Una nueva experiencia en seguridad hacking ético

Docente

Asesor Temático
Fernando Antonio Moreno Forero

Asesor Metodológico
Juan Manuel Silva Garcia

Estudiante

Jesús Hernán Vidal Londoño

Universidad San Buenaventura
Universidad Militar Nueva Granada
Especialización en Administración de la Seguridad
Santiago de cali
2016

Índice

Pág.

Listado de figuras

Pág.

Resumen

Las computadoras y todo dispositivo que use internet en todo el mundo son susceptibles de ser atacadas por crackers o hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones.

Es así que se han implementado una serie de medidas a nivel de seguridad informática para blindar todos aquellos dispositivos existentes en las grandes organizaciones. Una de esas medidas se ha ejecutado a través del Ethical Hacking, mediante el cual es posible detectar el nivel de seguridad interno y externo de los sistemas de información de una organización, esto se logra determinando el grado de acceso que tendría un atacante con intenciones maliciosas a los sistemas informáticos con información crítica. Mediante el uso de las técnicas utilizadas por los ciber delincuentes, se puede evaluar la efectividad de los controles de seguridad establecidos para proteger la información.

Una vez identificadas todas las brechas de inseguridad informática, los expertos en esta modalidad de seguridad han diseñado una serie de estrategias y métodos para blindarse ante un inminente ataque a sus diferentes sistemas informáticos, lográndose el compromiso de toda una organización para que su operación no se vea afectada o comprometida ante eventos inseguros.

Palabras clave: Hacking ético, delito informático, ciber crimen, seguridad informática, hackers, crackers.

Abstract

Computers and any device that uses Internet worldwide are susceptible to attack by hackers or crackers able to compromise computer systems and steal valuable, or delete a large part of her information. This situation makes it imperative to know whether these systems and data networks are protected from any intrusion.

Thus they have implemented a series of measures at the level of security to shield those devices in large organizations. One of these measures has been implemented through Ethical Hacking, through which it is possible to detect the level of internal and external systems of an organization's information security, this is achieved by determining the degree of access that would an attacker with malicious intent computer systems with critical information. Using the techniques used by cybercriminals, you can assess the effectiveness of the security controls in place to protect information.

Having identified any breaches of computer insecurity, experts in this type of security have designed a series of strategies and methods to shield against an imminent attack on different computer systems, achieving the commitment of an entire organization so that its operation is not affected or compromised to unsafe events.

Keywords: Ethical hacking, computer crime, cyber crime, computer security, hackers.

Introducción

Colombia es un país donde la seguridad en sus diversas formas ha empezado a tomar importancia y conciencia en las altas direcciones de las empresas públicas y privadas, pero la mayoría no le ha dado la importancia real a los Sistemas de Seguridad Informática.

En Colombia se ha generado un crecimiento agigantado de los medios informáticos, su ubicación y disposición brindan la facilitad a las empresas de que todos sus procesos interactúen al unísono, facilitando la organización de la información personal y empresarial, ocasionando que se abra una infinidad de posibilidades para que los delincuentes busquen formas de conseguir datos de vital importancia para los usuarios, como lo son el acceso a claves bancarias, correos electrónicos, información sensible personal y empresarial, debido en su mayoría a causa de la instalación de software maliciosos en los computadores, celulares o cualquier otro dispositivo.

A pesar de la existencia de departamentos de informática y TIC en las empresas, muy pocas han implementado medidas de Seguridad en los sistemas informáticos tendientes a blindarlas ante posibles y eventuales ataques informáticos por hackers especializados.

En la Gestión Integral de Riesgos y conforme a eventos que han ocurrido a nivel interno en las empresas, se han detectado una serie de brechas en la Seguridad de los sistemas informáticos. Es así como los expertos en Seguridad Informática generaron una metodología denominada Hacking Ético, con el fin de identificar aquellas vulnerabilidades y brechas que representen riesgos a la seguridad de los sistemas informáticos empresariales.

Todos estos antecedentes y sus consecuencias inmediatas, ha generado que los expertos en Seguridad Informática se pregunten si las empresas poseen las herramientas adecuadas y fiables que las blinden ante estos posibles eventos.

Como consecuencia de estos eventos inesperados y adversos, se genera la necesidad de identificar las herramientas en Seguridad Informáticas que ayudan a blindar a las empresas ante ataques cibernéticos, los cuales para su oportuno tratamiento en primera instancia y para

contextualizar a las empresas, se inicia por definir la terminología relacionada con la Seguridad Informática, se continua mostrando antecedentes reales sobre sobre la inseguridad informática a nivel nacional y en el Departamento del Valle del Cauca en especial en el sector industrial y se describen los métodos de Hacking Ético y Seguridad en los sistemas informáticos usados en las empresas del Sector Industrial del Departamento del Valle

Todo esto redunda en la identificación de métodos y estrategias que blinden a las empresas ante ataques cibernéticos, procurando evitar, neutralizar o mitigar estos posibles eventos.

1. Una nueva experiencia en seguridad hacking ético[*]

Situación actual de Colombia ante la seguridad informática

En la actualidad Colombia ha ocupado en puesto muy crítico en lo relacionado a las vulnerabilidades detectadas y encontradas en sus plataformas informáticas, la mayoría de las empresas colombianas han sido y están expuestas a una gran cantidad de amenazas que vulneran la seguridad de sus sistemas informáticos, se genera una incertidumbre de cuan seguras pueden estar sus plataformas, redes informáticas, es ahí donde se le empieza a dar importancia y a mantener la seguridad de los sistemas informáticos, ya que si se vulnera su seguridad traerá como consecuencias ataques informáticos que pueden poner en riesgo la integridad de su información, imagen y bienes de la empresa u organización.

Es de vital importancia que las empresas u organizaciones opten por implementar medidas que contrarresten cualquier ataque a sus sistemas informáticos, tomen las medidas de seguridad pertinentes a fin de dar continuidad a sus negocio, que no se vean afectadas por manos y mentes criminales, dañinas, donde su fin en unos casos puede ser causar daño y estragos colocando a la empresa en un estado crítico o donde otros solo quieren causar un impacto social, pero que a la mirada de otros como personas, empresas, organizaciones, el mismo gobierno, puede generar un impacto negativo en contra de la organización así no haya sido su intensión que se ocasionara o en su defecto si existía una responsabilidad por no haber acatado sugerencias o implementado medidas de seguridad y control a fin de evitar ataques a sus sistemas informáticos.

Los ataques informáticos siempre generarán traumatismos a la información sensible de cada organización, puesto que puede verse afectada en su integridad, modificada inadecuadamente, convertirse en pública, teniéndose en cuenta que puede ser información privilegiada tanto de la organización como de sus clientes, proveedores, contratistas, personas en misión, cooperados, etc., que al dejarse expuesta puede originar brechas más profundas en la organización que serán aprovechas por los ciberdelincuentes.

[*] Para la elaboración del ensayo se tomó como referencia la asignatura Sensibilización en Informática.

En Colombia se ha generado un crecimiento agigantado de los medios informáticos, su ubicación y disposición brindan la facilitad a las empresas de que todos sus procesos interactúen al unísono, facilitando la organización de la información personal y empresarial, ocasionando que se abra una infinidad de posibilidades para que los delincuentes busquen formas de conseguir datos de vital importancia para los usuarios, como lo son el acceso a claves bancarias, correos electrónicos, información sensible personal y empresarial, debido en su mayoría a causa de la instalación de software maliciosos en los computadores, celulares o cualquier otro dispositivo.

