Información Importante

Universidad de La Sabana

EVALUACIÓN DE SEGURIDAD A SISTEMAS DE INFORMACIÓN EN CUANTO A ATAQUES MALICIOSOS CON BASE EN NORMATIVIDAD, TENDENCIAS, IMPACTO Y TÉCNICAS VIGENTES PARA AMBIENTES EMPRESARIALES A NIVEL NACIONAL.

Universidad de La Sabana

PROYECTO PARA OPTAR AL GRADO DE INGENIERÍA EN INFORMÁTICA

MODALIDAD INDEPENDIENTE

PROFESOR DIRECTOR:

PUENTES PINTO CARLOS ALBERTO

AUTOR:

DAVID HERNANDO ALONSO TORRES

CÓDIGO: 200922130

UNIVERSIDAD DE LA SABANA

FACULTAD DE INGENIERÍA

CHÍA, CUNDINAMARCA

COLOMBIA

MARZO DE 2014

Universidad de La Sabana

Chía, Marzo 19 de 2015

Señores
Facultad de Ingeniería
La Ciudad

Cordial Saludo,

A través de la presente, nos permitimos presentar el proyecto modalidad independiente titulado: ***EVALUACIÓN DE SEGURIDAD A SISTEMAS DE INFORMACIÓN EN CUANTO A ATAQUES MALICIOSOS CON BASE EN NORMATIVIDAD, TENDENCIAS, IMPACTO Y TÉCNICAS VIGENTES PARA AMBIENTES EMPRESARIALES A NIVEL NACIONAL***, para optar al título de Ingeniería en Informática del Estudiante David Hernando Alonso Torres con Código 200922130.

La dirección del Proyecto estuvo a cargo del Profesor Carlos Alberto Puentes Pinto.

Gracias por su atención.

Atentamente;

CARLOS ALBERTO PUENTES PINTO
Director Proyecto de Grado

DAVID HERNANDO ALONSO T.
Estudiante Ingeniería Informática

Universidad de La Sabana

Contenido

Universidad de La Sabana

INDICE DE FIGURAS

Universidad de La Sabana

INDICE DE TABLAS

DEDICATORIA

Quiero dedicar este trabajo de Investigación en primer lugar a Dios, el creador, porque día a día con su infinita grandeza nos da la vida, salud y fuerza a mi familia y a mí para seguir adelante. Toda la Gloria es para Él.

A mis padres: María E. Torres y José R. Alonso; por su amor, trabajo, ejemplo y sacrificio durante este camino largo lleno de dificultades, retos, tristezas y decepciones, que Gracias a su apoyo, confianza, paciencia, afecto y cariño me han motivado en momentos duros donde mi resiliencia se ha puesto a prueba, por ellos he salido adelante siempre y son la luz en el camino de mi vida. Son mis héroes, el motor de mi vida, para ellos todos mis éxitos y triunfos, son mi vida, soy por ellos y son los mejores.

A mis hermanos, Fabián Alonso y Nicolás Alonso; por la paciencia que han tenido en mi vida universitaria, en ellos veo reflejada mi vida y la de mis padres, siempre serán el mejor apoyo y refugio que podré encontrar en el mundo. Vamos adelante que la vida es una sola.

“Lo imposible sólo tarda un poco más”

-Nonpalidece

Universidad de La Sabana

AGRADECIMIENTOS

A la Universidad de La Sabana, por haberme brindado la oportunidad de estudiar esta carrera que es apasionante y darme las herramientas necesarias para mi formación académica y profesional, que a pesar de los inconvenientes siempre ha demostrado que es un Alma Mater de personas para personas y ha salido adelante *por el bien ser y el bien estar* de toda la comunidad académica, porque puedo andar por todo el mundo orgulloso pregonando que *Ser Sabana, vale la pena.*

A mis amigos y sus familiares, por la paciencia, acompañamiento y apoyo desde el comienzo de mi carrera académica, sé que siempre estarán ahí en momentos difíciles, son motivación y me dan la fuerza para dar lo mejor de mí en cualquier situación de la vida.

A mi Director de Tesis: Carlos Puentes, por la paciencia, guía y motivación durante la vida universitaria y en especial en este Trabajo de Investigación, es pieza fundamental para terminar con éxito esta etapa, ya que gracias a su trabajo y profesionalismo me motivó a elegir la Seguridad Informática como camino a seguir en este gran mundo de la Informática.

A mis maestros, por los conocimientos y experiencia transmitida durante mi vida académica, con su profesionalismo han forjado en mí un Ingeniero que siempre tendrá los mejores recuerdos y consejos totalmente aplicados en el mundo laboral y en la vida misma.

Por último un agradecimiento especial a CIC Colombia, compañía donde trabajo actualmente, por la paciencia, apoyo y confianza transmitida para poder finalizar con éxito este trabajo de grado. A ellos muchas gracias.

GLOSARIO

Análisis de riesgos: Evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Autorización: Garantizar que todos los accesos a datos y/o transacciones que los utilicen, cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

Backup: copia de los datos de un archivo automatizado en un soporte que posibilite su recuperación.

Confiabilidad: Garantizar que los sistemas informáticos brinden información correcta para ser utilizada en la operatoria de cada uno de los procesos.

Confidencialidad: Garantizar que toda la información está protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia del respaldo o resguardo: ver backup.

Courier: Mensajero, correo. Persona o dispositivo mediante el cual se envían

Disponibilidad: Garantizar que la información y la capacidad de su tratamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de las actividades.

Eficacia: Garantizar que toda información que sea utilizada es necesaria y entregada de forma oportuna, correcta, consistente y útil para el desarrollo de las actividades.

Eficiencia: Asegurar que el tratamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.

Firewall (cortafuegos): Dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad de la organización que lo instala.

Herramientas de seguridad: Son utilitarios que sirven para identificar vulnerabilidades en un sistema. Pueden ser una amenaza si un intruso las utiliza en el sistema y detecta fallas en la seguridad de las que el administrador no está enterado.

Host: (sistema anfitrión, sistema principal) Ordenador que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. La acepción verbal (to host) describe el hecho de almacenar algún tipo de información en un servidor ajeno.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

ID: Nombre o identificación de usuario.

Ingeniería social: Consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, como revelar su contraseña o cambiarla.

Integridad: Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de las actividades en cada uno de los sistemas informatizados y procesos transaccionales.

Login: Conexión. Entrada en una red.

Logs: Registros de situaciones en un sistema informático, tales como actividades de usuarios, control de contraseñas, etc. Es el resultado de puesta en marcha del logging.

Normativa de Seguridad: Conjunto de reglas, normas, procedimientos, estándares e instructivos que regulan los aspectos funcionales y técnicos de la seguridad informática en una organización.

Password: (palabra de paso, contraseña) Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

Router: Sistema constituido por hardware y software para la transmisión de datos en una red. El emisor y el receptor deben utilizar el mismo protocolo de comunicaciones.

Scanners: Software, a veces asociado a equipamiento que permite realizar la inspección de comunicaciones, usualmente mediante el barrido de frecuencias.

1. RESUMEN

La Seguridad de la Información tiene un valor importante en las organizaciones, como bandera en la imagen corporativa y reputación de la misma, así mismo es la confianza que esperan los clientes a los que se hace manejo de información crítica y confidencial, canalizada a través de medios de acceso público; por consiguiente, para las empresas es necesario tener un nivel de aseguramiento alto con respecto a intrusión y ataques externos para la evaluación del riesgo en este campo, motivado por esto, se hará una investigación de acuerdo a tendencias, documentación, recursos especializados, herramientas y estadísticas referentes a los ataques informáticos maliciosos en la actualidad, que comprometan la confidencialidad, disponibilidad e integridad de la información.

Con base en esto, se quieren compilar procedimientos consolidados en una metodología, apoyados con técnicas y herramientas de Ethical Hacking específicas, que sirva como guía para las empresas en el desarrollo e implementación de sistemas seguros, y así contrarrestar dichas vulnerabilidades; contribuir para que los ambientes informáticos en las empresas públicas y privadas en el país, cuenten con lo necesario de acuerdo a la normatividad y legislación vigente, para lograr un adecuado nivel de seguridad informática.

El resultado será una investigación con el estado actual de los ataques maliciosos más comunes y el impacto que generan en las organizaciones en cuanto a robo o fuga de información, clasificación que será de acuerdo a unos criterios definidos a lo largo de la misma, apoyados en la legislación nacional. De esta forma, como valor agregado, generar una guía metodológica apoyada en las técnicas y procedimientos de Ethical Hacking y Pruebas de Penetración bajo software libre, para la prevención, detección corrección y buenas prácticas del Top. 5 de Vulnerabilidades clasificadas previamente, junto a una campaña de sensibilización que le dará relevancia social a la misma, todo aplicable a cualquier empresa sin importar el sector económico a nivel nacional.

2. ABSTRACT

Information security has a major value in the organizations, as a flagship of the corporate image and reputation, likewise is the confidence that customers expect from the management of critical and confidential information channeled through means of public access; therefore, it is necessary that the companies have a high level of assurance concerning the trespassing and external attacks for the risk assessment in this field, motivated by this, an investigation will be conducted according to the trends, documentation, specialized resources, collective learning and statistics regarding malicious computer attacks that compromise the confidentiality, availability and integrity of information.

Based on the above, the aim is to compile procedures in a consolidated methodology, supported by specific Ethical Hacking tools and techniques to guide the companies in the development and implementation of secure systems, and counteract these vulnerabilities; as well as contribute to the computing environments in public and private companies in the country have what they need according to current regulations to achieve a minimum level of computer security.

The result will be an investigation with the current state of the most common malicious attacks that have more impact in organizations regarding theft or leakage of information, this classification will be framed by defined criteria supported by the national legislation and policies, thereby, as an added value, generate a methodological guide supported by Ethical Hacking procedures and techniques, and Penetration Testing under free software, for the prevention, detection and correction of Top. 5 of Vulnerabilities previously classified, along with an awareness campaign that will give social relevance to it, all applicable to any company regardless the economic sector nationally.

3. INTRODUCCIÓN

Hoy en día, la informática hace parte esencial en nuestras vidas, en ambientes Personales, Familiares y Empresariales por la aparición de diferentes dispositivos, sistemas y técnicas que facilitan nuestro diario vivir, esto ayudado por la facilidad para acceder a las diversas tecnologías por su proliferación y bajos costos presenta un desafío para los Profesionales en Informática.

Con el paso de los años, el hombre ha tenido la necesidad de salvaguardar y mantener su privacidad, a través de diferentes mecanismos que han evolucionado a través del tiempo, se ha buscado siempre un ambiente para que el ser humano sienta la confianza necesaria de vivir, trabajar y resguardarse en un lugar seguro, sin sentir las amenazas que pusieran en riesgo su integridad y tranquilidad; sin embargo las formas de protección y defensa siempre han sido vulneradas y sus mecanismos de ataque perfeccionadas por delincuentes con el paso de los años y en la medida de los avances tecnológicos.

El interés por parte de las personas en cuanto a seguridad está latente, por otro lado, es importante que los usuarios se concienticen sobre la importancia de la Seguridad especialmente de la Información, si esto no ocurre, no se conseguirá mitigar el impacto de las amenazas informáticas, retomando el ejemplo anterior, esta situación es equivalente a una persona que se muestra desconfiada por la seguridad de su hogar, pero si no genera barreras como sistemas de alarmas, no hay protección en sus ventanas y acceso a cualquier persona, lo más probable es que sea una víctima más a la larga lista.

Ahora bien, los negocios han entrado en la dinámica del comercio electrónico, que facilita las transacciones en muchos factores, como costos, movilidad, tramitología, tiempo, entre otros; pero hay algo que es trascendental, que es la expansión, cobertura y facilidad de acceso a la Internet, la red mundial que se está convirtiendo en la ventana más grande de comunicaciones a nivel global. Entre los sectores económicos más comunes que cuentan con actividad a través

de la internet son el Bancario y de Comercio, entes que manejan entre sus transacciones miles de millones de pesos al año además de manejo de datos personales, es un punto de partida para empezar a pensar seriamente en Seguridad de la Información y realizar una evaluación para ver: qué hay, qué se necesita, cuáles son las amenazas, debilidades y riesgos; especialmente en el plano nacional.

Por esto, a través del trabajo de investigación desarrollado a continuación, se tratarán temas de interés para dar una guía a los actores más importantes en la labor de protección y defensa en los Sistemas a nivel empresarial, cómo lo son los encargados de la Seguridad de La Información; presentando un estado actual sobre Normatividad, Legislación, Estándares; además de esto, hacer un Top 5 de Vulnerabilidades en Sistemas de Información Empresariales, con su Impacto, Prevención y Detección, recomendaciones y metodologías y demás relacionadas con el mundo apasionante del Ethical Hacking. Hello World!

4. GENERALIDADES

4.1. PREGUNTA DE INVESTIGACIÓN

¿Cuáles son los ataques maliciosos a sistemas de información con mayor impacto en las empresas y como se contrarrestan de acuerdo a la normatividad nacional vigente y técnicas actuales?

4.2. JUSTIFICACIÓN

Para empezar, abordar el tema de investigación propuesto tiene diferentes connotaciones, no se quiere tener una base de estudio únicamente en literatura y bibliografía estándar, que hable sobre teoría y técnicas, se quiere tratar de forma global, incluyendo aspectos relevantes a nivel económico, social y organizacional soportados en estadísticas fiables sobre las empresas a nivel nacional y mundial consecuencia de ataques informáticos a sistemas de información, teniendo como

fuente recursos colaborativos con reputación sólida, organizaciones especializadas y certificadas a nivel mundial con bases de datos de acceso público que establecen clasificaciones de vulnerabilidades informáticas de acuerdo a varios niveles de impacto y criticidad en los sistemas.

Todo esto conlleva unas implicaciones técnicas que se deben tener en cuenta, entre las que se encuentran métodos con herramientas de Pentesting , test de vulnerabilidades y Escáneres Web, se plasmará en forma de guía metodológica que será presentada en conjunto con el trabajo de investigación, todo esto se logrará también con el apoyo de la normatividad y legislación nacional e internacional como: Normas Técnicas Colombianas, Circulares y lo establecido por la Organización Internacional de Normalización ISO en sus estándares establecidos vigentes, esto hará de la investigación un soporte sólido para argumentar y documentar los resultados obtenidos; será la frontera para la investigación, se ajustará a lo que realmente necesitan las empresas de cualquier sector de la economía a nivel Nacional para cumplir con las normas y leyes correspondientes.

Además en el desarrollo de la investigación se quiere hacer manejo de terminología cómoda para cualquier persona que acceda a ella, ya que actualmente por la aparición en los medios de comunicación de estos temas – hacking y relacionados -, son confusos y faltos de precisión para el público en general, en gran parte por su lenguaje intrincado, se ve en esto una oportunidad que agrega una relevancia social a la misma, para aclarar “tabús” y señalamientos errados en cuanto a Hacking y ataques informáticos y su práctica en la actualidad.

