CASOS DE ESTUDIO DE CYBERCRIMEN PARA EL MEJORAMIENTO DE LA SEGURIDAD INFORMATICA EN PYMES Y MEDIANAS EMPRESAS

CAMILA TRUJILLO CHAVARRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C, COLOMBIA
2019

CASOS DE ESTUDIO DE CYBERCRIMEN PARA EL MEJORAMIENTO DE LA SEGURIDAD INFORMATICA EN PYMES Y MEDIANAS EMPRESAS

CAMILA TRUJILLO CHAVARRO

MONOGRAFIA

Director de proyecto:

Esp. EDGAR ALONSO BOJACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)

ESPECIALIZACION EN SEGURIDAD INFORMATICA

BOGOTA D.C, COLOMBIA

2019

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

DEDICATORIA

Este proyecto va dedicado a Dios quien sin él no somos nada y nos la capacidad para afrontar cada reto que se nos presenta en la vida, a mis padres porque gracias a su apoyo y guía he logrado mis triunfos y a cada persona que me ayudo, guio o aconsejo en este proceso.

AGRADECIMIENTOS

Doy gracias a Dios quien me dio la capacidad, la sabiduría y la inteligencia para realizar esta especialización, a mi padre, madre y hermanos que estuvieron para apoyarme y finalmente a mi novio (Edward Fabian Mora Mora) que me dio fortaleza, me aconsejo y fue un gran apoyo en los momentos en los que quise rendirme.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

Amenaza

Es un peligro inminente que nace de un suceso que no ha pasado aun, pero en cualquier momento se puede materializar.[1]

ARPANET

Era una red de computadores creada en Estados Unidos por el departamento de Defensa con propósitos académicos y gubernamentales.[2]

Ataque Informático

Se produce por medio de una debilidad o vulnerabilidad que tenga un dispositivo, software o usuario para ingresar a un sistema informático.[3]

Cisco

Es una organización estadounidense que fabrica, vende, realiza mantenimientos y consultoría de dispositivos de telecomunicación.[4]

Computador

Es un dispositivo que permite realizar varias tareas agilizando las tareas diarias en la casa, oficina o negocio.[5]

[1] SIGNIFCADOS. Significado de Amenaza. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://www.significados.com/amenaza/

[2] DEFINICION ABC. Que es ARPANET. {En línea}. {Consultado 17 de octubre de 2019}. Disponible en: DEFINICION ABC. Que es ARPANET. {En línea}. {Consultado 17 de octubre de 2019}. Disponible en: https://www.definicionabc.com/tecnologia/arpanet.php

[3] CONSULTHINK. Qué es y en qué consiste un ataque informático. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://www.consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/

[4] DEFINICION ABC. Cisco. {En línea}. {Consultado 17 de octubre de 2019}. Disponible en: https://www.definicionabc.com/tecnologia/cisco.php

[5] GCFGLOBAL. ¿Qué es un computador? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://edu.gcfglobal.org/es/informatica-basica/que-es-un-computador/1/

Confidencialidad

Garantiza que personas mal intencionadas no ingresen a los sistemas donde se almacena la información.[6]

Disponibilidad

Garantiza que un sistema tenga un funcionamiento óptimo y que su recuperación ante un fallo sea rápida.[7]

eCommerce

Es la venta de productos, transacciones y marketing por internet que facilita la vida del consumidor porque evita desplazamientos o puede realizar compras de productos de diferentes países.[8]

Eficacia

Lograr una meta deseada por medio de una acción o plan ejecutado.[9]

Empresa

Unidad productiva que desarrolla una actividad económica conformada por personas y tienen un objetivo en común.[10]

Integridad

Garantiza que la información que se maneja en un sistema no sea falsa, modificada o eliminada.[11]

---

[6] DEFINICION. Confidencialidad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/confidencialidad/

[7] SEGURIDAD Informatica. Objetivos de la seguridad informática. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://infosegur.wordpress.com/tag/disponibilidad/

[8] RODRIGUEZ MERINO, Cristina. ¿Qué es E-commerce o comercio electrónico? {En línea}. {Consultado 14 de mayo de 2019}. Disponible en: https://marketingdigital.bsm.upf.edu/e-commerce-comercio-electronico/

[9] DEFINICION. Eficacia: {En línea}. {Consultado 14 de mayo de 2019}. Disponible en: https://definicion.de/eficacia/

[10] DEBITOOR. ¿Qué es una empresa? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://debitoor.es/glosario/definicion-empresa

[11] EL Significado. Significado de integridad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://elsignificadode.com/integridad/

Mediana Empresa

Son organizaciones que cuentan con máximo 100 personas para desarrollar su actividad económica.[12]

Microsoft

Es una multinacional especializada en desarrollo de software entre los más conocidos están Microsoft Windows y Microsoft Office.[13]

Prevención

Evitar o minimizar un peligro que está latente o que puede suceder en cualquier momento.[14]

Prioridad

Nivel de importancia que tiene una cosa respecto a otra.[15]

Pyme

Son organizaciones que cuentan con máximo 50 personas para desarrollar su actividad económica.[16]

Seguridad

Es la certeza que no hay ningún peligro frente alguna acción o cosa.[17]

[12] CONCEPTODEFINICION. Definición de Mediana Empresa. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://conceptodefinicion.de/mediana-empresa/
[13] TECNOLOGIA FACIL. ¿QUÉ ES MICROSOFT? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://tecnologia-facil.com/que-es/que-es-microsoft/
[14] DEFINICION. Prevención. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/prevencion/
[15] DEFINICION. Definición de Prioridad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/prioridad/
[16] TUS FACTURAS ONLINE. ¿Qué son las empresas PYME? ¿Qué significa PYME? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://tusfacturasonline.com/que-son-empresas-pyme-significado-pyme-tipos/
[17] DEFINICION. Concepto de Seguridad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/seguridad/

Servicio

Algo que se ofrece a un grupo de personas que generan un beneficio mutuo.[18]

Virus Informático

Es un software diseñado con un fin maligno, ya sea dañar un dispositivo o sustraer información sin el consentimiento del usuario. [19]

Vulnerabilidad

Punto débil que tiene un sistema o persona.[20]

Vulnerabilidad Informatica

Es una debilidad que presenta un sistema o software el cual no garantiza la confidencialidad, integridad, disponibilidad, control de acceso y consistencia en la información. Estas debilidades se deben al mal diseño del software.[21]

Wannacry

Es un tipo de ransomware que busca encriptar la información del computador para pedir un rescate por vía BitCoins.[22]

[18] CONCEPTO. Servicio. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://concepto.de/servicio/

[19] NORTON. ¿Qué es un virus informático? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://co.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

[20] SIGNIFICADOS. Significado de Vulnerabilidad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://www.significados.com/vulnerabilidad/

[21] TECNOLOGIA E INFORMATICA. Vulnerabilidades informáticas {En línea}. {Consultado octubre 21 2018}. Disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

[22] BENITEZ, Albert. ¿Qué es Wanna Cry y cómo evitarlo? {En línea}. {Consultado octubre 21 2018}. Disponible en: https://xpertix.com/que-es-wanna-cry-y-como-evitarlo/

RESUMEN

La presente monografía consiste en el estudio de casos de cibercrímenes presentados a nivel mundial para proponer pautas de mejoramiento de la seguridad informática en pymes y medianas empresas de Colombia. Estas organizaciones están siendo muy afectadas por sus escasos controles y consideran que tener un antivirus evita un ataque cibernético que se ha visto en crecimiento por su gran rentabilidad y fácil ejecución. También hay que recordar que detrás de este delito no solo se encuentra un hacker aficionado en busca de probar sus conocimientos si no que ahora es un crimen organizado que mejora los malvares antiguos haciéndolos eficientes y menos detectables.

La monografía tiene como función principal informar sobre un tema puntual basado en documentos periodísticos y/o científicos de interés para la comunidad por ende se estudiarán los casos de cibercrímenes sucedidos en el mundo con el fin de proponer un mejoramiento en la seguridad informática en pymes y medianas empresas por el gran riesgo que tienen de perder su información a causa de ciberataques que pueden ser ocasionados por vulnerabilidades en la infraestructura y el usuario, responsable de ejecutar un ciberataque sin ser consciente de ello.

1. INTRODUCCION

La globalización y el auge de las tecnologías han avanzado de manera exponencial la última década ha generado cambios en el estilo de vida permitiendo agilizar procesos que anteriormente tomaban más tiempo. Las organizaciones y usuarios son los más beneficiados por el uso de sistemas de información y comunicación, al tener datos instantáneamente en cualquier parte del mundo siempre y cuando se cuente con un dispositivo como celular, Tablet, portátil o pc, y acceso al internet por eso surge la necesidad de tener toda la información protegida y fueran del alcance de criminales.

Anteriormente las organizaciones no tenían que pensar en la seguridad que le daban a la infraestructura TI porque lo más valioso se manejaba en papel como datos de clientes, usuarios, nomina en fin todo se manejaba en físico, pero ahora con la necesidad de tener la información a la mano todo se encuentra en la nube; es el valor agregado que toda organización pueda prestar al usuario pero esto también a facilitado la vida del delincuente en el que ha tenido que cambiar la manera de realizar sus actos y esto se ve reflejado en el crecimiento de la ciberdelincuencia por ello la importancia de la seguridad informática que es el ente que vela por la protección de los datos garantizando la confidencialidad, integridad y seguridad, esto evita que una organización sea víctima de ataques informáticos, suplantación de identidad, entre otros métodos de robo que los ciberdelincuentes se han ingeniado.

Por esta razón es importante saber el estado actual de la seguridad informática en las pequeñas y medianas empresas de Colombia puesto que son las más afectadas con este tipo de crimen porque no ven necesario invertir en la seguridad de los activos tecnológicos ya sea por la resistencia al cambio en temas de TI o no creen que puedan estar bajo la mira de algún ciberdelincuente y es en este punto donde surge la curiosidad de saber que métodos, técnicas y herramientas emplean para ejecutar estas operaciones delictivas.

Debido a los robos, secuestros y suplantación de la información el cibercrimen debe tomar un lugar importante y primordial dentro de estas organizaciones porque se posee poca información y un desconocimiento total del modus operandi de este tipo de delincuencia. De acuerdo a esto se quiere dar una serie de pautas para mejorar la seguridad informática de las pymes y medianas empresas en el que se podrá llevar una idea clara y global de cómo están, estas organizaciones y por supuesto que acciones se pueden llevar a cabo para evitar al máximo un ataque informático.