Diferentes medios de comunicación manifiestan la vulnerabilidad de los sistemas informáticos de las empresas, mostrando en una forma real las consecuencias que estos presentan a las organizaciones.

> Los riesgos y amenazas a la seguridad informática de las empresas son evidentes. Solo en Colombia, el año pasado el Departamento de Delitos Informáticos de la Policía Nacional recibió 7118 denuncias por parte de víctimas de delitos informáticos, evidenciando un aumento del 40% con respecto al 2014. Las pérdidas económicas derivadas por estos actos representan al país alrededor del 0,14%, según el Banco Mundial (2014) del PIB Nacional, es decir, cerca de US$500 millones aproximadamente. (Manrique Horta. 2016. Diariamente en Colombia hay 10 millones de ataques informáticos. Diario del Huila).

Es evidente que Colombia y sus empresas han dejado al descubierto una infinidad de brechas de seguridad informática, las cuales son aprovechadas por los ciberdelincuentes.

Como consecuencia de todos estos antecedentes, las empresas colombianas han implementado mecanismos para protegerse de posibles ataques que afecten su integridad, su estabilidad económica y social, siendo conscientes de que están frente a una globalización tecnológica donde su información privada y sensible puede ser hurtada y dársele un mal manejo por posibles delincuentes informáticos que se encuentran diariamente en el mundo cibernético.

Actualmente el ciberdelincuente para obtener información personal o financiera de las personas cuenta con herramientas para acceder a todo el historial de su víctima, dentro de estas se encuentra el software malicioso malware, el cual por sus características informáticas puede estar oculto en un archivo adjunto de un correo electrónico, el cual una vez abierto empiezan a ejecutar una serie de funciones programadas en el sistema operativo de este software y en muchas ocasiones se vuelve casi invisible para el antivirus de la empresa. Este es uno de los tantos métodos que puede utilizar el ciberdelincuente para acceder a la información de la empresa o de las personas que allí laboran. De esto se hablará más adelante una vez se relacionen algunos métodos usados por los ciberdelincuentes.

Es un hecho que Colombia se ha ganado un puesto privilegiado, primero por ser un país donde se presentan a diaria un sinfín de ataques ciberdelincuentes a empresas nacionales pero también como el primer o segundo país del Latinoamérica que más ataques cibernéticos ocasionan a otros países.

EL Periódico el Espectador, Sección de Tecnología, redacta un informe dando a conocer lo siguiente

> Colombia lidera lista de ataques informáticos en países de habla hispana. Cuatro de los cinco ataques más comunes son realizados por Colombia. En el informe anual realizado por Digiware, primer integrador de seguridad informática de Latinoamérica, se reveló que Colombia es el país de habla hispana que genera más ataques informáticos en Latinoamérica, luego siguen Argentina, Perú, México y Chile. (Colombia lidera lista de ataques informáticos. 2014. Periódico el Espectador).

Son varios los antecedentes que enlutan a nuestro país ocasionados por delitos informáticos, es así que se muestra otra noticia, donde evidencia estos hechos

> En Colombia las cifras de delitos informáticos van en aumento. Colombia es actualmente el tercer país en Latinoamérica donde más se cometen. Se calcula que 187 denuncias mensuales son interpuestas por fraude a

> diferentes bancos. Así lo reveló en los últimos días el Colegio Colombiano de Juristas, que explicó que la lista de esta modalidad de delito la encabezan Brasil y México. Algunos de los delitos electrónicos que más se presentan en el país y que, según expertos de la Fiscalía, van en aumento son acceder a bases de datos de bancos u otras entidades sin permiso, sustraer archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas bancarias. (En Colombia las cifras de delitos informáticos van en aumento. 2102. El País).

2. Normatividad vigente en seguridad informática

Colombia en el ámbito de la seguridad informática ha dejado entrever que es muy vulnerable ante los ataques de la delincuencia informática, las brechas identificadas son ocasionadas por descuido, impericia, negligencia y falta de una cultura de seguridad informática, no se han establecido unos protocolos de seguridad eficaces y eficientes que de verdad lleven a muchas empresas colombianas a blindarse ante los ataques por parte de los delincuentes informáticas y/o a cómo enfrentar estas situaciones.

A pesar de existir una norma técnica colombiana como es la NTC-ISO/IEC 27001 Tecnología de la información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI) y una ley como la 1273 de 2009 Ley de Delitos Informáticos en Colombia, se sigue evidenciando que a pesar de tener a la mano todas estas ayudas y herramientas legales, no invierten ni se concientizan de la necesidad de hacer uso de ellas. Se demuestra que las empresas son reactivas más no preventivas ante todas estas situaciones que afectan la seguridad, integridad de sus activos intangibles como es la información sensible. Son muchas las empresas y gobiernos que han caído por no tomar acciones preventivas que lleven a blindar y contrarrestar acciones negativas que van en detrimento de la estabilidad y bienes de la empresa y sus asociados de negocio, no sin dejar de mencionar que el principal afectado es la persona como tal, el ser humano que está al frente y es el soporte y piedra angular de ese conglomerado empresarial.

El Gobierno Colombiano con el fin de ejercer control en el sector de las tecnologías de información y Comunicaciones ha emanado una serie de normas legales de estricto cumplimiento, de las cuales se nombraran algunas de relevancia e importancia a nivel empresarial y personal.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del 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". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. (Ley 1273. 2009. De la protección de la información y de los datos. Ministerio del interior y de justicia. República de Colombia. Gobierno Nacional. Bogota.)

El 30 de julio de 2009 el entonces Presidente Alvaro Uribe Velez decretó la ley 1341 la cual le garantiza a Colombia un marco normativo por el cual se modifica el código penal, se crea un nuevo régimen 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

> Artículo 1°. Objeto. La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes

> del territorio nacional a la Sociedad de la Información.(Ley 1341. 2009. Políticas públicas que regirán el sector de las tecnologías de la información y las comunicaciones. Ministerio del Interior y de Justicia. República de Colombia. Gobierno Nacional. Bogotá).

En el año 2012 el Gobierno Nacional Decreto la Ley Estatutaria 1581 del 17 de octubre de 2012 por la cual se dictan disposiciones generales para la protección de datos personales Habeas Data en Colombia

Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Ley Estatutaria 1581. 2012. Protección de datos personales Habeas Data en Colombia. República de Colombia. Gobierno Nacional. Bogotá.).

El Gobierno Nacional el día 11 de abril de 2016 a través del Consejo Nacional de Política Económica y Social aprobó la nueva política de Seguridad Digital CONPES 3854 de 2016 que reemplaza al 3701 del 2011, en el cual se establece una política de seguridad y defensa contra posibles ataques digitales a las entidades del Estado, convirtiendo a Colombia en el primer país de Latinoamérica y uno de los primeros en el mundo, en incorporar plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos “OCDE”. (CONPES 3854. 2016. Política Nacional de Seguridad Digital. Departamento Nacional de Planeación. República de Colombia. Bogotá).