Es importante hacer énfasis para la sensibilización inicialmente planteada, en el personal involucrado en los procesos relacionados con la seguridad de la información de las organizaciones, ellos cumplen un rol protagónico, al estar en contacto directo con los medios a atacar por parte de delincuentes, los convierte en objetivos vulnerables en gran parte quizá por falta de conocimiento y concientización de los temas de actualidad en cuanto a seguridad de la

información se refiere, por esta razón se quiere llevar el mensaje a estos con sensibilización acerca el tema a tratar y apoyados en indicadores estadísticos y documentación de acuerdo a la importancia que ellos cumplen en el aseguramiento de la información y sus posibles debilidades que hacen parte del flujo de un ataque informático malicioso dirigido a la organización a la que pertenecen; material multimedia de fácil acceso, propagación y aplicación.

De acuerdo a los resultados de la investigación se establecerá una utilidad metodológica para las organizaciones empresariales, ya que encontrarán una guía actualizada para la prevención, detección y corrección de las vulnerabilidades previamente analizadas y categorizadas en el Top 5, que puede ser aplicada para el aseguramiento de infraestructura tecnológica expuesta a Internet en cuanto a ataques maliciosos se refiere, que pueden provocar la fuga de información sensible de acuerdo a la actividad económica en la que se encuentren, todo esto apoyado por software categorizado de acuerdo a su naturaleza y tipo de uso, además como factor diferenciador, que sea un punto a favor para la economía de las empresas presentando un comparativo con auditorías o consultorías de Ethical hacking, su precio y las implicaciones que estos servicios conllevan.

Además, al final del trabajo se aclarará el panorama en el tema, ya que la guía resultante puede ser muy útil para reducir o contrarrestar el impacto económico o de reputación en las entidades afectadas con base en la Normatividad y Legislación Nacional vigente, es importante resaltar que los conceptos manejados en la guía metodológica intentarán tener una flexibilidad de acuerdo a las tendencias y proyecciones, es decir, que su aplicabilidad se pueda mantener en el tiempo con el mismo nivel de eficacia.

Uno de los fines por el que se elige desarrollar este tipo de temática, como motivación personal, es fomentar la investigación y poner los primeros ladrillos en un campo que será de gran utilidad para los estudiantes de Ingeniería Informática

de la Universidad de La Sabana, donde aquí, aplicando diferentes conceptos vistos en el plan de estudios del programa, se sientan motivados para tal vez continuar esta labor investigativa, se profundicen o elijan la Seguridad Informática como camino en sus vidas profesionales, motivar y generar pasión en este tema que por ausencia de un grupo o semillero de investigación relacionado con esto es poco conocido, pero que es de gran interés y proyección en el mundo laboral, acaparando la atención de los medios y organizaciones que invierten para su investigación a Nivel Nacional e Internacional.

4.3. MARCO TEÓRICO

La legislación colombiana presenta en sus estatutos diferentes leyes en las que se debe regir la actividad en internet y sus sistemas relacionados, desde la protección de datos personales hasta los Lineamientos de política para ciberseguridad y ciberdefensa, entre las más destacadas con una breve descripción se encuentran en el Anexo No.1. (Balanta, 2014).

VER ANEXO No. 1 – LEGISLACIÓN COLOMBIANA

Entidades como el Consejo Nacional de Política Económica y Social (CONPES), MinTIC's, Ministerio del Interior, han sido abanderados para la promoción y proliferación de esta legislación, estos son el espectro definido en cuánto a legislación nacional se refiere para el desarrollo de la investigación. (MinTic, 2011)

Las empresas, como parte del sistema de calidad en sus procesos y actividades, procuran estar a la par con la normatividad y estándares vigentes para ser certificados y así tener una ventaja competitiva en el mercado, para la Seguridad de la Información no existe excepción alguna, el gobierno y los entes certificadores hacen esfuerzos para mantener actualizada la documentación plasmada en forma de Normas, Circulares, Gestión del Riesgo y estándares para

los Sistemas de Gestión de Seguridad de la Información a nivel empresarial, entre las normas y demás se destacan las siguientes:

- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009
- Circular 052 de 2007 (Superintendencia Financiera de Colombia)
- ISO/IEC 27001/27002
- NTC (Norma Técnica Colombiana) 5254 de 2006
- Estándar RFC2196

Las técnicas y metodologías para los procedimientos que involucran la prevención, detección y corrección de las vulnerabilidades categorizadas durante el proceso de investigación, será con base en la infraestructura y software libre, haciendo el análisis de las mismas de acuerdo a su naturaleza y efectividad, acceso público y fácil implementación, destacando que estas herramientas siguen actualizadas con el apoyo de la comunidad en línea que las mantienen al tanto de los últimos avances en cuanto a Seguridad Informática se refiere con actualizaciones, entre las más destacadas herramientas se encuentran (González Pérez, Sánchez Garcés, & Soriano, Pentesting con Kali, 2013):

- Kali Linux (Distribución Linux)
- Metasploit
- OpenVAS
- Nessus
- Burp Suite

Todo esto apoyado con los procedimientos y metodologías definidas por las organizaciones internacionales certificadas en pro de la seguridad informática tales como: OWASP, ICASI, CERT entre otras.

Los modelos y proyectos implementados en cuanto a seguridad informática por parte del Gobierno Nacional en los últimos años son parte fundamental en la

investigación, identificar vacíos y como valor agregado, añadir actualizaciones y nuevas metodologías, entre ellos están:

- Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea
- Recomendaciones al Gobierno Nacional para la implementación de una Estrategia Nacional de Ciberseguridad

4.4. OBJETIVO GENERAL

Establecer y definir los parámetros mínimos para la Seguridad de la Información empresarial a nivel nacional, con base en legislación, normatividad, estándares y metodología vigente, para su aplicación en la actualidad, de acuerdo a los ataques maliciosos clasificados.

4.5. OBJETIVOS ESPECÍFICOS

- Identificar y estudiar la Legislación, Normatividad, Estándares y Circulares vigentes que cubren al territorio a Nivel Nacional para la Seguridad de la Información, haciendo énfasis en infraestructura, datos y aplicaciones empresariales de los diferentes sectores de la economía.
- Determinar cuáles son las fuentes de información, como foros, blogs, comunidades en línea confiables, de respaldo, tradición y reputación en internet además de la bibliografía adecuada para el proceso de la investigación.
- Identificar los ataques informáticos maliciosos comunes de acuerdo a las tendencias recientes (Último Año) a la infraestructura y sistemas de información, apoyados en las estadísticas de las entidades especializadas y las investigaciones al caso correspondientes, haciendo énfasis en las que más impacto tienen en las organizaciones.

- Establecer y determinar las herramientas y procedimientos de Ethical Hacking más eficientes y actualizadas para su uso y aplicación en la guía metodológica resultante al final de la investigación, haciendo análisis de acuerdo a su naturaleza (Gratuitas y De Paga), sus pros y contra, evaluar la efectividad y pertinencia para su uso en el desarrollo de la investigación.
- Evaluar los impactos en las organizaciones a causa de ataques maliciosos a sistemas de información y su consecuencia a nivel de reputación y económicamente, de acuerdo pública y de relevancia en los medios, además analizar la forma como la investigación contribuirá, con base en la legislación y normatividad correspondiente a cubrir aquellos espacios faltantes y brindar un nivel de aseguramiento de la información acorde a la naturalidad del negocio y lo que requiere la ley, todo esto con base en las técnicas, procedimientos y métodos desarrollados en el transcurso de la investigación.
- Observar el estado a nivel de seguridad de infraestructura y sistemas de información para nuevas tecnologías (Tecnología Móvil, Cloud Computing) y que posibles fallos pueden presentar en el futuro para las empresas, los nuevos desafíos.
- Investigar e implementar las técnicas y metodologías específicas para dado caso de Ethical Hacking recopiladas durante la investigación para la prevención, detección y remediación de las vulnerabilidades comunes previamente determinadas especificando el entorno y la infraestructura donde se aplicarán y como se ajusta a lo que el mercado, la legislación y la normatividad requiere**.**
- Aplicar apartes de la investigación a la relevancia social de forma sencilla en términos de concientización y educación para clientes de plataformas tecnológicas y sistemas de información y personal relacionado con tecnología de las empresas especialmente, en cuanto a seguridad de la información corresponde, buenas prácticas plasmadas de forma educativa, ejemplarizando las posibles consecuencias de un mal manejo o falta de

implementación de técnicas de seguridad en aplicaciones y sistemas de información; desarrollo de forma didáctica, videos y fichas informativas.

5. DESARROLLO DE LA INVESTIGACIÓN

5.1. MARCO LEGAL Y NORMATIVO

5.1.1. ENTIDADES GUBERNAMENTALES DE CONTROL Y LEGISLACIÓN VIGENTE

En Colombia, el marco legal y tecnológico en cuanto a Seguridad de La Información se refiere, está delegado por el Gobierno Nacional al *Ministerio de* Tecnologías de la Información y las Comunicaciones (http://www.mintic.gov.co/), sin embargo, se han creado las diversas iniciativas, con el afán de salvaguardar la seguridad informática nacional, todo esto, al ser un tema de Ciberdefensa Estatal, el Ministerio de Defensa y el MinTIC, ha establecido entes especializados entre los que se encuentran:

- **El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert)**, encargado de coordinar a escala nacional los aspectos de ciberseguridad y ciberdefensa. (http://www.colcert.gov.co/)

- **El Comando Conjunto Cibernético de las Fuerzas Militares (CCOC)**, que tendrá la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.

- **El Centro Cibernético Policial (CCP)**, tiene como función la prevención e investigación y judicialización de los delitos informáticos. Para ello, cuenta con un comando de Atención Inmediata Virtual (CAI Virtual), para recibir las denuncias de los ciudadanos. (http://www.ccp.gov.co/)

Todos estos entes gubernamentales son pieza fundamental en el tema de Seguridad de La Información en temas de Ciberdefensa y Ciberseguridad, de aquí

se obtienen boletines, alertas, eventos y consensos que son útiles para el manejo de las TIC's para las empresas.

En Marzo de 2014, la Revista Sistemas (http://www.acis.org.co/revistasistemas) de la Asociación Colombiana de Ingenieros de Sistemas, reseña una entrevista brindada por la *Dirección de Comunicación Sectorial (Oficina de Prensa) del Ministerio de Defensa Nacional,* que muestra el estado actual de la Seguridad Informática desde el punto de vista del Gobierno, a continuación unos apartes relevantes.

Por: Sara Gallardo
Para: Revista Sistemas, Edición 130, Marzo 2014

"Revista Sistemas. ¿Cómo define el Ministerio la seguridad informática, en el marco de la seguridad nacional?

MinDefensa: "En Colombia se ha incrementado considerablemente el uso de tecnologías de la información y las comunicaciones, elevando su nivel de exposición a amenazas cibernéticas; por tanto, la seguridad informática es una prioridad."

RS:"Finalizado el CONPES 3701, ¿está segura la continuidad de los entes creados para soportar la estrategia de ciberseguridad nacional?"

MinDefensa: "El CONPES 3701 de 2011 busca generar lineamientos de política en ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país, la estratega nacional continúa en desarrollo, así como los entes creados."

(Gallardo, 2014)

Es importante resaltar que es tema de interés del Gobierno Nacional el implementar estas instituciones, por esto se destaca lo propuesto en el Documento CONPES, este identifica inconvenientes fundamentales tales como que las instituciones públicas y privadas no han coordinado sus políticas frente al tema de ciberseguridad, que el marco normativo existente no es suficiente para hacer frente a los problemas de ciberseguridad y defensa, incluída la impunidad que existe actualmente para los delitos informáticos y el no pertencer a la comunidad mundial de delitos cibernéticos, y que los funcionarios públicos y privados no están debidamente capacitados para responder ante las amenazas cibernéticas, todo esto sumado a los esfuerzos plasmasdos en el Plan Nacional de Desarrollo 2010-2014 “Prosperidad para Todos”, como parte del Plan Vive Digital, la voluntad y el dinero del Gobierno está.

Para las empresas, es importante contar con un respaldo gubernamental en casos donde la integridad de los datos esté comprometida, los entes están dispuestos a trabajar en conjunto con sus pares internacionales, es un método que está en desarrollo pero es verdaderamente útil, la base del conocimiento se construye con base en casos reales y que mejor que las empresas gubernamentales y no-gubernamentales sean partícipes, una cultura de seguridad colaborativa

La creación de entes gubernamentales que vigilan, regulen los temas relacionados con la Seguridad de La Información como lo reseña el Presidente Santos, en declaraciones recientes.

“Hay sistemas de Guerra Nuevos, lo estamos viendo inclusive por la televisión, guerras que se libran desde miles de kilómetros de distancia, con un computador

y con unos aparatos que son manejados desde ese computador sin ninguna intervención humana. Frente a eso, Colombia, el Estado Colombiano está muy vulnerable, estamos en pañales." (Santos, 2014) Afirmó el mandatario el pasado 7 de Febrero.[1]

Para esto, como base, se presenta lo que está vigente, aún las modificaciones efecto de los pronunciamientos del Gobierno Nacional no han salido a flote, de acuerdo al enfoque de la investigación, que es netamente empresarial a nivel nacional, es importante resaltar la siguiente legislación, presentando lo relevante de acuerdo a cada Ley, Resolución o Circular, en cuanto a la Seguridad de La Información se refiere.

VER ANEXO No.2 – SEGURIDAD DE LA INFORMACIÓN EN LEGISLACIÓN

Todo esto debe estar ajustado a las necesidades del negocio, sin embargo, esto constituye la base legislativa para el diseño, implementación, desarrollo y ejecución de modelos de negocio basados en Tecnologías de La Información y Comunicación a Nivel Empresarial.

5.1.2. NORMATIVIDAD, CERTIFICACIONES Y ESTÁNDARES

La Seguridad de la información en Colombia, implementada en el ámbito empresarial presenta a nivel de normatividad, certificaciones y estándares, una tendencia que inevitablemente nos lleva a la implementación de un SGSI (Sistema de Gestión de Seguridad de La Información) fundamental en entes económicos, este sistema implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la

[1] http://www.rcnradio.com/noticias/gobierno-creara-la-agencia-nacional-de-seguridad-cibernetica-147786 - http://www.gerente.com/detarticulo.php?CodArticl=385

información, para asegurar la integridad, confidencialidad y disponibilidad de la información. (Pacheco, ESET: WeLiveSecurity, 2013)

En el desarrollo e implementación de un SGSI se debe estructurar un Modelo Normativo, este puede estructurarse documentando una política por cada dominio, y normas que complementen a la política y que aglomeren los objetivos de control que exista en la ISO 27001, este es un punto de partida fundamental, ya que esta norma internacional es la principal referencia este punto de la investigación.