Esta investigación se realizará por medio de una monografía basada en masas documentales científicas y periodísticas para informar el estado actual de los cibercrímenes que afectan este tipo de organizaciones al tal caso de llevarlas a la quiebra por la divulgación o corrupción de la información sensible. Para lograr materializar este trabajo es necesario contar con información de fuentes confiables que hablen del cibercrimen y todos sus aspectos y como se puede prevenir siguiendo una serie de pautas. Los resultados que se quieren obtener en esta monografía es informar a las pymes y medianas empresas de Colombia para que puedan minimizar o prevenir este riesgo siguiendo una serie de recomendaciones y buenas prácticas.

2. PLANTEAMIENTO DEL PROBLEMA

En los últimos años se ha incrementado los ataques cibernéticos a nivel mundial viéndose afectadas empresas como Telefónica, una empresa española y líder en telecomunicaciones que fue atacada en 2017 por un ransonware llamado Wannacry que encripto la información de varios servidores. Para recuperarla se debía pagar una suma de dinero representada en bitcoins con un plazo no mayor a tres días de no cancelar los datos se eliminaría automáticamente, también se apagaron varias terminales con el fin de evitar la propagación del virus por el resto de la red el cual llevo grandes pérdidas económicas. Este tipo de crimen se ha aumentado por el fácil acceso al internet que es el medio por el que se desplazan los cibercriminales para realizar sus acciones incentivadas por la valorización del bitcoin (moneda virtual).

Colombia también se vio afectada por el ransonware y las más perjudicadas fueron las pymes y medianas empresas debido a las vulnerabilidades de sus redes y políticas de seguridad, esto ocasiono pérdida de información, un activo valioso y sensible. Este código malicioso llego al país por medio de un correo que tenía como remitente una dirección de un banco mexicano, según investigaciones los creadores de este virus querían generar caos y pánico, el factor económico estaba en segundo plano. Los equipos que se vieron afectados eran equipos que tenían sistemas operativos y aplicaciones obsoletas o que no contaban con sus actualizaciones al día, eran vulnerables en la red, como medida Microsoft desplego una serie de actualizaciones a sistemas que todavía contaban con soporte, para el caso de Vista, XP y Windows más viejos la única era migrar los equipos a un sistema operativo actual, así mismo las empresas de antivirus se encargaron de generar actualizaciones para contra restar este ataque y por supuesto las empresas empezaron a trabajar en tiempo record para garantizar que todas las terminales de su compañía estuvieran actualizadas o aisladas en tal caso que ya estuvieran infectadas o con sistemas operativos obsoletos.

Este tipo de delitos en Colombia son sancionables de acuerdo a la ley 1273 de enero de 2009 en el que se indican las penas que puede tener una persona de acuerdo al delito informático que se ejecutó, para el caso el delito que se cometió fue daño informático que de acuerdo al artículo 269D tiene una prisión entre 48 y 96 meses y una multa de 100 a 1000 salarios mínimos.

Es alarmante los casos de cibercrímenes en pymes y medianas empresas en Colombia que se ven involucradas, por ende, de no realizarse esta monografía se estaría perdiendo la oportunidad de adquirir conocimientos en el ámbito de la ciberdelincuencia un tema muy común pero poco conocido además se dará unas pautas para tener buenas prácticas que pueden evitar la intrusión de personas no deseadas en la red y la importancia de la seguridad informática en toda empresa.

¿Cómo se puede mejorar la seguridad informática en las pymes y medianas empresas que están siendo afectadas por el crecimiento y rápida adaptación del cibercrimen?

3. JUSTIFICACION

Actualmente tener una infraestructura tecnológica robusta no garantiza que sea 100% segura debido a que cada día se crean nuevos métodos para atacarlas, una organización solida siempre busca cuidar su información pero en el caso de las pymes y medianas empresas no es prioritario ya sea por falta de presupuesto o por la falta de conocimiento que se tiene respecto al cibercrimen y se cree que es un problema lejano del entorno social y económico pero es todo lo contrario, está presente en el diario vivir en el que ha afectado a grandes compañías a tal punto de llevarlas a la quiebra ya sea por la indisponibilidad de un servicio, perdida de información o daño en la infraestructura.

El siguiente documento muestra cómo se encuentra actualmente la seguridad informática en las pymes y medianas empresas por medio de masas documentales y de información que muestran las modalidades del cibercrimen identificando metodologías, herramientas y técnicas, así como las estrategias utilizadas por este tipo de delincuencia.

Esto permitirá llevar una idea de lo perjudicial que es un ciberataque y de lo expuestas que están por no llevar unas buenas prácticas en el manejo de la infraestructura TI y sistemas de información, por consiguiente, se quiere lograr que de acuerdo a las recomendaciones dadas logren implementar políticas de seguridad que les permita tener un mayor control previniendo la filtración de personas o programas a la red para evitar pérdidas económicas por un ataque cibernético. También contribuir al desarrollo social de estas organizaciones que son vulnerables ante este tipo de problemática porque no pueden contar con un asesoramiento o área enfocada en la seguridad informática por su corto presupuesto. Este proyecto dará unas recomendaciones básicas que no generan ningún costo pero que a corto, mediano y largo plazo se verán beneficiadas por el conocimiento adquirido y las mejoras se hallan implementado.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Realizar un estado del arte que permita el diagnóstico del estado actual de la seguridad informática en las pequeñas y medianas empresas.

4.2. OBJETIVOS ESPECIFICOS

- Levantar información sobre las modalidades de cibercrímenes identificando metodologías, herramientas y técnicas con las que se realizan los ciberataques.

- Determinar las estrategias utilizadas por los ciberdelincuentes que vulneran la seguridad de las pymes y medianas empresas.

- Generar recomendaciones que mejoren la seguridad informática de las pymes y medianas empresas.

5. MARCO REFERENCIAL

5.1. MARCO TEORICO

5.1.1. Historia del Internet

Fue creado en los años 60s en la guerra fría por Estados Unidos para uso exclusivo militar, ya que temían el acceso de la información por parte de Rusia u otro país. Inicialmente se llamó ARPANET, y contaba con solo cuatro equipos distribuidos en varias universidades del país, después de dos años esta red ya contaba con cuarenta equipos, creció tan rápido que el sistema de comunicación quedo obsoleto, fue entonces que se creó el protocolo TCP/IP que actualmente se sigue utilizando.

ARPANET siguió expandiéndose por todo el mundo en el que cualquier persona con intensiones académicas o investigativas podían hacer uso de esta red, por esta razón dejo de ser un uso exclusivo militar y se creó MILNET creada también por Estados Unidos. La fundación Nacional de ciencia crea una red propia nombrada NSFNET que más adelante toma a ARPANET, se convierte una gran red con intensiones científicas y académicas. También se conocieron la creación de nuevas redes, pero al final también se unieron con NSFNET y este fue el inicio de lo que hoy en día se conoce como INTERNET.

En los años 80s esta era una tecnología solida pero pocos la conocían, era fundamentalmente textual por ende William Gibson creo el termino –ciberespacio- basándose en los videojuegos, con el pasar de los tiempo esta palabra fue el sinónimo de INTERNET, en el año 1990 ya se contaban con cien mil servidores, en este mismo año se creó un proyecto el cual consistía en sistema de almacenamiento y recuperación de datos, se llamó Word Wide Web o telaraña mundial, esto permitiría relacionar información de manera lógica por medio de las redes. Su contenido seria programada en lenguaje de hipertexto que asignaba una función a cada parte del contenido con un intérprete que sería un navegador.

En 1993 se creó la primera versión de un navegador llamado Mosaic contaba con una interfaz gráfica y se podía acceder con mayor facilidad a la WWW, lo ceo Marc Andreesen, quien fue uno de los que dirigió la creación del programa Netscape. Desde ahí el Internet fue más rápido que cualquier medio de comunicación de ese tiempo y en lo que es hoy en día.

5.1.2. Historia del Cibercrimen

No se tiene una fecha o registro puntual del primer delito informático, pero hay varios puntos de referencia que evidencian los inicios del cibercrimen que ocasionaron varios estragos y en aquel tiempo las personas no eran conscientes de la problemática en el que se iba a convertir ya que entre más avanzaba la tecnología también lo hacia este delito.

- En 1971 un manipulador telefónico llamado John Draper crea una caja azul con un silbido igual al de un conmutador que permitía realizar llamadas a larga distancia gratis. Se encargó de publicar un manual.
- En 1973 se utilizó un computador para depositar más de dos millones de dólares de un cajero local de Nueva York.
- En 1978 entro el primer tablón de anuncios en línea que se convirtió en un medio de comunicación para los cibernautas en el que se compartían conocimientos como trucos y consejos para vulnerar redes.
- En 1981 fue condenada la primera persona por un caso de ciberdelito era conocido como el capitán Zap, porque vulnero de red de AT&T y modifico el reloj interno de recargo de tarifas. La película Los Figones se inspiró en este personaje.
- En 1982 fue escrito el primer virus por un adolescente de 15 años de manera accidental que afecto un computador Appel II por medio de un disquete.
- En 1986 el congreso de Estados Unidos convierte el hackeo en algo ilegal aprobando una ley de fraude y abuso informático.
- En 1988 se lanzó el primer gusano auto replicable que afecto más de seis mil terminales de la ARPANET, su creador Robert Morris fue multado y tres años preso.

- En 1989 se reporta el primer Ransomware en que se descargaba un cuestionario.
- En 2000 yahoo, Ebay y varias plataformas son atacadas con una DDoS.
- En 2003 se crea un gusano de difusión rápida el cual fue SQL Slammer, que infecto más de 75.000 servidores de bases de datos en menos de 10 minutos.
- En 2007 se disparan los casos de hurto de datos y propagación de virus aumenta.

5.1.3. Historia de la Tecnología en Colombia

En marzo de 1957 llega a Colombia la IBM 650, el primer computador del país que causo en las personas fascinación y creían que era algo insólito, fue traído por la compañía Bavaria pionera en la sistematización de Colombia, era una gran adquisición del siglo XX por su gran tamaño y peso. También grandes empresas de esa época como Coltejer, Empresas públicas de Medellín y Ecopetrol adquirieron este dispositivo, al igual que la universidad Nacional y los Andes en los que se desarrollaron grupos de trabajo en sistemas informáticos.