En esta política se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

El CONPES 3854 de 2016 de Seguridad Digital integra los objetivos de defensa del país en relación con la lucha contra el crimen y la delincuencia en Internet, para lo cual se centra en la

implementación de cinco frentes de acción específicos, los cuales se mencionan a continuación, así:

- Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

3. Vulnerabilidad de los sistemas informáticos en las empresas del sector industrial del Departamento del Valle.

El Departamento del Valle ha sido catalogado como uno de los más chocados y atacados por los ciberdelincuentes, no se aleja mucho de la realidad que es debido igual que muchos otros a la falta de blindajes adecuados ante este accionar delincuencial, es así como ya son muchas las evidencias existentes, el periódico el país a través de su departamento judicial nos muestra a través de un artículo esta situación

> Valle del Cauca, el departamento más golpeado por los delitos informáticos. En lo corrido de este año se han presentado en el Valle del Cauca 1700 denuncias por delitos informáticos, cifra que convirtió a este departamento en el más golpeado del país por esta modalidad delictiva. Juan Carlos Valencia González, jefe de la Unidad de Delitos Informáticos del CTI en el Valle, dice que la lucha para contrarrestar estos delitos no ha

> sido nada fácil. Sin embargo, hay otro tipo de conductas delincuenciales que, aunque no atacan el bolsillo, sí hacen mucho daño a las personas: la violación a sus cuentas de correo o de redes sociales. La Ley 1273 de 2009, que regula la protección de la información y los datos, trabaja para conseguir penas de entre cuatro y ocho años de cárcel para quienes cometan delitos informáticos, conducta que va unida al concierto para delinquir, ya que nunca una persona actúa sola. (Valle del Cauca, el departamento más golpeado por los delitos informáticos. 2013. El País).

En todas las empresas Vallecaucanas en especial la Industrial se crean situaciones de inseguridad informática, frente a esta nueva modalidad delincuencial dado que un gran número de personas usan cuentas o correos electrónicos para administrar cuentas bancarias y ejercer transacciones electrónicas por intermedio de tarjetas de crédito o débito, por esta razón la digitalización de la información, su practicidad es cada vez mayor, como la comodidad que se genera en el usuario para realizar cualquier tipo de actividad bien sea laboral, comercial, financiera, pero en algunas ocasiones se han desatado problemáticas de vulnerabilidad, debido al interés de muchas personas en encontrar en este medio tecnológico una forma ilícita de incrementar su patrimonio o encontrar algún provecho para sí u otros, bien sea de cualquier carácter. Se convierte para el Estado en una tarea de control, una conducta que afecta a las empresas y organizaciones en general.

Toda esta información y sus muchos antecedentes de empresas que han sido atacadas por ciberdelincuentes, nos muestra cuan vulnerables y expuestos están los sistemas informáticos en las empresas vallecaucanas, a pesar de la existencia de los departamentos de TICS y de especialistas en informática. Se siguen presentando novedades desde muy menores hasta muy críticas a nivel interno en las empresas, y lo peor y más inconcebible es que no se denuncian estos hechos ante las autoridades por el solo hecho de no ver su nombre enlodado o menoscabada su imagen ante usuarios, clientes, contratistas, etc., esto lo demuestra la siguiente noticia del Periódico El País

> Delitos informáticos se han incrementado un 100% en Cali. La Ley 1273 de 2009 sobre delitos informáticos y la protección de la información y de

> los datos, establece penas de entre 6 y 14 años de prisión por hurto por medios informáticos y semejantes. Un investigador del CTI asegura que, comparando las cifras del año anterior, en Cali y el resto del Valle del Cauca los delitos informáticos se han incrementado en un 100%. El más reciente modus operandi funciona a través de correos electrónicos que envían supuestamente personas conocidas. En realidad lo que hacen los hackers es sustraer la información de los contactos de correo de su víctima a través de un mail o aplicación maliciosa que se activa con darle clic. (Delitos informáticos se han incrementado un 100% en Cali. 2015. El País).

Todas estas vulnerabilidades en los sistemas informáticos en las empresas han ocasionado grandes pérdidas millonarias en dinero e información sensible, y algo en lo que muchos no había imaginado que sucedería y es en el secuestro de la información sensible personal y empresarial.

Como se dijo anteriormente en Colombia y en especial en el Departamento del Valle uno de los grandes problemas que existen y por los cuales las autoridades no han podido desarrollar y aplicar la ley en la forma debida es por consecuencia de la "NO" denuncia de este tipo de hechos o delitos, a pesar de existir una norma que los tipifica como delitos. Todo se ha convertido en un panorama, en un día a día, que si no se toman las medidas necesarias para controlar y prevenir, se convertirá en un gran monstruo difícil de controlar. Veamos este antecedente que saca el periódico EL Tiempo.

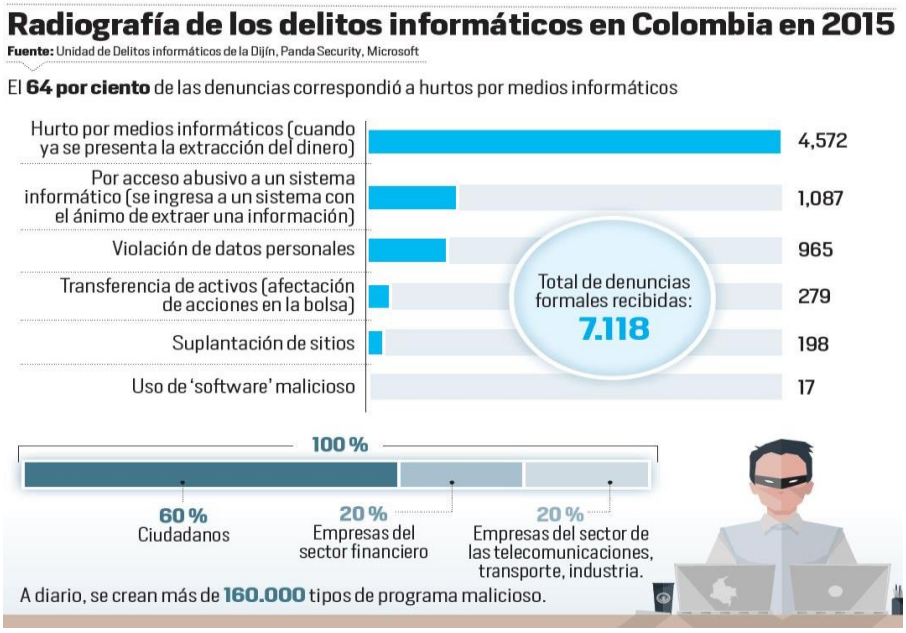
> En el 2015, la Unidad de Delitos informáticos de la Policía recibió más de 7.118 denuncias. La mayoría de los delitos informáticos denunciados en Colombia se relacionan con hurto. El cibercrímen representa el 15 por ciento de los ilícitos cometidos a empresas en Colombia y generó un daño económico cercano a 600 millones de dólares en el último año, reveló Intel Security. Uno de los puntos débiles de las compañías es el bajo presupuesto que destinan a seguridad informática. Es imperativo que las compañías implementen un modelo estructural que incluya las áreas de

seguridad como parte del equipo gerencial de la empresa. Uno de los principales focos de los cibercriminales son los altos ejecutivos, debido a que manejan información privilegiada. (En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. 2016. El Tiempo).

4. Radiografía de los delitos informáticos en Colombia

Diferentes medios de comunicación escrita, en este caso el Periódico El Tiempo, muestra una radiografía de los delitos informáticos en Colombia en el año 2015, donde a través de unidades especializadas como la del Grupo DIJIN de la Policía Nacional, suministran información real sobre las condiciones y situación actual por la que pasa el país frente a los delitos informáticos. (Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Radiografía de los delitos informáticos en Colombia en 2015. El Tiempo).

