MEDELLIN
2019

ANALISIS DE METODOLOGÍAS DE ETICAL HACKING PARA LA DETECCIÓN DE VULNERABILIDADES EN LAS PYMES

CRISTIAN CAMILO PENAGOS MUÑOZ.

Monografía para optar al título de: Especialista en Seguridad Informática.

Asesor
YOLIMA MERCADO PALENCIA
Ingeniero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD.
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA.
MEDELLIN
2019

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Medellín, 24 de Julio de 2019

TITULO

ANALISIS DE METODOLOGÍAS DE ETHICAL HACKING PARA LA DETECCIÓN DE VULNERABILIDADES EN LAS PYMES

DEDICATORIA.

A mi esposa Clara y a mis enanos; Martin y Violeta, por entender, acompañar, y esperar el momento indicado para compartir.

Martin y Violeta, son motores especiales de vida, y para ellos mi dedicación, esfuerzo y amor.

Clara es incondicional, comprometida, incansable, inteligente y amorosa, por eso y más, está y estará siempre en mi vida.

…De algún lado en la vida entendí que lo más importante es la familia…ellos son la mía y para ellos todo lo que tengo y todo lo que soy.

Gracias Familia.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

AMENAZAS: una acción externa o interna a un sistema de información, que puede explotar o materializar una vulnerabilidad existente.

ATAQUES INFORMÁTICOS: acción por la cual, un delincuente informático, intenta ejercer control, extraer información o alterar la misma de un sistema informático sin ningún tipo de autorización legal.

CIBERATAQUES: ataques informático con intensión de ejercer control, alterar o extraer información de un sistema informático, normalmente ejercido desde o en un sistema de procesamientos de datos desde internet.

CONFIDENCIALIDAD: posibilidad de acceso a la información, única y exclusivamente por las personas interesadas o autorizadas en su contenido.

DISPONIBILIDAD: la capacidad de mantener disponible para su uso, una infraestructura o una información cuando el usuario o propietario lo requiera.

ETICAL HACKING: describe una práctica de ingeniería, que se basa en el uso de metodologías de ataque a sistemas de información e infraestructuras tecnologías, para lograr entender y mejorar las condiciones de seguridad.

FALENCIAS TECNOLÓGICAS: son problemas normalmente en entornos tecnológicos, que denotan falta de algún control o de alguna solución complementaria, y que su ausencia puede derivar en vulnerabilidades en los sistemas de información y las arquitecturas dispuestas.

INTEGRIDAD: capacidad de conservación de los datos en una forma definida durante un tiempo determinado dentro de un sistema de información.

METODOLOGÍA: hace referencia a las metodologías empleadas en los procesos de evaluación del de vulnerabilidades y estudios de seguridad informática o seguridad de la información.

MINTIC: ministerio de tecnologías de Información y comunicaciones de Colombia.

PYMES: sigla que describe un segmento empresarial, conocido como Pequeñas y Medianas Empresas, es aplicado en el presente documento a las empresas objetivo.

SEGURIDAD DE LA INFORMACION: procesos y procedimientos enfocados a la protección de la información y su conservación de integridad, confidencialidad y disponibilidad necesarias.

SEGURIDAD INFORMATICA: conjunto de herramientas de hardware y software, destinadas a la protección de la infraestructuras tecnológica empresarial dispuesta para los proceso de negocio.

VULNERABILIDADES: las vulnerabilidades son puntos débiles de un sistema de información que pueden permitir la materialización de una amenaza hacia el sistema involucrado.

INTRODUCCION.

Las metodologías de Etical Hacking, más allá de tener la imagen de ser usadas para cometer delitos o para generar ataques contra la información de las empresas y las personas, es principalmente utilizada en la industria de la seguridad, para la evaluación e identificación de las vulnerabilidades de los sistemas de información, arquitecturas tecnológicas empresariales y hasta en los activos de información dispuestos en estas.

Las metodologías de Etical hacking, más algunas técnicas conocidas, han hecho que el mundo de la seguridad, se vea como la parte oscura de las tecnologías de la información y las comunicaciones, por esto, algunas empresas y profesionales de TIC se han alejado de sus prácticas, esto aunado al desconocimiento en temas de seguridad defensiva, han dejado algunas empresas, con falencias de seguridad en sus infraestructuras, sumado que nunca han evaluado su nivel de vulnerabilidad o no cuentan con personal que pueda implementar unas mínimas condiciones de seguridad en sus negocios o empresas.

A nivel de pequeñas y medianas empresas, la situación es más notoria, pues es un sector, que no permite desarrollar grandes inversiones en el medio tecnológico enfocadas a la seguridad de la información, también es cierto, el capital que podrían destinan a ello, lo invierten en suplir las necesidades básicas de productos y servicios de funcionamiento y las necesidades de seguridad no están dentro de la parrilla de necesidades, algunas veces aparece como iniciativa de su personal de TI, pero en otras, ni siquiera estos, las tienen en cuenta.

Es así, como para el desarrollo del presente trabajo de investigación, se tomó como punto de partida, esa necesidad de las pequeñas y medianas empresas de mejorar sus esquemas de seguridad, pero principalmente, de conocer, el estado actual de sus infraestructuras tecnologías de cara a conocer, que tan vulnerables son en sus procesos de negocio en términos de seguridad informática o seguridad de la información.

Cada empresa es un universo distinto, en el cual, los comportamientos desde el ámbito tecnológico pueden variar, desde la cantidad de usuarios que tenga, pasando por si cuentan con servicios tecnológicos publicados en internet, hasta la complejidad o no de sus infraestructuras. Estos factores convierten a las pequeñas y medianas empresas, en un universo objetivo para los ciberdelincuentes, que siempre y cuando, no encuentren que o quienes haga frente en las organizaciones,

van a terminar perjudicando a las empresas en cualquier frente, que finalmente, terminara reflejándose en el tema económico de cada una de ellas.

Para ello, se puede hablar de que, hacer frente a estas necesidades de protección, si es de la parrilla de necesidades, aunque con diferenciación en la operación o el objeto social del negocio, cada una de las metodologías de análisis de vulnerabilidades, están prestas a identificar con sus procesos metodológicos, como es posible proteger o salvaguardar cada uno de estos escenarios distintos de la industria Colombiana.

Implementar metodologías de Etical Hacking, Pentesting o análisis de vulnerabilidades, es una forma de iniciar en la batalla por mejorar la seguridad, y se dice iniciar, porque después de un buen análisis, debe ir la implementación de controles o políticas de seguridad a nivel corporativo, que permitan mitigar o reducir los riesgos asociados a esas vulnerabilidades encontradas.

Con todo esto, se va a iniciar en un proceso de análisis de metodologías de Etical Hacking que permita identificar la mejor o la más ajustada a los entornos corporativos de pequeñas y medianas empresas en Colombia, y que a su vez, pueda ser implementada de forma ágil, productiva y económica, ya que esas tres condiciones; la agilidad, la productividad y el bajo costo en la implementación, llevan a ser pueda ser la puerta de entrada en la empresa, de una cultura de seguridad de la información o seguridad informática, por esto, es de vital importancia, desarrollar un trabajo investigativo con el solo objetivo de poder aportar a la mejora de la seguridad informática y seguridad de la información de las empresas del sector productivo definido.

1. DEFINICION DEL PROBLEMA

La seguridad de la información no es una tema del todo aparecido en los últimos años o en las últimas décadas, históricamente, la necesidad de protección en términos de seguridad ha hecho que se implementen diferentes métodos para lograrlo, estos métodos, van desde la seguridad física y hoy se podría decir, que han llegado a la seguridad de los sistemas de información con una gran prioridad.

Hace un poco más de treinta años, los servicios de internet y telecomunicaciones no estaban lo suficientemente maduros, como para pensar enfáticamente en temas de seguridad informática, y aunque ya se trataban estos temas, no existía una situación marcada significativamente a nivel de riesgos de seguridad para las empresas, más porque no estaba masificado el concepto tecnológico dentro de las organizaciones. Aun, se trataba con medios diferenciados, alejados del mundo de la informática, y solo hasta ese entonces hacen sus apariciones, los primeros sistemas operativos comerciales y de cara a una interfaz gráfica de usuario, donde ya empezaron a brotar temas de confidencialidad y de seguridad de los datos, haciendo con esto, unos inicios silenciosos en temas de seguridad. Para las pequeñas y medianas empresas, esta acción pudo ser casi imperceptible, pues no contaban con los medios tecnológicos para poderlo evidenciar.

En la actualidad, las empresas colombianas, deben contar con una inversión en tecnología, que las obliga a estar al día en temas de seguridad, si no cuentan con grandes inversiones en TI como es el caso de las pequeñas y medianas empresa, inevitablemente están obligadas a tratar con las grandes apuestas tecnológicas de miles de empresas que si le apuestan de manera fuerte a la inversión en seguridad y altos niveles tecnológicos.

Esto hace, que de una u otra manera, las empresas del sector pyme, estén enfrentándose a los retos de la seguridad informática o seguridad de la información, por lo cual, es muy difícil, no contemplar que estas, deban hacer parte fundamental de las oportunidades de protección para la seguridad informática, que también vienen desde el área de tecnología y que, aunque estas no cuenten con grandes inversiones, esos pequeños aportes en tecnología, que les permiten o les obligan a interactuar con grandes sistemas informáticos corporativos, tanto públicos como privados, necesiten de una gestión oportuna de seguridad para la protección tanto de su información, como la información de sus clientes y partes interesadas.

La implementación de medidas de seguridad de la información, iniciando con la aplicación de metodologías para la evaluación y gestión de vulnerabilidades, va a

representar en un futuro, parte importante de la inversión de las empresas de forma que se convierta en una necesidad de primer orden al momento de pensar en cómo comunicarse, como enviar y recibir información, incluso, en cómo controlar de una forma efectiva el acceso a la información de su compañía para cada usuario que la utilice.

Es importante y se hace urgente, que cada una de las empresas, pertenecientes al sector objetivo, el sector de las pequeñas y medianas empresas, ingresen al medio de la seguridad de la información como un medio de protección, tanto de su información como de sus activos, y que lo contemplen, como uno de las premisas para poder subsistir dentro de un mercado, cada día más volcado a los servicios en internet y que necesitan que se implementen medidas de seguridad para la interacción con los demás actores del entorno.

Implementar desde ahora, herramientas y metodologías que permitan conocer el verdadero estado de la seguridad de las organizaciones, develando sus vulnerabilidades, va a ser un aporte muy significativo, en el inicio de la implementación de salvaguardas y controles de seguridad de la información o de seguridad informática, que permitan mantenerse y llegar con una visión clara de seguridad a etapas más maduras de intercambio de datos a través de plataformas tecnológicas, actuales y futuras. También, la implementación de metodologías, puede acercar a las empresas del sector objetivo a mantener cultura de seguridad al interior como protección tanto de sus patrimonios, como de la información propia de sus clientes y demás partes interesadas.

Como iniciar siempre es difícil, y más cuando se tiene de frente la necesidad de cara a los altos costos de implementación, es factible considerar el conocimiento previo de las necesidades reales de seguridad dentro del entorno corporativo. Aquí, conocer las debilidades corporativas en seguridad, vistas estas desde el punto de vista de cuáles son las principales amenazas y las vulnerabilidades a las que se expone cada compañía, puede incluso, cambiar la óptica de los empresarios y enfocar una mirada fija en la consecución de la protección de la información. Visto esto también, como la protección de su negocio.

Como existen vulnerabilidades también se puede hablar de las amenazas a las cuales están expuestas las empresas cuando cuentan con sistemas de información en sus organizaciones. Conocerlas requiere saber identificarlas y diferenciar cuando se habla de amenaza y cuando se habla de vulnerabilidad. Para ello, necesariamente se requiere tener una definición clara para estas. Cuando se habla de vulnerabilidad, básicamente puede definirse como una debilidad o falla que se

encuentra en alguno de los sistemas de información o activos de información de la compañía, esto incluye, software, hardware, infraestructura física y hasta personal vinculado entre otras clasificaciones. Cuando se habla de amenazas, se debe identificar, que son normalmente, agentes externos, que generen acciones enfocadas o no a explotar o aprovechar las vulnerabilidades dentro de la organización, estas amenazas, pueden provenir de agentes dirigidos como ataques externos, factores naturales conocidos y en muchos casos, negligencia de parte de los empleados en el manejo de la información entre otras clasificaciones.

Conociendo las amenazas y vulnerabilidades, las pequeñas y medianas empresas, van a llegar a encontrar un concepto, seguramente nuevo para ellas, y es, empezar a hablar de riesgos, de la probabilidad de que se produzca un incidente de seguridad o también la incertidumbre sobre un riesgo de la explotación de una de sus vulnerabilidades, que puede terminar en la pérdida o daño, parcial o total de la información de la empresa.

Todo esto, va a llevar a que las empresas del sector objetivo vean con más premisa la necesidad de conocer sus debilidades para de alguna forma, tratar de atacarlas con el objetivo de salvaguardar la integridad de su información y con ello, mantener su negocio vigente.

FORMULACION DEL PROBLEMA

¿Cuál es la metodología de Etical Hacking más apropiada para aplicar un análisis de vulnerabilidades al sector de pequeñas y medianas empresas en Colombia?

2. JUSTIFICACION

Se visualiza critico el panorama de seguridad a nivel de informática para las empresas del sector pymes en Colombia, “Cuatro de cada diez empresas en el país, no están preparadas para un ciberataque” [1] es fácil inferir, que las empresas Colombianas del sector pymes, están tratando de hacer frente a la compleja situación de seguridad informática, con herramientas tecnológicas obsoletas por su falta de inversión en tecnología adecuada [2] que pueda reducir los riesgos asociados a las múltiples amenazas de hoy, que a diario enfrentan estas compañías en el mundo exterior del internet. Peor aún, sin conocer sus propias vulnerabilidades, exponen servicios en internet y entregan accesos a servicios por medio de sus ISP a sus usuarios internos y externos sin ningún tipo de consideración de seguridad, exponiéndose cada vez más, a la materialización de amenazas que pueden no saber que existan.

Esta ignorancia de vulnerabilidades, aunado a la continua amenaza de ataques informáticos, convierten a las pymes, en un blanco fácil para los ciberatacantes dadas las condiciones de cada una de ellas, que hacen, que el trabajo de la ciberdelincuencia, se haga más fácil y comprometa mucho más la estabilidad de la información y las empresas del sector. Para Fortinet, una reconocida empresa del sector de la seguridad informática, halló que el 80% de las empresas en Colombia, son vulnerables a ataques informáticos. “Nuno Mantinhas, vicepresidente de Fortinet para el Caribe y Latinoamérica, aseguró que aunque la cifra parece alarmante, tal vez lo peor es que el otro 20 por ciento restante no posee un cifrado de su información destacable, sino intermedio, de la cual hacen parte las entidades gubernamentales.” [3]

El panorama nacional en cuanto a seguridad de la información, ha interesado a muchos, y aunque desde hace muchos años, el sector empresarial presenta dificultades dentro de las empresas por las mismas falencias y ataques cibernéticos,

---

[1] Portafolio, Cuatro de cada diez empresas en el país no están preparadas para un ciberataque. [En línea], 10 de Marzo de 2016, Disponible en: < http://www.portafolio.co/negocios/empresas/ciberataque-empresas-preparadas-colombia-492281 >

[2] Dinero, Las Empresas, combaten los ataques informáticos con tecnología obsoleta, [En línea], 29 de Enero de 2016, Disponible en: < http://www.dinero.com/empresas/tecnologia/articulo/informe-de-seguridad-de-cisco-2015-sobre-seguridad-informatica/218610 >

[3] CONTRERAS. Nicolás, Más del 80% de las compañías en Colombia, son vulnerables a ataques informáticos, [En línea] 09 de Junio de 2016, Disponible en: < http://caracol.com.co/radio/2016/06/09/tecnologia/1465469190_389745.html>

solo hasta el año 2016, “En Washington D.C. el Ministerio de Tecnologías de la Información y las Comunicaciones suscribió un convenio de cooperación con la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), para adelantar un estudio sobre el impacto que han tenido los incidentes cibernéticos en Colombia. La firma la realizaron el Embajador Andrés González, representante permanente de Colombia ante la OEA y Luis Almagro, Secretario General de la OEA.” [4], los esfuerzos continúan siendo menores de cara a poder llegar al sector pymes, y esto motiva la presente investigación, donde se pretende resolver un interrogante fundamental que deja todo este planteamiento, ¿Cómo pueden las empresas del sector pymes, reducir los riesgos asociados con la informática y proteger con sus propios recursos de forma proactiva y con bajos niveles de inversión la seguridad de sus activos de información,?. Esta pregunta se quiere resolver a través del desarrollo de la presente monografía, en la cual, con apoyo de los diferentes materiales existentes, referentes a metodologías válidas para identificación de vulnerabilidades y una cantidad de herramientas disponibles para el desarrollo de procesos de Ethical Hacking, se haga un aporte valioso a las pymes, que les permita fortalecer de forma proactiva la seguridad de sus activos de información en las empresas.

En los eventos conocidos, desatados en los últimos meses, se pudo conocer afectaciones por ciberataques, tales como WananCry, qua tocaron empresas de gran magnitud como Telefónica y a través de esta, llegó a afectar varias empresas colombianas, de las cuales, por razones de nombres, no fueron expuestas abiertamente a la opinión pública y sobre las cuales, “Juanita Rodríguez, directora de Estándares y Arquitectura del MinTic, aclaró que estas son las empresas que han pedido ayuda.” [5]. dentro de la aclaración, la funcionaria admitió, que sí encontraron afectaciones en empresas Colombianas.

Mencionado lo anterior, se deja expuesta la necesidad de apoyar, de la forma más oportuna posible, la gestión de riesgos informáticos al interior de las empresas, iniciando con poder conocer sus vulnerabilidades, aplicando alguna metodología valida de forma proactiva como mecanismo de prevención y protección de los activos de información.