En 2005, la Organización Internacional de Normalización (http://www.iso.org/), publicó la ISO 27001, es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (27001 Academy, 2013).

En Colombia, el ente certificador más reconocido es el ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación), representante de la Organización Internacional para la Estandarización (ISO), en Colombia, es el referente en cuánto a regulación del estándar ISO/IEC 27001:2013, una empresa con un SGSI con base en la norma, puede recibir la certificación por parte de la entidad, es la bandera corporativa y reputacional de las empresas ante el mercado y la competencia.

Se debe señalar que la única norma a certificar de la serie es la ISO 27001. No así la ISO 27002, anteriormente conocida como la ISO 17799, esta tan sólo establece una serie de recomendaciones y buenas prácticas, es importante

resaltar que para lograr la certificación en ISO 27001 no es necesario implantar todos los controles recomendados por la ISO 27002, sino que la organización debe priorizar y seleccionar aquellos controles que se alineen con su estrategia de riesgo, teniendo en cuenta la capacidad presupuestaria de la organización y sus necesidades de negocio. (Benjumea, 2010)

A nivel local, se encuentran como complemento y en dado caso, normas establecidas de acuerdo al sector económico, los medios utilizados, entre estas se resaltan las siguientes:

- **Resolución 2258 de 2009:** Expedida por la Comisión de Regulación de Comunicaciones (CRC - http://www.crcom.gov.co/-) para la adición y modificación de artículos a la Resolución CRT 1740 de 2007, la cual habla sobre las medidas, características y procedimientos que los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a la Internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad, inviolabilidad de los datos y red; A nivel empresarial es un aspecto de vital importancia, ya que gran parte la comunicación de los Sistemas de Información de cara a internet, van a través de canales provisionados por entidades reguladas por la CRC, además que los ataques maliciosos son a través de internet, el cumplimiento de esta resolución es garantía de seguridad en parte, de la información canalizada a través de internet. (CRC, 2009)

- **Circular 052 de 2007:** Expedida por la Superintendencia Financiera de Colombia, dónde obliga a la entidades financieras, tener en cuenta un conjunto de buenas prácticas fundamentales para el desarrollo de la Seguridad de la Información en Colombia, es un referente muy importante

para todos los sectores de la economía en el País, es evidente que las transacciones financieras a través de internet son las que hacen parte de los objetivos de los ciberdelincuentes, entre estas buenas prácticas se encuentran el Cifrado, Almacenamiento, Videovigilancia, Firewalls y demás sistemas de protección informática, Planes de Contingencia bajo el uso de Centros de Cómputo de Alta Disponibilidad, entre otros; puntos de referencia para el aseguramiento de la Información empresarial indiferente del sector económico donde se encuentren. (Superfinanciera, 2007)

- **Estándar RFC2196 – Site Security Handbook:** El Internet Engineering Task Force (IETF - https://www.ietf.org/ -) (Grupo de Trabajo de Ingeniería de Internet), la organización internacional que tiene como objetivo contribuir la ingeniería de internet, en especial de la seguridad de la información, presenta en el estándar un marco conceptual para definir de manera integrada un esquema de seguridad basado en políticas a todo nivel en los temas referentes al manejo de la información, especialmente en dos aspectos: Activos (Hardware, software, red, información y personal) y Riesgos (Vulnerabilidades, debilidades). El establecimiento de un Plan de Seguridad. (Piraquive, 2008)

Como lo relacionado con Seguridad de la Información, especialmente con ataques maliciosos representa un riesgo latente para las empresas, es importante considerar y poner en discusión la importancia de la normatividad relacionada con Gestión del Riesgo de La Información, para esto, en Colombia, se presenta la NTC (Norma Técnica Colombiana) 5254 de 2006, regulada por ICONTEC, en esta se evidencia la importancia la administración de Riesgos , que una parte fundamental de la Gobernabilidad corporativa que busca contribuir eficientemente en la identificación, análisis, tratamiento, comunicación y monitoreo de los riesgos del negocio, la NTC 5254 es una traducción idéntica de la norma técnica

Australiana AS/NZ 4360:2004 de amplia aceptación y reconocimiento a nivel mundial para la gestión de riesgos independiente de la industria o el negocio que desee emplearla. (Lozano Vila, 2008)

De acuerdo a la Tendencia 2014 de la Encuesta Nacional de Seguridad Informática, realizada en ACIS, por Andrés Almanza, especialista y referente en temas de la Seguridad de La Información, dónde se contó con la participación de 189 encuestados permitió conocer el estado actual del tema en la nación; es importante resaltar la siguiente conclusión:

"… Hoy en Colombia existen normativas como la regulación en los sectores financieros y la ley de protección de datos personales. Las regulaciones Internacionales inclinan la balanza hacia la seguridad de la información y nos enfrentan a un panorama todavía denso, en materia de ataques informáticos." (Almanza, 2014)

Sumado a esto, de acuerdo a la encuesta realizada por ISec Information Security Inc. (http://www.isec-global.com/), donde 700 profesionales de los diferentes sectores de la empresa colombiana, incluyendo empresa privada, sector gobierno, PYMES y empresas grandes, entre los resultados más importantes se resaltan los siguientes:

Por Alejandro Hernandez
ISEC Information Security Inc
Country Manager Colombia

*"**40%** de los encuestados NO revisa el marco normativo de seguridad de la información implementando en la empresa*

52% *no ha implementado en su empresa ningún estándar internacional.*

47% *nunca hizo ningún test de seguridad de las redes (Ethical Hacking, Análisis De Vulnerabilidades y/o Pruebas De Penetración en su empresa)*

47% *no cuenta con un Plan de Continuidad del Negocio que le permita seguir con las operaciones en caso de un evento no deseado."*

"Después de analizar las encuestas se llegó a la conclusión de que la empresa colombiana no distingue entre seguridad informática y seguridad de la información, inclusive conoce poco la legislación colombiana en materia de TICS: Todo esto no permite lograr una concientización en materia de seguridad de los actores que intervienen en la empresa colombiana, incluyendo clientes y proveedores." (Hernandez, 2011)

Todo esto nos indica que en materia de Normatividad y Estándares, existe un vacío en cuanto a fortalecimiento y conocimiento de estos temas a nivel empresarial, falta una cultura de Seguridad de la Información alineada con base en los estándares internacionales y la tendencia de los líderes en el campo.

Sin embargo, es importante destacar las iniciativas del Gobierno Nacional en cuánto a campañas, modelos, proyectos en cuanto a Seguridad de la Información se refiere, la estrategia del MinTIC que presenta el Modelo de Seguridad de la Información para soportar la Administración de la Seguridad de los entes del Gobierno en Línea, además define las brechas de seguridad, realiza la alineación y administración e implementación de un SGSI, para convertirlo en un modelo sostenible que cubra todos los aspectos relacionados con Seguridad de la Información, es una propuesta muy interesante para ser aplicada para varios sectores de la economía en Colombia, el diseño de un Modelo similar para sectores económicos agremiados en el país, podría ser una buena iniciativa para

las empresas que quieren tener a la vanguardia la infraestructura relacionada con Sistemas de Información. (MinTIC, 2011)

Para destacar, nos encontramos con la Carta Iberoamericana de Gobierno Electrónico, esta fue resultado del consenso alcanzado por los gobiernos iberoamericanos en Chile en Junio de 2007, la Carta define un nuevo paradigma en cuanto al uso de las tecnologías de la información y las comunicaciones (TIC) (CLAD, 2007); eventos como logran la retroalimentación en cuanto a Seguridad de La Información en América Latina, impulsar iniciativas y fomentar la interacción y apoyo entre los Gobiernos y sus Ministerios TIC, todo esto en pro de fortalecer metodologías y las buenas prácticas, este tipo de acontecimientos apoyados por la empresa privada, puede impulsar la implementación de SGSI actualizados y con normatividad a la vanguardia.

En cuanto al recurso humano, las certificaciones son un aspecto importante y para destacar en especial para los profesionales de Seguridad de la Información, estas certificaciones varían de acuerdo al enfoque o necesidades de las empresas, entre las principales están:

- **Certified Ethical Hacker por EC-Council:** ofrece un amplio programa de hacking ético y de formación de seguridad en redes para cumplir con los más altos estándares para profesionales.

- **Gerente Certificado de Seguridad de la Información (CISM) por ISACA:** Es el estándar aceptado globalmente para las personas que diseñan, construyen y gestionan los programas de seguridad de la información empresarial.

- **Profesional Certificado de Sistemas de Información de Seguridad (CISSP) por ISC2:** es un estándar reconocido a nivel mundial que confirma el conocimiento de un individuo en el campo de la seguridad de la información.

- **Profesional de la Seguridad Inalámbrica Certificado (CWSP) por Certified Wireless Network Professional (CWNP):** asegura que se tienen las capacidades para proteger las redes empresariales Wi-Fi de los hackers, sin importar qué modelos o marcas se implanten en la organización.

- **Cursos de Certificación Global Information Assurance (GIAC):** Proporcionan la seguridad de que una persona certificada tiene el conocimiento y las habilidades necesarias para ser un profesional en las áreas clave de la informática y la seguridad del software y la información.

Es importante hacer un repaso de este tipo de cursos, ya que las empresas que piensen en contratar un Profesional de la Seguridad de la Información, tengan criterios de decisión al evaluar a los posibles candidatos de acuerdo al tipo de certificaciones y si son las más adecuadas para desempeñar el cargo dentro de cada organización.

5.2. SEGURIDAD EN CLOUD COMPUTING Y TECNOLOGÍA MÓVIL: LOS NUEVOS DESAFÍOS

El Cloud Computing o como es popularmente conocido como la Nube consiste en un método de almacenamiento en línea que ha tomado fuerza en los últimos años debido a su flexibilidad, por eso ha sido adoptado en ambientes Empresariales como cotidianos, sin embargo, gracias a la expansión, crecimiento y uso de la Tecnología Cloud sigue generando incertidumbre en lo que se refiere a seguridad

y privacidad en los datos almacenados ya que los usuarios expresan un cierto nivel de preocupación, porque no les permite tener un control cercano sobre la información como si lo pueden obtener a través de un servidor local o físico propietario. De acuerdo a una investigación realizado por ESET, la multinacional especialista en Seguridad de la Información, presenta unas etapas que es importante tener en cuenta para entender el por qué de la importancia de la Seguridad en este ámbito, habla de tres etapas, el “Antes: La información puede ser robada antes de que sea subida a la nube”, esto se referencia ya que los datos que se encuentren almacenados en sistemas que estén infectados con un código malicioso ya el robo está hecho, sin necesidad de estar en la Nube; “Durante: La información puede resultar comprometida durante el envío a la misma nube”, el caso donde la información corre peligro es cuando la transmisión de datos a la nube sea haga a través de una conexión insegura – No VPN – podría sufrir de ataques como sniffing o robo de paquetes; y en tercera etapa, “Después: La información puede ser robada después de almacenada en la nube”, aquí ya entra a participar el proveedor del servicio de almacenamiento en línea, ya que tiene mucho que ver la seguridad que adopta el mismo, como el cifrado de datos, política de uso y seguridad, entre otras, esto también es factor determinante para la probabilidad de que una información almacenada en la nube pueda ser vulnerada (ESET Latinoamérica, 2014).

Esto presenta un desafío donde se involucran diferentes actores en el proceso de diseño, montaje, implementación y uso de información almacenada en la nube, ya que se debe establecer un modelo dinámico para que sean consideradas todas las amenazas y debilidades del sistema y así establezcan contramedidas y planes de remediación y recuperación inmediatos; sin afectar el dinamismo de cada uno de los módulos del proceso de Cloud Computing en una compañía en específico.

Por otra parte, están los dispositivos móviles, que están presentes cada día más Hogares y empresas como parte fundamental de su accionar, el uso de Smartphones y Tablets ha incrementado por su facilidad de acceso, funciones como multimedia y ocio, el precio y las tendencias del mercado hacen que sean

objetivo por parte de delincuentes informáticos que ven en ellos dispositivos que en caso de ser vulnerados, afecten directamente a sus usuarios, ya que la interacción de estos sistemas es inmediato. Para esto hay que tener claro lo siguiente, las vulnerabilidades son errores en la programación de un sistema en específico, por ende los atacantes aprovechan y buscan comprometer estos y robar información, por lo tanto, la tecnología móvil no está excenta de esta problemática, ya que a pesar de su tamaño y practicidad, también hacen uso de software y hardware que presentan fallas transformadas en vulnerabilidades, según lo reseñado por ESET, ha quedado en manifiesto que: "*Los cibercriminales están comenzando a enfocarse cada vez más en explotar agujeros de seguridad en sistemas operativos para móviles como Android."* (ESET Latinoamérica, 2014).

Descubrimiento de ataques como el *Troyano Obad* que permite a un tercero manipular los teléfonos móviles a través de mensajes de texto (SMS), para robar información sensible del usuario y que poseen la capacidad de descargar otras amenazas, dan alerta sobre los cuidados y desafíos que la Seguridad de la Información debe tener muy en cuenta de acuerdo a la tendencia. En esto tiene mucho que ver el usuario y una adecuada campaña educativa donde explique los riesgos que puede tener al hacer manejo no consciente de sus dispositivos móviles, porque en gran parte somos nosotros, como clientes, quienes abrimos la puerta a estas vulnerabilidades al instalar aplicaciones de dudosa procedencia pero que presentan soluciones inmediatas que es lo que realmente nos importa al hacer uso de estos dispositivos.

Por ejemplo, es importante educar a la persona del común sobre el uso y las formas como puede administrar sus dispositivos móviles, tratar de explicar que en Tecnología Móvil que cuente con Sistema Operativo Android – que muestra una marcada diferencia en equipos vendidos sobre otros SO – puede encontrar en sus Ajustes > Seguridad > Administrador de dispositivos, cuáles son las aplicaciones que pueden hacer "de todo" con su información y que no puede otorgar dichos permisos a cualquier aplicación sin saber su procedencia y uso de estos permisos sobre su dispositivo. Presenta un desafío además porque el malware en este caso

para Android, creció un 16% de 2012 a 2013 de acuerdo al estudio realizado también por ESET. En la relevancia social, se ha desarrollado una ayuda multimedia para ayudar a los usuarios con el uso de dispositivos móviles.

5.3. VULNERABILIDADES: ESTADÍSTICAS, TENDENCIAS, EVOLUCIÓN E IMPACTO ECONÓMICO EMPRESARIAL.

En esta etapa de la investigación, que representa la columna vertebral de la misma, ya que a través de la información recopilada, categorizada y evaluada, se encaminará el proceso de desarrollo e implementación de la Guía Metodológica de acuerdo a las herramientas de Hacking Ético y Vulnerabilidad definidas en la misma y también ajustada con la normatividad y legislación anteriormente mencionada, para esto se definen dos etapas que se desarrollarán a continuación.