Figura No. 1: Radiografía de los delitos informáticos en Colombia en 2015.



Fuente: Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Fuente. El Tiempo. Recuperada de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

Este estudio nos muestra en forma real de cómo el hurto por medios informáticos se ha convertido en una de los delitos más comunes en Colombia. El 64% de las denuncias generadas ante autoridades judiciales soportan el actuar del ciudadano colombiano en pro de tratar de controlar este flagelo y como las personas y empresas están dejando de lado el temor a denunciar, esto no teniendo en cuenta la gran cantidad de personas y empresas que no lo hacen.

La vulnerabilidad de que son objeto los sistemas informáticos en las empresas y a nivel personal, dejar entrever las brechas en seguridad informática, carencia de medidas y protocolos de seguridad que le hacen fácil al ciberdelincuente actuar sin temor.

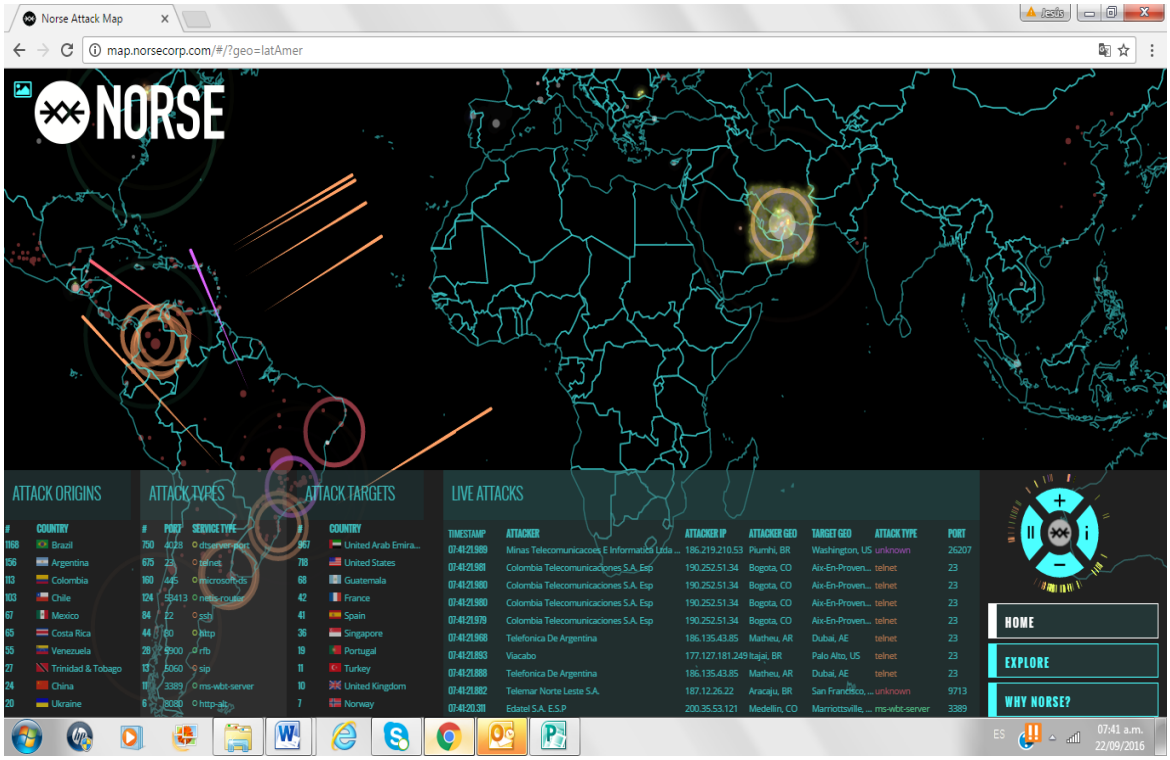
Es así como se muestra y evidencia otras formas de cómo los ciberdelincuentes acceden a los sistemas informáticos en las empresas. Estas son: Acceso abusivo a un sistema informático, violación de datos personales, transferencia de activos, suplantación de sitios, uso de software malicioso.

5. Prueba de Ciberataques Herramienta map.norsecorp.com

Con todos estos antecedentes sobre delitos informáticos, se hace una demostración de cómo los ciberdelincuentes colombianos han evolucionado en la forma de cómo lanzan sus ataques a otros continentes, ya no es por demostrar sus conocimientos y aplicarlos sin ocasionar mucho daño, ahora ven esto como un gran negocio que genera un gran lucro ya sea económico o como algo personal, es así como grandes organizaciones delincuenciales contratan a estos expertos para sacar provecho ilícito de estas acciones, donde los objetivos son las grandes transnacionales, las grandes organizaciones a nivel mundial.

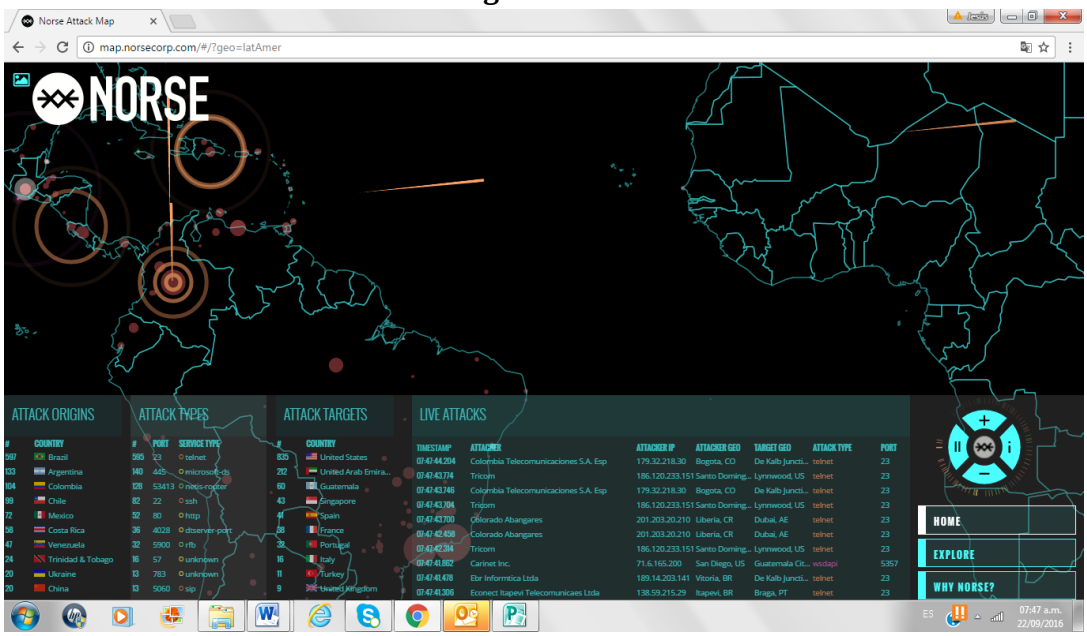
Vamos a realizar unas pruebas con la aplicación *map.norsecorp.com*, donde se detalla como Colombia se ha posicionado en un segundo y tercer lugar como uno de los países que más ataques cibernéticos ocasionan a otros países, así:

Figura No. 2. Ataque cibernético de Colombia a otros países. Día 22 de septiembre de 2016. 07:41 horas. Tercer puesto.