---

[4] MINTIC, MinTIC y OEA firman convenio para conocer el impacto de los incidentes cibernéticos en el país, [En línea], 22 DE Julio de 2016, Disponible en: < http://www.mintic.gov.co/portal/604/w3-article-15753.html >

[5] Caracol Radio, 10 empresas colombianas y una entidad estatal afectadas por ciberataque, [En línea], 13 de Mayo de 2017, Disponible en: < http://caracol.com.co/radio/2017/05/13/tecnologia/1494700226_689517.html >

Realizar un análisis de vulnerabilidades en cualquier empresa del sector de pymes en Colombia, va a permitir el inicio del cierre de las brechas de seguridad de la información, que actualmente, muchas de ellas sin conocerlas, hacen frente sin saber el cómo, en un escenario propio pero desconocido, poniendo en riesgo sin saberlo, la integridad de su información y la continuidad de sus negocios, y tras ellos, la estabilidad económica de miles de familias en todo el territorio nacional.

Conocer las vulnerabilidades, le va a permitir a las empresas del sector, definir un plan de implementación bajo la necesidad básica de prevención, asociada a los riesgos que con estos resultados se puedan identificar. Esto a su vez, permite iniciar un camino a la transformación digital de las mismas, hablando de temas de seguridad. Desde ahí van a encontrar oportunidades de diversificar sus negocios al contar con la posibilidad de usar servicios de las TICS, es así, como se impulsan procesos de E-Commerce, que "En el marco del Día Internacional de la Seguridad Informática, que se celebra el 30 de noviembre en Colombia y en más de 40 países, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en asocio con la Organización de Estados Americanos (OEA), llevó a cabo el taller 'Beneficios al hacer negocios en Internet de manera segura'."[6] . Es aquí, donde una temprana intervención para la adopción de procesos de seguridad de la información, le va a permitir a las pymes, incursionar con mayor facilidad en proyectos de orden público y privado, que les permiten su crecimiento en el orden nacional e internacional.

El desarrollo de la presente propuesta monográfica, entregará múltiples beneficios a las empresas del sector objetivo, algunos de esos, se podrán ver reflejados en el impulso a la adopción de nuevos negocios a través del uso seguro de las Tecnologías de la Información y las Comunicaciones TICs.

También se pretende abrir la visión de las empresas a la utilización segura de herramientas tecnologías, y permitir que al país sigan llegando oportunidades de capacitación a las empresas Colombianas, en este orden, "La Organización de Estados Americanos (OEA), la Fundación ICT4Peace, en colaboración con MinTIC, organizo el taller "Seguridad Internacional y Diplomacia en el ciberespacio", que se desarrolló en Bogotá del 18 al 20 de noviembre del 2014. Los dos primeros días del evento se familiarizo a servidores públicos encargados de asuntos de diplomacia en

[6] MINTIC, Las Mipyme se actualizan en el Día Internacional de la Seguridad Informática, [En línea], 30 DE Noviember de 2016, Disponible en: < http://www.mintic.gov.co/portal/604/w3-article-22318.html,>

seguridad cibernética y del desarrollo de políticas en torno al tema.” [7] , aquí, se trató de generar un impacto positivo, económico y social dado por la percepción de seguridad y de mejora en los procesos tecnológicos de cada organización.

[7] MINTIC, Taller sobre "Seguridad Internacional y Diplomacia en el Ciberespacio", [En línea], 07 DE Noviembre de 2014, Disponible en: < http://www.mintic.gov.co/portal/604/w3-article-7696.html >

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Documentar una metodología de Ethical Hacking existente, apropiada para la identificación oportuna de vulnerabilidades de seguridad en pequeñas y medianas empresas.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar metodologías de Ethical Hacking para ser aplicadas en entornos corporativos pymes.
- Describir amenazas y exposición en entornos corporativos del sector pymes para identificación de herramientas de pentesting necesarias.
- Detallar herramientas útiles para la ejecución de pruebas de penetración en las pymes asociado a metodologías referidas.
- Proponer una metodología conocida de Ethical Hacking, apropiada para la implementación de pruebas de seguridad en las pymes.

4. METODOLOGIA.

Para el desarrollo de la presente monografía, se va a utilizar una metodología de trabajo definida por etapas o fases, las cuales se definen a continuación.

Luego de la definición del tema, se plantea desarrollar un trabajo de investigación referenciada sobre el tema planteado, el cual, pretende hacer un análisis de varias metodologías existentes y que al final, se pueda hacer una recomendación concreta y sustentada de una de ellas para ser aplicada en un entorno corporativo de pequeñas y medianas empresas en Colombia. Las fases definidas para la monografía son:

- **Primera Fase, identificación de Metodologías.**

En la Identificación de metodologías existentes. Hacer una referenciación de la documentación, dando a conocer las generalidades de cada una de ellas y dejando claro el modo de aplicación de cada uno y su uso específico según sea desarrollada, esta fase, va a entregar una información concreta de las metodologías, que pueda ser fácilmente identificable para la ubicación de esta en un uso más acertado en temas de seguridad informática y seguridad de la información.

- **Segunda Fase, Identificación de amenazas.**

Para la Identificación de amenazas y vulnerabilidades. Se va a tratar de identificar las amenazas y las vulnerabilidades más comunes de las empresas del entorno empresarial objetivo, estas amenazas y vulnerabilidades, salen principalmente de la experiencia del autor y la documentación de fabricantes de equipos y software de seguridad, lo cual va a encaminar la documentación hacia las herramientas que posiblemente se puedan usar.

- **Tercera Fase, Herramientas y metodologías.**

Consolidación de herramientas aplicables a las metodologías. Se hará la documentación de múltiples herramientas que sean utilizadas dentro de cada metodología. Con esta documentación, se podrá definir según el alcance, y su aplicabilidad, una o algunas herramientas a ser utilizadas en un entorno definido de pequeñas y medianas empresa. Estas herramientas, van a marcar una parte importante del camino en la definición de la herramienta metodológica más apropiada para el sector.

- **Cuarta Fase, Recomendación.**

Con base en las fases anteriores, con sustento en la documentación referenciada y apoyada en la disponibilidad de herramientas de cada metodología, se va a recomendar una metodología con sus herramientas y modo de uso, para la aplicación de análisis de vulnerabilidades en las pequeñas y medianas empresas, esta recomendación final, hace parte integral de la monografía, de la cual, se espera, sea útil como medio de consulta y referenciación para la aplicación en los entornos productivos mencionados y que su aplicación, permita la identificación y gestión oportuna de amenazas y vulnerabilidades, para que las empresas, puedan mantener, la integridad, disponibilidad y confidencialidad de la información, implementando procesos y procedimientos de seguridad informática y seguridad de la información en sus entornos empresariales.

5. MARCO DE REFERENCIA

5.1. MARCO TEORICO.

Las pymes Colombianas, se encuentran reconocidas entre las cuatro principales[8] de Latinoamérica, al lado de Brasil, Argentina y México, estas empresas en Colombia, sostienen que dentro de sus principales retos durante los últimos dos años, ha sido mantener sus negocios e incrementar las rentabilidades y reconocen a las TICS, como un medio de crecimiento importante dentro de la región, los cuales les permitan, expandir sus negocios fuera del territorio nacional, para esto, indican que es de vital importancia encontrar más clientes, lo cual para ellos es mucho más fácil haciendo uso de las redes sociales y aplicaciones emergentes desde internet, esta práctica, por ende, les genera altos niveles de exposición para la seguridad de su información.

Algunas empresas a nivel regional y mundial exponen estudios y encuestas tratando de descifrar las necesidades de las pymes y allí, siempre sale a flote, el uso o la necesidad de las TICS en el desarrollo de sus negocios. "El sondeo, llamado 'Future of Business Survey' (Encuesta sobre el Futuro de los Negocios) ofrece una nueva perspectiva sobre cómo las pequeñas y medianas empresas ven el mundo, el panorama de negocios y el nivel de confianza de los próximos meses. Los datos recolectados en esta encuesta se consiguieron a través de más de 100.000 pymes de 22 países que están en Facebook. Diego Dzodan, vicepresidente de Facebook para América Latina, considera que Facebook ofrece una "mirada única sobre cómo los pequeños y medianos empresarios ven el ambiente de negocios y las perspectivas de la economía"[9]. En estos resultados, se puede ver como las pymes hacen uso continuo de redes sociales, principalmente, cuando quieren realizar publicidad de sus productos y hasta mencionan el uso de mensajería instantánea WhattsApp, como uno de sus principales canales de comunicación para generar o definir negocios de sus productos y servicios.

También existe un crecimiento en los usos de comercio electrónico dado por las

[8] ANGULO. Susana, LAS PYMES COLOMBIANAS TIENEN BUENAS EXPECTATIVAS SOBRE SU FUTURO, [En línea], 30 de Septiembre de 2016, Disponible en: < http://www.enter.co/especiales/claro-negocios/las-pymes-colombianas-tienen-buenas-expectativas-sobre-su-futuro/ >

[9] ANGULO. Susana, LAS PYMES COLOMBIANAS TIENEN BUENAS EXPECTATIVAS SOBRE SU FUTURO, [En línea], 30 de Septiembre de 2016, Disponible en: < http://www.enter.co/especiales/claro-negocios/las-pymes-colombianas-tienen-buenas-expectativas-sobre-su-futuro/ >

empresas del sector Pymes en el territorio colombiano, lo cual, deja ver un crecimiento pegado de la media del promedio global, esto indica que en Colombia, estas empresas si hacen uso continuo de las TICs para desarrollar sus negocios y poner en funcionamiento sus empresas en términos de exportaciones principalmente. Hablando del mercado Latinoamericano en cuanto a pymes, América Latina es el principal mercado para productos colombianos que son exportados por las pymes, siendo México y Ecuador los principales compradores, seguidos por Venezuela y Brasil. Así también, el 33% de las pymes exportadoras colombianas, tienen a México como su principal mercado objetivo. Corroborando esto, FedEx, como un proveedor de primera mano, adelanto un estudio[10], en el que da a conocer cifras muy importantes del sector Pyme en Latinoamérica incluida Colombia, que dejan ver que estas, cada vez más hacen uso de herramientas tecnologías en internet para mover sus negocios.

Por otro lado las pymes, reconocen que aumentar el uso de las herramientas tecnológicas, va a hacer crecer sus negocio, "las pymes deben buscar la adopción de nuevas tecnologías y una cadena de suministro eficiente. Las innovaciones adoptadas con más frecuencia, que probablemente llegarán a una audiencia de pymes más amplia en los próximos años, incluyen oficinas conectadas (28%), Internet de las Cosas (23%) y wearables de oficina (21%). Cuando se trata de la idea de apropiar tecnología de vehículos sin conductor, las pymes se muestran menos receptivas." [11] todos estos procesos, deben ir acompañados de implementaciones en temas de seguridad, ya que no es suficiente adoptar tecnologías desde la necesidad de los proveedores, cuando estas empresas van a exponer productos y servicio en internet. En este sentido, las empresas de mayor musculo económico o algunas prestadoras de servicios para las Pymes, ofrecen soluciones tecnológicas, las cuales les prestan mayor reconocimiento y exposición de sus mercados, pero pocas veces, ofrecen condiciones mínimas de seguridad para los entornos corporativos, lo cual, tampoco es un servicio asociado a estas, pero que por desconocimiento de ambas, se van creando grandes necesidades en la ciberseguridad, porque que no se conoce el nivel de exposición y en casos de adopción de tecnologías, se van a ir incrementando soluciones tanto de software como de hardware en las empresas, que crean y vuelven cada vez más grande la

[10] Fedex, Oportunidades para las PyMEs en el mercado internacional, [En Línea], Septiembre de 2015, Disponible en: < http://images.fedex.com/downloads/lac/global/infografico_esp_final.pdf >

[11] LUZARDO. Ana Maria, ECONOMÍA DIGITAL GENERA POSITIVISMO EN LAS PYMES COLOMBIANAS, ¿Qué oportunidades representa la economía digital para las pymes?, [En línea], 20 de Febrero de 2017, Disponible en: < http://www.enter.co/especiales/empresas-del-futuro/economia-digital-genera-positivismo-en-las-pymes-colombianas/ >

brecha de las empresas entre tener una infraestructura tecnológica robusta que apoye la gestión de sus empresas y tener una infraestructura robusta para el mismo fin, pero más segura.

"Los riesgos que corren los departamentos de T.I., y la dirección de las empresas relacionados con pérdidas de información son cada vez mayores. El diseño de un plan de seguridad de datos proporciona el conocimiento necesario para la gestión de ese riesgo y para mantenerse dentro de la legalidad."[12] En Estados Unidos, la cantidad de crímenes informáticos en una constante reflejada en las empresas de todo tipo, y en las cuales se ven descritas unas cifras verdaderamente comprometedoras, tanto a nivel gobierno como a nivel privado, ellas simplemente denotan una falencia en los esfuerzos por contener o desde otro punto de vista, una superioridad de fuerza de los ciberdelincuentes en contra de las estructuras de gobierno y de empresas privadas, esto se puede ilustrar con que un 85% de las empresas estadounidenses, han estado comprometidas en por lo menos una fuga de información.

Por el lado de Colombia y Latinoamérica, el panorama no es más alentador, "Colombia participó con el 8,05% del total de los delitos informáticos de América Latina, lo que equivale a pérdidas por más de US$6.179 millones." [13] Desde las fugas de información, las empresas han identificado que existe una mano negra dentro de las mismas, orquestada por los mismos empleados, principalmente descontentos, que buscan a toda costa, hacerse a información confidencial valiosa, esto junto a la escasez de controles en seguridad permiten que las empresas dobleguen diariamente ante las fugas de información sin conocer los focos o vectores asociados a ellos.

Dentro de los controles de seguridad de la información para las empresas, se debe tener presente, evitar la pérdida de documentos con la aplicación de controles de seguridad asociados a la posible manipulación de información de los empleados dentro de las mismas. Normalmente, las empresas cuentan con personal de confianza en el manejo de su información para la gestión empresarial, y desde la confianza de estos, se olvidan de la protección, que en la mayoría de los casos, hay que aplicar sobre esos funcionarios.

---

[12] JIMENO. Pablo, Seguridad en la información, [En línea], 06 de Noviembre de 2012, Disponible en: < https://news.sophos.com/es-es/2012/11/06/seguridad-en-la-informacion/ >

[13] Dinero.co, Los sectores económicos más impactados por el cibercrimen en Colombia, [En línea], 26 de Septiembre de 2017, Disponible en: < http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321 >

Todo el tema de la vulneración o vulnerabilidad de las personas dentro de las empresas con relación a la información, ha tomado grandes dimensiones, desde la definición del llamado eslabón más débil de la cadena de seguridad, se ha dicho por muchos expertos, que ante la falencia humana, no hay ningún sistema que pueda evitar una extracción de información o vulneración de sistemas, desde usuarios de bajo nivel y bajo acceso en la organización, hasta los más altos directivos, pueden ser víctimas de una planeada y exacta ingeniería social o pesca de información. Frente a esto, marcas reconocidas como Sophos, plantean mecanismos de encripción de información, los cuales, no parecen ser muy usados por las empresa en los diferentes sectores industriales, en los países donde este fabricante tiene influencia, lo que denota que existe un problema internacional que abarca la compleja situación local, en países como Colombia, donde su nivel adquisitivo, nivel de pymes y la cultura de seguridad está menos forjada que en algunos países desarrollados.

Con relación a las pymes, Sophos lanza una encuesta donde se evidencian las principales falencias de empresas de mediano tamaño o pymes, por el no aprovechamiento de tecnologías de encripcion. Iniciando el informe menciona que, "*44% of organizations are making extensive use of encryption to secure their data and a further 43% are encrypting to some degree. That may sound like a reasonable number, but if you consider that over 700 million records were compromised in 2014; then add in numerous high-profile breaches such as Sony, Experian, KBox and the Japan Pension Service where sensitive data wasn't always encrypted, the problem starts to become clear. Further divisions emerge when comparing encryption levels in companies of different sizes. Only 38% of smaller organizations (100-500 employees) are encrypting extensively, compared with 50% of larger organizations (501-2,000 employees). According to a 2014 Verizon reportii, 53% of confirmed data loss incidents were in organizations of less than 1000 users."* [14]

Las empresas encuestadas, manifiestan múltiples razones para no tener implementadas herramientas de encripcion y de las múltiples razones se pueden destacar tres de ellas y una particularmente aplicada y repetitiva en el sector de las pymes, los costos de inversión. Las otras son desconocimiento y complejidad en la implementación, lo cual puede resultar no cierto, dado que se sabe de herramientas de fácil implementación, muy comunes en el mercado y que presentan costo a nivel de cada tamaño de empresa que finalmente terminan siendo bajos en su inversión.

[14] Sophos, The State of Encryption Today. Results of an independent survey of 1700 IT managers, [En linea], Diciembre de 2015, Disponible en: < https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/the-state-of-encryption-today-wpna.ashx?la=es-ES >

La encuesta “The State of Encryption Today” realizada por Sophos confirma que, si bien el cifrado está siendo ampliamente utilizado y aceptado por las empresas, también pone de manifiesto deficiencias críticas. "Desafortunadamente, no hay sorpresa por los resultados ya que aún demasiadas personas creen de forma errónea que el cifrado es demasiado complicado o costoso de implementar. La realidad es que, las soluciones de cifrado modernas de última generación pueden ser fáciles de desplegar y muy rentables”. [15]
Sobre las herramientas se puede decir, que existe una gran variedad que pueden apoyar el proceso de investigación, para mencionar solo algunas, podríamos iniciar diciendo que se encuentran, desde análisis de puertos, hasta análisis extensivos de bases de datos, como SQLMap [16] La cual se emplea en pruebas automáticas de SQLInjection, esto, para tratar de detectar y aprovechar alguna vulnerabilidad expuesta en un servicio de motor de bases de datos, luego, identificada una o algunas vulnerabilidades, el atacante puede tener varias posibilidades de acceso, entre ellas listas usuarios y host y hasta acceder a contraseñas almacenadas.