La comercialización de microcomputadoras inicia en 1980 liderada por Manuel Dávila un ingeniero de sistemas e Ivan Obregon un matemático fundador de Microtek la primera empresa de microcomputadores en el país y fue representada por la marca RadioShack que aventajaron por un tiempo a Apple; Manuel Dávila con su grupo de trabajo fueron los creadores del primer software administrativo del país. Entre 1990 y 1995 entra al país el Internet inicialmente siendo aprovechada por las universidades esto hizo que la red se agrandara incrementado el servicio de ancho de banda por la cantidad de conexiones.

5.1.4. Estándares de la IEEE

Significa Instituto de Ingenieros en Eléctrica y Electrónica, fueron los que definieron los estándares de redes de área local. En los años 80´s la gran mayoría de los estándares fueron establecidos por el comité cuando estaban surgiendo las primeras redes entre PC. Muchos estándares de IEEE derivan de

la ISO como el estándar 802.3 del IEEE que deriva de la ISO 8802.3. A continuación se relacionaran algunos estándares que maneja este instituto.

- 802.1, este estándar define el significado de la palabra Redes.
- 802.2, este estándar define el control de enlaces lógicos que asegura que los datos se trasmitan de forma segura en el enlace de comunicación.
- 802.3,
- 802.5, este estándar define los protocolos que debe tener una red token ring como acceso, cableado e interfaz.
- 802.6, este estándar define el protocolo de velocidad de una red MAN porque esta ofrece servicios de datos, voz y video.

5.1.5. Modelo OSI

Es un estándar que diseñó el modelo de Interconexión de Sistemas Abiertos (OSI), es una guía para la elaboración estándares de dispositivos de cómputo para las redes, esto es con fin de que operen adecuadamente por la alta complejidad de los dispositivos que se conectan la red. Se compone de siete capas como las físicas, software, aplicación entre otros.

- Física, es la capa número uno y define la interfaz con el medio físico incluyendo los cables de red.
- Capa de enlace de datos, es la capa número dos, detecta y corrige los errores cometidos en la trasmisión de datos por el cable de red.
- Red, es la capa número tres y guía los datos de un nodo a otro.
- Transporte, es la capa número cuatro que proporciona y mantiene el enlace de comunicaciones respondiendo adecuadamente si el enlace falla.
- Sesión, es la capa número cinco y controla las conexiones de red entre los nodos.
- Presentación, es la capa número seis y da el formato de los datos para garantizar que sea legible para el dispositivo.
- Aplicación, es la capa número siete y proporciona funciones a las aplicaciones de los usuarios.

5.2. MARCO CONCEPTUAL

5.2.1. Seguridad Informatica

Es conjunto de herramientas, procesos y tácticas que garantizan tres pilares: integridad, disponibilidad y confidencialidad en un sistema de información. Se especializa por la protección de los datos y comunicaciones de una LAN o WAN y trata de garantizar sus principios básicos:

- Integridad de datos: todo tipo de modificación debe ser autorizado por el autor u organización.
- Disponibilidad del sistema: garantiza la continuidad del negocio por medio de los servicios para tener productividad y credibilidad en la organización.
- Confidencialidad: la exposición de los datos debe estar autorizados, así como protegerlos de cualquier ataque.[23]

La seguridad informática se fortalece invirtiendo en la ciberseguridad y empleando actividades para minimizar el riesgo con el objetivo de ralentizar el acceso de los hackers y saber con más precisión las amenazas. Algunas prácticas saludables para la seguridad informática son:

- Tener un inventario de los activos de información, hardware, usuarios y niveles de seguridad.
- Capacitar a los usuarios sobre la importancia de la seguridad de la información.
- Tener un corta fuegos, se recomienda de que sea de última generación.
- Hacer continuamente test de penetración a los sistemas de información para identificar las vulnerabilidades.
- Tener planes de contingencia para eventos de seguridad informática.

[23] SIGNIFCADOS. Significado de Seguridad informática. {En línea}. {Consultado noviembre 06 2018}. Disponible en: https://www.significados.com/seguridad-informatica/

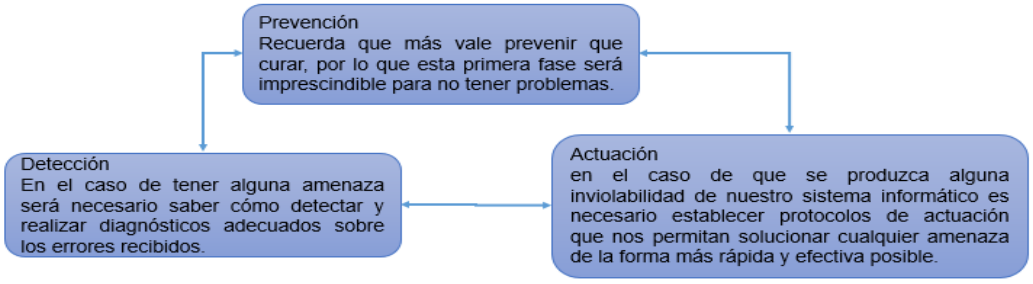
- Tener un sistema de backup.[24]

5.2.2. Políticas de Seguridad

Es un conjunto de pautas, medidas y etiquetas que busca velar por la seguridad de una organización combatiendo todos los riesgos a los que se expone en el ámbito tecnológico alejándolo de cualquier ataque externo debido a la cantidad de ciberdelincuencia que ataca organizaciones por medio de los dispositivos tecnológicos para adquirir información sensible utilizándolas en estafas o sacar algún beneficio.

Las políticas definen una serie de procesos internos los cuales se deben cumplir y actualizar de manera periódica esto aplica tanto en el tratamiento o manejo de los dispositivos de la red como al personal que se encuentra en la organización ya que la mayoría de los problemas se producen por errores humanos porque no son conscientes de la vulnerabilidad de los datos e información de una organización. También se deben establecer mecanismos de seguridad que se vayan a implantar en una organización como.[25]

Figura 1. Mecanismo de Seguridad



Fuente. Camila Trujillo

[24] MOVISTAR. La importancia de la seguridad informática en un negocio. {En línea}. {Consultado junio 05 2019}. Disponible en: https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/la-seguridad-informatica/

[25] EMPRENDE PYME.NET. Políticas de seguridad. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.emprendepyme.net/politicas-de-seguridad.html

5.2.3. Infraestructura de Redes

Son instalaciones de hardware que comprenden los servidores y los diferentes dispositivos que forman parte de la red como cableado estructurado, equipo de comunicación con alimentación eléctrica, cuarto de comunicación y red eléctrica.[26]

Switch

Es un dispositivo que se conecta entre equipos de una red LAN y contiene puertos en lo que se conectan físicamente otros dispositivos, como swtich, routers y servidores. Estos dispositivos cada día son más complejos pero su funcionamiento sigue siendo igual el cual trasmite un mensaje utilizando una dirección física de la tarjeta de red o MAC para proporcionar una comunicación entre los equipos de una red.

Hay varios tipos de switches, se diferencian por la clase de tecnología o servicio que ofrece como: wifi que es la capacidad que conectar varios dispositivos de forma inalámbrica siendo útil en hogares y organizaciones, VLAN permite segmentar redes para que no halla comunicación entre dispositivos, PoE alimenta de energía los equipos con el propio cable de red, STP conecta varios switches son ocasionar bucles, firewall y detector de intrusos.[27]

Routers

Este dispositivo permite la conexión de diferentes redes LAN responsable de llevar adecuadamente el tráfico, su funcionamiento es básico en el que utiliza direcciones IP para identificar el destino de los paquetes de datos esta funcionalidad no la tienen los switches.

[26] SISTEMAS. Definición de Infraestructura. {En línea}. {Consultado noviembre 06 2018}. Disponible en: https://sistemas.com/infraestructura.php

[27] SANCHEZ IGLESIAS, Angel Luis. ¿Qué es un switch? {En línea}. {Consultado junio 11 2019}. Disponible en: https://www.aboutespanol.com/que-es-un-switch-841388

Funcionamiento: cuando se ingresa a una URL el navegador consulta por medio del servidor de nombre de dominio la dirección IP de la página, el PC emite una solicitud al router, que establecerá el siguiente equipo por que el pasará los datos escogiendo la mejor ruta, estos dispositivos cuentan con tablas actualizadas de enrutamiento que funcionan como mapas para llegar a las direcciones destino más idóneas, hay muchos protocolos incluidos en esta labor.[28]

Firewalls

Son dispositivos de seguridad que controlan el tráfico entrante y saliente de la una red por medio de un conjunto de reglas. Un cortafuego puede ser hardware, software o la combinación de los dos, todos los mensajes que entran y salen por la red LAN pasan por este dispositivo en el que examina y determina si es confiable o peligroso, en tal caso de venir de una fuente de dudosa reputación lo bloquea.

Hay cinco tipos de cortafuegos que una organización puede implementar para la protección de la red, cada uno cuenta con ventajas y desventajas, la selección se basa en las necesidades (que tan urgente es adquirir el dispositivo), recursos (factor económico) y conocimiento del área de TI (nivel de estudio y experiencia del personal) que tengan la empresa.

- Packet-filtering firewalls: se conoce como contrafuego de filtrado de paquetes; funciona en el router y compara los paquetes recibidos por medio de unos criterios como direcciones IP, tipo de paquete y numero de puertos, esto se hace antes de enviarlo o eliminarlo.
- Circuit-level gateways: se conoce como pasarelas de nivel de circuitos; revisa el intercambio de datos por medio del protocolo TCP entre equipos locales y conexiones remotas para confirmar si el inicio de sesión es legítimo.