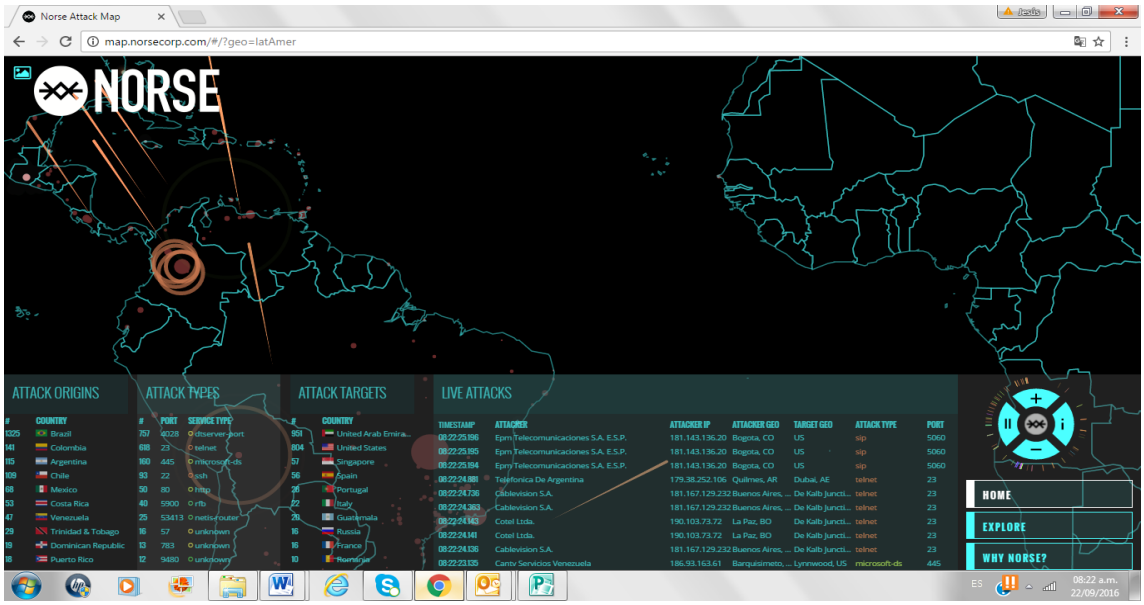
Fuente: Ataque cibernético de Colombia a otros países. Recuperada de http://map.norsecorp.com/#/?geo=latAmer.

Figura No. 3. Ataques de Colombia hacia otras naciones. Septiembre 22 de 2016 07:47 horas. Tercer lugar.



Fuente: Ataques de Colombia hacia otras naciones. Recuperado de http://map.norsecorp.com/#/?geo=latAmer.

Figura No. 4. Ataques de Colombia hacia otras naciones. Septiembre 22 de 2016 08:22 horas. Segundo lugar.



Fuente: Ataques de Colombia hacia otras naciones. Recuperado de http://map.norsecorp.com/#/?geo=latAmer.

En las gráficas 1, 2, 3 y 4 observamos como Colombia ocupa el segundo y tercer puesto a nivel latinoamericano como uno de los países que más ciberataques ocasionan a otros países. Así como Colombia ataca a otros países, igual Colombia es el blanco predilecto de muchos otros países del mundo, más debido a las vulnerabilidades que presentan sus sistemas informáticos.

6. Factores de riesgos en seguridad informática

Como se había mencionado anteriormente, debido a las falencias en medidas de seguridad y protocolos de seguridad de las que carecen muchas empresas del sector industrial del Departamento del Valle, se han identificado algunos factores de riesgos, los cuales mencionaremos a continuación:

Estos factores que se mencionan a continuación fueron identificados por la firma KPMG Advisory Services Ltda. Forensic Services. Encuesta de Fraudes en Colombia 2013.

1. Piratería: Este tipo de cibercrímen está relacionado con las reproducciones, utilización y distribución no autorizada de propiedad intelectual. En las empresas del Valle del Cauca la mayoría del software utilizado no poseen las licencias, son software no autorizado y se puede con esto presentar brechas de seguridad a nivel empresarial y personal.

2. Acceso no autorizado: Este hecho está relacionado con el acceso abusivo o no autorizado a un sistema informático. Esta brecha se presenta en las empresas al no existir protocolos de seguridad informáticos, al no tenerse políticas de controles de acceso con usuarios y pastword debidamente autorizados.

De igual forma se presenta este hecho al existir apoderamiento de la identidad de las personas de laboran en la empresa y que manejan información sensible, al presentarse esta suplantación puede presentarse acceso a la información sensible de la empresa y por ende apoderamiento por parte del ciberdelincuente haciendo uso indebido de esta.

Otra forma es la plantación de software malicioso en los equipos de las empresas en forma presencial por no existir controles y protocolos de seguridad de acceso de personas no autorizadas a ciertos oficinas o dependencias de la empresa o por no existir políticas de seguridad en las empresas al ingresas a paginas no seguros y de igual forma cuando se abren correos de procedencia insegura.

3. Vandalismo: Esta situación corresponde a todos aquellos actos inseguros ocasionados por personas maliciosas, malintencionadas o delincuentes informáticos, cuyo fin es el de causar destrucción de la información, apoderamiento o secuestro de información sensible, todo ocasionado a través de software maliciosos. Este hecho al igual que los otros se presentan por incumplimiento o a la no existencia de políticas y protocolos de seguridad informática. (Cortes Ignacio, Del Castillo Arturo. 2013. Cibercrímen. Encuesta de fraude en Colombia 2013. KPMG Forensic Services. KPMG en Colombia. Pp 33).

Con base en la información anterior se ha evidenciado que son varias las causas que los ocasionan, que a la mirada de muchos empresarios no se les ha dado la importancia del caso,

además por carecer de protocolos y políticas en seguridad informáticas. Algunas de esas causas evidenciadas por la Firma KPMG Advisory Services Ltda. Forensic Services. Encuesta de Fraudes en Colombia 2013, son:

1. Deslealtad de los empleados: Al no existir controles de seguridad informática que blinden sus sistemas de accesos no autorizados, puede ocurrir que el empleado objeto de llamados de atención o motivado por intereses propis o actuando bajo las ordenes de organizaciones criminales, se apropie de información sensible de la empresa o implante software maliciosos que originen la apropiación de información sensible de la empresa.

2. Fallas en la seguridad de tecnología: Son situaciones ocasionadas por personal interno o externo, por la no aplicación de controles de acceso o protocolos que no permitan el acceso a estos sistemas por personas no autorizadas. En muchos departamentos de TICS existen políticas de seguridad de acceso a sistemas por personal interno o externo, pero en muchos no cumplen con los protocolos de seguridad, dejando vulnerables estos sistemas.

3. Robo de dispositivos: A la falta de protocolos de seguridad a nivel interno de las empresas, donde se indiquen procedimientos de seguridad a cumplir con los dispositivos móviles de personal con cargos críticos dentro de la empresa, ha ocasionado que se produzcan robo de estos o se substraigan por unos cortos tiempos, con el fin de substraer información sensible o vital que hay dentro de estos.

4. Inadecuada disposición del activo: Muchas empresas han establecido o no protocolos de seguridad relacionados con la adecuada ubicación de los activos de la empresa, en este caso se refieren a computadores de escritorio, computadores portátiles, tabletas, los cuales poseen información vital de la empresa. Al no existir una adecuada disposición de estos activos, se convierten en un blanco fácil para el delincuente, que solo quiere es apoderarse y substraer información sensible de estos.

5. Fallas en la seguridad física: Muchas empresas no poseen espacios adecuados y seguros para resguardar los equipos o dispositivos informáticos, convirtiéndose en un objeto fácil de substraer por no existir barreras que impidan el acceso de personas no autorizadas.