También se puede contar con OpenVAS[17] , Es una herramienta de rápido crecimiento, pues en muy poco tiempo, fue adoptada dentro de Kali Linux, como unos de frameworks para realizar escáner de vulnerabilidades, tanto a sistemas operativos como a servidores de bases de datos y las mismas bases de datos. Esta herramienta, se dice que es una derivación de Nessus [18] o en otros comentarios, también se dices que tiene su propia base de lenguaje Open Source, pese a todo esto, está disponible en Kali Linux, es una de las importantes en proceso de escaneo de vulnerabilidades y tiene un amplio soporte en sistemas operativos y motores de bases de datos, lo cual la hace muy importante dentro del proceso de desarrollo temático que pretende realizar en la actual monografía. Todas estas herramientas, apoyadas metodologías validas de evaluación de vulnerabilidades o

---

[15] Sophos, Datos bancarios y sensibles de empleados, están en riesgo. Una exhaustiva encuesta del fabricante a responsables de TI evidencia las actuales carencias en seguridad por el desaprovechamiento de la tecnología de cifrado de datos, [En línea], 02 de Febrero de 2016, Disponible en: < https://www.sophos.com/es-es/press-office/press-releases/2016/02/state-of-encryption.aspx >

[16] Sitio Oficial, SQLMAP Automatic SQL injection and database takeover tool. Documentación herramienta usos. [En línea], Octubre de 2017, Disponible en: < http://sqlmap.org >

[17] SITIO OFICIAL OPEN VAS, Documentación herramienta. About OpenVAS , [En línea], 12 de Noviembre de 2017, Disponible en: < http://www.openvas.org/about.html >

[18] Tenable, Products Vulnerability Management. BUILT FOR RACTITIONERS, BY PRACTITIONERS, [En línea], Octubre de 2018, Disponible en: < https://www.tenable.com/products/nessus-vulnerability-scanner >

“tipos y análisis de seguridad” como lo definen Ezequiel Sallis, Claudio Caracciolo y Marcelo Rodriguez.[19]

Se puede definir con base en los planteamientos anteriores, que las principales brechas a nivel pymes sobre temas de seguridad de la información al interior de sus empresas, son generados principalmente, por los costos de inversión, el desconocimiento de las herramientas, las dificultades en procesos de implementación que algunas dicen presentar y finalmente, pero no la menos importante, sino la más relevante, el desconocimiento del Status Q de la seguridad de su información a nivel corporativo, estas brechas, son afectaciones directas a la conservación de sus activos de información y de gran manera, ponen en riesgo la continuidad de los negocios y los procesos comerciales que estas desarrollan.

Es claro también, que no es una problemática solamente de las pymes a nivel Nacional, sino que a nivel internacional, otros países afrontan dificultades similares dentro de sus empresas de un sector económico similar a las pymes Colombianas. Esto puede ser por varias razones, dadas algunas por temas económicos, académicos o sociales dentro de las empresas, de los cuales, la brecha generada, oculta las posibilidades de poder visualizar necesidades tan latentes antes de que, desafortunadamente, se logre materializar un ataque contra su información, puesto que los hackers van más rápido y cuentan con más recursos a la mano.

La presente propuesta de investigación, pretende proporcionar sustento académico y técnico, que pueda ser usado por las empresa del sector objetivo y aprovechado por ellas, para reducir las brechas existentes en sus organizaciones, lograr abrir espacios de valoración de activos de información, y contar con herramientas claras de gestión que puedan ser aplicables dentro de sus negocios de forma proactiva dentro de un ambiente que genere control hacia la información empresarial, vista desde el punto de vista de un activo vital para la organización.

Se pretende también, tener un proceso metodológico que de claridad a las empresas sobre los procesos de gestión del riesgo informático, que ellas, vean viable y cercano, poder implementar tecnologías de control en todos los procesos organizacionales, haciendo uso de los recursos humanos propios, con lo cual, no requiera incurrir en mayores costos de análisis e implementación de herramientas y para el caso del presente trabajo, que no requiera inversiones altas en firmas de

[19] E, C, M. Ezequiel Sallis, Claudio Caracciolo, Marcelo Rodriguez, “Tipos de análisis de seguridad”, in ETHICAL HACKING, Un enfoque metodológico para profesionales, D. Fernandez, G. Silveiro, Alfaomega Grupo Editor Argentino S.A. Buenos Arires Argentina, 2010, pp 11-27.

análisis de vulnerabilidades a la hora de valorar el estado y los procesos necesarios para salvaguardar su información.

Para las empresas del sector, va a ser valioso, encontrar un documento académico y técnicamente bien sustentado, con base en otros procesos investigativos y en múltiples referencias bibliográficas apropiadas, que les apoye en sus procesos tecnológicos, algunas de las empresas del sector, van a contar con mayor capacidad de inversión en recursos tecnológicos, las cuales, al tener algún avance en los procesos de inversión, van a aprovechar mucho más la generosidad de un documento en la explotación propia de sus vulnerabilidades, para realizar proceso de tratamiento y gestión del riesgo informático. La aplicación del análisis de metodologías, va a entregar a las empresas, un punto de partida importante en la consecución de unos buenos niveles de seguridad.

El descubrimiento para las empresas, de múltiples herramientas y metodologías que les apoye procesos tecnológicos de seguridad de la información, les va a permitir, iniciar un proceso proactivo de aseguramiento de sus activos de información y así, poder incursionar más rápidamente en procesos tecnológicos más exigentes de forma segura, que puedan ayudar a diversificar sus negocios y que aporten de forma eficiente y seguro al crecimiento y permanencia del negocio en el mercado.

5.2. MARCO CONCEPTUAL

- **Seguridad Informática y Seguridad de la información.**

Los sistemas de información, entendiendo estos como software y soluciones informáticas para el tratamiento de datos, se ven a diario inmersos en altos niveles de compromiso en su protección, esto, dado que se escucha a diario como se ven atacados diferentes tipos de información y diferentes tipos de empresas, lo cual compromete notablemente la información y que deja obligatoriamente, un compromiso de seguridad de la información y la seguridad informática como una tarea pendiente.

La seguridad informática o seguridad de la información, es en la actualidad, una de las tareas más importantes a nivel de tecnologías de la información y las comunicaciones, tanto a nivel operativo, como a nivel gerencial, donde se ha convertido en una actividad de continuo seguimiento y que se ve enfocada a salvaguardar la continuidad del negocio ya que parece, que por esta época, los

empresarios, entendiendo estos como administradores o propietarios, han comprendido la importancia de mantener la disponibilidad de la información, llevando esto a los términos del negocio, reconociendo así la importancia de conservar la información, en muchas ocasiones, sin la necesidad de definir premisas de disponibilidad, integridad y confidencialidad, sino simplemente, reconociendo la información y la tarea de seguridad como importante para cada negocio.

- **Para que salvaguardar la Información empresarial.**

Las directivas organizacionales, sin importar el tamaño o tipo de organización, necesitan que los datos, como activo de información y como elemento de gran valor para la gestión empresarial, este siempre protegido y pueda ser usado en la toma de decisiones dentro de cada empresa, esto, algunas veces a costos muy significativos según el tipo de empresa, pero que al ver el costo beneficio en cuanto a tenerla disponible o no, puede variar el punto de vista del concepto costo.

Las empresas de gran tamaño, son las que más se podrían evidenciar grandes inversiones en pro de la conservación de la información, dado que llevan ventaja en la identificación de su información como activo fundamental y esto, de la mano con su crecimiento han obligado a mantener la seguridad de la información y a adoptarla, desde una buena práctica, hasta convertirla en el pilar fundamental de su gestión organizacional.

- **La necesidad de seguridad informática y seguridad de la información.**

El termino Etical Hacking, surge en los años 90, como una respuesta a ataques informáticos, que empezaban a notarse en las empresas y que obligaron a hacer frente con un poco de su mismo que hacer, y eso, obligo a las industrias, a contar con personal con características avanzadas en manejo de herramientas de hardware y software, que pudieran aplicar conocimiento en la implementación de estas para evitar ser atacados. A estas personas que también podría clasificarse como hackers, se les dio el calificativo de éticos, dado que hacían su trabajo, del lado de salvaguardar la información de las empresas y no de atacarlas, haciendo uso de las misma herramientas o técnicas para este fin.

Contemplando esta panorámica, cada día se puede ver que el sector empresarial, hace más y mejores esfuerzos desde la capacitación de su personal hasta la puesta en marcha de estrategias de comunicación y divulgación para todas las estrategias de seguridad informática o seguridad de la información. Todo esto, porque se requiere llegar hasta lo más remoto de los usuarios de la información corporativa, y

crear conciencia de la importancia y de la forma como cada una de las compañías está trabajando para mantener niveles de seguridad eficaces.

- **Como lograr la seguridad de la información.**

Una premisa muy común en el medio de la tecnología y más en el entorno de la seguridad informática, es que, ningún sistema de información, es cien por ciento seguro, lo cual, deja abierta una brecha apta para la aplicación de múltiples metodologías que apoyan los proceso de seguridad en las organizaciones, desde la identificación de las necesidades hasta la implementación de procesos de apoyo y metodologías de evaluación que permiten a las compañías de cualquier sector conocer que tan seguros son sus sistemas de información.

Indiscutiblemente, haya que iniciar con conciencia, con algo de conocimiento sobre la problemática, que como ya se ha expuesto, no es ajena a ningún sector económico y que viene en alza cada vez, que las empresas adquieren más sistemas de información y en general cualquier activo de información que pueda representar algún tipo vulnerabilidad, más aun, cuando las compañías, usan desde cualquier punto de vista, servicio tecnológicos públicos en sitio web o infraestructuras de terceros, donde por muchas razones, es mucho más probable ser víctima de algún tipo de problema de seguridad.

Lograr la implementación de sistemas de gestión de seguridad de la información o básicamente, contar con procesos y activos de información que aporten a la seguridad de la informática y seguridad de la información en las organizaciones, es una tarea, no propia únicamente desde el área de TI, realmente, es una tarea de iniciativa de la alta gerencia, quien desde la inyección de recursos y el planteamiento de las necesidades de la compañía, basados en una misión y una visión a futuro de la organización, identifica necesidades que aportan al cumplimiento de los objetivos, que por lo general, están en la necesidad de la disponibilidad de la información para la continuidad de la prestación de los servicio y que pueden llegar hasta la protección del buen nombre de las instituciones, convirtiendo esto en un activo importante para estas y que va ligado a la prevención de incidentes de seguridad.

- **Un mejor panorama empresarial.**

Sería muy interesante contar con una cultura empresarial referente a la seguridad informática o seguridad de la información, donde cada uno de los actores de la compañía, tengan un papel importante en el desarrollo de los esquemas y de las tareas de protección del día a día. Esto lograría un compromiso alto de toda la organización y aportaría a mejorar los niveles de seguridad dentro de la misma.

Las personas son identificadas como el eslabón más débil de una cadena de seguridad y es ahí, donde hay que iniciar el trabajo de fortalecimiento en la construcción de procesos de seguridad de la información, donde se involucre a ese activo de información, como parte fundamental del proceso aseguramiento de la información.

- **Conocerse es importante.**

No importa el tamaño de la organización o el tamaño de su infraestructura instalada, su arquitectura empresarial o la cantidad de servicio internos o externos que a nivel de tecnología usa, lo realmente importante para iniciar procesos de aseguramiento de la información, es conocer oportunamente sus vulnerabilidades y las amenazas a las que se está expuesto, pues cada una de las industrias, cada una de las empresas, tiene una realidad diferente y debe encontrar escenarios particulares con relación a su objeto social, su definición institucional y la disponibilidad tecnológica con que cuente. Siendo esto una parte fundamental en la construcción de sistemas de información más seguros cobra relevancia la necesidad de implementar metodologías de Etical hacking en la identificación de vulnerabilidades en las empresas.

5.3. MARCO LEGAL

La legislación colombiana en temas de delitos informáticos, tiene sus mayores aportes en las últimas décadas, en las cuales, con base en temas de normatividad a nivel institucional, se han creado una cantidad de parámetros de cumplimiento para las empresas, emitidos entre leyes y otras normatividades, que obligan a las empresas a mejorar sus características de seguridad.

- **Los aportes más recientes.**

Algunas de las más sonadas últimamente, es la ley de protección de datos 1581 de 2012, en la cual, se entregó una base normativa muy importante, de cara a la protección de la información de las personas en las distintas organizaciones comerciales de todos los sectores.

Esta ley, fortalece la anteriormente conocida como Habeas Data, la cual intentó regular algunas acciones del sector financiero y realmente, dio paso a la ley 1581 de 2012 aplicable al resto de sectores comerciales Colombianos. Esta ley, se emitió y fue apropiada por la Superintendencia de Industria y Comercio para su implementación y cumplimiento en el año 2012.

- **Sobre delitos Informáticos.**

Hablando de delitos informáticos, ésta, se puede definir como una conducta consagrada en el código penal colombiano, es ahí, donde se hace una claridad muy importante. Los delitos no son las conductas que hacen que se materialice un delito, si no, cada artículo, definido y consagrado en el código penal colombiano para tal fin, por lo cual, la identificación y la tipificación, se debe hacer desde un incumplimiento de la ley, según las leyes mencionadas y dispuestas aplicables al presente trabajo y su asociación con los delitos, definidos en la ley 1273 de 2009.

Tener claro el concepto de delito y de tipificación, va a permitir, identificar claramente cada conducta y poder definir límites de actuar en cuanto a las necesidades de ejecución de tareas en pro de la ejecución de actividades de seguridad informática. Es importante el conocimiento de la ley, esto, permite no caer en problemas jurídicos por desconocimiento de estos.

- **Identificando la normatividad legal.**

Tomando definiciones de la Ley 1273 de 2009.[20] Se va a desarrollar un contenido teórico del marco legal, dando a conocer la normativa aplicable dentro de las actividades de ejecución de análisis de vulnerabilidad.

Del Capitulo primero, definido como: De los atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos se pueden identificar varios artículos para su análisis y aplicación en cada ejercicio.

A continuación, se identificara gráficamente en la Figura 1, los artículos aplicables tratados en el presente capitulo, los cuales fueron seleccionados según la aplicación dentro del proceso de análisis de vulnerabilidades.

[20] MIONTIC, LEY 1273 de 2009, [En línea], Enero de 2009, Disponible en: < https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf >

Figura 1. Ley de delitos informáticos.

Fuente: El Autor.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

Tener en cuenta, que el ejercicio de evaluación de vulnerabilidades debe llevar una autorización voluntaria, previa, expresa e informada, que detalle el nivel de acceso al cual puede llegar o la definición de un objetivo específico de revisión dentro de un sistema de información o una infraestructura tecnológica disponible para tal fin.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA. INFORMÁTICO O RED DE TELECOMUNICACIÓN.

Desarrollar pruebas de penetración, sea cual sea la finalidad, sin estar facultado, es decir, con una autorización previa y que sumado a esto, se ejecute y deje inaccesible el sistema informático o la red de telecomunicaciones, va a incurrir en la violación al artículo 269B de la presente ley. Esto puede representar una gran falta dentro de un proceso de verificación de vulnerabilidades.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

La interceptación, es una actividad propia de las entidades de defensa del estado, las cuales, al ser desarrolladas por un particular, estaría tipificándose el delito enmarcado dentro del presente artículo, una prueba de pen testing, eventualmente puede incurrir en una captura de tramas de paquetes de voz o captura de mensajes propios de una conversación privada. Aquí, hay que tener presente la delimitación de las pruebas, tanto en posición como en alcance y aplicar los controles necesarios para no incurrir en una interceptación de datos no autorizados.

Artículo 269D. DAÑO INFORMÁTICO.

Las actividades desarrolladas dentro de los procesos de identificación de vulnerabilidades, están encaminadas a la identificación de problemas de seguridad, estas actividades, no deben comprometer la integridad, disponibilidad y accesibilidad de os datos, con esto, se debe mantener presente, que las actividades ejecutadas, no deben comprometer los activos de información dentro de las pruebas de penetración, a menos, que estas, sean desarrolladas, no en entornos productivos sino en entornos de laboratorio a fin de identificar posibles problemas representado en la perdida de información, sea esta, de captura, borrado, alteración o alguna otra variación de la misma que represente compromiso real de la misma en disponibilidad, integridad y confidencialidad.

Artículo 269E. USO DE SOFTWARE MALICIOSO.

El software malicioso, es expresamente el desarrollado para realizar acciones fraudulentas dentro de los sistemas de información o las redes de datos, es diferencial de las herramientas útiles para la ejecución de las actividades de evaluación, que aunque puedan parecer malware para algunos sistemas de detección de intrusos o sistemas antivirus, deben diferenciarse cada uno de estos y no incurrir en uso de malware para ejecución de pruebas, caer en una mala práctica en la aplicación de las herramientas de las pruebas, puede materializar un delito basado en uso de software malicioso.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES.