Se tendrá en cuenta lo relacionado con estadísticas y análisis realizados sobre amenazas por entidades reconocidas a nivel mundial, en especial con Aplicaciones y Sistemas de Información (Software Inseguro) que debilita la seguridad en la infraestructura informática de importantes sectores de la economía nacional en la cual la protección, confiabilidad, disponibilidad e integridad de sus datos representa su reputación en el mercado y reconocimiento ante sus clientes.

5.3.1. CLASIFICACIÓN Y METODOLOGÍA

Para empezar, es importante definir los aspectos fundamentales para la clasificación de la información levantada en cuanto a estadísticas y análisis de vulnerabilidades para la posterior generación de criterios plasmados en una matriz, teniendo en cuenta el objetivo de evaluar los impactos en las organizaciones de tipo económico y de reputación, asimismo involucrando la

legislación y normatividad previamente compilada y delimitada, que es lo que se tratará a continuación.

5.3.1.1. Marco Legal y Normativo: Su Asociación a los Principios Básicos de La Seguridad de La Información:

A partir de los principios básicos de la Seguridad de La Información y que tienen como objetivo definir las propiedades (principios) de Confidencialidad, Disponibilidad e Integridad, que hacen un sistema sea "seguro", estas propiedades son explicadas más en detalle a continuación:

- **Confidencialidad:** La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus directrices para la Seguridad de los Sistemas de Información define la confidencialidad como: "El hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada". (Aguilera López, 2010)

- **Disponibilidad:** El programa MAGERIT (Methodology for Information Systems Risk Analysis and Management) define la disponibilidad como: "grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La Disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información. (Aguilera López, 2010)

- **Integridad:** Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado. (Aguilera López, 2010)

Además se hace referencia a un concepto que no hace parte de la Triada CIA (del inglés: "Confidentiality, Integrity, Availability"), el cuál es la Autenticación, se considera de gran importancia en consecuencia a la tendencia en los ataques maliciosos: La suplantación del usuario final. A continuación una referencia y definición específica

- **Autenticación:** Es la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos, normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña, pero, cada vez más se están utilizando otras técnicas más seguras. La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. La decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger. (Mifsud, 2012)

Por esto, de acuerdo a la investigación previa, se hace un análisis según la Legislación y Normatividad profundizada, para identificar cuáles componentes de cada una de ellos impactan estos principios básicos de la Seguridad de La Información, con esto se le dará un peso correspondiente para la matriz de evaluación de las vulnerabilidades posteriormente.

Normatividad y Estándares:

En esta parte, se toma como referencia las Normatividades: ***ISO/IEC 27001, NTC 5254, RFC 2196,*** donde se identificaron los Capítulos, Secciones, Apartes y/o Similares en cada una de ellas, que impactan el objetivo de la investigación y se clasificaron en los Principios Básicos de la Seguridad de la Información, como se muestra en el Anexo No.3.

VER ANEXO No.3 – PRINCIPIOS DE LA SEGURIDAD Y LA INFORMACIÓN: NORMATIVIDAD Y ESTÁNDARES

Legislación:

De acuerdo con el Marco Legal, se establece la siguiente tabla, la cual nos brinda un panorama que define según su definición aproximada a los temas relacionados con Seguridad de la Información a cuáles principios básicos referenciados anteriormente, tiene más impacto, se puede observar a continuación:

LEY / DECRETO	CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD	AUTENTICACIÓN
Ley 527 de 1999 - COMERCIO ELECTRÓNICO	X			X
Ley 599 DE 2000	X	X	X	
Ley 962 de 2005		X		
Ley 1150 de 2007	X	X		
Ley 1273 de 2009		X	X	
Ley 1341 de 2009		X	X	
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009				X
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	X	X	X	X
Ley 1581 de 2012	X		X	

Tabla 1 – Principios de la Seguridad de La Información ajustados a la Legislación Colombiana

5.3.1.2. Identificación de Fuentes: Entidades, Organizaciones y Grupos de Investigación

Por otra parte, la identificación de las fuentes que brindarán la clasificación, referencias, estadísticas y documentación es primordial en esta parte del trabajo investigativo, ya que se ha establecido dentro de los objetivos específicos de la misma, a partir de esto se hace referencia a las siguientes entidades consultadas y utilizadas para el diseño de la metodología en la creación de la matriz de evaluación de vulnerabilidades ajustadas.

Se tendrá como base el proyecto denominado “Top 10” realizado por la Organización OWASP (*Open Web* Application Security Project) que es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas las herramientas, documentos, foros y capítulos de OWASP son gratuitos y abierto a cualquiera interesado en mejorar la seguridad de aplicaciones. (OWASP, 2014). Al ser un proyecto sin ánimo de lucro y sin impulso y motivación económica para su ejercicio por parte de la empresa privada, da la certeza que los documentos extraídos cuenten con la imparcialidad necesaria.

La clasificación de vulnerabilidades que es referenciada por estándares, libros y herramientas, está soportada por diferentes organizaciones, entre las más destacadas están las siguientes:

MITRE *The MITRE Corporation:* es una organización estadounidense sin ánimo de lucro localizada en Bedford, Massachusetts y McLean, Virginia. Provee ingeniería de sistemas, investigación y desarrollo, y soporte sobre tecnologías de

la información al gobierno de Estados Unidos de América. (Bloomberg Businessweek, 2014)

PCI SSC *PCI Security Standards Council:* es un foro mundial abierto, establecido en 2006, que se encarga de la formulación, gestión, educación y conocimiento de las Normas de seguridad de la industria de tarjetas de pago (PCI), entre ellas: La Norma de seguridad de datos (DSS), la Norma de seguridad de datos para las aplicaciones de pago (PA-DSS) y los requisitos de Seguridad de transacciones con PIN (PTS). (PCI Security Standards Council, 2014)

DISA *Defense Information Systems Agency*: es una agencia de apoyo de combate del Departamento de Defensa (DoD). La agencia se compone de cerca de 6.000 empleados civiles; más de 1.500 militares en activo del Ejército, Fuerza Aérea, la Armada y la Infantería de Marina; y aproximadamente 7.500 contratistas de defensa. La agencia ofrece, opera, y asegura el mando y control y las capacidades de intercambio de información y una infraestructura de información para soportar lo referente a los organismos militares de Estados Unidos. (DISA, s.f.)

Entre otras organizaciones, estas al ser polos de investigación de relevancia mundial en el ámbito de seguridad informática, nos presentan un panorama global, confiable y de referencia, que facilitará la identificación de las amenazas más frecuentes, de mayor impacto y de gran trascendencia en las empresas a nivel mundial.

Por otra parte, es importante hacer referencia a proveedores y entidades privadas, a nivel nacional e internacional que proveen información actualizada relacionada con Seguridad de La Información

CERT Computer Emergency Response Team: es una División del Software Engineering Institute (SEI), fue creado en 1988 como el Centro de Coordinación CERT en respuesta al incidente gusano Morris. La pequeña organización creada para coordinar la respuesta a los incidentes de seguridad en Internet ahora cuenta con más de 150 profesionales de seguridad cibernética que trabajan en proyectos que tienen un enfoque proactivo para la protección de sistemas. (CERT SEI, s.f.)

SANS: El Instituto SANS es una organización de investigación y educación a profesionales de la seguridad de todo el mundo entre los que se encuentran: auditores y administradores de red, a los oficiales jefes de seguridad de la información, dando solución a los desafíos que enfrentan. SANS es la mayor fuente de formación en seguridad y certificación de la seguridad en el mundo. También desarrolla, mantiene y pone a disposición sin costo alguno, la mayor colección de documentos de investigación sobre diversos aspectos de la seguridad de la información, y que opera el sistema de alerta temprana del Internet - el Internet Storm Center. (SANS, s.f.)

SYMANTEC: es una empresa especializada en protección de la información cuyo objetivo es ayudar a particulares, empresas e instituciones gubernamentales a aprovechar libremente las oportunidades que les brinda la tecnología, en cualquier momento y lugar. (SYMANTEC CORP, 2014)

ISACA (Information Systems Audit and Control Association): Es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información, ayuda a empresas y líderes de TI a construir confianza en y maximizar el valor de la información y de los sistemas de

información. ISACA es una fuente confiable de conocimiento, estándares, comunidad, y desarrollo de carrera para los profesionales en gobierno, privacidad, riesgos, seguridad, aseguramiento y auditoría de sistemas. (ISACA, s.f.)

Cada una de estas organizaciones son la base de conocimiento en esta etapa del presente trabajo, proveen información actualizada y sustentada acerca de los acontecimientos relacionados con la Seguridad de La Información y los cuales harán de la clasificación de vulnerabilidades algo acorde con vigencia y aplicabilidad a través del tiempo.

5.3.2. IMPACTO ECÓNÓMICO Y REPUTACIONAL EMPRESARIAL POR ATAQUES INFORMÁTICOS EN COLOMBIA

La Seguridad de la Información transforma la confianza y reputación en el activo intangible más valioso para una compañía que realice transacciones con datos personales, dinero o información que involucre la integridad de los usuarios, por lo tanto esto representa un objetivo que al ser vulnerado, se transforma en millones y millones en pérdidas además de una afectación en el mercado que genera desconfianza y por lo tanto una devaluación del producto ante los demás competidores. Los temas de ataques maliciosos y los daños que causan en las compañías en particular en Colombia son manejados con bajo perfil, por el mismo hecho que su posible difusión a través de los medios de comunicación que ven en este tema algo de morbo dado a los hechos recientes y por lo tanto afectaría de gran forma la reputación de las empresas afectadas, por lo tanto, las cifras e impactos conocidas por estudios realizados por empresas reconocidas como HP Enterprise Security Products (Santos M. , 2013), PwC, Center for Strategic and International Studies, Certicámara y las multinacionales de seguridad McAfee y Symantec son a nivel general y no específico.

A nivel global, según reseña McAfee (Revista Dinero, 2014), en su estudio estimó el costo de los ciberataques para la economía mundial entre unos US$375.000 millones y US$575.000 millones, con una pérdida de unos 350.000 empleos en Estados Unidos y Europa; un valor considerable teniendo en cuenta en los modelos de negocio y utilidades obtenidas en el ejercicio económico específico de cada empresa. Es importante reseñar casos donde el impacto reputacional fue muy grave y de mucha difusión, como lo son el CASO TARGET (Noviembre 2013) y el CASO SONY (Abril 2011).

Por otra parte, ya en el plano nacional, se destaca el estudio realizado por Symantec y Certicamara, que afirma que el daño del cibercrimen en el último año alcanzó en Colombia ***464 millones de dólares,*** unos 917.000 millones de pesos. Dicha cifra incluye no solo la pérdida física del activo, sino la inversión que tuvieron que hacer las empresas para reparar el daño. El incremento anual del costo de los ciberataques en el país, además, es cercano a 36 por ciento (Symantec, Certicamara, 2014).

5.3.3. MATRIZ DE EVALUACIÓN PARA VULNERABILIDADES AJUSTADA AL MARCO LEGAL Y NORMATIVO COLOMBIANO CON BASE EN OWASP TOP 10 2013:

En esta etapa se establecerá una Matriz de Evaluación que será de ayuda para identificar de acuerdo a las Vulnerabilidades publicadas por los entes especializados a nivel mundial y apoyado en una calificación de los principios básicos de la Seguridad de La Información con base en la Legislación, Normatividad y los estándares aplicados en el país en el ámbito empresarial, se desarrolla de la siguiente forma:

Como base, se tomará una metodología que se ajusta en gran parte al objetivo de la investigación y el resultado que se quiere obtener al finalizar esta, se trata

del OWASP Risk Rating Methodology, esta examina factores de probabilidad comunes y factores de impacto para cada debilidad común, además define numerosos factores que ayudan a calcular el riesgo de una vulnerabilidad identificada, que incluye tres factores de probabilidad para cada vulnerabilidad (Frecuencia, posibilidad de detección y facilidad de explotación) y un factor de impacto (impacto técnico), los datos de frecuencia se han recopilado de las estadísticas de un conjunto de organizaciones entre las que se encuentran: Aspect Security, HP, Minded Security, Softek, Trustwave Spider Labs, VeraCode, WhiteHat Security, entre otras. (OWASP, 2013). Todo esto hace de la matriz de evaluación un factor decisivo, sólido, con información consecuente, actualizada, participe de un proceso de investigación global liderada por la Organización OWASP y respaldada por entes certificados a nivel mundial.

A continuación se presenta la matriz y criterios de evaluación:

MATRIZ DE EVALUACIÓN PARA VULNERABILIDADES AJUSTADA AL MARCO LEGAL, NORMATIVO COLOMBIANO CON BASE EN OWASP							
50%			25%	25%			
25%	10%	15%		9%	5%	5%	6%
Vectores de Ataque	**Prevalencia de Debilidades**	**Detectabilidad de Debilidades**	**Impacto Técnico**	**Impacto Marco Legal y Normativo: Colombia**			
				Confidencialidad	**Disponibilidad**	**Integridad**	**Autenticación**
Fácil (3)	Difundido (3)	Fácil (3)	Severo (3)	1-3 (Alto:3 | Medio:2 | Bajo: 1)	1-3 (Alto:3 | Medio:2 | Bajo: 1)	1-3 (Alto:3 | Medio:2 | Bajo: 1)	1-3 (Alto:3 | Medio:2 | Bajo: 1)
Promedio (2)	Común (2)	Promedio (2)	Moderado (2)				
Difícil (1)	Poco Común (1)	Difícil (1)	Menor (1)				

Tabla 2 Matriz De Evaluación Para Vulnerabilidades Ajustada Al Marco Legal, Normativo Colombiano Con Base En OWASP

Niveles de Evaluación:

- Fácil: Requiere un nivel básico para acceder, sólo con el uso de herramientas, escenario ideal para Script-Kiddles
- Promedio: Necesita un nivel de conocimiento intermedio para perfilar ataques o detectar vulnerabilidadsa través de software especializado.
- Difícil: Para acceder y detectar las vulnerabilidades, se requiere conocimientos avanzados de Ethical Hacking.
- Severo: La recuperación del Sistema de Información causa alto impacto en la organización transformado en tiempo y dinero.
- Moderado: Los impactos en la infraestructura requiere intervención dejando fuera de línea los aplicativos, pero la recuperación no implica dinero.
- Menor: Los tiempos de recuperación son inmediatos y no se ve afectada la integridad de los datos.
- Vectores de Ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema. (SYMANTEC, s.f.)
- Prevalencia de Debilidades: Es la propagación de la vulnerabilidad desde el tiempo que se detecta, se prolifera y se corrige.
- Detectabilidad de Debilidades: Es la posibilidad y efectividad de detección de una vulnerabilidad de parte de un atacante en el sistema objetivo.
- Impacto Técnico: Probabilidad de daño o afectación en la infraestructura donde involucra los tiempos de respuesta, recuperación y restauración del sistema involucrado.
- Impacto Marco Legal y Normativo en Colombia (Previamente definidos), clasificados como: Impacto Bajo (1), Impacto Medio (2), Impacto Alto (3).
    - Confidencialidad
    - Disponibilidad
    - Integridad
    - Autenticación

5.3.4. RESULTADOS

La matriz de evaluación, previamente definida, presenta los siguientes resultados de acuerdo a las fuentes seleccionadas y las amenazas y/o vulnerabilidades ajustadas de cara al desarrollo de una Guía Metodológica para prevenir, detectar y corregir dichas amenazas y vulnerabilidades, haciendo énfasis en las relacionadas con Aplicaciones y Sistemas de Información de cara a Internet o de acceso público.