4. Fallas en la seguridad de terceros: Muchas dispositivos o medios informáticos son dados a terceros para su administración o protección, pero a la falta de medidas de seguridad pueden ser sustraídos por delincuentes o personas mal intencionadas. (Cortes Ignacio, Del Castillo Arturo. 2013. Cibercrímen. Encuesta de fraude en Colombia 2013. KPMG Forensic Services. KPMG en Colombia. Pp 33).

Son muchos los factores identificados que ocasionan las brechas de inseguridad informática en las empresas, pero también son muchas las consecuencias que se han generado a nivel empresarias, mencionaremos algunos de estas consecuencias identificadas por la firma KPMG Advisory Services Ltda. Forensic Services. Encuesta de Fraudes en Colombia 2013, así:

- Daño Económico.
- Perdida de información sensible de la compañía.
- Extorsión/chantaje.
- Daño a imagen corporativa.
- Piratería de activos de la compañía.
- Demandas judiciales, laborales o comerciales.
- Multas y sanciones. (Cortes Ignacio, Del Castillo Arturo. 2013. Cibercrímen. Encuesta de fraude en Colombia 2013. KPMG Forensic Services. KPMG en Colombia. Pp 33).

7. Hacking & Ética

Antes de hacer la relación entre hacking y Ética, vamos a definir lo que es un Hacker y que la Etica.

Según Wikipea el término hacker tiene diferentes significados: Según el diccionario de los hackers, es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información al alcance de todos constituye un extraordinario bien. De acuerdo a Eric Raymond el motivo principal que tienen estas personas para crear software en su tiempo libre, y después distribuirlos de manera gratuita, es el de ser reconocidos por sus iguales. El término hacker nace en la segunda mitad del siglo

XX y su origen está ligado con los clubes y laboratorios del MIT. (https://es.wikipedia.org/wiki/Hacker).

De igual forma Wikipedia manifiesta que el término Ética proviene de la palabra griega ethos, que originariamente significaba "morada", "lugar donde se vive" y que terminó por señalar el "carácter" o el "modo de ser" peculiar y adquirido de alguien; la costumbre (mos-moris: la moral). La ética tiene una íntima relación con la moral, tanto que incluso ambos ámbitos se confunden con bastante frecuencia. La Ética son el conjunto de normas que vienen del interior y la Moral las normas que vienen del exterior; es decir, de la sociedad.

La evolución de los sistemas informáticos y la necesidad de las grandes empresas en blindarse contra ataques de ciberdelincuentes, obligaron en que se contratarán una serie de personas con habilidades poco comunes como eran las de vulnerar cualquier sistema informático y a través de esta forma poder identificar todas aquellas brechas que generaran impactos nefastos para estas.

Todo esto ocasionó que se generara un marco diferenciador entre los Hacker buenos o sea aquellos que vulneraban un sistema informático de una empresa con permiso expreso de sus propietarios bajo parámetros de seguridad, confidencialidad y ética y otro los hacker malos o crackers que vulneraban los sistemas informáticos de las empresas buscando un provecho para sí mismo o para terceros.

El Hacking Ético hace la diferencia entre los bueno y lo malo, siempre va por el camino de la rectitud, lo positivo y lo bueno. Su filosofía y actuar es buscar brechas inseguras que coloquen en riesgo la estabilidad de una empresa, siempre bajo parámetros seguros que no atenten contra la integridad física y moral de la empresa y sus representantes.

El Hacker Ético es aquella persona que coloca por delante sus principios éticos y normas morales positivas, todo redunda en buscar el bien sin ocasionar el mal o malestar a quien presta sus servicios o en su defecto si es para perfeccionar sus conocimiento en esta gran mundo de la informática

EL Hacker Etico es quien aplica sus conocimientos con fines defensivos y legales, guiándose siempre bajo los principios de esenciales de seguridad de las tecnologías de la información: confidencialidad, autenticidad, integridad y disponibilidad.

8. Hacking Ético en las empresas del sector industrial del departamento del valle

Con ocasión a todas estas situaciones que menoscaban la integridad de la empresa, dejando al descubierto situaciones y brechas en la seguridad informática, se empieza a darle importancia a la forma como deben de blindarse ante los ataques inminentes de los ciberdelincuentes, es así como se empieza a darle uso a metodologías aplicadas por expertos en estos temas y aparece el especialista en Hacking Ético, para lo cual se hará una explicación de la labor que realiza esta personas.

Cabe mencionar unos conceptos que son dados por expertos en seguridad informática sobre lo que se denomina Hacking Ético, es así como se menciona lo siguiente

> La palabra hacker se encuentra en boca de todos. Existen diferentes puntos de vista en cuanto a su función en la sociedad. Existen varios tipos de hackers diferenciados por sus intenciones y métodos. Por esta razón se hace tan extensa su clasificación, que, en muchas ocasiones, va más allá del umbral entre el bien y el mal. Sin embargo, los más reconocidos se agrupan en dos categorías: ‘white hat’ hackers y ‘black hat’ hackers.
>
> La denominación ‘white hat’ hackers (hackers de sombrero blanco, o hackers éticos) proviene de la identificación de los héroes de las antiguas películas del viejo oeste, en donde quienes pertenecían al bando de los buenos utilizaban sombreros de este color, diferenciándose así de los villanos quienes utilizaban la prenda en color negro. Estos héroes del ciberespacio se encargan de penetrar la seguridad de las empresas para encontrar vulnerabilidades y así lograr prevenirlas. Por lo general, se desempeñan como consultores de seguridad y trabajan para alguna compañía en el área de seguridad informática.

> En contraposición se encuentran los ‘black hat’ hackers o hackers de sombrero negro quienes constantemente andan buscando la manera de romper la seguridad tanto de empresas como individuos con el fin de sacar provecho económico, político o estratégico de la información que obtienen. (El hacking ético y su importancia para las empresas. 2014. Enter.Co).

En este medio del Hacking Ético es común escuchar sobre el Hacker de Sombrero Blanco o Caja Blanca o Hacker de Sombrero Negro o Caja Negra, que no es más que la forma legal o ilegal de cómo se obtiene información de un sistema informático o como se violenta su seguridad, con o sin autorización de los propietarios. En este caso los dueños de empresas pequeñas, medianas y grandes, por los antecedentes anteriormente mencionados y que se han visto afectados por ataques de ciber delincuentes, han optado por contratar los servicios de personas expertas en hackear sistemas informáticos (Hacker Ético), con el fin de determinar qué tan vulnerables y expuestos se encuentran sus sistemas informáticos ante ataques por parte de los ciber delincuentes.

Cabe mencionar que estos servicios contratados por las empresas o sus representante, se hace mediante procedimientos controlados y bajo parámetros de seguridad, a fin de asegurar un debido procedimiento y donde no se vea afectada la integridad de sus información, es así que se realiza esta actividad bajo autorización escrita y bajo protocolos de confidencialidad.

Un programa o actividad de Hacking Ético consiste en la penetración o vulneración controlada al sistema informático de una empresa, de la misma forma en que lo haría un ciber delincuente o Hacker, pero esta actividad se haría de una forma Ética, donde el fin no es el de causar daño, bajo previa autorización escrita del propietario del sistema informático.