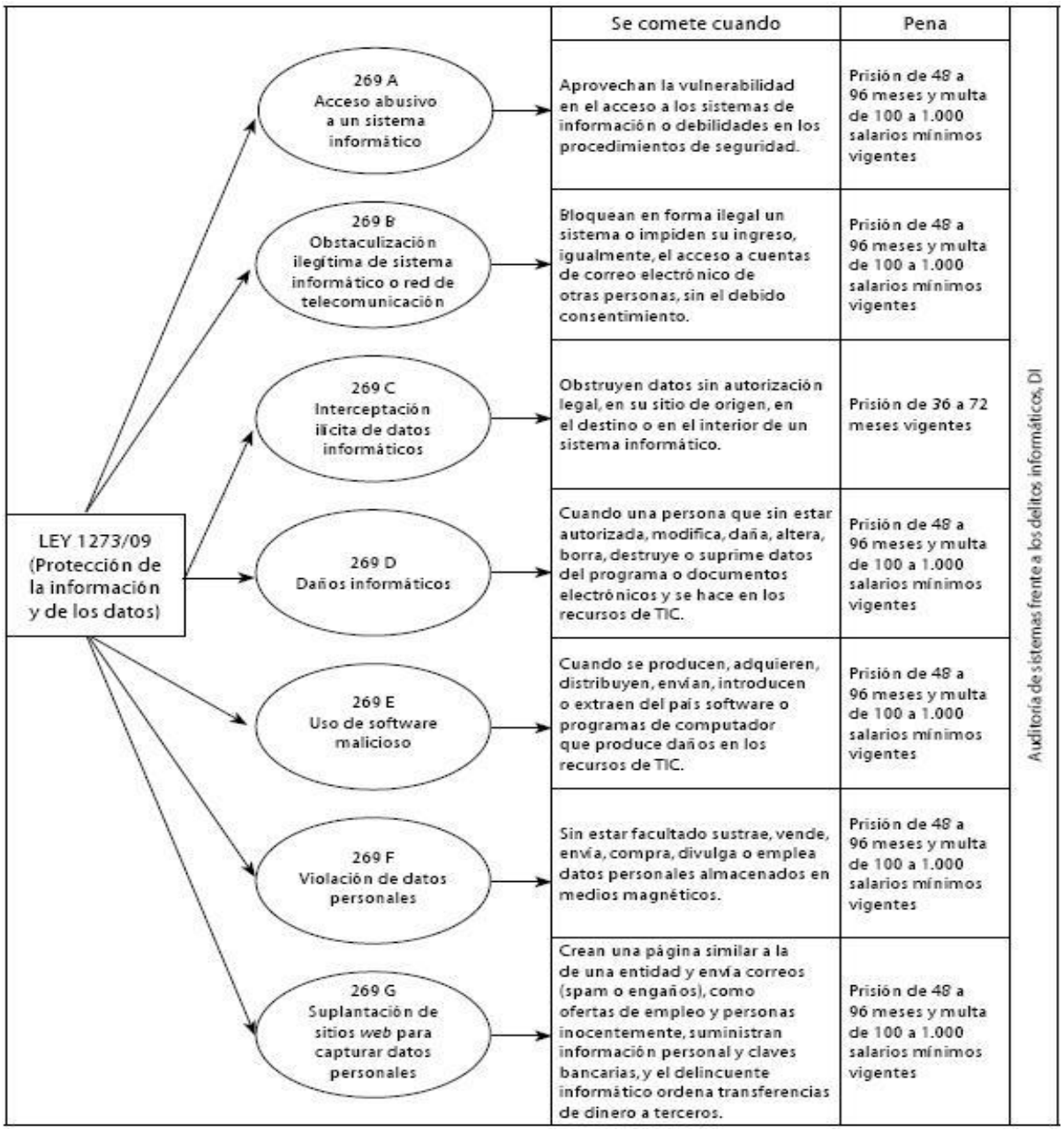
Aprovecharse de los niveles de acceso otorgados para hacer uso mal intencionado de la información que se alcance a obtener o visibilizar, puede materializar un delito de violación de datos personales. Aquí, se hace muy importante, delimitar los

niveles de acceso y ser éticos en el manejo de la información que se logre acceder en las pruebas de desarrolladas.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere bajo alguno de los siguientes agravantes definidos dentro de la presente ley.

Las circunstancias de agravación punitiva, se identifican gráficamente en la Figura 2, Haciendo una ampliación al concepto describiendo cuando se tipifica o comete y la pena aplicable.

Figura 2. Asignación de penas según la ley 1273.



Fuente: www.scielo.org.co

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

Sobre el artículo anterior, es conveniente aclarar, que la agravación punitiva, refiere a factores dados, que acompañan la ejecución del delito y que según su definición, agravan la concepción del delito, esto indica en todos los casos, aumentas las penas impuestas para cada caso luego de la valoración de este artículo.

Del Capitulo segundo, definido como: De los atentados informáticos y otras infracciones, se puede analizar su pertinencia en la aplicación de pruebas de vulnerabilidad de las pymes, cuando en estas, se pueda afectar alguna de las definiciones de los siguientes artículos. Factores como el aprovechamiento de la confianza, engaño intencionado o cometer el delito a una entidad del estado, son agravantes en el momento de tasar la pena.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

Principalmente la ley de delitos informáticos enmarca en gran medida, las disposiciones restrictivas y preventivas expuestas en procesos de análisis de vulnerabilidades, atendiendo a que estos proceso, pueden resultar, sino son llevados bajo la rigurosidad de la autorización expresa y su ajustada ejecución, a templar la materialización de algunos de los delitos identificados dentro de la presente ley, la cual, tipifica claramente cada uno de los delitos en los que se puede incurrir.

Es importante aclarar, que para la legislación Colombiana, esta ley no se desarrolló para control de las pruebas de penetración, o evaluaciones de vulnerabilidad en la aplicación de metodologías de Ethical hacking, sino, que es una forma de penalización de delitos, que no estaba cubiertos dentro de marco penal Colombiano y que para efectos del presente trabajo, resultan útiles a la hora de enmarcar, la importancia de la claridad en el desarrollo de los procesos de evaluación de seguridad informática o seguridad de la información, cuando esta se presente desde pruebas de penetración.

6. IDENTIFICACIÓN Y DOCUMENTACIÓN DE METODOLOGÍAS DE ETICAL HACKING

Contando con un amplio número de metodologías y principalmente de herramientas que pueden apoyar el proceso de evaluaciones de vulnerabilidades, se van a incluir dentro del análisis, las metodologías más reconocidas y las que se puedan encontrar documentación suficiente, así como la disponibilidad de obtener las herramientas que usa, para generar opiniones de juicio y poder elegir la que más se preste apara la finalidad que se están evaluando, esto incluye, que no se tendrán en cuenta, soluciones o metodologías que impliquen incursionar en gastos de licenciamiento o de asesorías especializadas de cara a los proceso de implementación.

Por estas razones, se van a analizar de forma profunda, cada una de las siguientes metodologías propuestas, dado que cumplen con algunas características de las ya mencionadas y que no representan altos costos de inversión ni en dinero ni en tiempo para las empresas que decidan implementarlas. Se pretende desarrollar un análisis a partir de la información suministrada por cada fabricante o creador de la metodología para poder contar con un proceso de análisis y decisión objetivo.

6.1. OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL

La metodología OSSTMM, que traduce, Manual de Metodologías Abiertas para verificación de la Seguridad, que actualmente, se desarrolla y mantiene por el ISECOM, Institute For Security and Open Methodologies, Es conocido como un gran manual para el testing de seguridad en ambientes de Tecnologías de información y Comunicaciones.

Según la definición en el sitio oficial, [21] *"The OSSTMM is about operational security. It is about knowing and measuring how well security works. This methodology will tell you if what you have does what you want it to do and not just what you were told it does.*" La metodología básicamente se encarga de medir que también trabaja la

[21] Open Source Security Testing Methodology Manual (OSSTMM), Consulta En Línea, Sitio Oficial, Disponible en: http://www.isecom.org/research/

seguridad de la organización, validando que sus herramientas hagan lo que deben hacer en varios espacios corporativos.

Esta metodología, ofrece dentro su ejecución, la posibilidad de realizar procesos evaluativos de seguridad de una forma integral a toda la organización, esta integración, se describe como una interconexión entre los proceso de TI asociados a la seguridad y cada uno de los actores que la metodología define, puntualmente menciona la existencia relacional entre el personal dentro de cada una de las organizaciones, los procesos que al interior se desarrollan, los sistemas que utilizan y el software dentro de las empresas.

Se define como una prueba de seguridad para las operaciones, dado que, debido a la configuración de las soluciones y los sistemas de software principalmente, los cuales han sido logrados con uso de componentes ya desarrollados, por lo que no se puede garantizar en algún momento que estos no estén realizando exactamente lo que se programaron o fueron destinados a desarrollar, es aquí, donde la interconexión de elementos de la metodología, cobra relevancia en su implementación.

6.1.1. Definición de secciones a evaluar.

El desarrollo de la metodología, es definido por secciones, en las cuales, se ve cómo se realiza una evaluación progresiva de cada uno de los componentes de interconexión lo cual, ha permitido tener una metodología ampliamente usada por profesionales de la seguridad y que presenta un aval en el mercado de profesionales de la disciplina. La Metodología es muy exigente en su aplicación y es determinante para ella, cumplir con rigurosidad cada una de las secciones, independiente en cuál de ellas requiera hacer la evaluación.

Sección A: Seguridad de la Información.

1. Revisión de la Inteligencia Competitiva
2. Revisión de Privacidad
3. Recolección de Documentos

Sección B: Seguridad de los procesos.

1. Testeo de Solicitud
2. Testeo de Sugerencia Dirigida
3. Testeo de las Personas Confiables

Sección C: Seguridad de las tecnologías de internet.

1. Definición de logística y de control
2. Sondeo de la red.
3. Clasificación de los Servicios de TI
4. Buscar información de competitividad
5. Validación de la privacidad
6. Obtener-capturar documentos
7. Buscar y verificar vulnerabilidades
8. Probar aplicaciones que están en internet.
9. Enrutar redes de datos.
10. Prueba de sistemas confiados
11. Pruebas los controles de Acceso
12. Pruebas de IDS
13. Probar las contingencias
14. Desencripción de password.
15. Pruebas de DoS,Denial of services
16. Validar políticas de seguridad.

Sección D: Seguridad en las comunicaciones.

1. Pruebas de servidores de telefonía,
2. Pruebas de mensajes y correos hablados.
3. Verificación de FAX
4. Pruebas del modem

Sección E: Seguridad Inalámbrica.

1. Validación Electromagnética (EMR)
2. Validación de Redes Inalámbricas con [802.11]
3. Validación de red de equipos por bluetooth
4. Validación de equipos de entrada inalámbricos
5. Validación de equipos inalámbricos de mano.
6. Validación de comunicaciones wifi
7. Validación de vigilancia inalámbrica
8. Validación de transmisiones inalámbricas
9. Validación de RFID
10. Validación de soluciones con Infrarrojos
11. Pruebas de privacidad

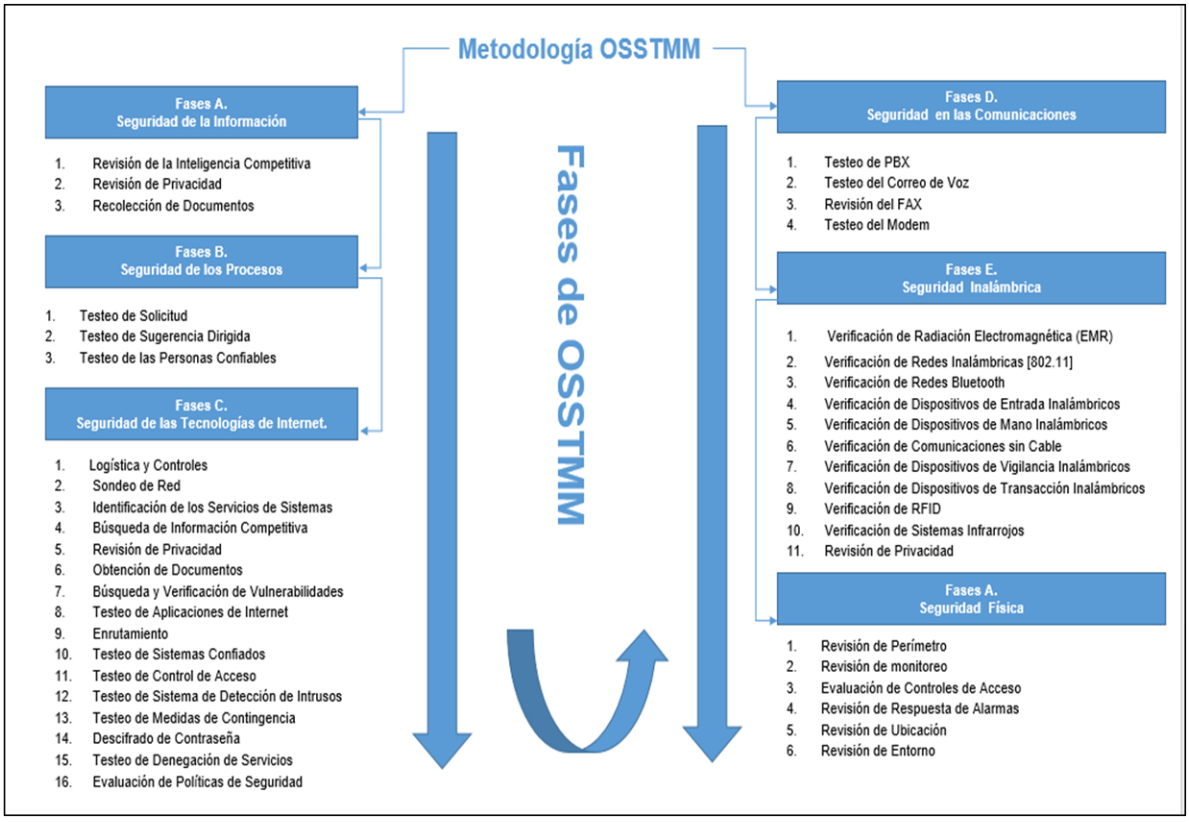
Sección F: Seguridad física.

1. Velicación del Perímetro
2. Revisión monitoreos realizados

3. Revisión de sistemas de Control de Acceso
4. Validación de Respuestas por alarmas
5. Validación de geolocalización y ubicación.
6. Validaciones generales del entorno.

Graficando la información descrita anteriormente, se hace una ampliación cronológica de las etapas mencionadas en la metodología OSSTMM en la Figura 3, aquí, se describe cada una de las fases y se acompaña de las actividades ejecutadas en cada una de ellas.

Figura 3. Identificación Fases Metodología OSSTMM.



Fuente: El autor.

6.1.2. El proceso de análisis de seguridad

La metodología enmarca el proceso de análisis de seguridad en un esquema de pasos claros que se deben dar para conformar y llevar a cabo un proceso de análisis de seguridad, estos pasos son conocidos como Dimensiones de seguridad.

Visibilidad: Define todo aquello a nivel corporativo, que puede verse o monitorearse sin necesidad de usar ningún dispositivo electrónico.

Acceso: Definido como una entrada o punto de acceso a nivel de seguridad, puede ser un punto de red, una página web o cualquier cosa que permita ser definido como un casi público en temas de poder acceder a un sistema.

Confianza: Se define como una ruta especializada a nivel de seguridad, teniendo en cuenta su integridad y nivel de acceso a un recurso en particular.

Autenticación: Es la medida de privilegios en la autenticación de cada proceso.

No Repudio: garantiza que ninguna persona pueda negar su participación en una actividad o proceso.

Confidencialidad: Es la certeza de que solo las partes autorizadas de una comunicación tengan acceso a la información.

Privacidad: Indica que el proceso solo es conocido por las partes interesadas.

Autorización: Es la certeza, de que el proceso, cuenta con la razón y la justificación del negocio para su ejecución.

Integridad: Es la certeza que el proceso tiene finalidad, y no poder desviado, modificado, continuado o reservado, sin el consentimiento de las partes interesadas.

Seguridad: Define la seguridad de los medios, por los cuales, un sistema, no puede dañar otros sistemas de información, aun cuando exista una falla total.

Alarma: Es una notificación adecuadas que advierten de actividades que violentan o intentan violentar cualquier dimensión de seguridad aplicada.

Esta es una definición del autor, sobre su esquema de testeo “Donde básicamente, define que es una prueba de seguridad diferenciada frente a una prueba de intrusión la cual se apoya en combinaciones creativas de múltiples bases de datos de conocimiento sobre metodologías y temas legales principalmente.

6.2. ISSAF (INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK)

Básicamente, es un marco de trabajo, para modelar y evaluar requisitos a nivel de procesos internos en seguridad de la información, esta metodología, define un plan de pruebas, basado en una metodología basada en dominios en los cuales se van a basar las pruebas.

Esta metodología, logra abarcar una gran cantidad de procesos de tecnología de información y también, cubre procesos de alto nivel asociados a las TICs. Es principalmente usado en procesos de entidades financieras, tecnológicas y de servicios a nivel mundial.

La fortaleza de sus procesos de evaluación, son fundamentados en permitir que se desarrollen etapas de pre evaluación de los procesos de auditoria o de pentesting, en los cuales se pueden definir momentos y espacios de evaluación de cada una de las dimensiones establecidas.

Los procesos de evaluación durante, ya entran a la variación de la parte práctica de la aplicación de las técnicas y la materialización de los aspectos planeados en cada una de las dimensiones en la planeación previa.

Se cuenta también con post evaluación, es una revisión de la ejecución de los procesos planeados y ejecutados con base en las dimensiones establecidas.