MATRIZ DE EVALUACIÓN PARA VULNERABILIDADES AJUSTADA AL MARCO LEGAL, NORMATIVO COLOMBIANO CON BASE EN OWASP

		50%			25%	25%					
		25%	10%	15%		9%	5%	5%	6%		
Ref. OWASP	**Vulnerabilidad**	**Vectores de Ataque**	**Prevalencia de Debilidades**	**Detectabilidad de Debilidades**	**Impacto Técnico**	**Impacto Marco Legal y Normativo: Colombia**				**Referencias**	**Puntaje Final**
						Confidencialidad	**Disponibilidad**	**Integridad**	**Autenticación**		
A1	Inyección	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	1	1	3	2	CWE-77; CWE-89; CWE-564	2.41
A2	Pérdida de Autenticación y Gestión de Sesiones	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	3	1	2	3	CWE-287; CWE-384	2.45
A3	Secuencia de Comandos en	Fácil Promedio	Difundido Común	Fácil Promedio	Severo Moderado	1	1	3	2	CWE-79	2.36

	Sitios Cruzados (XSS)	Difícil	Poco Común	Difícil	Menor						
A4	Referencia directa insegura a objetos	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	3	2	1	3	CWE-639; CWE-22	2.5
A5	Configuración de Seguridad Incorrecta	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	3	1	2	3	CWE-2; CIS SC Benchmarks	2.55
A6	Exposición de Datos Sensibles	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	2	3	2	3	CWE-310; CWE-312; CWE-319; CWE-326	2
A7	Inexistente Control de Acceso a Nivel de Funcionalidades	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	2	1	1	3	CWE-285	2.35
A8	Falsificación de Peticiones en Sitios Cruzados (CSRF)	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	3	2	1	3	CWE-352	2.11
A9	Uso de Componentes con Vulnerabilidades Conocidas	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	1	1	1	3	MITRE	1.9
A10	Redirecciones y reenvíos no válidos	Fácil Promedio Difícil	Difundido Común Poco Común	Fácil Promedio Difícil	Severo Moderado Menor	2	1	2	2	CWE-601	1.92

Tabla 3 – Resultados Matriz Evaluación

En resumen, este es el Top 5 de vulnerabilidades de acuerdo a la matriz de evaluación:

- 1. A5: Configuración de Seguridad Incorrecta – 2.55pts/3pts
- 2. A4: Referencia directa insegura a objetos – 2.5pts/3pts
- 3. A2: Pérdida de Autenticación y Gestión de Sesiones – 2.45pts/3pts
- 4. A1: Inyección – 2.41pts/3pts
- 5. A3: Secuencia de Comandos en Sitios Cruzados (XSS) – 2.36pts/3pts

5.4. HACKING ÉTICO: ESTADO ACTUAL, METODOLOGÍAS Y HERRAMIENTAS

5.4.1. CONCEPTO Y ESTADO ACTUAL

En la actualidad, en el mundo y especialmente en Colombia, el término “Hacking”, “Hacker”, “Hackeado”, “Cracker” entre otros similares han estado apareciendo en los medios de comunicación por movidas políticas, ataques a empresas entre otros, tanto así que la Real Academia de la Lengua Española ya incluye la palabra “*Hacker”* y la define como: ‘Pirata informático’ (RAE, 2013), sin embargo técnicamente es importante realizar un análisis del estado actual de los términos, involucrados, los fines de cada uno de ellos para poder dar una definición cercana a lo relacionado con “Hacking Ético”, que es la técnica en la cual se apoya la metodología de prevención, detección y corrección de vulnerabilidades comunes a sistemas de información a nivel empresarial en el país.

La referencia más inmediata y reciente con respecto al tema Hacking en Colombia, dado a su aparición en los medios y relevancia por el tema político cercano a las elecciones ejecutivas, es el relacionado con Andrómeda, una fachada militar de inteligencia informática, descubierta 24 de enero de 2014, cuando el CTI ocupó un local ubicado en el barrio Galerías llamado *Ethical Hacking "Comunidad Buggly"* (Enter.CO, 2014). En medio del escándalo se dijo que el sitio estaba siendo utilizado para interceptar los correos de los negociadores del Gobierno en La Habana. (El Espectador, 2014). A partir de ahí, el tema de moda era el hacking y la confusión sobre las actividades relacionadas con seguridad informática se proliferaban por los medios de comunicación, tergiversando conceptos transmitiendo al público la idea que los Hackers en general, cometen actos delictivos y siendo señalados como delincuentes, por lo tanto, siendo consecuentes con el objetivo de relevancia y concientización social de la investigación, se hará una breve reseña acerca de los Tipos de Hackers y sus objetivos.

- **Black Hat | Crackers:**

  Definición: Es quién se dedica a la obtención y explotación de vulnerabilidades en sistemas de información, bases de datos, redes informáticas, sistemas operativos, determinados productos de software, etc.

  Objetivos: Robo de información, inserción de virus o malware y creación de puertas traseras, para beneficio personal o lucro. (Red, 2012)

- **White Hat Hackers:**

  Definición: Profesionales con conocimientos de seguridad de la información que utilizan técnicas de Hacking para asegurar y proteger los sistemas de Tecnologías de la Información y comunicación.

  Objetivos: Prevenir, detectar y corregir vulnerabilidades en los sistemas informáticos para quién trabajan, evitar ataques y estar actualizados sobre nuevas técnicas de vulnerabilidad y fallas de dichos sistemas. Su trabajo

consiste en atacar los sistemas a proteger con el consentimiento previo y así descubrir vulnerabilidades efectuando planes de acción.

- **Gray Hat Hackers:**

  Definición: Personas con conocimientos similares a los Black Hat o Crackers, los cuales los utilizan para ingresar en sistemas de información no autorizados, buscar vulnerabilidad alguna y luego ofrecer servicios para su remediación o reparación.

  Objetivos: Conseguir a través de los servicios de remediación, dinero y contratos para compañías o particulares. (Pacheco & Jara, Ethical Hacking , 2012)

- **Lammer o script-kiddie:** Personas con habilidades informáticas técnicas, pero sin conocimientos de hacking, aprendizaje obtenido por herramientas encontradas en la web de fácil acceso, que utilizan sin medir las consecuencias que puede afectarlos a ellos mismos y su real funcionamiento.

  Objetivos: Demostrar conocimiento y tener poder sobre sistemas de información al no tener una formación adecuada del tema hacking.

- **Phreaker:** Especialistas en telefonía, con conocimientos de redes, arquitectura de dispositivos móviles, denominados como monstruos telefónicos.

  Objetivos: Utilizar las habilidades en telefonía para desbloquear, registrar de forma ilegal celulares en muchos casos robados, obtener saldos gratuitos para hacer llamadas entre otros.

- **Newbie:** Denominados novatos, son los que les apasiona el tema hacking al comienzo, pero no tienen conocimiento alguno, solo se encuentran con herramientas y/o utilidades para hacer ataques sin saber función y su trasfondo.

  Objetivos: Poner a prueba las herramientas que encuentran, a ver si logran tener fortuna de novato al penetrar algún sistema vulnerable. (Red, 2012)

Es importante hacer una aclaración y reflexión final, para esto cito a Juan Carlos Martínez, un Ingeniero que a través del Diario El Espectador hace referencia al tema con un mensaje contundente y de gran importancia, se resalta lo siguiente:

"…Originalmente la palabra hacker define a una persona que fabrica muebles con un hacha, pero, dentro de las definiciones de hacker especializadas, es "una persona que disfruta explorando los detalles de los sistemas programables y como ampliar sus capacidades, a diferencia de la mayoría de los usuarios, que prefieren aprender sólo el mínimo necesario", pero también describe al hacker como "un experto o entusiasta de cualquier tema. Uno de ellos puede ser por ejemplo un astrónomo hacker". Se debe aclarar que un hacker no es un entrometido malicioso que intenta descubrir información sensible por hurgar. El término correcto es Cracker.

En la sociedad del conocimiento, hay hackers que han hecho grandes aportes, como por ejemplo Linus Torvalds (creador del sistema operativo Linux), Steve Wozniak (constructor del primer computador personal y cofundador de Apple), Bill Gates (hacker del ALTAIR y negociante en Microsoft), Tim Berners-Lee (creador de la world wide web WWW) y muchos más, como el mismo Julian Assange (Wikileaks y editor de parches para PostgreSQL).

En los múltiples contextos de la sociedad, los hackers han desarrollado un papel importante para iniciar proyectos de gran impacto en la humanidad, por ejemplo, Wikipedia, el sistema operativo Linux, el sistema operativo Android, la licencia Creative Commons, Internet como lo conocemos hoy en día y más. Por esta razón, llamar hackers a los husmeadores se presta para generalizar ideas erróneas acerca de este conjunto de personas que dedican su tiempo a la pasión de crear herramientas que faciliten la vida de la humanidad..." (Martínez Rodríguez, 2014)

De forma ilustrativa se quiere presentar esta información para el público en general, a través de afiches, videos y una página web donde se encontrará además, los apartes y resultados de la investigación.

5.4.2. METODOLOGÍAS

Primero que todo, para hablar de metodologías de Hacking Ético, es importante definir un concepto base denominado *Pentesting,* básicamente este se refiere a un test de intrusión que evalúa los niveles de seguridad de un sistema informático o red mediante la simulación en un entorno controlado de un ataque por parte de un usuario malicioso conocido comúnmente como Hacker. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013), a través de este test, que se realiza desde la perspectiva de un atacante tiene como propósito es determinar las viabilidad de un ataque y la cantidad de impacto; de esta forma se afirma la teoría que la mejor manera de demostrar la fuerza de una defensa es tratando de penetrar en ella, estos están dirigido a la búsqueda de agujeros de seguridad de forma focalizada en uno o varios recursos críticos, como puede ser el firewall o el servidor Web, aplicaciones móviles, además siendo indiferente el sistema operativo. (UNAD, 2014). Este tipo de test en muchas ocasiones al ser una simulación de un ataque, es posible que sean restringidas por la ley o por las políticas de seguridad de la compañía o el ambiente informatizado donde se va a realizar el 'Ataque Controlado', para esto, se debe plasmar en un documento físico firmado por las partes involucradas en el proceso, dónde se indiquen cuáles serán las fases del test.

Existen diferentes metodologías, con estándares definidos para que el proceso de Hacking Ético se haga de manera lógica y ordenada siendo las siguientes metodologías Open Source las más adoptadas (Arias, 2013):

- OSSTMM (Manual de Metodología Abierta de Evaluación de Seguridad).
- ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información).
- OWASP (Proyecto de Seguridad de Aplicaciones Web Abiertas).

Las metodologías mencionadas presentan una estructura documental muy fuerte, y están diseñadas especialmente para Auditorías de Seguridad de la Información a profundidad, por tal motivo, haremos referencia a las fases de un test de intrusión o pentesting que es suficiente para la aplicación de la Guía Metodológica estructurada en este documento.

Estas etapas o fases a la hora de realizar un Pentesting si no son realizadas en el orden correcto, podrá complicar el desarrollo del mismo y especialmente generar problemas con el cliente o el dueño de los sistemas de información donde se va a realizar el test ya que puede poner en riesgo los ambientes de producción o puede estar accediendo a sitios no autorizados poniendo en riesgo la propiedad intelectual de la organización.

Las fases del Pentesting son las siguientes (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013):

- **Reglas de Juego: Alcance y términos del Test de Intrusión:** En esta fase se llega a un acuerdo sobre los objetivos a los cuales quiere llegar el cliente o el dueño de los SI, definir los límites y campos de acción para quienes realizarán el Pentesting, ya que la información, el activo más preciado de una compañía estará a disposición de los Testers, para esto se hacen acuerdos y/o contratos de confidencialidad, definidos en un documento firmado.
- **Recolección de Información:** Es una etapa netamente práctica, donde el equipo de testers utilizará técnicas tales como Footprinting, Fingerprinting, Google Hacking, entre otras para intentar obtener la mayor cantidad información sobre a Organización Objetivo, todo esto es muy importante porque si se conoce la forma de actuar de un sistema o mecanismo de protección se puede desarrollar un sistema de contramedidas para vulnerarlo.

- **Análisis de las vulnerabilidades:** Posterior a la recolección de información, se debe analizar y organizar los resultados, ya que a partir de estos se puede detectar agujeros de seguridad para así calibrar los ataques de forma más específica; modelar el método de ataque más eficaz que se adapte a la solución. El uso de escáneres y análisis de puertos, entre otros, son los procedimientos habituales en esta etapa.
- **Explotación de las Vulnerabilidades:** Esta es la etapa más importante y que mayor satisfacción genera en los que realizan los ataques, ya que se trata de acceder, romper, burlar los sistemas de acuerdo a la recolección de información y el perfil de ataque, sin embargo es la de más cuidado, ya que por tratar de acceder a como dé lugar, es posible que se destruya o afecte a integridad de los datos, no se debe caer en el error de la automatización de ataques, se debe tener certeza que el perfil del ataque sea el adecuado al Sistema de Información Objetivo.
- **Post-explotación del sistema:** Esta fase consiste –asumiendo que se tiene control y un nivel de acceso sobre la máquina o el sistema- en que el auditor hará escalamiento de privilegios y/o permisos sobre la infraestructura para demostrar qué tanto puede acceder un posible atacante y que control tendrá sobre el Sistema de Información comprometido, tratando en lo posible controlar todos los equipos de la red corporativa dado el caso. Exploración de puntos débiles desde adentro.
- **Generación de Informes:** Se finaliza presentando al Cliente cada una de las acciones realizadas durante cada una de las fases del Pentesting y a su vez los resultados obtenidos, que pueden ser alimentados con documentación, capturas de pantalla, rutas encontradas, parámetros y agujeros de seguridad encontrados durante la exploración, además se recomienda hacer la recopilación de esta información durante cada una de las fases y no al final ya que puede ser una tarea tediosa. Al final se obtendrá en el documento final de la auditoría se debe incluir cada una de las tareas que se han realizado y todas las técnicas y herramientas, la forma como fueron utilizadas, los tipos de vulnerabilidades que se han descubierto y el

nivel de riesgo e impacto que tienen en la seguridad de la organización. Hay que tener en cuenta que se deben clasificar los informes, entre técnicos y ejecutivos, esto condiciona el nivel de profundidad técnica en cada uno de ellos, así como en las recomendaciones y buenas prácticas para corregir dichas vulnerabilidades. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013)

5.4.3. EVALUACIÓN HERRAMIENTAS

El estado actual del Hacking y Hacking Ético, como se presentó anteriormente, nos muestra en todos los escenarios el apoyo a través de metodologías y de herramientas (software) que al final son el motor que impulsa el éxito en cada procedimiento de ataque y/o detección de vulnerabilidades, como esta investigación y desarrollo de la guía metodológica está enfocada para empresas que bien o no pueden contratar un servicio de consultoría de Ethical Hacking por su alto costo o no cuentan con un Profesional de la Seguridad de la Información por el tamaño de su organización, es importante hacer una evaluación sobre estas herramientas, para especificar su funcionamiento, su naturaleza, costo, popularidad y efectividad, para así dar valor agregado al resultado de la misma, la mejor opción desde nuestro punto de vista en herramientas hacking para las empresas.