[28] ECURED. Router. {En línea}. {Consultado junio 16 de 2019}. Disponible en: https://www.ecured.cu/Router

- Stateful inspection firewalls: se conoce como contrafuegos de inspección de estado; examina y realiza seguimiento de cada paquete confirmando si una sesión TCP es legítima.
- Application-level gateways: se conoce como pasarelas a nivel de aplicación y combina propiedades del firewall de filtrado de paquetes y pasarelas a nivel de circuito.
- Multilayer inspection firewalls: se conoce como contrafuegos de inspección multicapa; combina el filtrado de paquetes y la monitorización de circuitos.[29]

Servidores

Es un equipo que ofrece servicios en una red, las cuales pueden ser de aplicación, web, ftp, impresoras entre otros, provee datos que son solicitados por los navegadores de otras terminales. Los servidores almacenan información por medio de páginas web y el protocolo HTTP o HTTPS.[30]

5.2.4. Software de Infraestructura

Abarca todo lo que son los sistemas operativos de las terminales y servidores como parte de la infraestructura de TI. Estos son muy necesarios debido a que permiten el funcionamiento del hardware.[31]

5.2.5. Cibercrimen

Se basa en la creación de malware o tipos de ataques por parte de grupos de hackers con el fin de materializar sus objetivos buscando sacar provecho inicialmente económico, algunos lo realizan como pasa tiempos o para ver las vulnerabilidades que tiene la organización para luego cobrar a piratas por la información. Estos malware son creados con los siguientes objetivos:

[29] PANDA. ¿Qué es un Firewall? {En línea}. {Consultado junio 16 2019}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/que-es-un-firewall/
[30] MASADELANTE. ¿Qué es un servidor? - Definición de servidor. {En línea}. {Consultado junio 16 2019}. Disponible en: https://www.masadelante.com/faqs/servidor
[31] MALDONADO, Diego. ¿Qué es Infraestructura de TI y cuáles son sus componentes? {En línea}. {Consultado noviembre 06 2018}. Disponible en: http://www.icorp.com.mx/blog/infraestructura-de-ti-componentes/

- Tener acceso a las cuentas de códigos bancarios.
- Utilizar los recursos de equipos infectados para promocionar servicios.
- Chantajear a la víctima por medio de robo de información personal.

Cómo protegerse frente al cibercrimen

Para la protección en este tipo de ataque es recomendable la utilización de antimalware que consisten en la detección basada en firmas, análisis total de la máquina y tecnologías basadas en la nube para proteger los dispositivos e información frente a las cambiantes y actualizadas amenazas del mundo informático.[32]

5.3. MARCO LEGAL

5.3.1. Ley 1273 de 2009

Se crea esta ley en 2009 que modifica el código penal de Colombia que sanciona los delitos informáticos debido al aumento del cibercrimen y al poco control que tenían ya que no era sancionable, cuenta con dos capítulos. El capítulo 1 habla sobre la confidencialidad, integridad y disponibilidad de los datos y sistemas de información distribuida en ocho artículos que indican las sanciones económicas y los meses de cárcel que puede tener el infractor. El capítulo 2 habla sobre atentados y otras infracciones informáticas que son sancionables.

Para consultar más sobre la ley 1273 de 2009 puede ingresar al enlace:

http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf[33]

[32] KARPERSKY LAB. Qué es el cibercrimen - Definición. {En línea}. {Consultado noviembre 06 2018}. Disponible en: https://www.kaspersky.es/resource-center/threats/cybercrime

[33] DIARIO OFICIAL. LEY 1273 DE 2009. {En línea}. {Consultado octubre 21 2018}. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

6. MODALIDADES DEL CIBERCRÍMEN

6.1. LAS NUEVAS APLICACIONES

El progreso de los sistemas y dispositivos electrónicos tecnológicos hace que surjan aplicaciones para diferentes tipos de usuarios que facilitan las actividades diarias, como saber el estado del clima o la hora en diferentes países del mundo, pero estas aplicaciones pueden llegar a administrar nuestra información confidencial y vale preguntarse qué tan seguras son y si vale la pena obtenerlas ya que pueden quedar en manos equivocadas.

Según José Parada gerente de ventas de redes los servicios en línea están ascendiendo y se requiere de la protección de los servidores. Las organizaciones deben saber que la seguridad informática pasó de ser un tema de bancos y servicios en línea a ser el pilar de seguridad de cualquier empresa, hoy en día el blanco ideal son las aplicaciones por las altas vulnerabilidades que pueden tener, aunque un atacante no descarta los diferentes huecos que puede tener la infraestructura de una organización.[34]

6.2. APLICACIONES VULNERABLES UTILIZADAS EN CIBERATAQUES

En 2017 existieron muchas vulnerabilidades de día cero activamente explotadas no sólo en ataques selectivos, sino también de forma masiva. A diferencia de las estadísticas del año pasado, los exploits para vulnerabilidades en Adobe Flash Player e Internet Explorer han ido disminuyendo, siendo reemplazados por exploits para Microsoft Office. La creación de exploits confiables para Flash Player se ha convertido en un proceso que consume mucho tiempo y dinero para el ciberpirata promedio. No se trata sólo de encontrar y explotar una vulnerabilidad en Flash Player, sino que también hay que superar las medidas de seguridad en los modernos navegadores web. Y como todos los principales

[34] UNIVERSIDAD LIBRE. Las nuevas aplicaciones y los cibercriminales. {En línea}. {Consultado octubre 21 2018}. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/517-las-nuevas-aplicaciones-y-los-cibercriminales

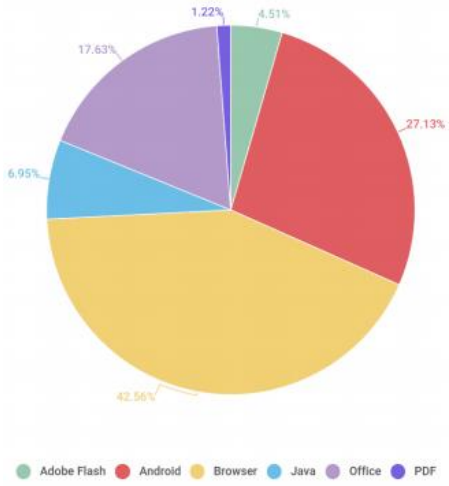
actores de kits de exploits se retiraron del mercado en 2017, sólo los atacantes altamente sofisticados son capaces de desarrollar un exploit para Flash Player.

Debido a que el mercado de kits de exploits, tradicionalmente dominado por los exploits para navegadores y Flash Player, está decayendo, hay un crecimiento sustancial de ataques contra usuarios de Microsoft Office: un 4% en este año o un escalofriante 14% en los dos últimos años. La principal razón para este aumento radica en las numerosas vulnerabilidades día cero descubiertas en Office en los últimos 12 meses. Las vulnerabilidades de corrupción de memoria binaria se utilizaron en ataques APT, aunque no fueron más ampliamente usadas en campañas de spam malicioso debido a la complejidad y baja confiabilidad de los exploits. Los exploits para tres vulnerabilidades 'lógicas' han sido utilizadas este año en la mayoría de los ataques tipo spear-phishing. Según las estadísticas de KSN, más del 90% de los documentos de Microsoft Office con exploits detectados contenían exploits para las vulnerabilidades CVE-2017-0199 o CVE-2017-8759, lo que los coloca muy por encima de otros exploits. Resulta interesante que muchos de los documentos con un exploit para Microsoft Office en 2017 también contenían un componente phishing, en caso de que la víctima ya hubiese parchado la vulnerabilidad.

Los exploits para Android también mostraron un alza anual del 6%, sumando el 27% de todos los exploits. El rápido crecimiento del año pasado aún continúa, principalmente debido a un aumento en la cantidad de exploits que facilitan el escalamiento de privilegios de raíz en dispositivos móviles Android. Pero, el principal suceso - no sólo del segundo trimestre, sino de todo el año 2017 - fue la publicación del archivo comprimido 'Lost in Translation' por parte del grupo de hackers Shadow Brokers. Este archivo comprimido contenía múltiples exploits de red para varias versiones de Windows. E incluso a pesar de que la mayoría de esas vulnerabilidades no eran en realidad del tipo día cero y que Microsoft las había parchado con la actualización MS17 - 010 un mes antes, la publicación tuvo graves consecuencias. Los daños causados por los gusanos de red, troyanos y programas ransomware cifradores que se propagaron a través de la

red con la ayuda de los exploits EternalBlue y Eternal Romance SMB, así como a través de los usuarios infectados, son incalculables. En las estadísticas anuales sobre los ataques de red bloqueados por el componente IDS fue una de las vulnerabilidades de red más explotadas durante varios meses.[35]

Figura 2. Distribución Exploits



Fuente. Kaspersky: Boletín De Seguridad Estadísticas Generales De 2017

Esta imagen muestra la distribución de los exploits usados en ciberataques, por tipo de aplicación atacada entre noviembre de 2016 y octubre de 2017 donde se evidencia que la aplicación más afectada es el browser o navegador en el que hoy en dia las aplicaciones son webs y la menos afectada es PDF.

6.3. LOS CIBERDELINCUENTES DAN UN GIRO Y ADOPTAN NUEVAS ESTRATEGIAS Y TÁCTICAS

En el 4.º trimestre de 2017, se registraron una media de ocho nuevos tipos de malware por segundo, en comparación a los cuatro tipos nuevos por segundo del 3.er trimestre. Este trimestre se ha caracterizado por la utilización de nuevas

[35] KARPERSKY LAB. Kaspersky: Boletín De Seguridad Estadísticas Generales de 2017 {En línea}. {Consultado octubre 21 2018}. Disponible en: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164544/KSB_statistics_2017_SP_final.pdf

herramientas como códigos maliciosos basados en PowerShell y la minería de criptomonedas, que ha aumentado debido al alto valor del bitcoin.

PowerShell: en 2017 se observó un ascenso del malware PowerShell del 267 % durante el 4.º trimestre, y del 432 % interanual, debido a que es la herramienta preferida por los ciberdelincuentes por las facilidades de uso y que es una herramienta que permite la administración del sistema de un equipo ya sea PC o servidor.

Minería de criptomonedas: esta moneda virtual permite realzar actividades ciber delictivas como comprar códigos maliciosos y pagos de liberación de información a causa del ransomware. Los ciberdelincuentes infectan máquinas de usuarios que navegan por la red para utilizar los recursos de la víctima porque una computadora de minería es bastante cara que puede superar los 5000 dólares.

Ransomware: en 2017, hubo un incremento interanual del ransomware del 59 %, con un aumento del 35 % solo en el 4.º trimestre. Se identificaron nuevos métodos como extorsionar al usuario para obtener dinero y también crear nuevas estrategias para no ser detectados, pero aun así se ha logrado desmantelar varias redes entre esos los responsables de la expansión del ransomware CTB Locker.[36]

6.4. FACTORES QUE FAVORECEN EL CIBERCRIMEN

A continuación, se listarán los principales factores que han afectado principalmente las pymes y mediana empresas por su poco presupuesto, control y conocimiento sobre el cibercrimen; modalidad que ha aumentado y trasformado en los últimos años por el crecimiento exponencial de la tecnología.