El ISSAF, es un marco de trabajo para evaluación de políticas y procesos de seguridad de la información en las organizaciones. En esta metodología, se integran herramientas de gestión, las cuales hace en conjunto, un proceso de evaluación completo para las organizaciones. Para esto, se definen unas herramientas de gestión y listas de control interno así:

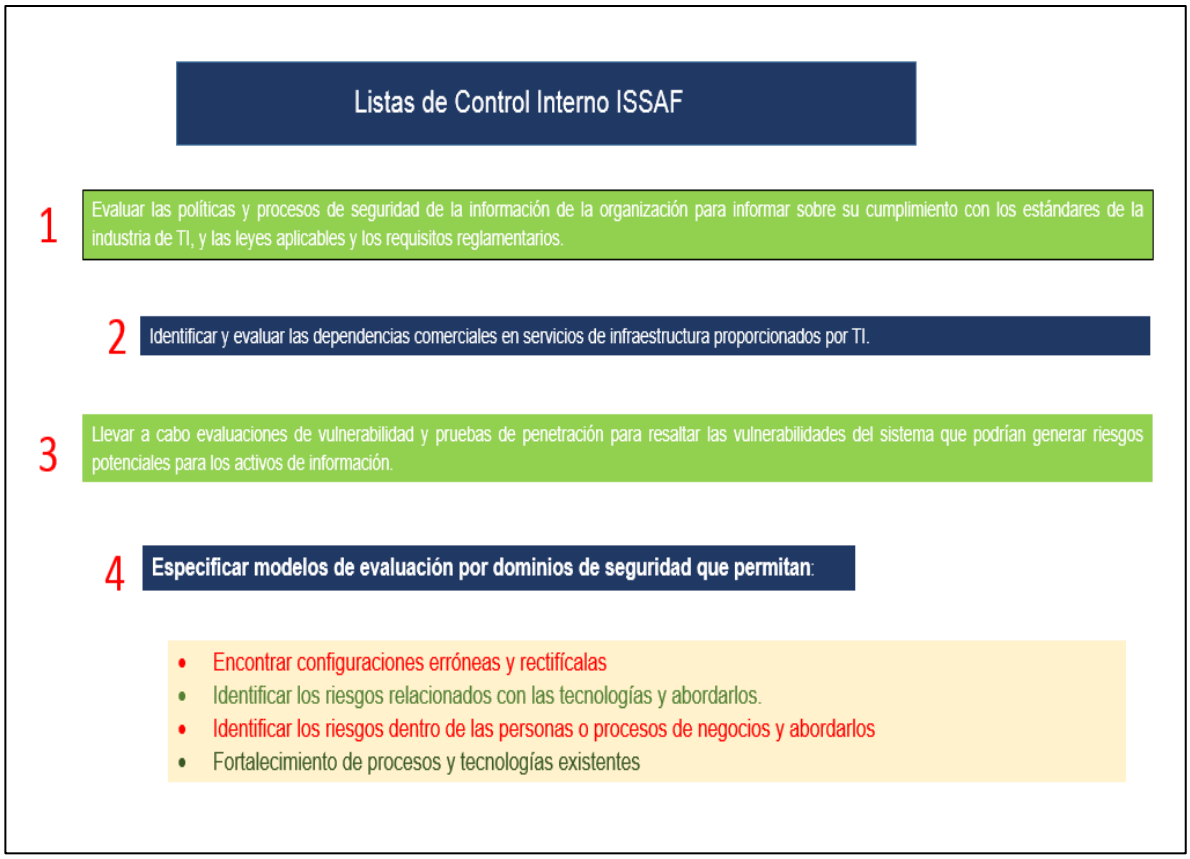
1. Evaluación de políticas y procedimientos de seguridad de la información en las empresas para reposte de cumplimiento de estándares industriales en TI y normatividad legal aplicable.
2. Identificación y evaluación de áreas de comercio de servicios de infraestructuras que se prestan desde las áreas de TI.
3. Desarrollar análisis de vulnerabilidades y pentesting para identificar vulnerabilidades que puedan representar algún riesgo potencial a cualquier activo de información de las organizaciones.

4. Definir un modelo ideal de valoración por dominios de seguridad, con los cuales se pueda:

    - Detectar alguna configuración problema y corregirla.
    - Detectar riesgos asociados a las tecnologías instaladas y tratarlos.
    - Determinar riesgos asociados a personal y a los procesos de negocio y tratarlos.
    - Fortalecer procedimientos y tecnologías existentes en las organizaciones.

Propiciar más y mejores prácticas y procesos para salvaguardar definiciones de continuidad de negocio, son favorables a las mediciones enfocadas en procesos de normas como IEC /SIO 27001 entre otras, agregando valor a los programas de maduración corporativa asociados a procesos de TIC. La Figura 4. Grafica cuatro controles fundamentales de la metodología.

Figura 4. Lista de Controles ISSAF.



Fuente: El Autor.

6.3. OS (OFFENSIVE SECURITY)

Identificando lo más claro posible esta metodología, se puede decir que se trata de ejecución de herramientas informáticas, originalmente orientadas a causar problemas en los sistemas de información, para con ellas, conocer de forma práctica los huecos de seguridad o las vulnerabilidades de seguridad informática que se encuentran en los entornos corporativos. Esta metodología, puede ser la más práctica que se conoce, pues centra sus análisis en la utilización de las mismas herramientas con al que se llevaría a cabo un ataque determinado y trata de llegar, sin afectar la operación real de las compañías hasta la explotación para demostrar cada hallazgo.

En análisis de seguridad, se puede definir desde el punto de vista de su aplicación a nivel de Seguridad Informática, como un proceso evaluativo, de comprobación de vulnerabilidades dentro de un sistema de información o infraestructura tecnológica definida. En el cual, se realizan una serie de ataques, en entonos varios, en los cuales se pretende descubrir fallos de seguridad. [22]

6.3.1. Pasos para ejecutarlo adecuadamente

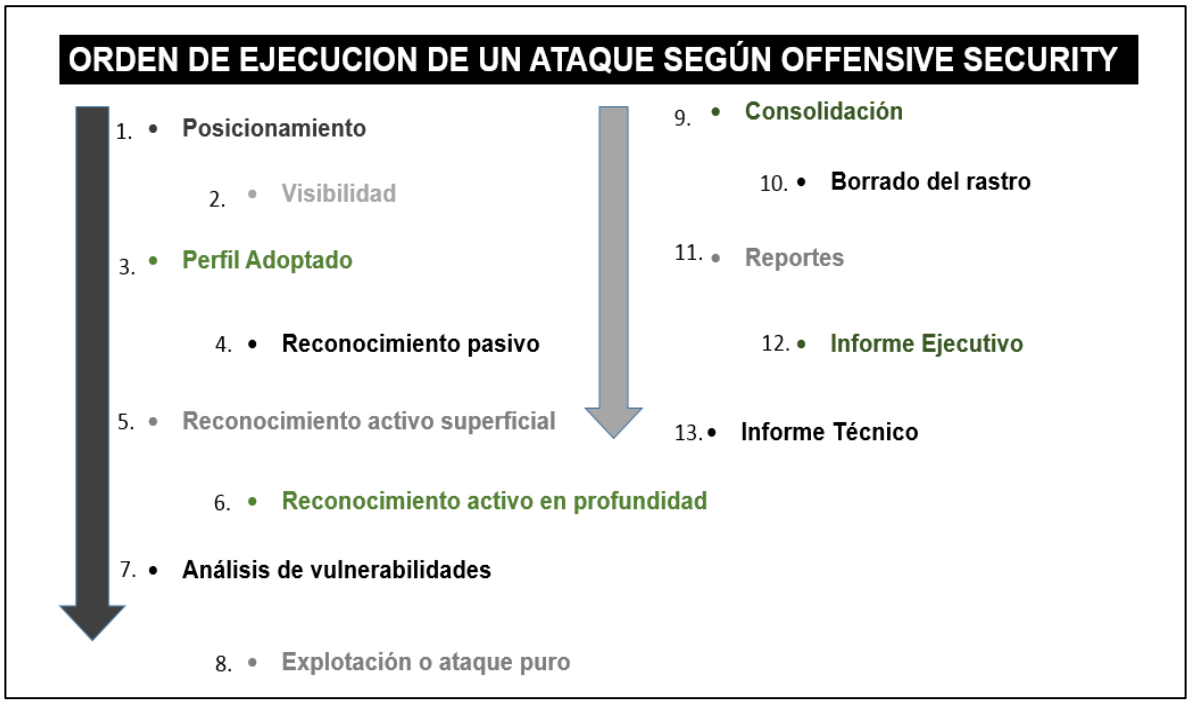
Siguiendo esta orientación, se deben analizar recomendaciones que permitan un enfoque más claro acerca de lo que se quiere obtener desde la visión del cliente o proveedor, esto cuando el proveedor ejerce la acción.

Se cuenta con conceptos desde la preparación y su ejecución de un pentesting, que también enmaran, buenas prácticas asociadas a análisis de vulnerabilidades.

[22] E, C, M. Ezequiel Sallis, Claudio Caracciolo, Marcelo Rodriguez, "Tipos de análisis de seguridad", in ETHICAL HACKING, Un enfoque metodológico para profesionales, D. Fernandez, G. Silveiro, Alfaomega Grupo Editor Argentino S.A. Buenos Aires Argentina, 2010, pp 11-27.

Ampliando los conceptos de orden de la metodología OS, La Figura 5, describe secuencialmente y grafica de inicio a fin, el orden de actividades propuesto para la ejecución de análisis bajo esta metodología los cuales se va a desarrollar a continuación.

Figura 5. Orden de Ejecución Ataques Offensive Security.



Fuente: El Autor.

- **Posicionamiento**

Se refiere a como se ubican el analista de seguridad o un determinado atacante con relación al objetivo de su análisis, las posiciones pueden ser internas o externas, lo cual define varios aspectos sobre lo que el cliente espera obtener.

- **Visibilidad**

Hace referencia al tipo de información que se permite ver al analista, previamente a la ejecución del análisis, la información visible, incluye sistemas de información, archivos y documentación de la disposición de la red, esto define también, la posibilidad de conocer el nivel de exposición interno o externo hacia la información corporativa.

- **Perfil Adoptado**

Aquí, se pueden definir varios perfiles según el tipo de análisis y la formación del atacante, y a su vez, también los define la necesidad del cliente, entre estos se podrían identificar usuarios que cuenten con suficientes privilegios en la red, que puedan acceder físicamente, o que no lo pueda hacer, también, puede ser un perfil avanzado o de conocimiento básico según sea la necesidad del usuario.

- **Reconocimiento pasivo**

Normalmente el cliente hace entrega la información necesaria para la actividad, pero de igual forma se intenta conseguir información relacionada por otros medios, esta tarea, permite que se informe al cliente sobre la visibilidad de los objetivos propuestos desde afuera de la organización. [23]

- **Reconocimiento activo superficial**

Se identifican puntos-claves con relación directa al objetivo, con la idea de encontrar alguna actividad y posteriormente realizar análisis más profundos de los objetos encontrados.

- **Reconocimiento activo en profundidad**

En este instante se usan los objetos identificados anteriormente para realizar una revisión o análisis profundo, aquí, se validan puertos, protocolos y servicios disponibles y principalmente, que tan actuales están sus aplicaciones y software instalado en estos.

- **Análisis de vulnerabilidades**

Se inicia a determinar potenciales vulnerabilidades en la infraestructura instalada y sus componentes de software, es una etapa crítica de análisis, ya que se pueden presentar algunos falsos positivos a tratar.

- **Explotación o ataque puro**

En esta etapa se desarrolla la explotación de vulnerabilidades encontradas en etapas anteriores, esto permite ejecutar código para su explotación y realizar mediciones finales.

---

[23] E, C, M. Ezequiel Sallis, Claudio Caracciolo, Marcelo Rodriguez, "RECONOCIMIENTO PASIVO", in ETHICAL HACKING, Un enfoque metodológico para profesionales, D. Fernandez, G. Silveiro, Alfaomega Grupo Editor Argentino S.A. Buenos Aires Argentina, 2010, pp 29-42.

- **Consolidación**

Hasta este momento, ya existe un avance significativo del análisis y se da inicio a los procesos de intrusión, dejando comprometida alguna información, equipos o servicios que se lograron vulnerar.

- **Borrado del rastro**

En esta etapa se debe eliminar cualquier tipo de rasgo que permita identificar una intrusión.

- **Reportes**

Finalizando, esta etapa se da estructura a la información recolectada, generando informes de tipo Ejecutivo para la gerencia y de tipo técnico para las áreas de TIC y auditoria dentro de las organizaciones.

6.3.2. Etapas de Implementación de la metodología Offensive Security

Las etapas de implementación de la metodología, hacen parte fundamental de la definición de la posición al momento de la ejecución del análisis, es un referente que determina desde el inicio, ruta a seguir en el trazado de su desarrollo, estas etapas, aportan a definir la ruta de ejecución, identificando entre otros aspectos, la definición de objetivos como inicio fundamental y el momento de ataque y verificación, siendo estos entre otros, muy relevantes en el desarrollo de un análisis usando esta metodología

6.3.2.1. Planeación para implementación

Para la etapa de planeación, la metodología define unos sub etapas, que amplían el concepto de planeación para la implementación y definiendo con más puntualidad algunas variables claves a tener en cuenta.

Definir los objetivos: de cara a satisfacer las necesidad de una empresa, se deben conocer sus principales necesidades para establecer los objetivos que se tienen con el análisis de seguridad, para esto, el desarrollo de una reunión, donde participen la parte directiva de la organización y el personal de TIC va a permitir conocer esto de primera mano en el inicio de la planeación.

Definir los espacios a utilizar: Aquí la organización define en donde quiere llevar a cabo el análisis de seguridad, esto, porque alguna empresa, puede tener preferencia a complementar o a probar su data center, a probar sus servicios web o a revisar solamente el estado de la red corporativa de cara a como se ven desde adentro o desde afuera la seguridad de sus máquinas clientes. Aquí, la empresa con el grupo de expertos define la posición que se usara de cara al análisis.

Levantar Información preliminar existente: El conocimiento de la empresa, es fundamental, saber a qué se dedica, cuantas sedes tiene, que tipo de tecnologías usa, que servicios tiene disponibles en la nube, las actividades que se desarrollan al interior y al exterior de la empresa, sus horarios, saber si han tenido algún ataque, si realizaron algún análisis previo y si es así, evidenciar sus reportes, medir desde el punto de vista de la información preliminar las condiciones de estado actuales del cliente y su infraestructura.

Asociación de procesos y servicios: Identificar como los procesos empresariales, se podrían afectar con la vulneración de la seguridad de la red del cliente, esto se logra al identificar, las herramientas o servicios, principalmente de TIC asociados a dichos procesos, para un ejemplo, podríamos saber en esta entrevista que el área de mercadeo cuenta con una aplicación de CRM que esta publicada, lo que nos indicaría, que la afectación a esta publicación seria directa al área mencionada.

Identificación de infraestructura del cliente: Conocer de primera mano la composición de la infraestructura del cliente, su distribución, como acceder, donde esta físicamente ubicados los servicios, los servidores, las sedes alternas, sus policitas de seguridad existentes y como se realizan los procesos administrativos de las mismas. Esto, con el fin de tener una imagen global que permita definir posición e iniciar los procesos de descubrimiento.

6.3.2.2. Descubrimiento para el análisis

En esta etapa, vamos a develar alguna información muy importante para el proceso, que no fue entregada en la etapa de planeación, esta, es más una tarea del experto en seguridad, que requiere datos más técnicos y específicos de como se ve la compañía tanto a nivel interno como externo.

Análisis previos: Los análisis previos incluyen revisar la consecuencia de la información levantada en planeación, validando que es consecuente y que si constituye una normalidad tecnológica dentro de las actividades desarrolladas por

la empresa, es decir, que la información entregada si es coherente para iniciar el descubrimiento.

Visibilidad desde posición Externa: Definida la visibilidad del experto desde la reunión de planeación, podemos usar la externa, para ver cómo se ven los servicios publicados, como se accede a su página web, como es la publicación de sus servicio a nivel externo, también podemos conocer sus servidores de nombres, las direcciones ip públicas disponibles, algunos hosting, configuración de DNS, subdominios y mucha más información, que puede obtenerse desde la ejecución de herramientas disponibles en internet y hasta por simple consulta u observación en diversos portales de internet.

Visibilidad desde posición Interno: A nivel interno, la visibilidad es muy diferente, aquí, se pueden evidenciar niveles de permisos en los usuarios, estados de la configuración de las maquinas tanto clientes como servidores, dispositivos de almacenamiento y todos los componente de la infraestructura tecnológica reportada, que partiendo de sus observaciones previas, pueden identificarse como vectores de análisis dados alguno brotes identificados por observación o inspección al interior de la compaña, por ejemplo, identificar que los usuarios cuentan con servicios de internet abiertos, puede ser una buena antesala de información para procesos de inspección de ingeniería social como herramienta en el desarrollo del análisis.

Desarrollo de ingeniería social: Es parte fundamental de una etapa de descubrimiento, tener algún contacto con las `personas de la compañía, conocer cómo piensa, de que hablar, que dicen, que cargos desempeñan. Hacer algo de networking con ellas, permite identificar posibles fallos de seguridad humanos y en algunos casos, identifica fallos en el desarrollo de los procesos tecnológicos que sirven como punta de entrada a los análisis tanto internos como externos que el experto requiera hacer desde la ejecución de sus análisis de seguridad.

6.3.2.3. Ataque y verificación

En las etapas anteriores, se recolecta toda la información relevante de la organización, su infraestructura y componente de servicios al interior de sus organizaciones, con ellos, se realiza un descubrimiento para complementar la visibilidad de los expertos, todo esto para abrir paso a la etapa de ataque puro.

En esta etapa, se concretan los objetivos de explotación de las vulnerabilidades detectadas, al hacer uso de diferentes herramientas que permiten la posibilidad de encontrar información sensible dentro de las arquitecturas empresariales y en algunos casos, permite la ejecución de códigos arbitrarios, los cuales son aprovechados en el análisis y que apoyan los procesos de explotación. En
La etapa de ataque puro es la culminación de un proceso practico de análisis de vulnerabilidades, con base en prácticas de descubrimiento análisis y explotación de vulnerabilidades.

6.3.2.4. Generación de informes

En esta etapa, se va a consolidar la información obtenida, aquí, el cliente, obtiene un consolidado detallado, de los hallazgos obtenidos durante todo el proceso, no solo a nivel de pruebas, sino también a nivel de entrevistas, descubrimiento y en general de todo el proceso de evaluación. La generación de informes se centra básicamente, en la generación de dos reportes que son entregados al cliente y que tienen información respectiva a cada uno así:
Informe Ejecutivo: Es dirigido a la alta gerencia o directivos de la organización, este, se desarrolla en un lenguaje coloquial, tratando de no utilizar tecnicismos, Evidenciando el cumplimiento de los objetivos planteados durante la planeación y resaltando a nivel empresarial y tecnológico, sus fortalezas y debilidades, a la vez, que se emiten las recomendaciones básicas de cómo resolver las vulnerabilidades encontradas.

Informe Técnico: Aquí, se desarrolla un informe con el mismo contenido del ejecutivo, pero enmarcando la terminología en un lenguaje altamente técnico, que permita expresar el resultado del análisis con mucha claridad para la empresa, este informe, es mucho más profundo y detallado, y va a ser socializado y entregado a los profesionales de las áreas de TIC y de auditoria de la organización.

Tal como se acaba de describir, las etapas obedecen a una secuencia de ejecución que permiten la correcta ejecución de las pruebas usando la metodología OS, La Figura 6. Etapas Implementación Offensive Security, grafica secuencialmente el proceso de ejecución de las fases de implementación, aquí, se describe con una flecha vertical descendente el orden a llevar.