Es importante aclarar, que las herramientas/software es especializado, es decir, cada uno cumple un vector de “ataque” específico, en el Anexo No.4 se presentan las más populares y destacadas, con una breve descripción.

VER ANEXO No.4 – HERRAMIENTAS PENTESTING Y DESCRIPCIÓN

De la misma forma, es importante hacer el análisis desde el punto de vista económico y técnico (plataformas), además tener en cuenta el uso de herramientas compiladas bajo un mismo sistema operativo todo esto para obtener una mayor flexibilidad en la ejecución de las actividades, su ciclo de vida, cumplimiento de las restricciones planteadas.

Herramienta	Plataformas			Precio (USD)
	Windows	Linux	MacOS	
NetScan Tools « http://www.netscantools.com/ »	✓	X	X	$249
Nmap « http://nmap.org/»	✓	✓	✓	Freeware
Ncat «http://nmap.org/ncat/»	✓	✓	✓	Freeware
Metasploit Framework « http://www.metasploit.com/ »	✓	✓	X	Freeware para Estudiantes y Pequeñas Empresas
Retina Network Security Scanner « http://www.beyondtrust.com/ »	✓	X	X	$1200
John The Ripper «*http://www.openwall.com/john/* »	✓	✓	✓	Freeware
OpenVAS «http://www.openvas.org/»	✓	✓	X	Freeware
Burp Suite «http://portswigger.net/burp/»	✓	✓	✓	$299
Maltego «https://www.paterva.com/web6/»	✓	✓	✓	Freeware en Linux ($760)
Nessus «http://www.tenable.com/»	✓	✓	✓	$1500
Wireshark «https://www.wireshark.org/»	✓	✓	✓	Freeware

Tabla 4 – Evaluación Herramientas Pentesting

La tabla nos muestra una prevalencia de las herramientas y su ejecución sobre sistemas operativos Windows, en segundo lugar se encuentra Linux y cualquiera de sus distribuciones y por último se encuentra MacOS; sin embargo es importante destacar, que Linux al ser un sistema operativo Open Source (Libre), es el predilecto en el mundo hacker por su flexibilidad y claro, por su gratuidad; por esto mismo, presentamos la opción más viable de acuerdo a la relación Calidad/Precio apoyados en el hecho de que las herramientas de propósito general que realizan actividades específicas en cada etapa de un test de penetración por su precio y la plataforma donde están implementadas inclinan la balanza a favor del uso de un sistema operativo o distribución que cuente con un conjunto de herramientas que cubran cada una de estas etapas, para esto presentamos: Kali Linux.

Figura 1. Presentación Kali Linux

Imagen tomada de https://www.kali.org/

Kali Linux es una proyecto/distribución libre (Gratuito) basada en Debian y desarrollado por el Offensive Security (*https://www.offensive-security.com/*) un

equipo de expertos en Seguridad de La Información a Nivel Mundial, que ofrece un abanico de posibilidades completamente nuevo, proporcionando compatibilidad a más de 300 herramientas para realizar labores de pentesting, cumpliendo los estándares, las políticas de uso de Debian como software libre y siguiendo las mejores prácticas de uso en dicho entorno, entre las características principales de Kali Linux se encuentran las siguientes:

- La empresa desarrolladora es totalmente partidaria del uso y desarrollo de código abierto, para el uso y disfrute de los usuarios para los que deseen conocerlos, modificarlos o reconstruirlos, siempre respetando el espíritu *Open Source*.
- Gran soporte para dispositivos inalámbricos, permitiendo que funcionen correctamente una amplia variedad de hardware, como numerosos USB y otros dispositivos de almacenamiento masivo.
- El equipo de desarrollo de Kali es un grupo reducido de personas de confianza con alto nivel técnico que interactúan con los paquetes que componen los repositorios haciendo uso de protocolos seguros, todo ello para garantizar un entorno de desarrollo fiable. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013)

El uso de Kali Linux es muy intuitivo, además que cuenta con una interfaz gráfica agradable y presenta modos de trabajo a través de los cuales es posible completar las labores profesionales con el único objetivo de minimizar tiempo y esfuerzo, llegando a obtener los resultados deseados.

A través de un Live-CD, donde se busca hacer uso de la distribución sin necesidad de tenerla instalada físicamente en la máquina, solamente en arrancándola desde la unidad de cd, que presenta una gran ventaja si solo se quiere usar una o algunas herramientas en el sistema operativo y por otra parte una Instalación en físico, que requiere un Archivo ISO que se encuentra en la web oficial *www.kali.org*.

A través de la investigación, se ha tenido en cuenta en todas las etapas, la tendencia actual en el mundo de los Profesionales de la Seguridad de la Información, por esto Kali Linux se resalta dentro de las distribuciones de seguridad informática, ya que hace un compendio de acuerdo a diferentes estudios realizados por Offensive Security basados en estadísticas de uso, encuestas de popularidad y resultados basados en su amplia experiencia en el mundo de la seguridad informática de las herramientas de seguridad denominada "Top 10 Security Tools", lo más relevante de esta lista, es que las mencionadas en dicho ranking, hacen parte de la lista de herramientas en estudio Económico/Técnico reseñado anteriormente, este es el Top 10, que se encuentra en Kali Linux (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013):

1. Aircrack-ng
2. Burp Suite
3. Hydra
4. John (John The Ripper)
5. Maltego
6. Metasploit
7. Nmap
8. SqlMap
9. Wireshark
10. Zaproxy

Además sobre la plataforma Kali, al ser distribución base de Linux se puede ejecutar herramientas como OpenVAS y Nessus.

Por estas razones, evaluamos y elegimos a Kali Linux como un compendio de herramientas lo suficientemente efectivas que serán de apoyo para la ejecución de la guía metodológica que se presentará en el siguiente módulo, además presenta una referencia sobre las herramientas adecuadas para los que apenas les empieza a apasionar el tema de Seguridad de la Información.

6. GUIA METODOLÓGICA

6.1. DESCRIPCIÓN

La Guía Metodológica para el Top. 5 De Vulnerabilidades en Ambientes Informatizados de cara a Internet ajustada en la Normatividad, Legislación y Estándares a Nivel Empresarial aplicados en Colombia quiere mostrar de una forma clara, concisa, efectiva y práctica la forma de Prevenir, Detectar y Corregir estas vulnerabilidades para que se convierta en una herramienta de primera mano para los interesados en hacer un diagnóstico en sus PyMES y MiPyMES que no cuentan con los recursos económicos suficientes para realizar una Auditoría de Seguridad de la Información en Sistemas Informatizados empresariales. Será una herramienta actualizada y diseñada para que sea persistente de acuerdo a la evolución de los ataques informáticos, por lo que se tuvo en cuenta el histórico de los mismos, y que su aplicación de una idea sobre el estado actual de los sistemas de información objetivo.

6.2. FORMATO E IMPLEMENTACIÓN

Se ha diseñado el siguiente formato/puntos para sustentar lo necesario en cada una de las vulnerabilidades para la Guía Metodológica, a continuación se explica su contenido.

6.2.1. DESCRIPCIÓN

Se hará un resumen técnico del concepto de la Vulnerabilidad, su origen, por qué ocurre, que infraestructura está involucrada en el proceso y qué consecuencias trae su explotación.

6.2.2. ESCENARIO

6.2.2.1.1. Diagrama por Fases y Criterios de Evaluación

Agentes de Amenaza	Vectores de Ataque	Debilidades de Seguridad		Impactos Técnicos	Impacto Marco Legal y Normativo				Impactos al Negocio
Específico de la Aplicación	*Explotabilidad*	*Prevalencia*	*Detección*	*Impacto*	*Confidencialidad*	*Disponibilidad*	*Integridad*	*Autenticación*	*Específico de la Aplicación*

Tabla 5 – Diagrama por Fases y Criterios de Evaluación

Este diagrama nos presentará en detalle qué escenario presenta la vulnerabilidad en cada una de las fases y criterios de evaluación previamente definidos, a su vez también incluye los Agentes de Amenaza (Quiénes pueden explotar el agujero de seguridad) y el Impacto en el Negocio - es importante aclarar que este impacto solo se puede saber con certeza de acuerdo al Sistema de Información objetivo, ya que cada uno de estos presenta información distinta, en este diagrama se trata de hablar de Impacto en el Negocio de forma global e hipotética-.

6.2.2.2. Escenarios de ataque

Aquí se presenta en lenguaje técnico, de que formas el sistema presenta la vulnerabilidad y cómo un posible atacante puede explotarlas, se muestra de forma global y en casos hipotéticos, se toman algunos escenarios, ya que una vulnerabilidad puede atacarse de muchas formas.

6.2.3. PREVENCIÓN

6.2.3.1. ¿Soy vulnerable?

Presenta en forma de caso, la posibilidad que la vulnerabilidad analizada sea evidente en el sistema de información objetivo, dando pautas para asegurar la infraestructura según sea el caso.

6.2.3.2. ¿Cómo Prevenirlo?

De acuerdo al escenario de vulnerabilidad presentado previamente, aquí se habla de cuáles son los puntos principales de forma técnica a cuidar en la

implementación o aseguramiento de los aplicativos o la infraestructura dependiendo del Fallo de Seguridad analizado.

6.2.4. DETECCIÓN

6.2.4.1. Metodología

En la etapa de detección, de forma técnica, se utilizará la metodología de Pentesting referenciada anteriormente, solo llegaremos al punto de Explotación de las Vulnerabilidades, ya que la fase de: Post-Explotación no es necesaria porque no queremos escalar en privilegios, solo se quiere demostrar que la vulnerabilidad está presente, y la fase de: Generación de Informes es un compendio del análisis de las 5 Vulnerabilidades presentadas en esta guía metodológica. Estas son las fases metodológicas que se tratarán en este punto:

- Reglas de Juego: Alcance y términos del Test
- Recolección de Información
- Análisis de las vulnerabilidades
- Explotación de las Vulnerabilidades

6.2.5. CORRECCIÓN Y BUENAS PRÁCTICAS

Sumado a la etapa de prevención, aquí se quiere dar pautas de buenas prácticas en la infraestructura involucrada en la vulnerabilidad analizada, además de consejos para los encargados de la Seguridad de la Información para tratar las contingencias y establecer planes de recuperación y respaldo en los Sistemas de Información.

6.2.6. REFERENCIAS

Se mencionan las referencias de las entidades internacionales tales como MITRE, OWASP, CWE entre otras que cuentan con conceptos técnicos más específicos de las vulnerabilidades, para orientar a los usuarios de la guía si necesitan apoyo más técnico y definido.

6.3. DESARROLLO DE LA GUÍA

VER ANEXO No.9: GUIA METODOLÓGICA VAINLEEC

7. SENSIBILIZACIÓN – REELEVANCIA SOCIAL

A través de la Investigación, se identificó que existe una confusión acerca del tema relacionado con Hacking, Hackers y relacionados, todo esto por la relevancia que le han dado los medios de comunicación por la aparición en temas políticos y de interés nacional, por lo tanto se ha diseñado la siguiente estrategia de Sensibilización para Profesionales de la Seguridad de la Información y el público en general, trabajando en diferentes frentes.

7.1. EQUIPO INVESTIGATIVO

Una de las principales motivaciones para realizar el presente trabajo de investigación, es el fomentar el interés de los estudiantes de Ingeniería Informática de la Universidad en el tema de la Seguridad Informática, por esto, se ha creado un nombre, logo, página de internet, redes sociales y demás donde se empezará, apoyado en los recursos colaborativos, blogs, entidades de confianza y otras organizaciones identificadas en el trascurso de la Investigación, para gestionar contenido, noticias, tips, actualizaciones e información de interés relacionadas con el Mundo Hacker.

A esta iniciativa se dio como nombre: ***Exploit Sabana Team,*** nombre en referencia al fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. El logo -*que se puede ver en la siguiente figura*- representa el símbolo de Kali Linux además de vectores que representan a la Universidad de La Sabana, inicialmente esto será a modo demostrativo, aunque las plataformas están implementadas y los dominios registrados, se entiende que la puesta en marcha requiere una autorización por parte de la Universidad por la referencia de su nombre.

Figura 2. LogoExploitSabanaTeam

Entre el contenido multimedia de la Campaña de Sensibilización se encuentra:

7.2. POSTERS INFORMATIVOS

Estos son las fichas o afiches desarrollados para contribuir con el objetivo de relevancia social:

- *¿Cuántos tipos de 'Hackers' conoces?:* En este poster, se presentan las diferentes clasificaciones de Hackers que existen, con imágenes que hacen referencia a cada uno de ellos de acuerdo a su nombre, lo que se quiere conseguir con esto, es aclarar al público en general, el concepto y el objetivo de cada uno de acuerdo a su actividad, y desmitificar la idea general de que todos los hackers son delincuentes.
- *¡Alerta profesionales de las TIC! – Tips: Seguridad = Tranquilidad:* En esta parte se dirige el arte hacia los Profesionales de las Tecnologías de la Información y Comunicación, mostrando 9 Simples pero efectivas buenas prácticas para mantener un nivel de aseguramiento básico de los aplicativos y activos de información que tienen a cargo.
- *Seguridad Móvil: Un paso delante de los delincuentes:* La ficha presenta 4 buenas prácticas de seguridad para salvaguardar los datos, la privacidad e integridad de los mismos en casos de robo o pérdida de los dispositivos móviles, apoyado en la experiencia se habla sobre la funcionalidad de las aplicaciones antirrobo que no son tan populares entre los usuarios pero que presentan miles de ventajas, la seguridad en las aplicaciones instaladas, los mecanismos de desbloqueo del dispositivo con su utilidad particular y por

último, la forma de contribuir con la lucha contra el robo de celulares al identificar de qué forma estos, al ser hurtados, se puedan dejar inservibles.