- Cada vez son más activos los ciberdelincuentes y no dejan rastros

[36] MCAFEE. Informe de McAfee Labs sobre amenazas {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/reports/rp-quarterly-threats-mar-2018.pdf

Muchas terminales que se conectan a Internet sin protección son un refugio seguro para los atacantes cibernéticos. Según cifras recientes, en los últimos tres meses, la cantidad de computadores afectados en redes de bots se ha maximizado y podrían llenar Internet con más de cien mil millones de mensajes de tipo spam cada día.

- Los ciberdelincuentes se benefician de la recesión mundial

  El escenario puede agravarse si los inconvenientes más temibles como la crisis económica mundial y una continua guerra para acabar el terrorismo, sean solo su foco de atención. Anteriormente no era necesario como lo es ahora pensar en la seguridad de Internet, por las oportunidades que tienen los ciberdelincuentes para lograr una tajada jamás han sido mayores y el precio para los consumidores, la industria y la seguridad nacional sigue aumentando.
- El miedo de los consumidores lo aprovechan los ciberdelincuentes

  Los ciberdelincuentes sacan provecho de que la disminución económica impulsara en todo el planeta un uso más continuo de Internet para consultar las buenas ofertas y trabajos, y administrar sus finanzas. Se aprovechan del temor y de la inseguridad, porque los consumidores suelen ser muy frágiles y muy negligentes en los tiempos difíciles. De igual manera, las oportunidades de un ataque van creciendo.
- Ataque nacional una amenaza constante

  El uso de Internet es considerado como un arma para el espionaje ya sea para fines económicos, políticos o militares. Trata de una tendencia que no se ha disipado en los últimos doce meses, como prueba la cantidad de ataques identificados. A menudo es considerado una amenaza del ciberterrorismo sobredimensionada, pero, hay quienes consideran que los ciberdelincuentes terminaran siendo lo bastante intrépidos y eficaces realizando ataques que perjudican y destruyen componentes de la infraestructura local de importancia alta.
- La seguridad es un tema secundario para los gobiernos

  Pese al aumento del peligro para la seguridad, los gobiernos continúan estando sobrecogidos frente a la primera dificultad en lo que a cibercrimen

se refiere. No observan la ciberseguridad como una necesidad por la ignorancia técnica y la insuficiente previsión de peligros comunes y a largo plazo, y dedicar tiempo ni recursos legales.[37]

6.5. LA WEB

A continuación, se indicarán algunas vulnerabilidades encontradas en la web dado a que es la principal herramienta que utiliza hoy en día la sociedad para comunicarse dado a la globalización por ende los ciber atacantes se enfocan en explotar las vulnerabilidades que tiene esta plataforma.

- 1 de cada 13 URLs analizadas en el gateway fueron consideradas malintencionadas. En 2016 esa cifra fue 1 de cada 20.
- Hubo un aumento de 62% en la actividad general de botnets identificada en el gateway.
- Con el transcurso del año, los ataques web bloqueados en los endpoints presentaron tendencia de crecimiento, impulsados por las actividades de minería de criptomonedas.
- Hubo un aumento de 448% en las actividades de kit de exploit bloqueadas en los endpoints.[38]

[37] MCAFEE. Informe sobre Criminología Virtual de McAfee amenazas {En línea}. {Consultado marzo 19 2019}. Disponible en: https://www.estudiocriminal.eu/wp-content/uploads/2017/03/Informe-sobre-criminologia-virtual-de-McAfee.pdf

[38] SYSTEMATIC. Informe Sobre las Amenazas para la Seguridad en Internet {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://tecno.com.mx/site1/wp-content/uploads/2018/06/ISTR23-FINAL_ES.pdf

7. VULNERABILIDADES DE LAS PYMES Y MEDIANA EMPRESAS

7.1. PYMES DE AMÉRICA LATINA, MÁS EXPUESTAS A CIBERATAQUES

Frente a las amenazas cibernéticas a las que se exponen las empresas de todo el mundo, las pequeñas y medianas empresas denuncian más vulnerabilidad, por falta de inversión, en muchos casos, propiciada por fragilidades financieras, en Latinoamérica, los riesgos son muy marcados, ante la falta de interés y la confianza en que los delincuentes no van a mirar para estas latitudes, pese a que tal como indicó Juan Marino, gerente de Ventas de Cisco Argentina, "es indiscutible que no hay fronteras geográficas para el cibercrimen".

Por parte de Ghassan Dreibi, gerente de Desarrollo de Negocios de Security Cisco Latinoamérica, marcó que "las pymes son más vulnerables porque no tienen tanta inversión, y porque no hay un producto adecuado a este tipo de empresas". La modalidad más frecuente es la "ingeniería social", que implica un trabajo previo de conocimiento de actividades y dinámicas de la víctima, para luego proponerle una situación que le resulte razonable y que lo haga obedecer, "Muchos ataques implican: 'se debe hacer una transferencia bancaria a esta cuenta con este dinero por tal razón'. Y si eso tiene sentido o suena normal en el negocio, los empresarios lo hacen", comentó Marino.[39]

7.2. ES "DESPIADADO" EL CRECIMIENTO DEL CIBERCRIMEN

Se ha determinado como un anexo de la existencia del siglo XXI el cibercrimen, mientras la cantidad de víctimas y sucesos crece. Según un nuevo reporte de Europol, asegura que el incremento continuo está dado por el aumento de cibercriminales y en las oportunidades rentables que aprovechan gracias al usuario. El cibercrimen en algunos países de la UE ha superado el crimen

[39] CIBERSEGURIDAD LATAM. PyMEs de América latina, más expuestas a ciberataques {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.ciberseguridadlatam.com/2018/04/27/pymes-de-america-latina-mas-expuestas-a-ciberataques/

tradicional debido a la evaluación que ha tenido en los últimos años. Ha aumentado la amenaza del ransomware debido a que se han afectados sectores de la salud y también se ha implementado malware para la red de cajeros automáticos que puede afectar el servicio a nivel mundial.[40]

7.3. PAÍSES LATINOAMERICANOS, POCO PREPARADOS CONTRA EL CIBERCRIMEN

La seguridad de la información es un proceso de mejora continuo por el dinamismo de las vulnerabilidades de seguridad, consecuente de nuevos riegos y nuevas amenazas desarrolladas. Lo anteriormente dicho tiene más relevancia si se desea aumentar y optimizar la seguridad informática de los estados. Para esto se debe especificar los aspectos a evaluar y como se debe calcular el nivel de seguridad de un país ya que, lo que no se mide no se puede controlar y lo que no se controla no se puede mejorar.

Según el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), los países latinoamericanos están poco preparados en el tema de las amenazas del cibercrimen que cada día va en ascenso. Esto es de gran importancia si se considera aumentar y mejorar la seguridad de los países.[41]

La siguiente imagen muestra los tipos de ataque que está recibiendo Colombia por segundo, clasificándose en ocho grupos como vulnerabilidades, tráfico de dudosa procedencia, flujo de localización del código malicioso cuando el usuario realiza la búsqueda manual, ataques de DDoS, entre otras.

[40] PURBA, Narinder. El crecimiento del cibercrimen es “despiadado” según Europol. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.welivesecurity.com/la-es/2016/09/28/crecimiento-del-cibercrimen-despiadado/

[41] MENDOZA, Miguel Angel. Países latinoamericanos, poco preparados contra el cibercrimen según nuevo informe. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.welivesecurity.com/la-es/2016/04/05/paises-latinoamericanos-poco-preparados-cibercrimen/

Figura 3. Ataques cibernéticos a Colombia 2018

Fuente: kaspersky Map

Esta imagen muestra el número de ataques que esta recibiendo Colombia por segundo, a continuación, se indicara que significa cada convención. **OAS, (On-Access Scan)** indica el flujo de detección de códigos maliciosos cuando los objetos son accesados al momento de copiar, ejecutar, abrir o guardar. **ODS, (On Demand Scanner)** cuando el usuario busca manualmente los virus por medio del botón "Buscar virus" en la consola. **MAV**, escanea los mensajes entrantes e invoca a OAS al guardar los adjuntos a un disco. **WAN, WAV (Web Anti-Virus)** muestra el flujo de detección de malware cuando una página html de un sitio web se abre o un archivo se descarga. **IDS, (Sistema de Detección de Intrusos)** muestra el flujo de detección de los ataques a las redes. **VUL, (Vulnerability Scan)** muestra el flujo de la detección de vulnerabilidades. **KAS, (Kaspersky Anti-Spam)** indica el tráfico dudoso y no deseado indicado por el Filtrado de Reputación de Kaspersky Lab. **BAD, (Detección de Actividad Botnet)** muestra estadísticas sobre direcciones IP de víctimas de ataques DDoS y servidores botnet.[42]

[42] KARPERSKY LAB. Ciberamenazas Mapa en Tiempo Real. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://cybermap.kaspersky.com/es/subsystems/

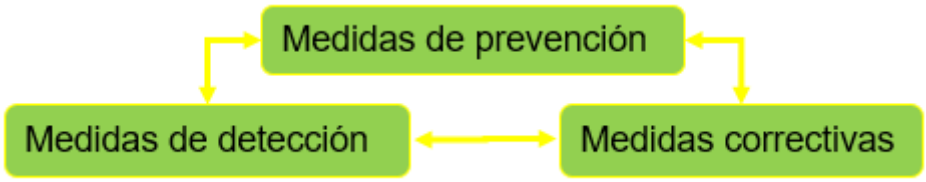
7.4. LAS COMPAÑÍAS COLOMBIANAS EN JAQUE POR LOS CIBERATAQUES

Los ciberataques cada día van en aumento y resulta más difícil descubrir los asaltos a los que se encuentran expuestas las organizaciones nacionales apresa de que Colombia es el único estado de Latinoamérica que posee un plan de lucha contra de los ciberataques[43]. Todo parece tener un futuro desalentador debido a que las organizaciones solo toman las prevenciones mínimas para protegerse de los ciberataques, pero esto es muy preocupante porque creen que con controlar los remitentes y spam en los correos y cambiar continuamente las claves no los ponen en riegos, pero el acceso al internet hace que estén en permanente peligro. Algunos datos sobre el ciberdelito:

- Los fraudes y robos en las empresas casi siempre son ejecutados desde su interior ya sea por complicidad de algún empleado o descuido.
- Los ciberdelincuentes utilizan las redes sociales para cometer sus actos.
- El usuario es el eslabón más débil dentro de un ciberataque.
- Se ha visto un crecimiento en la seguridad en las compañías de Colombia.
- Se reduce hasta un 70% el riesgo de fraude si se implementa controles de seguridad en dispositivos de cómputo.
- Las nuevas tecnologías mejoran la gestión, pero tiene también grandes riegos de seguridad
- Casi siempre las empresas comerciales y medianas empresas son los que más ataques reciben.
- Los dispositivos móviles traen consigo grandes vulnerabilidades y riesgos.
- Se ha incrementado la fuga de datos.
- 7 de 10 empresas de Colombia han tenido fraude electrónico en el último periodo.