Figura 6. Etapas Implementación Offensive Security.

Fuente: El autor.

6.4. OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

También conocido como Proyecto Abierto para Seguridad en Aplicaciones Web. (OWASP), es un proyecto de código abierto, que permite a las organizaciones, desarrollar procesos de verificación de la seguridad de la información y seguridad informática, en sus procesos de desarrollo de software, lo cual indica, que tiene un enfoque claro en desarrollo de aplicaciones y servicios para la web.

La metodología cuenta con varias herramientas dispuestas de forma gratuita a los usuarios que requieran hacer uso de ellas, entre ellas se presentan; documentación, foros y capítulos publicados, el proyecto OWASP, se enfoca en resolver la seguridad en las aplicaciones como un problemas general de personas, procesos y

tecnologías, dado que se ha establecido que la mejor metodología para enfrentar los problemas de seguridad, es atacar cada una de estas áreas del entorno empresarial.

La metodología, desarrollo una lista de problemas de seguridad comunes, que llamo [24]OWASP Top Ten (10). Aquí, se agrupan ceca de 500 mil potenciales vulnerabilidades entre miles de empresas y miles de soluciones de software, estas vulnerabilidades, se clasifican y priorizan de acuerdo con varias estimaciones de explotación, factibilidades e impactos.

El principal objeto es instruir a los encargados de desarrollo de software y desarrolladores entre otros actores del proceso de construcción de software sobre consecuencias potenciales de vulnerar la seguridad en aplicaciones web

La tabla del Top Ten de OWASP, enumera 10 tipos de riesgos en la seguridad de las aplicaciones web, los cuales, son explicados de forma que el usuario final, para este caso, personas con conocimientos en temas de desarrollo de software, que son quienes están al frente de los proyectos, puedan interpretar con facilidad a que se refiere cada uno de estos riesgos y que a partir de allí, se puedan organizar los esquemas necesarios haciendo uso de las herramientas pertinentes para evitar este tipo de problemas dentro de los desarrollo web crecientes.

Dentro del Top Ten, se pueden encontrar definiciones claras sobre fallas de inyección SQL, así como en SO y protocolos LDAP, también menciona algunos problemas relacionados con la perdida de autenticación y perdida de gestión de las sesiones establecidas en las aplicaciones. También temas referentes a las configuraciones de seguridad incorrectas que obliga a proponer protocolos de instalación y configuración sobre toda la estructura que soporta y desarrolla una aplicación web, esto incluye, desde equipos de cómputo, pasando por servidores y aplicaciones de desarrollo, hasta llegar a las aplicaciones de desarrollo, navegadores y todo el software involucrado completamente monitoreado y limpio de problemas de configuración.

Cuestiona fuertemente los procesos o funcionalidades de gestión de acceso o controles de autenticación dentro de las aplicaciones dado que, en muchas de estas, se carece de procesos de fuertes, aquí se sugiere controles que permitan

[24] OWASP Top 10 Most Critical Web Application Security Risks, [En línea], 12 de Mayo de 2018, Disponible en: < https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf >

hacer las verificaciones antes de llegar al servidor las peticiones de los externos, que pueden ser potenciales atacantes.

Finalmente, dentro del top ten, hay una referencia a la redirección o los reenvíos no validados, esto se refiere, a la redirección de los usuario de las aplicaciones hacia otros sitios, proceso en el cual, se utilizan daros no confiables para la transacción de información, aquí, se conjunta unas validaciones inadecuadas que ponen en riesgo cualquier tipo de transacción, que en su caso más común, pueden transportar información de credenciales de acceso, las cuales pueden ser interceptadas a través de scripting y caer en manos de la ciberdelincuencia.

La especificación de la Metodología.

Dentro de la metodología, su Top Ten, invita mediante una mención explícita de cada uno de los riesgos asociados, a validar la existencia o exposición del riesgo en la aplicación web a determinar, para esto, emplea una definición dentro de cada [25] ficha de riesgo que provee información sobre explotación, debilidades, impactos y hasta algunas recomendaciones de prevención.

A1. Inyección: Considerar y tener presente cualquier actor que pueda suministrar información no confiable desde cualquier nivel de usuario y posición.

A2. Perdida de autenticación y gestión de sesiones: Considerar algún atacante externo e internos, que puedan tomar información ajena o cuentas y otros que quieran traslapar acciones fraudulentas.

A3. Secuencia de comandos en sitios cruzados (XSS): Contemplar cualquier actor del entorno, que pueda suministrar datos erróneos a las aplicaciones, sea interno o externo.

A4. Referencia directa insegura a objetos: Contemplar los usuarios que puedan tener acceso parcial o temporal a determinados datos en las aplicaciones.

A5. Configuración de seguridad incorrecta: Contemple personal que pueda suplantar cuentas o intentar acceder fraudulentamente el software, deben ser incluidos como potenciales, usuarios del interior o exterior de las organizaciones.

[25] OWASP Top 10 Most Critical Web Application Security Risks, [En línea], 12 de Mayo de 2018, Disponible en: < https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf >

A6. Exposición de datos sensibles: Contemple quien pueda acceder a datos sensibles de la aplicación y a algún backup de ellos, tenga en cuenta datos transaccionales, en tránsito, almacenados y hasta el navegador del cliente final.

A7. Ausencia de control de acceso a funciones: Contemple que usuarios o qué tipo de estos pueden hacer peticiones al software, usuarios anónimos, internos o externos y con qué tipo de privilegios os in ellos.

A8. Falsificación de peticiones en sitios cruzados (CSRF): Contempla cualquier actor, que pueda infectar los navegadores de un usuario que obligue a cargar o entregar información y que con ello pueda generar algún tipo de ataque.

A9. Utilización de componentes con vulnerabilidades conocidas: Utilizar componentes con vulnerabilidades conocidas, pueden ser explotados con facilidad luego de su implementación en desarrollo de software web.

A10. Redirección y reenvíos no validados: Contemplar la posibilidad de la ejecución de códigos o engaños que obliguen a los usuarios a acceder a otros sitios o reenviar información de la aplicación desarrollada.

OWASP, Open Web Application Security Project tiene entre sus finalidades como proyecto metodológico de Etical Hacking enfocado al software seguro en la web; promover desde todo punto de vista el desarrollo seguro, enfoca esfuerzos orientados a la prestación de servicios a la web, trabaja principalmente en el Back End y mucho menos en cuestiones de diseño, y se ofrece como un recurso gratuito metodológico para cualquier equipo o personal que se dedique al desarrollo de software.

Dentro de las herramientas que provee la metodología, se pueden encontrar, acompañando el Top Ten, algunas como Guía de desarrollo OWASP, las Guías de testing OWASP, Guías para las aplicaciones web seguras entre otros documentos.

7. AMENAZAS DE SEGURIDAD INFORMATICA EN ENTORNOS CORPORATIVOS DE PEQUEÑAS Y MEDIANAS EMPRESAS.

Hablar de amenazas en entornos corporativos de pequeñas y medianas empresas, seria delimitar a que este sector, tiene alguna particularidad de amenazas, pero no es así, básicamente, se podría decir, que puede tener algunas amenazas diferenciadas de empresas de mayor tamaño dados los tipos de tecnologías que estos manejan y las pymes aun no tengan implementadas. [26]" La seguridad de los datos sigue siendo un problema que afecta a las empresas de todos los tamaños. Tanto las grandes y las pequeñas empresas pueden ser el objetivo. Y la amenaza puede venir de cualquier parte".

Hablando de manazas y vulnerabilidades, necesariamente hay que decir, que van de la mano, ya que la amenaza, es quien materializa un riesgo al explotar una vulnerabilidad dentro de un entorno empresarial.

Para la ilustración el nivel de exposición de las pymes, y lograr plasmar que tan vulnerables pueden llegar a ser las empresas del sector, se van a identificar algunas amenazas de mayor relevancia y en lo posible, que sean comunes a la mayoría de entornos corporativos de pymes.

- **Ataques desde el interior de la compañía.**

La mayoría de las empresas, parten de la confianza depositada en sus empleados, más aun, cuando estos, hacen parte de entornos familiares, los cuales también son muy comunes en el sector pymes y de donde se deposita mucha más confianza en el personal, delegando acceso a la información olvidándose un poco de las medidas de seguridad necesarias y dejando mucho más a la deriva una adecuada protección de esta. La amenaza desde el interior de la compañía puede ser un vuelvo de este tipo de empleados, que aunque su confianza para el manejo de información es muy alta dada su condición, también puede convertirse en empleados insatisfechos que inician desde el interior a crear ataques simples, plasmados en fuga de información o deterioro de la misma.

Los ataques internos, también pueden llegar de empleados con conocimientos avanzados del negocio, e incluso avanzado en temas de tecnología que les

[26] Cepymenews. Las cuatro amenazas más comunes de ciberseguridad que pueden afectar a las pymes en 2019. El ransomware se ha convertido en una gran amenaza para las empresas de todos los tamaños, [En linea], 12 de Marzo de 2019, Disponible en: <https://cepymenews.es/amenazas-ciberseguridad-pueden-afectar-a-las-pymes-en-2019>

permiten extracción de la misma o acceso no autorizado a la información y posterior uso de ella, las empresas, cuando inician sus procesos de implementación de seguridad, inicialmente están mirando hacia el exterior, pensando siempre en protegerse de un acceso no autorizado, pero pocas veces se logra identificar la necesidad de protegerse de un acceso no autorizado a la información desde el interior de la compañía.

- **Mal uso del servicio de internet por parte de los usuarios.**

El internet es un servicio que ofrece muchas vulnerabilidades y múltiples amenazas para las empresas de todo sector económico, también es uno de los principales focos de control a la hora de hablar de seguridad, ya que este servicio puede llegar a representar una amenaza muy grande para las empresas. Viéndolo de otra forma, adquirir un virus, o ser víctima en internet de un secuestro de información de un solo usuario, puede afectar toda la información de la compañía, pensar en esto, debe dejar cierta preocupación cuando se habla de internet como una amenaza, y no es precisamente el internet, es la ingenuidad de los usuarios y su presencia en sitios no requeridos para las actividades empresarial lo que deja la alta exposición de la información.

Dejar abierto el servicio de internet al uso sin control de los empleados, puede permitirles a estos, desarrollar actividades que van en contra de la protección de la información, algunas como cargar o descargar información empresarial en almacenamientos personales, enviarla por correo electrónico, acceder a páginas con contenido peligroso y visitar a redes sociales de manera no controlada, son para las empresas del sector pymes la conformación de una gran amenaza por uso no adecuado del internet.

- **El usuario final como el eslabón más débil.**

Muchas de las amenazas pueden ser identificadas y tratadas con el fin de disminuir o impedir que se materialicen, pero el usuario, ha sido siempre catalogado como el eslabón más frágil de la cadena de la seguridad de la información o la seguridad informática, esto, porque en algunos casos, múltiples problemas de seguridad se generan con la complicidad ingenua de un usuario desprevenido, en algunos casos, ocioso y en su mayoría imprudentes.

La ingeniería social, sería la más común de las amenazas que llega a materializarse, usando como instrumento al usuario de la información. Ingeniería Social, vista también como un ataque, parte de la ingenuidad del usuario, al revelar algún tipo de información que permita acceder a esta y vulnerar su integridad, confidencialidad y

disponibilidad, lo más común es entrega de contraseñas, o transferencia de información confidencial sin ni siquiera darse cuenta a haberlo hecho.

- **Dispositivos mal configurados.**

Se puede inferir que en los entornos objetivos de las pymes, no hay una inversión considerable en tecnología, lo cual, también lleva a no contar con los recursos suficientes para implementar de forma segura mucha de esa tecnología que se pueda adquirir. Estas implementaciones se llevan a cabo por personal interno, que, en algunas ocasiones, no cuenta con experiencia suficiente en los procesos de configuración permitiendo algunas ventajas que terminan siendo vulnerabilidades para las empresa.

Ilustrando un poco más el concepto, se puede hablar de dispositivos de red, tan básicos como un (AP) - Access Point o un switch de distribución, que inicialmente se pensaría que no requiere de mucha experiencia para configurarlo, pero que pueden quedar desde servicios web del mismo expuestos, hasta configurar parámetros de contraseñas débiles y en protocolos de una fácil identificación con uso de herramientas de hacking y en algunas veces, hasta usando la simple lógica de prueba error hasta encontrar el acceso deseado.

Algunas llegan a implementar dispositivos de seguridad perimetral, pero estos terminan siendo un enemigo para para TI como para la misma empresa, y todo a raíz de no ser configurados correctamente, siendo este un dispositivo muy relevante a la hora de hablar de seguridad perimetral.

- **Servidores comprometidos en internet.**

Si ya se cuenta con una solución de perimetral tipo firewall, se inicia con los procesos de publicación de servidores, publicación de servicios en la web que requieren ciertos controles desde y hacia internet.

Una mala configuración de un servidor en una publicación en internet puede dejar la empresa de puertas abiertas para un ataque a través de éste. Siendo una de las formas de análisis tanto para personal de seguridad como de ciberdelincuencia, hacer un escaneo de puertos, a una dirección ip publica o hacia un servidor, sea dentro o fuera de la empresa, entrega aria la información de exposición a nivel de publicación de puertos y servicios.

Esta amenaza, puede ser incluso mucho más comprometedora en las vulnerabilidades que podrían generarse, si por desconocimiento se hace una

publicación de cualquier servidor o servicio sin una herramienta adecuada de seguridad perimetral.

- **Problemas de respaldo y recuperación de información.**

Vulnerabilidad o amenaza, puede verse desde las dos ópticas ya que materializa un riesgo alto de no poderse recuperar ante algún evento de seguridad que comprometa la información.

Desde el punto de vista de la amenaza, se puede valorar cualquier evento que ponga en riesgo la información y que luego de estar comprometida se requiera su recuperación y no se cuente con esta o no sea posible recuperarla. Desde el punto de vista de ser vulnerabilidad, se debe generalizar en cualquier tipo de compañía el mismo concepto, si no se cuenta con la información, la vulnerabilidad es alta aunque no se una vulnerabilidad expuesta, no es expresa ni explotable por una amenaza directa aunque se conozca, de antemano su inexistencia, simplemente hace parte de los planes de protección de la información que deben surtir como parte de un esquema de seguridad de la información.

- **Usuarios con dispositivos móviles corporativos.**

Las empresas actualmente permiten más conectividad a sus empleados, permitiendo el uso de sus equipos de cómputo personales desde la casa, el acceso al correo electrónico corporativo desde el teléfono celular o Tablet y obviamente acceder aplicaciones web con información empresarial desde estos mismos dispositivos.

Cualquier dispositivo que use un empelado para acceder a la información de la empresa cuando este no es de propiedad de esta, es un dispositivo que se convierte en una estación de trabajo para la empresa y de la cual, no tiene ningún tipo de control. Entrar y sacar información desde allí, no es controlable y mucho menos, quien más va a acceder a la misma, siendo este dispositivo de un común acceso para las personas cercanas al trabajador, pero sin ningún tipo de vínculo ni control para el empresario, lo cual, puede terminar hasta con perdida voluntaria o involuntaria de información empresarial.

- **Obsolescencia del software instalado.**

El software instalado juega un papel importantísimo en cómo se ven las empresas a nivel de seguridad desde el exterior, este exterior, comprende la posibilidad de ser analizados con alguna herramienta y poder encontrar la falta de algún parche de

seguridad, principalmente sistemas operativos, que permitan mediante su explotación el acceso a la información almacenada en su equipo de cómputo.

Los sistemas operativos, con los primeros que deben estar actualizados, pues estos, son las plataformas más básicas para almacenar la información empresarial. Algún otro software de terceros, también pueden ser afectados por obsolescencia en alguno de sus componentes usados que no cuente con la versión actualizada y que esta contenga alguna vulnerabilidad conocida.

Principalmente los productos Microsoft, con comúnmente los más atacados en sus plataformas de sistemas operativos, tienen los ojos encima de sectores para explotarlos como el mismo fabricante para protegerse, pero forman una parte fundamental en la prevención de ingreso a los sistemas de información.

8. HERRAMIENTAS ASOCIADAS A LAS METODOLOGÍAS DE ETICAL HACKING

En la identificación de herramienta que pueden ser objeto de prácticas de penetración, hay una gran variedad, algunas de ellas, enfocadas a una finalidad en particular y otras compuestas por un pool de aplicaciones que permiten para cada fin, encontrar un software con variedad de opciones para realizar sus taques o como es llamado en este documento, prueba de penetración.

Existen diferentes rankings de las mejores aplicaciones en internet, y aun, cuando logremos mencionar una gran cantidad de estas, pues contar con todas estas, como que fueran las más apropiadas para el desarrollo de las actividades de evaluación de vulnerabilidades a las empresas objetivo.

Hay que hacer claridad, que existen herramientas de un objetivo particular o enfocado a una herramienta o servicio específico dentro de una infraestructura tecnológica. Para el caso, se van a valorar algunas herramientas, principalmente que cumplan con objetivos generales de evaluación de vulnerabilidades y que permitan cubrir la mayor parte de las necesidades de las empresas según la disponibilidad de la arquitectura.

8.1. METASPLOIT PENETRATIONS TESTING SOFTWARE

Es una herramienta de validación y explotación de vulnerabilidades, su utilización, ayuda a los profesionales de seguridad, a dividir las tareas de gran magnitud en cuanto a seguridad, en tareas más pequeñas y de fácil ejecución, es una herramienta práctica de alto impacto de seguridad y con gran experiencia y respaldo a nivel mundial en el sector seguridad.

Cuanta con una interfaz de usuario la cual, permite de forma muy clara, hacer las evaluaciones de vulnerabilidades y las validaciones de seguridad en los entornos corporativos. Metasploit, también le permite automatizar el proceso de descubrimiento y explotación y proporciona las herramientas necesarias para realizar la fase de prueba manual de una prueba de penetración.

Metasploit se puede utilizar para buscar puertos y servicios abiertos dentro de cualquier infraestructura de red, también, explotar vulnerabilidades, pivotar más en

una red, recopilar pruebas y crear informes de los resultados generados en las pruebas.