- *Los desafíos del Cloud Computing:* Esta infografía muestra a través de 5 pasos, los retos para los usuarios y administradores de plataformas que hacen uso del Cloud Computing en sus Sistemas de Información, hace referencia los desafíos en las fases y como deben ser abordados para obtener resultados ideales y con la menor cantidad de riesgo existente.

7.3. PÁGINA WEB – WWW.EXPLOITSABANATEAM.COM

Se ha creado el portal www.ExploitSabanaTeam.com, este será el medio por el cual se publicarán Noticias, Tutoriales, Actualizaciones, Legislación, Estándares y demás relacionado con Seguridad de La Información especialmente a Nivel Nacional, recopila información de fuentes confiables que se identificaron en el trascurso de la investigación, como Portales de Noticias, Compañías desarrolladoras de software de seguridad, entre otros.

Figura 3. Página www.ExploitSabanaTeam.com

7.4. TWITTER @EXPLOITUSTEAM – FACEBOOK.COM/EXPLOITSABANATEAM

Por medio de las redes sociales populares como Twitter y Facebook, se dará a conocer las novedades relacionadas con el mundo de la Seguridad de La Información, será un *Feed* de noticias, aparición en los medios, eventos y todo lo que gira alrededor del mundo de la Seguridad de la Información.

Figura 4. Facebook Exploit Sabana Team

Figura 5.Twitter @ExploitUSTeam

8. CONCLUSIONES

Al empezar este trabajo de investigación se partió con la idea de que se necesitaba un análisis del estado actual de la seguridad de la información en cuanto a legislación, estándares y normatividad, sin embargo se identificaron otras partes en el proceso de aseguramiento de Sistemas de Información que son muy importantes, como las iniciativas del gobierno a través de estrategias y grupos de apoyo para incidentes relacionados con seguridad de la información, a pesar que Colombia está lejos de los países líderes en Seguridad Informática como mecanismo de Ciberdefensa, es uno de los destacados en la región por este tipo de iniciativas y la gestión de uno de los mejores ministerios, como es el MinTIC, el vacío identificado en este aspecto es la falta de proliferación de la información.

A lo largo del Proyecto de Investigación la frontera de consulta se expandió debido a la cantidad de procesos, datos, información y componentes involucrados, especialmente en el análisis de las vulnerabilidades y sus impactos en el proceso de definición, gestión e implementación de una estrategia efectiva para contrarrestar las amenazas por parte de los ataques maliciosos a Sistemas de Información expuestos a internet, se concluye que para realizar un trabajo en producción aplicando lo visto en la Investigación, se necesita la participación activa de todos los involucrados en los procesos de presupuesto, diseño, implementación y puesta en marcha de un servicio web y/o aplicativo.

Con el análisis realizado se pudo identificar que a nivel mundial la tendencia se mantiene, a través de los años las vulnerabilidades y su esencia no ha cambiado, a pesar de la evolución de las tecnologías, sin embargo se ha visto un avance en las técnicas de penetración y ataque por parte de delincuentes, por esto se llega a la conclusión que el Profesional de la Seguridad de La Información debe estar siempre actualizado aplicando los últimos mecanismos de defensa para mantener un nivel de aseguramiento de los Sistemas de Información adecuado.

A través de la guía metodológica se logró identificar un factor muy importante, que es la contextualización del problema, es posible que esta sea la causa de procedimientos erróneos en cuanto a remediación de vulnerabilidades informáticas, ya que el profesional tiene una referencia de por qué, por cuál agujero y de qué forma puede ser atacado, sino simplemente se limita a aplicar las herramientas y parches sugeridos, sin saber con certeza si los procedimientos son los adecuados para el tipo de vulnerabilidad, esto deriva a que el conocimiento por parte de Profesional de la Seguridad de la información debe tener una visión global acerca de su infraestructura, la guía no reemplaza una auditoría de seguridad de la información, pero si puede mostrar el estado actual de la organización objetivo a muy bajo costo.

Las empresas, sin importar su tamaño e infraestructura encontrarán en el trabajo de investigación una referencia importante en su accionar y traza de objetivos en cuanto a niveles de aseguramiento de la información, se concluye que la teoría es muy importante pero que nada vale si no se inculca una consciencia y se asume una responsabilidad sobre el uso y las buenas prácticas en diferentes ambientes, como la tecnología móvil, cloud computing, aplicativos web y relacionados; en cada uno de los involucrados en los procesos de las compañías. Se debe dar la importancia necesaria a la Seguridad de la Información, tanto en esfuerzo humano como en presupuesto por parte de la alta gerencia. En este punto es cuando toma valor la implementación de campañas de sensibilización con relevancia social sobresaliente.

Para finalizar, el Trabajo de Investigación, presenta un escenario para los profesionales de las TIC y los estudiantes que motiva a profundizar más en el tema de la Seguridad de la Información, a nivel académico son las primeras piedras para el avance en este campo, para retomar esta iniciativa, especialmente

a la que tiene que ver con el Grupo de Investigación; se concluye que a pesar de los esfuerzos de limitar este tema, el campo de conocimiento es muy amplio y necesario entender, que requiere de un estudio a profundidad para cubrir todos los componentes involucrados para la Ciberdefensa a nivel empresarial.

9. RECOMENDACIONES

El profesional de la seguridad de la información no se debe limitar con las herramientas presentadas en este trabajo de investigación, se sugiere la búsqueda de técnicas y metodologías que complementen lo presentado anteriormente, esto en pro de motivar e incentivar el aprendizaje y el interés en este campo.

Se recomienda consultar no solo el Top. 5 de vulnerabilidades que más impacto generen, si no todos los fallos posibles, porque en realidad una vulnerabilidad representa una debilidad que puede ser trasformada en riesgo inmediatamente, día a día las bases de datos de ataques y vulnerabilidades se están actualizando evidenciando un crecimiento notable en los últimos años debido a la facilidad de acceso por parte del público en general a la tecnología, esto los hace objetivos y blancos fáciles para ser atacados.

A nivel gubernamental, se destacan las iniciativas en pro de la seguridad, sin embargo se sugiere que se publicite, informe y se realicen campañas que publiciten dichas iniciativas, que hagan participe a la comunidad en general en todos los niveles socio-económicos del país, se enteren del qué, el por qué y el para qué y así se convierta la Seguridad de la Información en política defensa nacional.

Para finalizar, se recomienda la capacitación y certificación de los profesionales de la seguridad y/o Administradores de sistemas en cuanto a lo mencionado en el trabajo de investigación, realizar procesos de aseguramiento y defensa a amenazas requiere un nivel de destreza y conocimiento bastante amplio.

10. BIBLIOGRAFÍA

PCI Security Standards Council. (12 de Enero de 2014). *Acerca del PCI Security Standards Council*. Obtenido de https://es.pcisecuritystandards.org/minisite/en/about.php

27001 Academy. (20 de Enero de 2013). *27001Academy*. Obtenido de http://www.iso27001standard.com/es/que-es-iso-27001/

Aguilera López, P. (2010). *Seguridad informática.* Madrid.

Almanza, A. (2014 de Junio de 2014). *ACIS: Revista Sistemas.* Recuperado el 8 de Octubre de 2014, de http://acis.org.co/revistasistemas/index.php/component/k2/item/164-tendencias-2014-encuesta-nacional-de-seguridad-inform%C3%A1tica

Álvarez Huerta, L. (30 de Mayo de 2014). *OpenWebinars.net*. Obtenido de https://openwebinars.net/openvas-en-linux-explorando-nuestros-sistemas/

Arias, R. (1 de Enero de 2013). *Seguro de Estar Seguro.* Obtenido de http://segurodeestarseguro.blogspot.com/2013/01/metodologias-de-hacking-etico_1.html

Balanta, H. (15 de Junio de 2014). *DerechoInformático.co*. Obtenido de http://derechoinformatico.co/legislacion-que-protege-la-informacion-en-colombia/

Benjumea, O. (10 de Noviembre de 2010). *¿Sabes diferenciar la ISO 27001 y la ISO 27002?: RedSeguridad.com*. Recuperado el 8 de Octubre de 2014, de http://www.redseguridad.com/opinion/articulos/sabes-diferenciar-la-iso-27001-y-la-iso-27002

Bloomberg Businessweek. (12 de Enero de 2014). *Company Overview of The MITRE Corporation*.

CERT SEI. (s.f.). *About Us: CERT*. Obtenido de http://www.cert.org/about/

CLAD. (1 de Junio de 2007). *Centro Latinoamericano de Administración para el Desarrollo.* Recuperado el 9 de Junio de 2014, de http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/cartagobelec.pdf

CRC, C. d. (23 de Diciembre de 2009). *Resolución 2258 de 2009.* Recuperado el 2014 de Octubre de 2014, de http://www.etb.com.co/guiadeconsulta/contratos/Resolucion_2258.pdf

DISA. (s.f.). *Our Work: DISA 101*. Obtenido de http://www.disa.mil/About/Our-Work

El Espectador. (17 de Mayo de 2014). *De Andrómeda a los 'hackers'*. Obtenido de http://www.elespectador.com/noticias/investigacion/de-andromeda-los-hackers-articulo-492933

Enter.CO. (05 de Febrero de 2014). *Buggly, la comunidad en la que el ejército camufló a sus hackers*. Obtenido de http://www.enter.co/chips-bits/seguridad/asi-es-la-presunta-fachada-de-la-central-de-hackeo-del-ejercito/

Gallardo, S. (2014). Más Allá de las TIC en MinDefensa. *Revista Sistemas*, 20-22.

González Pérez, P., Sánchez Garcés, G., & Soriano de la Cámara, J. M. (2013). *Pentesting con Kali.* Madrid: 0xWord.

González Pérez, P., Sánchez Garcés, G., & Soriano, J. M. (2013). *Pentesting con Kali.* Madrid: 0xWord.

Hernandez, A. (1 de Agosto de 2011). *InfoSecurity: InSeguridad de la Información en la Empresa Colombiana*. Recuperado el 7 de Octubre de 2014, de http://www.infosecurityvip.com/newsletter/estadisticas_ago11.html

ISACA. (s.f.). *Acerca de*. Obtenido de http://www.isaca.org/spanish/Pages/default.aspx

Lozano Vila, A. (14 de Febrero de 2008). *Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo.* Recuperado el 6 de Octubre de 2014, de https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fwww.sarlaft.com%2Fhtml%2FRESUMEM%2520NORMA%2520TECNICA%2520COLOMBIANA%2520NTC%252052541.doc&ei=52c5VOL8JrWCsQTmpICgBg&usg=AFQjCNHAWxS8LZh9QN8Q

Marcela Díaz Sandoval. (21 de Marzo de 2014). *El Espectador*. Obtenido de http://www.elespectador.com/tecnologia/colombia-lider-inseguridad-informatica-latina-articulo-482097

Martínez Rodríguez, J. C. (27 de Noviembre de 2014). *La desmitificación de los hacker*. Obtenido de http://www.elespectador.com/noticias/investigacion/los-hackers-contexto-articulo-530053

Mifsud, E. (Lunes de Marzo de 2012). *Datateca Universidad Nacional Abierta y a Distancia.* Obtenido de http://datateca.unad.edu.co/contenidos/233001/Material/Unidad%20I/Proteccion_seguridad_infomatica.pdf

MinTic. (Julio de 14 de 2011). *Ministerio TIC.* Obtenido de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

MinTIC. (1 de Diciembre de 2011). *MinTIC: Gobierno en Línea.* Recuperado el 8 de Octubre de 2014, de http://programa.gobiernoenlinea.gov.co/apc-aa-

files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

OWASP. (2014 de Noviembre de 2014). *Sobre OWASP*. Obtenido de https://www.owasp.org/index.php/Sobre_OWASP

OWASP, F. (2013). *OWASP Project Top 10 - 2013.*

Pacheco, F. (10 de Septiembre de 2013). *ESET: WeLiveSecurity.* Recuperado el 7 de Octubre de 2014, de http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

Pacheco, F., & Jara, H. (2012). *Ethical Hacking .* Buenos Aires: USERS.

Piraquive, F. N. (2008). Principales estándares para la seguridad de la información IT. *Revista EOS*, 77-109.

RAE. (1 de Septiembre de 2013). *Diccionario panhispánico de dudas*. Obtenido de http://lema.rae.es/dpd/srv/search?key=hacker

Red, H. e. (15 de Agosto de 2012). *Tipos de Hackers, Hackers en La Red*. Obtenido de https://hackersenlared.wordpress.com/2012/08/15/tipos-de-hackers/

SANS. (s.f.). *About Us: SANS*. Obtenido de http://www.sans.org/about/

Santos, P. J. (7 de Febrero de 2014). Agencia Nacional de Seguridad Cibernética. (R. Radio, Entrevistador)

Superfinanciera, C. (25 de Octubre de 2007). *Circular Externa 052 de 2007.* Recuperado el 25 de Octubre de 2014, de https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCEQFjAB&url=https%3A%2F%2Fwww.superfinanciera.gov.co%2Fdescargas%3Fcom%3Dinstitucional%26name%3DpubFile7553%26downloadname%3Dce05207.docx&ei=d4k-VK7HC_j8sAS924GgCA&usg

SYMANTEC CORP. (1 de Junio de 2014). Obtenido de Informe sobre las amenazas para la seguridad de los sitios web: 2014: https://www.symantec-wss.com/campaigns/15106/cala4/assets/symantec-wstr-2014-cala.pdf

SYMANTEC. (s.f.). *Glosario de Seguridad 101*. Obtenido de http://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

UNAD. (21 de Enero de 2014). *Universidad Nacional Abierta y a Distancia: Test de Penetración*. Obtenido de http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_26_test_de_penetracin.html

Witigo's Blog. (8 de Enero de 2014). *Witigo's Blog*. Obtenido de http://witigo.wordpress.com/seguridad/nessus/%C2%BFque-es-nessus/

11. ANEXOS

11.1. ANEXO No. 1 – LEGISLACIÓN COLOMBIANA

- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación
- **Ley 1032 de 2006:** Modifica el Código Penal en especial, sobre la prestación, acceso o uso ilegales de los servicios de telecomunicaciones y Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones
- **Ley 1266 de 2008:** Se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países
- **Ley 1273 de 2009:** Se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1581 de 2012:** Se dictan disposiciones generales para la protección de datos personales
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012 habeas data.
- **Ley 1712 de 2014:** Se crea la ley de transparencia y del derecho de acceso a la información pública nacional.
- **Conpes 3701 de 2011**

11.2. ANEXO No.2 – SEGURIDAD DE LA INFORMACIÓN EN LEGISLACIÓN

LEY / RESOLUCIÓN CIRCULAR	TEMA
Ley 527 de 1999 - COMERCIO ELECTRÓNICO	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
Ley 599 DE 2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea

	la Agencia Nacional del Espectro y se dictan otras disposiciones.
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

Ley 1581 de 2012	Se reglamentan aspectos relacionados con la autorización del Titular de la Información para el Tratamiento de Sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los titulares de información y las transferencias de datos personales.