[43] COLOMBIA DIGITAL. Los ciberataques mantienen en jaque a las compañías colombianas. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/8589-los-ciberataques-mantienen-en-jaque-a-las-companias-colombianas.html

Figura 4. Seguridad



Fuente: Camila Trujillo

- Para tener una gestión más eficiente de los riegos de seguridad se debe tener presente lo siguiente:
- Las empresas se deben apoyar de proveedores certificados, reconocidos y que manejen de manera adecuada la información.
- Las compañías deben invertir en plataformas que estén evolucionado constantemente para que en el futuro no sean tan costosas.[44]

7.5. LAS EMPRESAS NO SE PREPARAN BIEN Y EL CIBERCRIMEN SIGUE CRECIENDO

Según un reporte de PWC el cibercrimen es el segundo crimen más notificado y ha afectado casi a un tercio de las empresas en los últimos dos años porque aún no están preparadas para afrontarlo. Las empresas que son atacadas por el cibercrimen presentan grandes pérdidas llegando casi a los 5 millones de dólares y esta modalidad va creciendo porque casi la mayoría de las organizaciones no cuentan con un plan de seguridad. Solo el 37% de las organizaciones cuenta con un plan ante un incidente y aún cuando el 61% son conscientes de los grandes peligros a los que se enfrentan ante este tipo de delito.[45]

[44] COLOMBIA DIGITAL. Los ciberataques mantienen en jaque a las compañías colombianas. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/8589-los-ciberataques-mantienen-en-jaque-a-las-companias-colombianas.html

[45] ELLISON, Kyle. Las empresas no se preparan bien y el cibercrimen sigue creciendo. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.welivesecurity.com/la-es/2016/03/11/empresas-no-se-preparan-cibercrimen/

7.6. EL MODELO DE NEGOCIO DEL CIBERCRIMEN Y SU CADENA DE VALOR

La seguridad ha evolucionado donde los ataques informáticos buscan generar ganancias económicas a los creadores o financiadores por ende el crecimiento y evolución de códigos maliciosos en los que se han visto afectados usuarios y empresas. La ciberdelincuencia cuenta con un modelo de negocio en el que no es necesario tener conocimientos técnicos para realizar un ataque debido a que esta modalidad se ofrece como un servicio en que cualquier persona puede acceder.

Servicios del cibercrimen al mejor postor

Este modelo de negocio ha tenido un gran crecimiento debido a que la oferta responde a la demanda y ha generado grandes ganancias a los desarrolladores de código malicioso porque tiene beneficios económicos con el robo de información y a la expansión de portafolios de servicios ya sea generando afectación a una organización o usuario.[46]

7.7. ORGANIZACIONES COLOMBIANAS SON VULNERABLES A CIBERATAQUES

El 42% de las empresas colombianas no tienen grupo de trabajo dedicado a la ciberseguridad el cual podría monitorear la conducta, amenazas y asaltos de los sistemas de información. La firma de consultoría y servicios profesionales EY indico que las empresas de todo el mundo coinciden que los negocios están en riegos de sufrir un ataque cibernético, debido a la apresurada conectividad que debe tener cada compañía y al incremento de uso de dispositivos que introducen nuevas vulnerabilidades que representan más opciones para los atacantes cibernéticos.

[46] MENDOZA, Miguel Angel. El modelo de negocio del cibercrimen y su cadena de valor. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.welivesecurity.com/la-es/2016/11/03/modelo-de-negocio-del-cibercrimen/

Para el caso de Colombia las compañías invierten menos de 1’000.000 de dólares por año en tácticas para evitar ataques informáticos por esta razón sea incrementado este tipo de delito porque no hay una concientización de la importancia de proteger la información y la de los clientes.[47]

7.8. COLOMBIA Y AMÉRICA LATINA SON LA PREFERENCIA DE LOS CIBERATAQUES

Existe una gran preocupación en la industria de la banca, el retail y el gaming porque se ha multiplicado los eventos masivos de eCommerce en el que se disparan las vulnerabilidades enfrentándose a mayores riegos de ciberataques, también las páginas web están siendo atacadas que se originaron en Estados Unidos por más de 97 millones, seguido por Brasil (19.379.729), Canadá (8.519.773) y México (1.055.756). En cuanto a la seguridad, las organizaciones no se alcanzan a imaginar el precio que puede tener un ciberataque para el negocio, ya que la divulgación de datos y la indisponibilidad de los servicios podría finalizar una marca.

Colombia se mantiene alerta

Muchos gobiernos están tomando acciones frente a esta nueva problemática, en el caso de Colombia ha incrementado el presupuesto el cual destinará casi treinta millones de dólares para fortalecer la ciberseguridad, el cual sería el primer país del mundo en implementar las recomendaciones de la Organización para la Cooperación y el Desarrollo Económico. Una de las medidas que tomo el Gobierno colombiano fue actualizar las políticas de ciberseguridad y ejecuto nuevas disposiciones para afrontar el crimen digital con herramientas más modernas.[48]

[47] COLOMBIA DIGITAL. Estudio de EY: Organizaciones colombianas son vulnerables a ciberataques. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://colombiadigital.net/actualidad/bytes/item/10031-estudio-de-ey-organizaciones-colombianas-son-vulnerables-a-ciberataques.html

[48] COLOMBIA DIGITAL. Colombia y América Latina en el radar de los ciberataques. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://colombiadigital.net/actualidad/bytes/item/9717-colombia-y-america-latina-en-el-radar-de-los-ciberataques.html

7.9. AMENAZAS DEL CIBERCRIMEN EN COLOMBIA

En los últimos tres años se han recibido 15.565 incidentes informáticos. Se identificaron los delitos informáticos más comunes en Colombia que han afectado las organizaciones de tal manera que algunas han quedado en la bancarrota por el gran impacto generado a la información y la falta de credibilidad por parte de los clientes.

- Se ha aumentado el cibercrimen en las empresas debido a que representa mayor rentabilidad la actividad criminal en comparación a un usuario común.
- Las plataformas de comercio electrónico son utilizadas para estafar por medio de phishing.
- Los ciberdelincuentes encontraron la manera de utilizar las plataformas del gobierno para difundir malware y robar información.[49]

7.10. EN COLOMBIA INCREMENTA CIFRAS DE CIBERCRIMEN POR EL ALTO ACCESO A INTERNET

Bogotá, Cali, Medellín, Barranquilla, Cartagena y Bucaramanga reúnen 74% del cibercrimen en Colombia porque tienen mayor acceso al internet. Ya son casi 12.000 denuncias como robo por medios informáticos y violación de datos personales. A pesar de este incremento Colombia es el segundo país de América Latina con un gran número de certificados de seguridad para páginas web, con estándares altos de confiabilidad. También Certicámara SA, en los últimos años ha generado más de doce mil certificados SSL/TLS.[50]

[49] POLICIA NACIONAL. Informe: Amenazas del Cibercrimen en Colombia 2016-2017. {En línea}. {Consultado diciembre 9 de 2018}. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

[50] COLOMBIA DIGITAL. Alto acceso a Internet en Colombia incrementa cifras de Cibercrimen {En línea}. {Consultado diciembre 9 de 2018}. Disponible en: https://colombiadigital.net/actualidad/analisis/item/10102-alto-acceso-a-internet-en-colombia-incrementa-cifras-de-cibercrimen.html

8. ANTECEDENTES DEL CIBERCRIMEN

8.1. ATAQUE A YAHOO

Fue un ataque dirigido, el acceso de Yahoo con cuatro acusados. Alexsey Belan ya se encontraba en la lista negra de los crackers más buscados del planeta que realizo la labor de reconocimiento una vez dentro de este gigante de internet, en la exploración se descubrió dos activos importantes para la organización: la base de datos de usuarios de Yahoo (UDB) y una herramienta conocida como Account Management Tool. Los contenidos de la base de datos brindaron a Belan y a dos agentes de la inteligencia rusa información que podían utilizar para ubicar determinadas cuentas de su interés y la segunda herramienta podía modificar cualquier cuenta objetivo hasta la contraseña.

También descubrieron una herramienta que falsificaba las cookies para tener acceso a las cuentas sin tener que cambiar las contraseñas. Al parecer, cada usuario en la base de datos contenía un número criptográfico relacionado con la cuenta, que se usó para generar las cookies posteriores a la autenticación.