"[27] Metasploit is a penetration testing platform that enables you to find, exploit, and validate vulnerabilities. The platform includes the Metasploit Framework and its commercial counterparts: Metasploit Pro, Express, Community, and Nexpose Ultimate."

Metasploit, cuenta con varias versiones en sus distribuciones de trabajo, en las cuales, se puede identificar, Metasploit Pro, Express, Community y Nexpose Ultimate, estas versiones, pueden variar según el producto, con respecto a las utilidades o funcionalidades ofrecidas por la marca en términos de vulnerabilidad y de explotación.

Sobre estas versiones disponibles, se menciona Metasploit Framework[28], el cual, es la base de software con la que se desarrollan productos comerciales como exploit, es una herramienta de uso libre y código abierto, que permite realizar pentesting y varios tipos de auditoria.

8.2. SETOLLKIT, SOCIAL ENGINEER TOOLKIT SOFTWARE

[29]Es una herramienta de código abierto impulsada por Python destinada a pruebas de penetración en torno a la Ingeniería Social., Kit de Herramientas de Ingeniería Social, suena como una herramienta enfocada 100% a hacer ingeniería social, pero no es así, es una herramienta robusta, dentro de las cuales, se destacan su capacidad de ataque a sitios web, principalmente, con una integración de la herramienta en entornos suite de análisis de vulnerabilidades que la convierten en una importante herramienta a la hora de complementar otras soluciones.

SET, es una suite completa dedicada principalmente a la ingeniería social como modo de análisis de vulnerabilidades y ejecución de ataques, El kit de herramientas SET está especialmente diseñado para realizar ataques avanzados contra el

---

[27] Metasploit. , Getting Started, Metasploit Implementation. [en línea], Noviembre de 2018, Disponible en: < https://metasploit.help.rapid7.com/docs/getting-started >

[28] Metasploit Getting Started, Metasploit Framework, [En línea], Noviembre de 2018, Disponible en: < https://metasploit.help.rapid7.com/docs/getting-started >

[29] Trustedsec, A Powerful Tolls For Social Engineering, The Social-Engineer Toolkit (SET), [En linea], Noviembre de 2018, Disponible en: < https://www.trustedsec.com/social-engineer-toolkit-set/ >

elemento humano dentro de la cadena de seguridad de la información, el cual ha sido denominado históricamente, como el elemento más débil dentro de la cadena de seguridad.

SET, integra algunas funcionalidades que también presente en Metasploit dentro de su Suit Community, de igual forma, puede usarse desde la distribución de Metasploit, e incluso desde Kali Linux.

8.3. NMAP NETWORK MAPPER, FREE SOFTWARE SCANNER

Aunque no es una suite de herramientas, sino, una herramienta que está incluida en las principales suite de análisis de vulnerabilidades de seguridad, por lo menos en las más comerciales está incluida y hace parte de las más usadas, no solo a nivel de seguridad en tareas de análisis de vulnerabilidades, sino también, en los procesos de administración de plataformas tecnológicas ya que sus principales usos van enfocados a la identificación de servicio y puertos en las plataformas tecnológicas y servicios implementados en servidores.

Entre las características principales de la herramienta, se pueden destacar:

- *Flexible*: Permite variedad de técnicas avanzadas para descubrimiento de redes que cuenten con dispositivos perimetrales como firewall, filtros de direccionamiento IP, Reuters y cualquier obstáculo de intrusión, esto incluye escaneo de puertos en red, versionamiento de SO-Sistemas Operativos y barridos ICMP por ping entre otras.

- *Potente:* Nmap se puede usar para revisión y escaneo de redes con gran cantidad de número de máquinas y equipos conectados.

- *Portátil:* Casi todos los SO-Sistemas Operativos, son compatibles, incluidos Linux , MS-Windows , Free-BSD , Open-BSD , Solaris , IRIX , Mac-OS X , HP-UX , NetBSD , Sun OS, puede corree en ellos y llegar a ellos desde alguna suite que lo contenga.

- *Sencillo y fácil:* La herramienta cuenta con versiones en línea de comandos y entornos gráficos para diversos sistemas operativos, esto permite una sencillez y facilidad al uso acompañado de su documentación en línea.

- Gratuito: La finalidad del proyecto es mejorar la seguridad de los entornos tecnológicos, permitiendo uso de herramientas de código abierto, Nmap, se ha destacado en el medio, por ser una herramienta usada por administradores y personal de seguridad de forma proactiva en sus actividades diarias. Todo esto ha permitido una gran acogida en los entornos empresariales.

Nmap, también está incluido en la suite de Kali Linux, y puede usar incluso desde su versión de interface gráfica llamada Zenmap.

8.4. DRADIS REPORTING AND COLLABORATION FOR INFORMATION SECURITY TEAMS

Es una herramienta de pentesting Open Source, que permite en su uso, la organización de la información generada en un repositorio centralizado, esta herramienta, también permite el uso de plugins, lo cual, la convierte en una ideal en la ejecución de proyectos de pentesting, es una aplicación flexible, ya que es portable y esto, independiza el uso de ella a las plataformas tradicionales, entregando flexibilidad a los usuarios.

Cuenta con una instalación simple, y requiere una configuración mínima de parámetros para que se pueda iniciar a funcionar, permite ser instalada tanto en plataformas Linux como sistemas operativos Windows, y se encuentra suficiente información para sus procesos de implementación en la web oficial del fabricante.

[30]Esta herramienta, desarrolla una integración interesante con metodologías de análisis de vulnerabilidades como OSSTMM, OWASP Top 10 y OWASP Web testing entre otras, de las cuales se hacen una composición de resultados en su análisis de datos para proporcionar información clara y consistente.

[30] Dradisframework, Deliver Consistent Results, Quality and Consistency, [En línea], Noviembre de 2018, Disponible en: < https://dradisframework.com/consistency.html >

8.5. KALI PENETRATION TESTING AND ETICAL HACKING LINUX DISTRIBUTION.

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd[31].

Como referencia más común, [32]"Una de las principales virtudes de Kali Linux son las más de 300 herramientas y aplicaciones relacionadas con la seguridad informática que incluye esta distribución, destacando algunas tan conocidas como Nmap, que permite escanear los puertos de un sistema, el crackeador de contraseñas Jack the Ripper o la suite Aircrack-ng para comprobar la seguridad de las redes inalámbricas."

Esto, básicamente, nos integra algunas de las herramientas ya mencionadas en este documento, que aunque hacen parte de una familiar de soluciones para el desarrollo de tareas de evaluación de seguridad en las organizaciones, por si solas, no todas cumplen con la función total de evaluación de seguridad. Pero en Kali, ya se encuentran integradas de forma que se pueda encontrar dentro de la misma distribución, como complementos o utilidades de uso en temas de seguridad.

Esto, convierte a Kali Linux, en una de las principales herramientas de identificación de vulnerabilidades del mercado de la seguridad informática. Aunque parece ser para fines de explotación, que normalmente, se asocian con delincuencia en la red, esta herramienta, se diseñó inicialmente, para fines forenses, con lo cual, su éxito hizo que se fuera difundiendo y terminará siendo la principal herramienta de análisis de seguridad del mercado Open Source.

Ser Open Source, le ha servido para que múltiples aplicaciones de su misma naturaleza de licenciamiento, se vayan adicionando a la distribución, y esto, enriquezca diariamente su tamaño y utilidad.

---

[31] Offensive-Security, Kali Linux Downloads – Virtual Image. Download Kali Linux VMware and VirtualBox Images, [En línea], Noviembre de 2018, Disponible en:< https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-hyperv-image-download/ >

[32] Computerhoy, Qué es Kali Linux y qué puedes hacer con él, [En línea], Noviembre de 2018, Disponible en: < https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671 >

[33]La distribución, cuenta con versiones de 32 y 64 bits, disponibles tanto para plataformas Linux como unos paquetes de distribución disponibles para VirtualBox y Vmware.

Es una completa herramienta con fines empresariales, que permite hacer desde el escaneo de la red para identificar los host dentro de esta, hasta la explotación de las vulnerabilidades que mediante cualquiera de sus herramientas de escaneo, se puedan evidenciar, que se constituye esta, en una herramienta privilegiada para el objetivo de este documento.

También se puede mencionar aquí, la herramienta que dio origen a Kali, y es [34]Back Track, al cual siendo de la misma casa de Offensive Security, sigue disponible como una alternativa de software frente a Kali. Viendo Kali como la evolución de Back Track, aún se distribuye y actualiza la segunda, pero la primera, ha sabido copar la mayoría del mercado de seguridad, y aunque entre ellas comparten gran parte de sus aplicaciones disponibles, difieren en especial, en que Back Track, adiciono algunas aplicaciones comerciales a la distribución, lo que no sucede con Kali, la cual conserva su filosofía de Open Source total.

8.6. CLASIFICACIÓN DE HERRAMIENTAS DISPONIBLES.

Dentro de la validación de herramientas disponibles para desarrollar procesos de análisis de vulnerabilidades, se pueden encontrar herramientas independientes, orientadas a un servicio, a un tipo de protocolo, a una capa del modelo OSI y hasta solo a presentar reportes o tan simples como un escáner de host para su identificación en la red, lo cual también puede ser un aporte para un análisis de vulnerabilidades.

La disponibilidad de las herramientas adecuadas, puede ser una de las dificultades de las empresas a la hora de poder emprender un proceso de análisis de vulnerabilidades dentro de cada una de las empresas, y esto, aunado al desconocimiento de su personal en temas de seguridad, puede convertirse en el inicio y el fin de los procesos de análisis en las organizaciones, principalmente las pymes.

---

[33] Kali, Kali Linux Downloads, Download Kali Linux Images, [En Linea], Noviembre de 2018, Disponible en: < https://www.kali.org/downloads/ >

[34] OffensiveSecurity, BackTrack Linux, Back | Track Linux Penetration Testing Distribution, [En linea], Disponible en: < https://www.offensive-security.com/community-projects/backtrack-linux/ >

En esta revisión de herramientas, se hizo una elección de herramientas más comunes y de mejores prestaciones dentro de las que se lograron identificar durante la investigación, lo cual, entrego una visión más específica de cada una de ellas y permitió encontrar las herramientas a cada tipo de necesidad que pueda terne una pyme para su análisis de seguridad.

Las herramientas individuales, aunque tiene su uso y son eficientes en ello, dejarían un vacío de proceso o extenderían las actividades necesarias para el desarrollo de los análisis, en el peor de los casos, sería un factor para abortar la idea, luego de que por desconocimiento, algunas puedan determinar una inversión alta de tiempo y opten por no continuar con su desarrollo. Esto, teniendo en cuenta, que de igual forma, el ejercicio de análisis de vulnerabilidades, cumpliendo con algunas de las metodologías disponibles, debe llevar un componente de tiempo a emplear que depende entre otras, del tamaño de la organización a nivel de equipos y de disposición de la plataforma tecnológica.

La disposición de la plataforma, refiere tanto a como está construida, lo cual indica su topología y distribución, y también, a como esta su uso, lo cual puede dificultar actividades donde se requiera ventanas de mantenimiento para su desarrollo, en etas actividades, y mirándolas conjuntamente, se ve que se requiere una inversión de tiempo, que para ser más óptimos en el uso d este, deben ir acompañadas de una buena planeación para su ejecución.

Para evitar dificultades en términos de disponibilidad, estos análisis de vulnerabilidades, deben ser una iniciativa de la organización en términos de impulso desde la gerencia o la máxima directiva, ya que no tendría el mismo efecto dentro de la comunidad laboral si es propuesta o desarrollada únicamente por iniciativa del personal de TIC.

La optimización del tiempo, también se ve reflejada en el uso de una única herramienta pentesting o en el uso de una cantidad de aplicaciones que requieren instalación, configuración e integración lo cual retrasaría de alguna forma los procesos, por esto, hay que ser cuidadosos en la elección de al herramienta, la cual, permita la integración de los procesos y la facilidad de ejecución de las herramientas a la vez, que cuente con documentación disponible como referencia para la ejecución de las tareas de evaluación.

8.6.1. Herramientas individuales de análisis.

Las herramientas individuales, aunque funcionales, pueden representar alguna dificultad a la hora de su uso. Esto no indica que no sea viable su utilización, sino, que simplemente, acordar la utilización de herramientas compactas dada su existencia, puede aportar en la construcción del proceso dentro de las organizaciones.

Las herramientas individuales, aunque agrupadas cada una de ellas tiene el mismo fin, se plantea la posibilidad de contar con estas en un entorno compacto de herramientas que permitan abarcar todos los aspectos disponibles en la organización para evaluar y no tener que salir de una misma instalación que posiblemente indique cambios deposiciones dentro el proceso de evaluación y que finalmente segmente mucho a la información recolectada.

Cuando se usan las herramientas de forma individual, el proceso se dificulta al tener que estar en diversos espacios en internet en la búsqueda de estas y de cómo se implementan o usan, desde el punto de vista utilitario, esto puede representar una dificultad para las personas que de alguna forma conozcan herramientas integradas, pero también para aquellas que vayan a tener su primer contacto con estas herramientas y más aún, si van a iniciar en su aplicación y desconocen los temas de integración o de como complementar unas con otras y sacar así el mejor provecho de cada una.

La utilización de las herramientas individuales, puede representar una ventaja en cuanto a la utilización y aplicación de los pasos de evaluación de manera parcial, lo cual, puede representar una ventaja en termino de tiempo, poca indisponibilidad de la plata de personal o la infraestructura, por uso en los procesos de evaluación, también, podría identificarse una afectación menos, esto, contando con que alguna de las evaluaciones aplicadas, puedan representar alguna afectación en la calidad de los servicio instalados.

Finalmente, la disponibilidad de herramientas permite una variedad de ventajas respecto a la posibilidad de implementación de acciones en tiempos diferenciados sin necesidad de abrir amplias ventanas de mantenimiento, lo cual, termina beneficiando a la organización, pero va a ralentizar un poco el desarrollo de la actividad, nuevamente aquí, cobra valor, la capacidad de planeación que se tenga en la implementación del proceso de evaluación de vulnerabilidades.

8.6.2. Suites de herramientas de análisis.

En cuanto a las suites de herramientas, estas, hacen parte de un modelo de contenedor de herramientas en este caso, orientadas desarrollo de pruebas de vulnerabilidad y aunque históricamente, personas ajenas a este medio, refiriéndonos al medio tecnológico, han sabido entender el uso de las mismas como herramienta para la criminalidad, en la actualidad no es más importante ese uso, pues la masificación de estructuras académicas y tras de ellas las estructuras organizacionales este tipo de herramientas, han tomado un lugar importante en la prevención de ataques, en la prevención de materialización de vulnerabilidades y en algunos casos, hasta han podido aportar a la implementación de controles de sistemas de gestión de seguridad de la información.

Las suites, soportan una gran cantidad de reunión de aplicaciones, los cual es bueno para los profesionales de seguridad de la información, que dentro de estas aplicaciones encuentran múltiples herramientas que pueden ser útiles para la implementación de procesos y la resolución de muchos incidentes de seguridad principalmente, en las organizaciones y en su día a día.

Estas herramientas, se pueden encontrar de varios tipos, entre ellas, de licenciamiento, en los que como es común a nivel de software, en su gran mayoría son desarrollo de Open Source y otra más poca cantidad, hacen parte de aplicaciones propietario que de alguna forma, han llegado a estas herramientas consolidadas, pero que en la práctica, aun al presentar productos muy buenos, terminan no ayudando mucho al usuario de estas suite, dado que estos, buscan como es tradicionalmente en estas, aplicaciones Open Source que les permitan resolver sus problemas de seguridad entre otros y encontrarse con aplicaciones de pago, cierra la posibilidad de la existencia de una gratuita e invita indirectamente al usuario no hacer uso de ella.

Esta característica, se ha identificado en la distribución Back Track, la cual, en su versión 4, entrego aplicaciones de pago entre todas las open Source históricamente disponibles, lo cual genero muchos comentarios entre los usuarios de la misma. Esta condición, no le quita usuarios a la distribución, pero si le suma más adeptos a otras como Kali Linux quien conserva su filosofía 100 % Open Source.

8.7. PROPUESTA DE USO DE HERRAMIENTA

Entre las herramientas más comunes y completas, se puede identificar Kali Linux, como la más relevante, esta herramienta nace desde Offensive Security, como herramienta base dentro de la metodología de análisis de vulnerabilidades. Aquí, se puede ver como Kali Linux, es una mejora en el tiempo, por compilación y funcionalidades con respecto a BackTrack y en general, al resto de herramientas, ya que ellas, están incluidas aquí y ésta, ofrece una Suit integral de aplicaciones para suplir las necesidades de análisis de seguridad.

Actualmente Kali Linux, conserva esa misma utilidad y hace un ejercicio de agrupamiento de más de 300 aplicaciones relacionadas con diferentes temas dentro de las necesidades de evaluación de activos de información de cualquier organización.

Kali Linux es una distribución con base en Debían, que actualmente corre en arquitecturas de 32 y de 64 bits, lo cual la convierte en una de las más versátiles y completas disponibles en Open Source. Compone una suite de aplicaciones que llegan a integrarse desde su propia ventana de terminal con la ejecución de sus aplicaciones en modo consola, algunas de estas, cuentan con interfaces graficas amigables, pero en su gran mayoría conservan esa mística de las tecnológicas open Source de manejo de líneas de comando para la ejecución de sus utilidades.

Esta suite, permite una disponibilidad de herramientas que aportan a los procesos de desarrollo de pentesting en las organizaciones, cuenta con diversas herramientas que pueden apuntar al mismo objetivo de evaluación, y eso la hace más rica en su ofrecimiento de utilidades. Contar con una gran cantidad de herramientas, la hace una solución ideal a la hora de implementación de evaluaciones de seguridad informática y tareas de auditoria a sistemas de información e infraestructuras de cualquier tamaño.