Es así que Emanuel Abraham, Ethical Hacker de la empresa Security Solutions & Education (SSE), representantes para Colombia de EC Council (Consejo Internacional de Comercio Electrónico), manifiesta lo siguiente

> El hacker o pirata informático de hoy puede ser un simple curioso o un estudiante, así como el más peligroso criminal profesional. La diferencia principal es que el hacker de sombrero negro busca vulnerar sistemas sin

> permisos, para robar datos, espiar, destruir información, modificar páginas web o algún otro ciberdelito.
>
> El ejecutivo agregó que "el hacker ético trabaja en encontrar estas vulnerabilidades para que no sean explotadas por otros hackers. Trata de adelantarse e identificarlas antes que los criminales". (El hacking ético y su importancia para las empresas. 2014... Enter. Co).

El Hacker Ético, mediante el uso de técnicas utilizadas por los ciber delincuentes, evalúa la efectividad de los controles de seguridad establecidos por las empresas para proteger su información digital sensible, el cual mediante un informe menciona e identifica los sistemas en los que se ha logrado penetrar y muestra la información sensible, confidencial obtenida.

Dentro de los objetivos de una Hacker Ético, se pueden mencionar los siguientes:

- Identificar vulnerabilidades existentes en los sistemas informáticos, antes de que estas sean aprovechadas por los ciber delincuentes.

- Obtener un informe de las vulnerabilidades detectadas, determinando su nivel de criticidad y cómo remediarlas.

- Cumplir, o ayudar a cumplir, con las legislaciones relacionadas con la Seguridad de la información que se apliquen dentro de su sector.

Actualmente en las empresas se presentan dos formas de realizar un Hacking Ético o un Pentesting y es a través de dos formas:

1. White Box o Caja Blanca: El profesional o Analista en Pentesting, tiene a su disposición información sobre la infraestructura de la empresa y la profundidad del análisis está pactada de antemano con el dueño de la empresa o del proceso como tal.

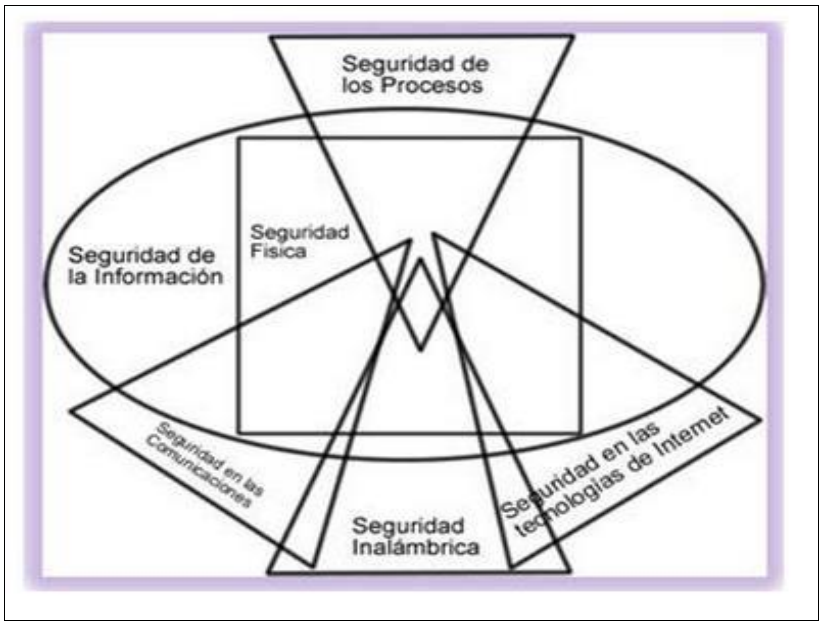
2. Caja Negra o Black Box: No se dispone casi de información del objetivo, con lo cual en este caso la fase de reconocimiento es fundamental. El analista llegará hasta donde sus habilidades y las medidas de seguridad implementadas se lo permitan. Aquí todo el

procedimiento se hace desde el exterior, a fin de tratar de vulnerar el sistema informática de la empresa que contrata el servicio.

Muchas empresas del sector industrial en el valle del cauca a través de sus especialistas en seguridad, han adaptado unas metodologías y estándares de seguridad a fin de blindarse ante ataques de los ciber delincuentes garantizando la continuidad del negocio, tomando como guía el Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, por sus siglas en inglés) o el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP). (Guevara. 2012. Hacking ético: mitos y realidades. Revista seguridad defensa digital | 1 251 478, 1 251 477. Seguridad cultura de prevención para TI).

Según el Mapa de Seguridad propuesto por el OSSTMM, las secciones a las cuales se aplican el hacking ético son las siguientes:

Figura No. 5: Mapa de Seguridad propuesto por el OSSTMM.



Fuente: Mapa de Seguridad propuesto por el OSSTMM: 2012. Hacking ético: mitos y realidades. Revista seguridad defensa digital | 1 251 478, 1 251 477. Seguridad cultura de prevención para TI. Recuperado de http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades

1- Seguridad Física: Las empresas han generado una serie de protocolos de seguridad física a fin de proteger sus activos informáticos, dentro de los procedimientos se encuentran:

- Revisión periódica del perímetro.
- Revisión de monitoreo.
- Evaluación de controles de acceso.
- Revisión de respuesta de alarmas.
- Revisión de ubicación.
- Revisión del entorno.

2- Seguridad de las Comunicaciones: Se crean protocolos de seguridad a fin de proteger sus telecomunicaciones digitales y analógicas y las redes de datos que se relacionan con todos los sistemas electrónicos y redes de datos cableados.

3- Seguridad Inalámbrica: Se crean protocolos de seguridad a fin de proteger todas sus comunicaciones electrónicas, señales y emanaciones de señales que se producen en el espectro electromagnético.

4- Seguridad en las tecnologías de internet: Se generan por los expertos en seguridad informática protocolos de seguridad a fin de evitar que los sistemas informáticos de la empresa sean objeto de intrusiones por parte de ciber delincuentes. Se crean barreras a través de software especializado en detectar intrusiones, antivirus confiables, pero ante todo procedimientos de control por parte de todo aquel que tenga acceso a los sistemas informáticos de la empresa. Se apoyan en pruebas de intrusión periódicas a las aplicaciones web a fin de detectar cualquier brecha o vulnerabilidad que pueda generar inseguridad a sus sistemas informáticos.

5- Seguridad del resguardo de información: Se generan formas de resguardar la información utilizando medios de almacenamiento confiables, sean a través de dispositivos o en la contratación de empresas confiables que administren su información.

6- Seguridad de los procesos: Este es uno de los métodos más representativos a nivel de la empresa, ya que se generan por parte de la empresa políticas de seguridad informáticas a modo de blindar a toda la organización ante ataques por ciber delincuentes. Se crean protocolos de seguridad informática a fin de evitar el acceso a su información privilegiada y sensible, donde

por voluntad propia o involuntariamente un empleado puede dar acceso a un ciber delincuente a los sistemas informáticos de la organización a través de medios como el teléfono, e-mail, chat, redes sociales, etc.

Las empresas Colombianas y en especial las del Sector Industrial del Departamento del Valle del Cauca, enfrentan un reto muy importante para consolidar sus negocios y potenciar su prestigio ante clientes, proveedores, socios estratégicos, contratistas entre otros y, para lograr todo esto es blindándose ante todo ataque y vulneración a sus sistemas informáticos, generando políticas y protocolos de seguridad a fin de controlar, mitigar todo acto inseguro que genere inestabilidad y coloque en juego la continuidad de su negocio.