Las cookies se falsificaron en dos fases: la primera al interior de la red de Yahoo, y después en sistemas que controlaban. Por medio de esta técnica lograron crear cookies definidas para acceder a cuentas objetivo. El grupo de atacantes logro generar cookies externas, es decir sin entrar a la red interna de la organización cuando Belan copio parte de la base de datos en su propio ordenador por medio de un FTP. Este plan tuvo un fallo porque los números criptográficos se modificaban cuando los usuarios cambiaban las contraseñas entonces las cookies creadas externamente fallaban con las nuevas claves. Las cookies que no funcionaron permanecieron en los registros de los sistemas de Yahoo, lo que los llevo a detener el ataque.[51]

[51] AGUDO, Sergio. El FBI explica cómo fue hackeado Yahoo: mediante un ataque de spear phishing {En línea}. {Consultado junio 23 de 2019}. Disponible en: https://www.genbeta.com/seguridad/el-fbi-explica-como-fue-hackeado-yahoo-mediante-un-ataque-de-spear-phishing

8.2. ATAQUE A SONY

Según el FBI Corea del Norte estuvo detrás del hackeo de Sony. Expertos seguridad, hackers, personas familiarizadas con las redes y un examen muy detallado concluyeron que cualquiera hubiera podido realizar el ataque: un empelado insatisfecho de Sony, piratas informáticos con deseo de tener dinero, Corea del Norte o la combinación de los tres. A continuación, se listarán una serie de hechos sobre este ataque:

- Se utilizaron servidores en Bolivia, Chipre, Italia, Polonia, Singapur, Tailandia y Estados Unidos para el ataque.
- Según el FBI las direcciones IP que se asociaron a los servidores en este ataque anteriormente fueron relacionadas con Corea del Norte.
- Según el FBI el malware que se utilizó tenía líneas de código y métodos de eliminación de datos parecidos al código malicioso utilizado por agentes norcoreanos.
- Según el FBI en 2013 se utilizó un software de eliminación informática contra bancos y medios de prensa de Corea del Sur, este mismo se utilizó en Sony.
- El programa malicioso tenía idioma coreano.
- A Sony Pictures le exigieron que eliminara la película La Entrevista para evitar inicios de guerra.

Por estos hechos el gobierno de EEUU acuso a Corea del Norte de atacar a Sony Pictures, pero muchos expertos no están tan convencidos porque las pruebas técnicas realizados indican que cualquiera hubiera podido hackear servidores y en el mundo de la programación los códigos se comparten y configurar el idioma que se desee.[52]

[52] VALDERRAMA, Álvaro. ¿Quién causó realmente el ataque a Sony? {En línea}. {Consultado junio 23 de 2019}. Disponible en: https://cnnespanol.cnn.com/2014/12/25/quien-causo-realmente-el-ataque-a-sony/

8.3. ATAQUE A TELEFONICA

El 12 de mayo de 2017 la empresa española Telefónica fue hackeada por un ataque masivo de ransomware aprovechando una vulnerabilidad en Windows y ejecutado tras abrir un link enviado por medio de un correo electrónico por parte de un empleado de la organización a partir de ahí se propagó por toda la red.

Aun no sea conformado el origen de la infección, pero varias fuentes indican que proviene de China y si las compañías afectadas quieren recuperar la información deben pagar una suma de dinero representada en bitcoins. Este ataque informático paralizo parte de la red de Telefónica y muchos empleados no lograron realizar las actividades cotidianas. Se ordenó apagar todos los equipos, incluidos colaboradores externos de la organización que se conectan por medio de VPN. Muchos equipos han mostrado pantallas azules y errores a causa de la desconexión de la red, mientras que otros han mostrado mensajes e imágenes en referencia al rescate.

Telefónica fue la más afectada por este código malicioso que encripta la información, cerca de un 85% de los equipos fueron afectados por el gusano informático, que es una versión de WannaCry y utilizo una vulnerabilidad de ejecución de comandos remota a través de SMB.[53]

[53] TOLEDANO, Bruno. Hackean la red interna de Telefónica y de otras grandes empresas españolas. {En línea}. {Consultado junio 25 de 2019}. Disponible en: https://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html

9. ESTRATEGIAS UTILIZADAS POR LOS CIBERDELINCUENTES PARA VULNERAR LA SEGURIDAD

9.1. ATAQUES MASIVOS DE VIRUS INFORMÁTICOS

Con el objetivo de cometer cibercrímenes de todo tipo tales como robo de datos, generación de ingresos o reclamación de pagos a cambio de información hurtada, los criminales informáticos crean y propagan gusanos de red causando grandes daños infectando a millones de dispositivos en Internet. El cibercriminal en la función obtener lo deseado, modifican la forma en que se expanden los virus informáticos. Algunos gusanos de los más conocidos son:

- Mydoom
- Bagle
- Warezov (enfocado al e-mail)
- Limitación de la propagación del ataque de un virus informático

Al contrario de lo que se pensaría, algunos cibercriminales optan por limitar la cantidad de dispositivos que infectan, evitando así llamar la atención de la ley u organismos de control; en vez de infectar la mayor cantidad posible de usuarios, al actuar de esta forma, el cibercriminal puede decidir acceder a un sitio que haya sido infectado. Monitoreando este sitio web será más fácil definir la cantidad máxima de equipos que serán el objetivo del virus logrando así un ataque de manera más controlada y metódica.[54]

9.2. LOS CIBERDELINCUENTES SE ESFUERZAN POR MEJORAR

En el primer trimestre de 2018, McAfee Labs registró una media de cinco nuevas muestras de malware por segundo, frente a las ocho muestras nuevas por

[54] KARPERSKY LAB. Evolución de los métodos de distribución de los virus informáticos y el malware. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://latam.kaspersky.com/resource-center/threats/virus-delivery-methods

segundo del 4.º trimestre. A pesar del descenso del 31 % de un trimestre a otro, durante el primer trimestre se observaron importantes avances técnicos entre los ciberdelincuentes que buscan mejorar las últimas tecnologías y tácticas que funcionan con éxito, con el fin de vencer a las defensas de los objetivos.

De PowerShell a LNK: en 2017 se evidencio un aumento en la explotación de tecnologías inofensivas para fines maliciosos, como PowerShell. En el primer trimestre de 2018, los ciberdelincuentes se alejaron de los exploits de PowerShell, que descendieron un 77 %, en favor de las funciones de LNK. El nuevo malware basado en LNK aumentó un 59 % durante el primer trimestre.

De Locky a Gandcrab: la actividad del ransomware Gandcrab también demostró agilidad técnica. Aunque el crecimiento general del nuevo ransomware se ralentizó un 32 % en el primer trimestre, Gandcrab infectó 50 000 sistemas durante las tres primeras semanas del trimestre, sustituyendo a las variantes del ransomware Locky como líder del trimestre en esta categoría. Gandcrab utiliza nuevos métodos delictivos, como realizar el pago de rescates a través de la criptomoneda Dash, en lugar de bitcoins.

Criptojacking —infectar y recaudar: las criptomonedas también siguieron dibujando el panorama de ciberamenazas durante el primer trimestre, ya que los ciberdelincuentes ampliaron la actividad al criptojacking, la infección de los sistemas de los usuarios con el fin de secuestrarlos y utilizarlos para minería de criptomonedas.

El malware minero de monedas aumentó un impresionante 629 % hasta los más de 2,9 millones de muestras conocidas en el primer trimestre, desde las casi 400 000 muestras del 4.º trimestre. Esto sugiere que los ciberdelincuentes se preparan ante la perspectiva de convertir en dinero las infecciones de los sistemas de los usuarios, sin pedir a las víctimas que realicen pagos, como en el caso de conocidos ataques de ransomware. Comparado con otras actividades de ciberdelincuencia bien consolidadas, como el robo de datos y el ransomware,

el criptjacking es más simple, más directo y menos arriesgado. Lo único que tienen que hacer los ciberdelincuentes es infectar millones de sistemas y empezar a rentabilizar el ataque mediante la minería de criptomonedas en los sistemas de las víctimas. Sin intermediarios, sin tramas fraudulentas, sin víctimas a las que pedir un rescate y que podrían hacer una copia de seguridad de los sistemas de antemano y negarse a pagar.[55]

9.3. AUMENTAR LA EFICACIA EN ATAQUES

Cisco, en colaboración con Level 3 Threat Reserch Labs y con Limestone Networks, detectaron y aislaron la más grande operación del kit de aprovechamiento de vulnerabilidades Angler en EE. UU, que afectaba diariamente a 90.000 víctimas y generándole a los autores millones de dólares anualmente.

SSHPsychos una de las botnets de denegación de servicio distribuida (conocida por sus siglas DDoS) fue debilitada drásticamente al ser identificada por cisco y sus colaboradores; lo que destaca la importancia de la colaboración entre compañías para solventar estos problemas. Otros botnets muy conocidos identificados por cisco son: Bedep, Gamarue y Miuref.

Una de las fuentes de filtración de datos de las empresas más ampliamente explotada por los cibercriminales son las extensiones maliciosas de navegador, dicha vulnerabilidad se ha identificado en el 85% de organizaciones, los atacantes también se han estado aprovechando de vulnerabilidades ya conocidas como las que presenta Adobe Flash o atacando Webs expuestas como por ejemplo las desarrolladas en WordPress.

Análisis de Cisco concluyeron que la mayoría de malware (91,3%) utiliza DNS, usando lo que se llama la investigación retrospectiva de consultas. Estos análisis

[55] MCAFEE LAB. Informe de McAfee Labs sobre amenazas. {En línea}. {Consultado diciembre 9 de 2018}. Disponible en: https://www.mcafee.com/enterprise/es-es/assets/reports/rp-quarterly-threats-jun-2018.pdf

llevaron a cisco a descubrir resolvers (Usuarios DNS maliciosos) teniendo a los clientes en total desconocimiento del uso de resolvers por parte de los empleados.

En otros tipos de análisis más enfocados a analizar tendencias se observa que el tráfico cifrado HTTPS será en un futuro el dominante de tráfico en la red, aunque dicho cifrado protege a los clientes de ataques, también dificulta la eficacia de las medidas de seguridad en cuanto al monitoreo de amenazas, infraestructuras obsoletas aumentan las vulnerabilidades en las organizaciones, tras analizar 115000 dispositivos Cisco en funcionamiento se descubrió que de estos:

- 92% ejecutaban software con vulnerabilidades ya conocidas por los cibercriminales.
- 31% ya no se comercializan.
- 8% alcanzaron su ciclo de vida útil.

Lo que en 2015 llevo a los ejecutivos de cisco encargados de la seguridad a desconfiar en menor medida en las herramientas y procesos a comparación del año inmediatamente anterior. Pasando del 64% en 2014 al 59% en 2015 de organizaciones que consideraron su infraestructura de seguridad actualizada.

Este análisis también mostro que las PYMES utilizan menos medidas de seguridad que las grandes organizaciones. Principalmente se observaron dos disminuciones preocupantes entre el año 2014 y 2015 en las pequeñas y medianas empresas lo que lleva a una mayor vulnerabilidad de clientes facilitando ataques informáticos.

- El uso de seguridad web paso del 59% al 48%.
- El uso de herramientas de parches y configuración del 39% al 29%.