11.3. ANEXO No.3 – PRINCIPIOS DE LA SEGURIDAD Y LA INFORMACIÓN: NORMATIVIDAD Y ESTÁNDARES

12. NORMATIVIDAD Y ESTÁNDARES

CONFIDENCIALIDAD	***ISO/IEC 27001***	A.11.2 Gestión del acceso de usuarios A.15.1 Cumplimiento de los requisitos legales A.11.3 Responsabilidades de los usuarios A.11.6 Control de acceso a las aplicaciones y a la información A.12.3 Controles criptográficos A.12.4 Seguridad de los archivos del sistema A.5.1 Política de seguridad de la información A.10.6 Gestión de la seguridad de las redes A.10.8 Intercambio de la información
	NTC 5254	3.2.2 Establecimiento del contexto externo 3.3 IDENTIFICACIÓN DE LOS RIESGOS 3.4.3 Consecuencias y posibilidad 3.6 TRATAMIENTO DE LOS RIESGOS
	RFC 2196	Política de Privacidad Política de Acceso Política de Autenticación Declaración de Disponibilidad Política de informes de incidentes o violaciones de seguridad
DISPONIBILIDAD	***ISO/IEC 27001***	A.10.10 Monitoreo A.11.2 Gestión del acceso de usuarios A.11.7 Computación móvil y trabajo remoto A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información A.10.9 Servicios de comercio electrónico A.10.5 Respaldo A.5.1 Política de seguridad de la información

		A.10.4 Protección contra códigos maliciosos y móviles A.12.6 Gestión de la vulnerabilidad técnica A.12.5 Seguridad en los procesos de desarrollo y soporte
	NTC 5254	3.2.2 Establecimiento del contexto externo 3.2.5 Desarrollo de los criterios del riesgo 3.3 IDENTIFICACIÓN DE LOS RIESGOS 3.4.2 Evaluación de los controles existentes 3.6 TRATAMIENTO DE LOS RIESGOS 3.7 MONITOREO Y REVISIÓN
	RFC 2196	Declaración de Disponibilidad
INTEGRIDAD	***ISO/IEC 27001***	A.12.3 Controles criptográficos A.10.5 Respaldo A.12.4 Seguridad de los archivos del sistema A.5.1 Política de seguridad de la información A.10.8 Intercambio de la información A.10.4 Protección contra códigos maliciosos y móviles
	NTC 5254	3.2.5 Desarrollo de los criterios del riesgo 3.3 IDENTIFICACIÓN DE LOS RIESGOS 3.4.3 Consecuencias y posibilidad 3.6 TRATAMIENTO DE LOS RIESGOS
	RFC 2196	Política de Responsabilidad
AUTENTICACIÓ	***ISO/IEC 27001***	A.11.2 Gestión del acceso de usuarios A.11.4 Control de acceso a las redes A.11.6 Control de acceso a las aplicaciones y a la información A.5.1 Política de seguridad de la información

	NTC 5254	3.3 IDENTIFICACIÓN DE LOS RIESGOS 3.6 TRATAMIENTO DE LOS RIESGOS
	RFC 2196	Política de Privacidad Política de Acceso Política de Responsabilidad Política de Autenticación

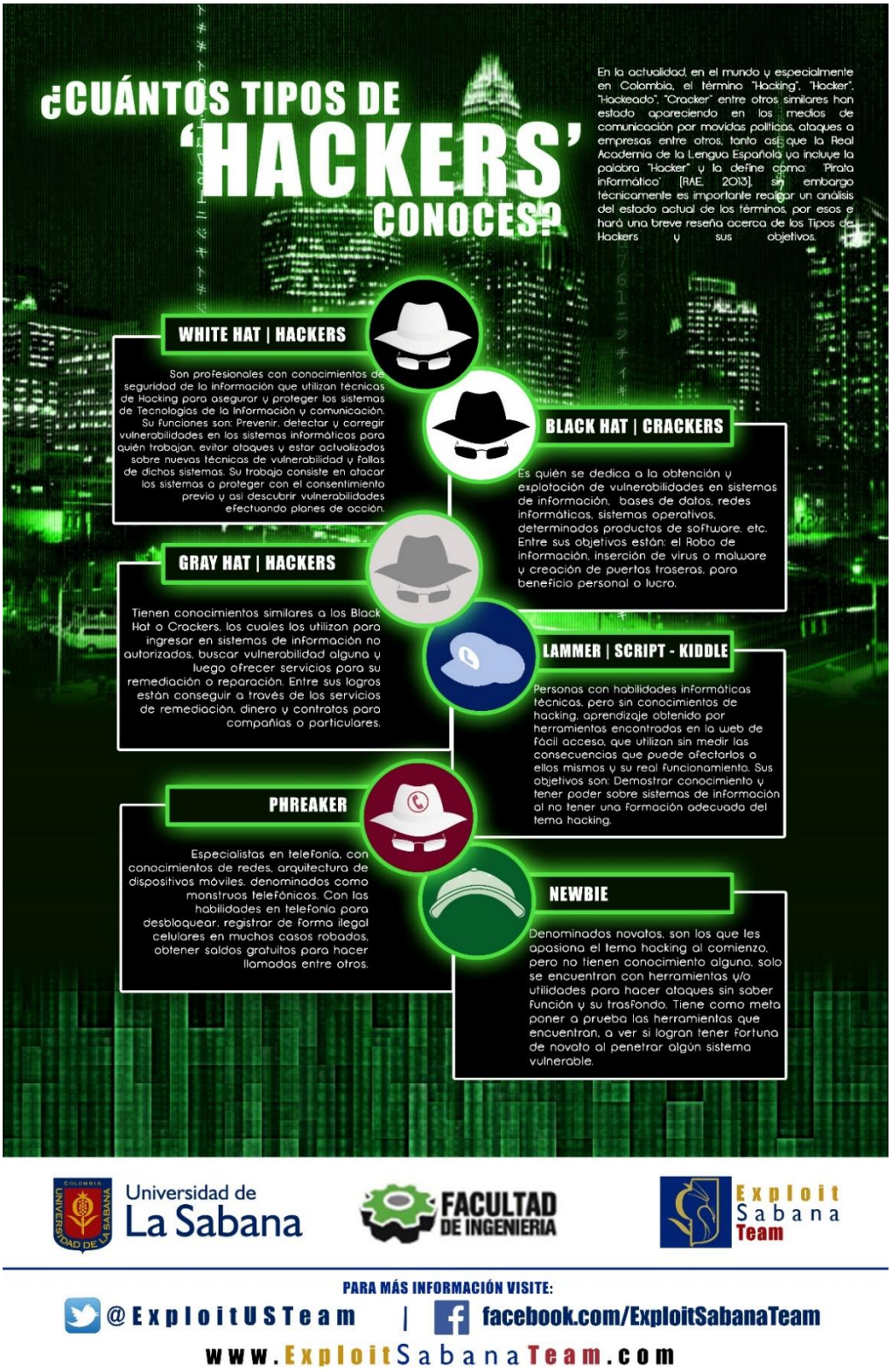
11.4. ANEXO No.4 – HERRAMIENTAS PENTESTING Y DESCRIPCIÓN

HERRAMIENTA	DESCRIPCIÓN
NetScan Tools « http://www.netscantools.com/ »	Conjunto de herramientas de internet en un solo paquete para plataformas Windows.
Nmap « http://nmap.org/»	Es un programa por consola de comandos que sirve para efectuar rastreo de puertos y se usa para evaluar la seguridad de sistemas informáticos. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013)
Ncat «http://nmap.org/ncat/»	Es la herramienta considerada como la evolución de Netcat, es un utilidad que permite leer y escribir datos a través de conexiones de red usando la pila de protocolos TCP/IP. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013)
Metasploit Framework « http://www.metasploit.com/ »	Provee información y herramientas útiles para pruebas de penetración, investigadores de seguridad y desarrolladores de IDS's .

Retina Network Security Scanner « http://www.beyondtrust.com/ »	Poderosa solución para la administración de vulnerabilidades diseñada para ayudar a las organizaciones de cualquier tamaño en la identificación, protección mitigación de Vulnerabilidades.
John The Ripper « *http://www.openwall.com/john/* »	Software para password cracking, actualmente disponible para varios sistemas Unix, Windows, DOS, BeOS y OpenVMS.
OpenVAS «http://www.openvas.org/»	OpenVAS es una herramienta diseñada para ayudar a los administradores de red/sistemas en la identificación de vulnerabilidades, detección de intrusiones y por tanto, amplio abanico en la prevención de ataques. (Álvarez Huerta, 2014)
Burp Suite «http://portswigger.net/burp/»	Es una herramienta escrita íntegramente en Java que permite realizar test de intrusión en aplicaciones web, permitiendo combinar técnicas manuales y automáticas para analizar, detectar, atacar y explotar aplicaciones web. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013)

Maltego «https://www.paterva.com/web6/»	Es una aplicación de minería y recolección de información utilizada durante la fase de Data Gathering, proceso en el cual se trata de obtener el mayor número de información posible sobre un objetivo para su posterior ataque. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013)
Nessus «http://www.tenable.com/»	Es un programa de escaneo de vulnerabilidades. Consiste en dos partes *nessusd*, el daemon Nessus, que es el encargado de realizar el escaneo en el sistema objetivo, y *nessus*, el cliente (basado en consola o gráfico) que muestra el avance y resultados de los escaneos. (Witigo's Blog, 2014)
Wireshark «https://www.wireshark.org/»	Es un analizador de paquetes que permite examinar datos de una red viva o de un archivo de captura salvado en disco. (González Pérez, Sánchez Garcés, & Soriano de la Cámara, Pentesting con Kali, 2013)

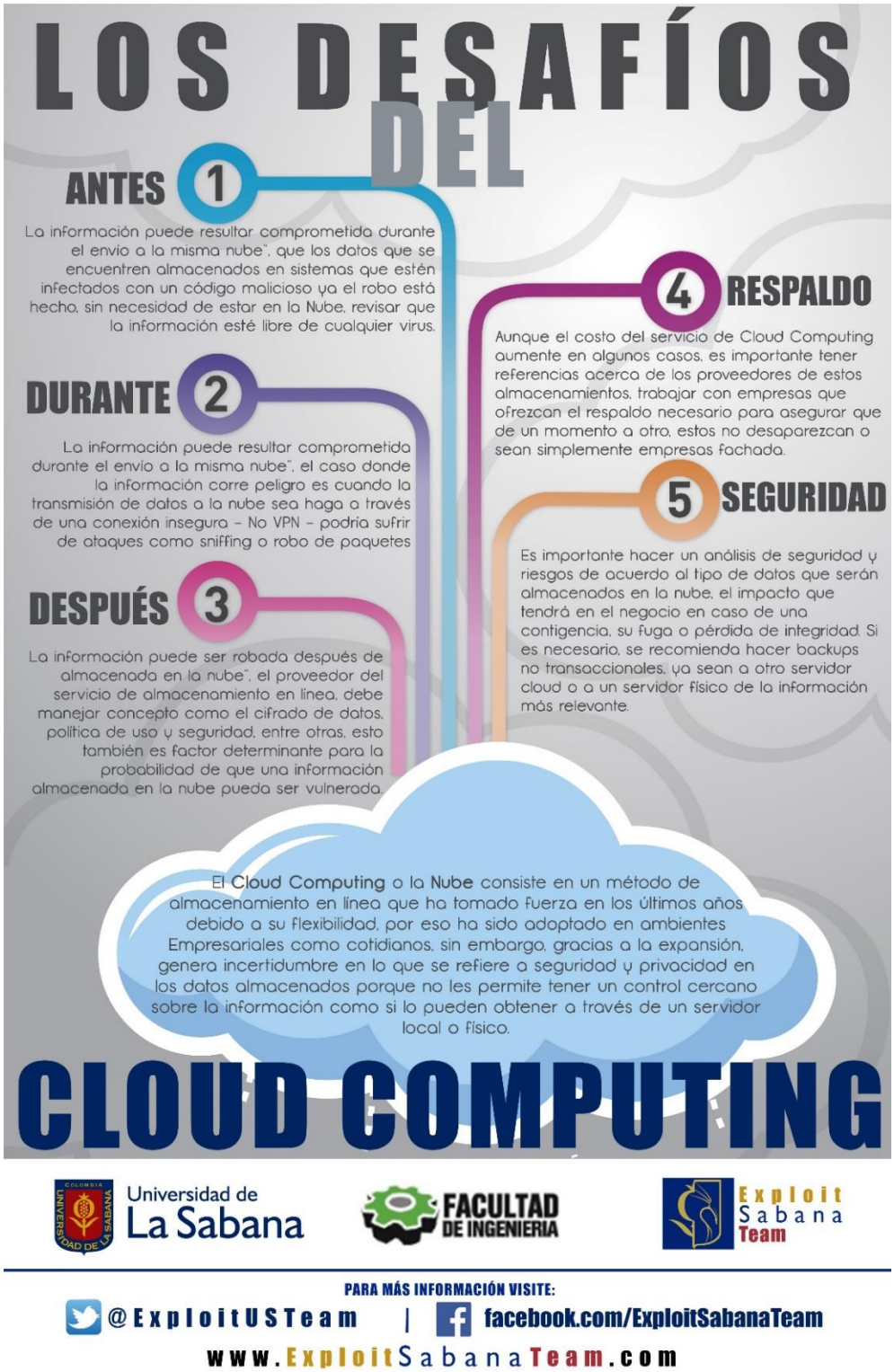
11.5. ANEXO 5 - ¿CUÁNTOS TIPOS DE 'HACKERS' CONOCES?



11.6. ANEXO 6 - ¡ALERTA PROFESIONALES DE LAS TIC! – TIPS: SEGURIDAD = TRANQUILIDAD

11.7. ANEXO 7 - SEGURIDAD MÓVIL: UN PASO DELANTE DE LOS DELINCUENTES

11.8. ANEXO 8 - LOS DESAFÍOS DEL CLOUD COMPUTING



11.9. ANEXO 9 – GUÍA METODOLÓGICA PARA EL TOP 5 DE ATAQUES MALICIOSOS – VAINLEEC-

(Hacer Clíc en la imagen para acceder a la guía)