Conclusiones

En la actualidad Colombia ha ocupado en puesto muy crítico en lo relacionado a las vulnerabilidades detectadas y encontradas en sus plataformas informáticas, la mayoría de las empresas colombianas han sido y están expuestas a una gran cantidad de amenazas que vulneran la seguridad de sus sistemas informáticos.

En Colombia se ha generado un crecimiento agigantado de los medios informáticos, su ubicación y disposición brindan la facilitad a las empresas de que todos sus procesos interactúen al unísono, facilitando la organización de la información personal y empresarial, ocasionando que se abra una infinidad de posibilidades para que los delincuentes busquen formas de conseguir datos de vital importancia para los usuarios, como lo son el acceso a claves bancarias, correos electrónicos, información sensible personal y empresarial, debido en su mayoría a causa de la instalación de software maliciosos en los computadores, celulares o cualquier otro dispositivo.

Los riesgos y amenazas a la seguridad informática de las empresas son evidentes. Solo en Colombia, el año pasado el Departamento de Delitos Informáticos de la Policía Nacional recibió 7118 denuncias por parte de víctimas de delitos informáticos, evidenciando un aumento del 40% con respecto al 2014. Las pérdidas económicas derivadas por estos actos representan al país alrededor del 0,14%, según el Banco Mundial (2014) del PIB Nacional, es decir, cerca de US$500 millones aproximadamente.

Colombia en el ámbito de la seguridad informática ha dejado entrever que es muy vulnerable ante los ataques de la delincuencia informática, a pesar de existir una norma técnica colombina como es la NTC-ISO/IEC 27001 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI) y una ley como la 1273 de 2009 Ley de Delitos Informáticos en Colombia, se sigue evidenciando que a pesar de tener a la mano todas estas ayudas y herramientas legales, no invierten ni se concientizan de la necesidad de hacer uso de ellas.

El Departamento del Valle ha sido catalogado como uno de los más chocados y atacados por los ciberdelincuentes, no se aleja mucho de la realidad que es debido igual que muchos otros a la falta de blindajes adecuados ante este accionar delincuencial. En lo corrido de este año se han presentado en el Valle del Cauca 1700 denuncias por delitos informáticos, cifra que convirtió a este departamento en el más golpeado del país por esta modalidad delictiva.

Colombia ocupa el segundo y tercer puesto a nivel latinoamericano como uno de los países que más ciberataques ocasionan a otros países. Así como Colombia ataca a otros países, igual Colombia es el blanco predilecto de muchos otros países del mundo, más debido a las vulnerabilidades que presentan sus sistemas informáticos.

El Hacker Ético, mediante el uso de técnicas utilizadas por los ciber delincuentes, evalúa la efectividad de los controles de seguridad establecidos por las empresas para proteger su información digital sensible, el cual mediante un informe menciona e identifica los sistemas en los que se ha logrado penetrar y muestra la información sensible, confidencial obtenida.

En este medio del Hacking Ético es común escuchar sobre el Hacker de Sombrero Blanco o Caja Blanca o Hacker de Sombrero Negro o Caja Negra, que no es más que la forma legal o ilegal de cómo se obtiene información de un sistema informático o como se violenta su seguridad, con o sin autorización de los propietarios. En este caso los dueños de empresas pequeñas, medianas y grandes, por los antecedentes anteriormente mencionados y que se han visto afectados por ataques de ciber delincuentes, han optado por contratar los servicios de personas expertas en hackear sistemas informáticos (Hacker Ético), con el fin de determinar qué tan vulnerables y expuestos se encuentran sus sistemas informáticos ante ataques por parte de los ciber delincuentes.

Las empresas Colombianas y en especial las del Sector Industrial del Departamento del Valle del Cauca, enfrentan un reto muy importante para consolidar sus negocios y potenciar su prestigio ante clientes, proveedores, socios estratégicos, contratistas entre otros y, para lograr todo esto es blindándose ante todo ataque y vulneración a sus sistemas informáticos, generando políticas y protocolos de seguridad a fin de controlar, mitigar todo acto inseguro que genere inestabilidad y coloque en juego la continuidad de su negocio.

Referencias

Manrique Horta. (2016). Diariamente en Colombia hay 10 millones de ataques informáticos. Diario del Huila. Recuperado de http://diariodelhuila.com/economia/%E2%80%9Cdiariamente-en-colombia-hay-10-millones-de-ataques-informaticos%E2%80%9D-cdgint20160312211955155)

Colombia lidera lista de ataques informáticos. (2014). Periódico el Espectador. Recuperado de http://www.elespectador.com/tecnologia/colombia-lidera-lista-de-ataques-informaticos-paises-de-articulo-523201)

En Colombia las cifras de delitos informáticos van en aumento. (2102). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento)

Valle del Cauca, el departamento más golpeado por los delitos informáticos. (2013). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/valle-cauca-departamento-golpeado-por-delitos-informaticos)

Delitos informáticos se han incrementado un 100% en Cali. (2015). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/delitos-informaticos-han-incrementado-100-cali)

En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. (2016). El Tiempo. Recuperado de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Radiografía de los delitos informáticos en Colombia en 2015. El Tiempo. Recuperada de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

Delitos informáticos se han incrementado un 100% en Cali. (2015). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/delitos-informaticos-han-incrementado-100-cali)

En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. (2016). El Tiempo. Recuperado de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

Cortes Ignacio, Del Castillo Arturo. (2013). Cibercrímen. Encuesta de fraude en Colombia 2013. KPMG Forensic Services. KPMG en Colombia. Pp 33. Recuperado de https://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Encuesta%20de%20Fraude%20en%20Colombia%202013.pdf

El hacking ético y su importancia para las empresas. (2014). Enter.Co. Recuperado de (http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

Guevara. (2012). Hacking ético: mitos y realidades. Revista seguridad defensa digital | 1 251 478, 1 251 477. Seguridad cultura de prevención para TI. Recuperado de http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades)

Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Radiografía de los delitos informáticos en Colombia en 2015. El Tiempo. Recuperada de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

Ataque cibernético de Colombia a otros países. Día 22 de septiembre de 2016. 07:41 horas. Tercer puesto. Recuperada de http://map.norsecorp.com/#/?geo=latAmer

Ataques cibernéticos de Colombia hacia otras naciones. Septiembre 22 de 2016 07:47 horas. Tercer lugar. Recuperado de http://map.norsecorp.com/#/?geo=latAmer

Ataques de Colombia hacia otras naciones. Septiembre 22 de 2016 08:22 horas. Segundo lugar. Recuperado de http://map.norsecorp.com/#/?geo=latAmer

Mapa de Seguridad propuesto por el OSSTMM. (2012). Hacking ético: mitos y realidades. Revista seguridad defensa digital | 1 251 478, 1 251 477. Seguridad cultura de prevención para TI. Recuperado de http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades

Ley 1273. 2009. De la protección de la información y de los datos. Ministerio del interior y de justicia. República de Colombia. Gobierno Nacional. Bogota

Ley 1341. 2009. Políticas públicas que regirán el sector de las tecnologías de la información y las comunicaciones. Ministerio del Interior y de Justicia. República de Colombia. Gobierno Nacional. Bogotá.

Ley Estatutaria 1581. 2012. Protección de datos personales Habeas Data en Colombia. República de Colombia. Gobierno Nacional

CONPES 3854. 2016. Política Nacional de Seguridad Digital. Departamento Nacional de Planeación. República de Colombia. Bogotá