9. RECOMENDACIÓN DE METODOLOGIA DE ETHICAL HACKING PARA LAS PYMES.

Las referencias presentadas en las metodologías expuestas, se pueden valorar aspectos relevantes de estas, que van a soportar la pertinencia de cada una para su posible aplicación en un ejercicio de identificación de vulnerabilidades en una empresa del sector objetivo, esta misma valoración de aspectos, va a permitir ubicar cada una de las metodologías dentro de una línea clara de actuación, cuando para una aplicación de enfoque más directo.

Metodología OWASP

Afirmar que la metodología OWASP, debe ser descartada en su totalidad, dado que se requiere una metodología, que permita atender completamente un entorno empresarial, donde se tengan en cuenta todos los aspectos corporativos en relación con las tecnologías de Información y Comunicaciones, relacionadas directamente con la seguridad informática y la seguridad de la información.

Claramente se observa al repasar la descripción de información reportada en el presente trabajo, más la validación en los portales oficiales de la metodología, que OWASP, esta fielmente enfocado a procesos de mejora, evaluación y buenas prácticas de configuración en aplicaciones y proceso de desarrollo de software y que desde sus inicio, aunque cumplió con funciones de testing de seguridad en aplicaciones web, hoy en día, tiene fortalecida su estructura en procesos de mejores prácticas en desarrollo de software seguro y en presentar marcos de trabajo con relación al desarrollo seguro y al testing de aplicaciones en desarrollo, así como la publicación de recursos para apoyo directo a la áreas de desarrollo, principalmente fortaleciendo productos e Back End para las soluciones web.

Metodología ISSAF

Extrayendo su orientación a través de sus metodologías usadas y la forma como se desarrolla su estructura, es claramente identificable, que la metodología ISSAF, es una metodología enfocada a cumplir en procesos de seguridad informática, los cuales asociados a procesos de gestión empresarial, reciben un aporte valioso de la metodología, esta, la encargada de evaluar su nivel de madurez, esta metodología, se basa en los procesos organizacionales, para implementar su seguridad en estos y la principal característica de su integración a los procesos, es que puede usar la matriz de riesgos de la organización o pude desarrollar su propia matriz enfocada a los temas de tecnología. Todo esto, hace de la misma, una

metodología, altamente ejecutiva, que ejerce mucho control administrativo sobre los procesos empresariales y complementa muy bien la gestión corporativa por procesos.

Metodología OSSTMM

OSSTMM, es una metodología que indudablemente, ha entregado a las organizaciones, un proceso claro y con una estructura global, que le permite implementar procesos de valoración de seguridad en las organizaciones, con base en sus procesos de negocio[35]. Algunas de las características más relevantes de la metodología, se pueden evidenciar en la estructura de sus procesos base, donde se puede identificar como al conformar una especie dominios, que sugieren cubrir todos los puntos organizaciones a nivel tecnológico, aquí, se puede evidenciar un modelo especifico hacia la seguridad de la información, la seguridad de los procesos de negocio, la seguridad en las tecnológicas de usan el servicio de internet, la seguridad en las comunicaciones, las cuales, incluyen comunicaciones donde se usan operadores externos, también las conexiones inalámbricas, en al cuales, se incluyen tanto las desarrolladas por las organizaciones como las prestadas por terceros y finalizar, con una concepción de seguridad física que termina aportando en temas tanto de infraestructura tecnológica, como de infraestructura fascia. Todo esto se logra, gracias a que la metodología, compila sus dominios, de cara a la aplicación de ellos en los procesos de la organización.

La metodología plantea unas categorías de desarrollo de su proceso y cubre lo que para ella representa ser la metodología ideal en los entornos corporativos, dentro de esto:

La Búsqueda de Vulnerabilidades: Validaciones de los sistemas implementados en los entornos empresariales.

Escaneo de la Seguridad: Busca principales de vulnerabilidades, puntos débiles en los sistemas de información y realiza un análisis individual de cada uno de los existentes.

Test de Intrusión: Aquí se busca permear la seguridad de los sistemas de información empresariales.

---

[35] Juanta de Andalucia, Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM), Introducción. [En línea], Disponible en: < http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551 >

Evaluación de Riesgo: Indica referencia a los análisis de seguridad, que se desarrollan con entrevistas y con procesos de investigación de nivel medio bajo, esto incluye justificaciones legales y de industria aplicables.

Auditoria de Seguridad: Auditar el cumplimiento de las políticas de seguridad, así como de sus controles.

Hacking Ético: Ejecución de test de intrusión para develar vulnerabilidades.

9.1. METODOLOGIA RECOMENDADA PARA LAS PYMES.

Luego de los análisis previos de las metodologías citadas en el presente trabajo, y previa exposición de las bondades o enfoques de las mismas con relación al desarrollo de cada metodología, se recomienda la metodología Offensive Security, llega a ser la metodología más acertada a modelo de identificación y valoración de vulnerabilidades. Es una metodología de enfoque de explotación y un alto nivel práctico, orienta a los resultados inmediatos, sin sacrificar la disposición de la documentación p los procesos, pues también cuenta con una estructura metodológica, aplicable a cualquier tipo de empresa, y que cubre los aspectos más importantes en la generación de un test de seguridad.

Como se pudo observar anteriormente en la descripción de cada una, para el caso de esta metodología, cumple unas etapas muy puntuales en su proceso, las cuales se pueden identificar como; recolección de información, Análisis de vulnerabilidades, Definición de Objetivos secundarios, Ataque y Análisis de resultados.

Aquí, se puede identificar o valorar el Ataque, como el centro de la metodología, esto no quiere decir, que otras metodologías no lo hagan, efectivamente otras también cumplen con la etapa de ataque, pero específicamente la Offensive Security, tiene el ataque como su estampa más importante, dado que esta, se caracteriza por su modelo practico aplicado y por su referencia a ser una metodología altamente invasiva, ya que usa el ataque como materia prima de sus análisis, es decir, ataca realmente los sistemas para obtener las vulnerabilidades y con esto, poder entregar un diagnostico puntual, que indique la forma más adecuada de protección, esto la hace aplicable a cualquier tipo de empresa, independiente de su tamaño o de enfoque económico, es una metodología de gran aceptación en el medio, principalmente por su practicidad.

10. CONCLUSIONES.

- Las metodologías de Etical hacking, son un aporte a la informática defensiva que le permite a las empresas conocer anticipadamente, cuáles son sus vulnerabilidades frente a la exposición tecnología de su infraestructura, teniendo en cuenta los servicios expuestos en internet y la configuración de los mismos al interior de las organizaciones.

- En la búsqueda de metodologías apropiadas para cada compañía, es importante la observación de un experto en el reconocimiento de su infraestructura instalada, esto, ya que pueden existir objetivos diferenciados o dirigido para la aplicación de un análisis de vulnerabilidades para lo cual, también se pueden encontrar herramientas en la metodología recomendada o aplicar alguna metodología puntual, según lo requiera el objetivo definido.

- Las vulnerabilidades y las constantes amenazas en los diferentes ambientes empresariales, hace que persista una exposición constante de la de información en cualquier ámbito empresarial, principalmente en el sector objetivo de esta investigación, ya que no siempre, invierten en controles suficientes que mitiguen los riesgos asociados, lo cual, los hace un sector más vulnerable a la perdida de información y a poder recibir algún tipo de ataque informático.

- Las pymes no cuentan con suficiente musculo económico para procesos de Etical hacking continuos o procesos de implementaciones robustas, allí, se pueden hacer análisis parciales y actividades de mitigación programadas que le permitan el cierre de brechas de seguridad de una forma oportuna. Contar con una identificación oportuna de sus vulnerabilidades, les va a brindar oportunidades de corrección de sus aspectos débiles de seguridad de la información.

- Existe una amplia variedad de herramientas asociadas a la metodología Ofensiva recomendada, las cuales, son principalmente de uso libre y que pueden ser aplicadas en los análisis de vulnerabilidad de las empresas objetivo, estas herramientas, están en algunas suites conocidas de como Kali Linux y que presta varias utilidades con relación a las pruebas a desarrollar en cada entorno empresarial, también se pueden encontrar en internet, herramientas disponibles en la suite mencionada, de forma individual, las cuales cuentan con documentación disponible en sus portales oficiales.

- Existen empresas del sector de TIC con experiencia en procesos de Etical hacking y uso de diversas herramientas que pueden apoyar los procesos de evaluación de cualquier organización. Para la aplicación de parte de un externo, se debe tener claridad de la infraestructura instalada para proporcionar la información adecuada para su aplicación.

- La metodología de Seguridad Ofensiva, puede ser empleada en la identificación de vulnerabilidades, ya que hace evaluación exacta y entrega información inmediata de las vulnerabilidades encontradas para su oportuna gestión, al ser ejecutada sobre los entornos de producción, puede llegar a ser invasiva para el entorno productivo, lo cual no permite dejar de lado una ejecución controlada en un ambiente de pruebas.

- Cualquier empresa del sector pymes puede implementar Etical hacking, por lo cual, aplicar la metodología recomendada le va a permitir obtener información oportuna para la preparación de defensas y reducción del riesgo en sus entornos productivos.

11. RECOMENDACIONES.

- Conocer la infraestructura tecnológica administrada a fondo por parte del personal encargado del área de tecnología, esto, con el fin de poder definir una posición de seguridad de la información o seguridad informática clara y aportante a la protección de la misma, lo cual también, permite ejercer control sobre la misma infraestructura y los servicios prestados en ella.

- Crear conciencia empresarial sobre una cultura de seguridad informática y seguridad de la información como una iniciativa de la alta gerencia, esta iniciativa desde la gerencia, apalanca la necesidad de controles desde TIC, con los cuales los administradores de tecnología apoyan de forma significativa procesos posteriores de seguridad de la información en las empresas.

- Implementar la metodología recomendada ya sea con recursos humanos contratados o propios, siempre y cuando estos recursos propios, tengan la formación necesaria para identificar y ejecutar las pruebas adecuadas sin que estas, afecten el entorno productivo de la organización.

- Elegir un entorno de pruebas con información real para la implementación de los análisis con la metodología recomendada, cuando esta, sea ejecutada por personal propio que no cuente con experiencia suficiente, todo con miras, a salvaguardar la continuidad de la operación, pero a su vez, poder identificar las vulnerabilidades, lo cual también obliga, a que sea un entorno exacto al de producción.

- Diseña e Implementar políticas de seguridad de la información que entreguen lineamientos de control a los diferentes actores del manejo de la información empresarial, estos deben incluir tanto al usuario final y la alta gerencia, como también a proveedores y otros actores que se puedan identificar en un análisis previo.

- Planear análisis segmentados de seguridad cuando estos se deban realizar contra la infraestructura en el entorno productivo, esto va a permitir, disminuir el riesgo de quedar fuera de aire en varios servicios al tiempo y también, puede permitir, dedicar el tiempo suficiente a las etapas de explotación pura y análisis de la metodología recomendada.

- Mantener actualizado el software instalado, esto disminuye la posibilidad de ataque informático, principalmente en sistemas operativos y software de terceros, más aun, cuando las maquinas que lo contienen, sean equipos clientes o servidores, están expuestos en internet, ya sea como actores de navegación o con servicios publicados.

- Documentar los procesos del área de gestión TIC con relación a controles de seguridad de la información, principalmente en temas de respaldo y recuperación de la información, que, a su vez, incluyan procesos de restauración y verificación de medios de almacenamiento que permitan mantener una disponibilidad clara al momento de requerir la recuperación de la misma.

12. REFERENCIAS BIBLIOGRAFICAS.

ANGULO. Susana, LAS PYMES COLOMBIANAS TIENEN BUENAS EXPECTATIVAS SOBRE SU FUTURO, [En línea], 30 de Septiembre de 2016, Disponible en: <http://www.enter.co/especiales/claro-negocios/las-pymes-colombianas-tienen-buenas-expectativas-sobre-su-futuro/>

Caracol Radio, 10 empresas colombianas y una entidad estatal afectadas por ciberataque, [En línea], 13 de Mayo de 2017, Disponible en: <http://caracol.com.co/radio/2017/05/13/tecnologia/1494700226_689517.html>

Computerhoy, Qué es Kali Linux y qué puedes hacer con él, [En línea], Noviembre de 2018, Disponible en: <https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671>

CONTRERAS. Nicolás, Más del 80% de las compañías en Colombia, son vulnerables a ataques informáticos, [En línea] 09 de Junio de 2016, Disponible en: <http://caracol.com.co/radio/2016/06/09/tecnologia/1465469190_389745.html>

Dinero, Las Empresas, combaten los ataques informáticos con tecnología obsoleta, [En línea], 29 de Enero de 2016, Disponible en: <http://www.dinero.com/empresas/tecnologia/articulo/informe-de-seguridad-de-cisco-2015-sobre-seguridad-informatica/218610>

Dinero.co, Los sectores económicos más impactados por el cibercrimen en Colombia, [En línea], 26 de Septiembre de 2017, Disponible en: <http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321>

Dradisframework, Deliver Consistent Results, Quality and Consistency, [En línea], Noviembre de 2018, Disponible en: <https://dradisframework.com/consistency.html>

E, C, M. Ezequiel Sallis, Claudio Caracciolo, Marcelo Rodriguez, “Tipos de análisis de seguridad”, in ETHICAL HACKING, Un enfoque metodológico para profesionales, D. Fernandez, G. Silveiro, Alfaomega Grupo Editor Argentino S.A. Buenos Arires Argentina, 2010, pp 11-27.

E, C, M. Ezequiel Sallis, Claudio Caracciolo, Marcelo Rodriguez, “RECONOCIMIENTO PASIVO”, in ETHICAL HACKING, Un enfoque metodológico

para profesionales, D. Fernandez, G. Silveiro, Alfaomega Grupo Editor Argentino S.A. Buenos Aires Argentina, 2010, pp 29-42.

Fedex, Oportunidades para las PyMEs en el mercado internacional, [En Línea], Septiembre de 2015, Disponible en: <http://images.fedex.com/downloads/lac/global/infografico_esp_final.pdf>

JIMENO. Pablo, Seguridad en la información, [En línea], 06 de Noviembre de 2012, Disponible en: <https://news.sophos.com/es-es/2012/11/06/seguridad-en-la-informacion/>

Juanta de Andalucia, Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM), Introducción. [En línea], Disponible en: <http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551>
Kali, Kali Linux Downloads, Download Kali Linux Images, [En Linea], Noviembre de 2018, Disponible en: <https://www.kali.org/downloads/>

LUZARDO. Ana Maria, ECONOMÍA DIGITAL GENERA POSITIVISMO EN LAS PYMES COLOMBIANAS, ¿Qué oportunidades representa la economía digital para las pymes?, [En línea], 20 de Febrero de 2017, Disponible en: <http://www.enter.co/especiales/empresas-del-futuro/economia-digital-genera-positivismo-en-las-pymes-colombianas/>

Metasploit Getting Started, Metasploit Framework, [En línea], Noviembre de 2018, Disponible en: <https://metasploit.help.rapid7.com/docs/getting-started>

Metasploit. , Getting Started, Metasploit Implementation. [En línea], Noviembre de 2018, Disponible en: <https://metasploit.help.rapid7.com/docs/getting-started>

MINTIC, MinTIC y OEA firman convenio para conocer el impacto de los incidentes cibernéticos en el país, [En línea], 22 DE Julio de 2016, Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-15753.html>

MINTIC, Las Mipyme se actualizan en el Día Internacional de la Seguridad Informática, [En línea], 30 DE Noviembre de 2016, Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-22318.html>

MINTIC, Taller sobre "Seguridad Internacional y Diplomacia en el Ciberespacio", [En línea], 07 DE Noviembre de 2014, Disponible en: <http://www.mintic.gov.co/portal/604/w3-article-7696.html>

MINTIC, LEY 1273 de 2009, [En línea], Enero de 2009, Disponible en: <https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>

OffensiveSecurity, BackTrack Linux, Back | Track Linux Penetration Testing Distribution, [En linea], Disponible en: <https://www.offensive-security.com/community-projects/backtrack-linux/>

Offensive-Security, Kali Linux Downloads – Virtual Image. Download Kali Linux VMware and VirtualBox Images, [En línea], Noviembre de 2018, Disponible en:<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-hyperv-image-download/>

Open Source Security Testing Methodology Manual (OSSTMM), Consulta En Línea, Sitio Oficial, Disponible en: <http://www.isecom.org/research/>

OWASP Top 10 Most Critical Web Application Security Risks, [En línea], 12 de Mayo de 2018, Disponible en: <https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf>

OWASP Top 10 Most Critical Web Application Security Risks, [En línea], 12 de Mayo de 2018, Disponible en: <https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf>

Portafolio, Cuatro de cada diez empresas en el país no están preparadas para un ciberataque. [En línea], 10 de Marzo de 2016, Disponible en: <http://www.portafolio.co/negocios/empresas/ciberataque-empresas-preparadas-colombia-492281>

SITIO OFICIAL OPEN VAS, Documentación herramienta. About OpenVAS , [En línea], 12 de Noviembre de 2017, Disponible en: <http://www.openvas.org/about.html>

Sitio Oficial, SQLMAP Automatic SQL injection and database takeover tool. Documentación herramienta usos. [En línea], Octubre de 2017, Disponible en: <http://sqlmap.org>

Sophos, Datos bancarios y sensibles de empleados, están en riesgo. Una exhaustiva encuesta del fabricante a responsables de TI evidencia las actuales carencias en seguridad por el desaprovechamiento de la tecnología de cifrado de datos, [En línea], 02 de Febrero de 2016, Disponible en: <https://www.sophos.com/es-es/press-office/press-releases/2016/02/state-of-encryption.aspx>

Sophos, The State of Encryption Today. Results of an independent survey of 1700 IT managers, [En linea], Diciembre de 2015, Disponible en: <https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/the-state-of-encryption-today-wpna.ashx?la=es-ES>

Tenable, Products Vulnerability Management. BUILT FOR RACTITIONERS, BY PRACTITIONERS, [En línea], Octubre de 2018, Disponible en: <https://www.tenable.com/products/nessus-vulnerability-scanner>

Trustedsec, A Powerful Tolls For Social Engineering, The Social-Engineer Toolkit (SET), [En linea], Noviembre de 2018, Disponible en: <https://www.trustedsec.com/social-engineer-toolkit-set/>