Los diferentes estudios y análisis llevados a cabo por Cisco año tras año le han permitido reducir el tiempo de detección de amenazas conocidas (TTD) de 17 horas en 2015 a una mediana TTD de 4.6 horas para el 2017. Mejora que también se atribuye al uso de la seguridad basada en la nube.[56]

9.4. TIPOS DE CIBERCRIMEN

9.4.1. Phishing

Reside en el envío de email electrónicos que, parecieran provenir de fuentes confiables como entidades bancarias, intentando sacar datos privados del usuario, que después son utilizados para algún tipo de fraude. Esto puede incluir un link que, al ser cliqueado, lleva a páginas web falsas. Es así como, el usuario, cree estar en un sitio confiable, ingresa la información requerida que, en realidad, va para el estafador.

Figura 5. Phishing

Fuente: https://www.pandasecurity.com/es/security-info/cybercrime/phishing/

[56] CISCO. Cisco 2016 Informe anual de seguridad. {En línea}. {Consultado diciembre 8 de 2018}. Disponible en: https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

El phishing causa:

- Robar la identidad y los datos personales de los usuarios. Puede llevar a pérdidas económicas para los usuarios o incluido llegar a perder el acceso a sus cuentas.
- Pérdida de producción en una organización.
- Gasto de recursos de las redes de una organización (saturación de canales de internet, saturación del correo, etc.).

El componente más utilizado generalmente es la creación de un email electrónico falso que aparente proceder de una compañía de confianza, para engañar a los clientes. Este mensaje tendrá vínculos que direccionan a una o varias páginas web que son iguales en todo o en parte el aspecto y funcionalidad de la empresa, y se busca que el receptor mantenga una relación comercial. La relación entre spam y phishing, pareciera claro que esta clase de mensajes de distribución intensiva puede ser una mejor forma de atracción utilizada por los ciberdelincuentes. Es más, una de las técnicas más utilizadas de contacto para la comisión de delitos informáticos es el email.

Pero, el medio de contacto para llevar estos delitos no se limita únicamente al email, sino que también es posible generar ataques de phishing por medio de mensajes de texto, conocido como smishing, o de telefonía IP, distinguido como vishing. En el smishing a el usuario le llega un SMS pretendiendo convencerle de que visite un enlace falso. En el vishing el usuario contesta una llamada telefónica que presume proceder de una entidad financiera pidiendo verificar una serie de datos.[57]

9.4.2. Spear Phishing

Es una estafa focalizada por email con el único propósito es tener acceso no autorizado a datos personales. A diferencia de las técnicas por phishing que se

[57] PANDA SECURITY. Phishing. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.pandasecurity.com/es/security-info/cybercrime/phishing/

centran en un grupo u organización puntual, el objetivo es hurtar propiedad intelectual, datos bancarios, secretos organizaciones o militar y otros datos sensibles.[58]

El cibercriminal le mientes a un empleado con privilegios a información financiera para que ejecute una transferencia a una cuenta que cree que es de un cliente o proveedor, pero la plata termina en la cuenta bancaria de la organización delincuencial. Pero ¿cómo son burlados? La organización detrás de estos ataques es muy compleja. No son los antiguos correos de estafa que contienen errores de gramática y ortografía, mezcla de idiomas o historias exageradas, sino que generan emails completamente profesionales. Por esto, los criminales ejecutan técnicas como el spear-phishing, el robo de identidad, la ingeniería social o el uso de programas malignos. Ellos continúan buscando métodos más avanzados que pasen desapercibidas para realizar estas acciones engañosas, ya que el regreso de la inversión es enorme.[59]

9.4.3. Virus Informáticos

Es un programa con fines maliciosos que ingresa a un computador, sin permiso o sin juicio de su usuario, para modificar su funcionamiento y, exclusivamente, con el fin de alterar o dañar el sistema. Por regla general, se añaden a un archivo ejecutable, quedando la terminal infectada cuando se ejecute tal archivo. Las aplicaciones malignas, por otro lado, causan daños en los dispositivos, tanto en el hardware, como, en el software. En el primer caso, un virus puede afectar las unidades de disco duro minimizando su rendimiento y efectividad, calentar el microordenador o lesionar el sistema básico de la BIOS, entre otros problemas, en relación al software, estos programas maliciosos llegan a modificar y eliminar aplicativos y registros, disminuye el funcionamiento del sistema operativo, hurta

[58] INFOLAFT. Lo que debe saber sobre el cibercrimen en Colombia. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

[59] PANDA SECURITY. Las estafas BEC causan las mayores pérdidas económicas en empresas. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/estafas-bec/

información sensible y datos del usuario o afectar los canales de internet, a continuación, se muestran los métodos y sitios virtuales de contagio más comunes:

- Para los desarrolladores de amenazas las redes sociales se han convertido en un campo ideal para su ejecución.
- Los sitios web falsos; no obstante, también existen los que, pese a ser legales, se hallan infectados.
- Las descargas con obsequio pueden tener un virus en la instalación, porque en muchas ocasiones, en los mensajes como “Haz clic y ganas mil euros” se puede ocultar la ejecución de un programa malicioso.
- El ingreso de dispositivos que están infectados, como USB, CD o DVD.
- Abrir archivos adjuntos que estén en el correo no deseado, también es distinguido como spam.

9.4.3.1. Tipos

- Boot´s
  Son programas que perjudican al sector de arranque del PC y al inicio del del sistema operativo. Por ende, la amenaza se inicia cuando se enciende el ordenador.
- Bombas lógicas o de tiempo
  Son virus que se inician cuando se produce una acción puntual, como la llegada de una fecha puntual o la mezcla de teclas puntuales por parte del usuario sin que éste lo conozca.
- Virus de enlace
  Estos programas modifican las direcciones de acceso de los archivos y, el resultado es impedir la ubicación de documentos guardados.
- Virus de sobreescritura.

Son programas que sobrescriben el contenido de algunos documentos, causando la pérdida de la información original.[60]

9.4.4. Malware

Es un aplicativo malicioso o programa informático creado para contaminar una terminal de un usuario legítimo y dañarla de diferentes formas. El programa maligno puede contagiar computadoras y dispositivos de muchas maneras y se presenta en varias formas, algunas son virus, gusanos, troyanos, spyware y más, es esencial que todos los usuarios puedan reconocer y protegerse del malware en todos sus tipos. El programa maligno puede mostrarse a través de diversos comportamientos:[61]

- El PC se torna lento. Los principales efectos de un programa maligno es disminuir la velocidad del sistema operativo, tanto en su navegación por Internet como las aplicaciones utilizadas localmente.
- El equipo se llena de mucha publicidad molesta que no tendría que estar ahí. Las noticias emergentes de improviso son un signo característico de una infección por un programa maligno.
- Se bloquea constantemente el sistema o sale una pantalla azul, que pareciera cuando un sistema Windows encuentra un error crítico.
- El equipo este teniendo una pérdida misteriosa de espacio libre en el disco, seguramente lo esté ocupando un indeseado malware que se esconde en el disco duro.
- Se genera un aumento insólito en la actividad del sistema en Internet o navegación.
- La utilización elevada anómala de recursos del sistema y el cooler del equipo empieza a trabajar a toda velocidad, esto señala que la actividad

[60] VALOR TOP. ¿Qué es un virus informático? Definición y tipos. {En línea}. {Consultado abril 22 de 2019}. Disponible en: http://www.valortop.com/blog/virus-informatico-definicion-tipos
[61] KASPERSKY LAB. Más información sobre el malware y cómo proteger todos tus dispositivos. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

del programa maligno se ha adueñado de los recursos del sistema en segundo plano.

- El navegador cambia sin permiso la página de inicio. De igual manera, los links en los que hace clic lo llevan a un destino web no conocido.
- Las barras del navegador se llenan repentinamente al igual que las extensiones o complementos.
- El antivirus deja de funcionar y no se puede actualizar, dejando desprotegido el computador contra el malware que lo deshabilitó.
- Se puede producir un ataque de malware perjudicial e intencional para dañar la infraestructura.[62]

9.4.5. Ransomware

Es un malware que infecta los equipos en busca de bloquear los datos que se almacenan en estos dispositivos con el fin de generar un cobro para la recuperación de esta. Los ataques más peligrosos que ha ocasionado el ransomware han sido WannaCry, Petya, Cerber, Cryptolocker y Locky. Lo diseñaron estafadores con un alto conocimiento en programación informática.
Puede ingresar en la computadora mediante un adjunto de email o por medio de un navegador si se consultan páginas web infectadas con este tipo de malware, también puede ingresar atreves de la red.[63]

Cada día es más popular el ransomware a nivel mundial. Pero, los mensajes de recuperación y métodos para obtener dinero pueden cambiar según las regiones, dadas a las prioridades y cultura de las organizaciones para enfrentar este tipo de situaciones, por ejemplo:

- Notificaciones falsas sobre aplicaciones sin licencia

[62] MALWARE BYTES. Malware. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://es.malwarebytes.com/malware/
[63] AVAST. Ransomware. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.avast.com/es-es/c-ransomware

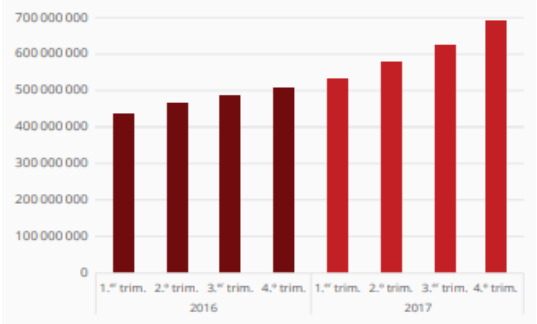
Los troyanos continuamente afirman haber identificado aplicaciones sin licencia ejecutándose en la máquina de la víctima y exigiendo un pago, esto se presenta en algunos países.

- Falsas reclamaciones sobre contenido ilegal

  La piratería de software en algunos países es mínima por ende el cibercriminal no tiene enfoque a este tipo de delito. En reemplazo, el mensaje procedente de ransomware puede fingir que proviene de las fuerzas de seguridad y aseverar que ha encontrado pornografía infantil u otro contenido ilegal en la PC. El mensaje va acompañado de la exigencia de pago de una multa.[64]

A continuación, se muestra el crecimiento de ataques por ransomware entre los años 2016 y 2017 debido a las vulnerabilidades presentadas en las empresas por la falta de conciencia ante la importancia de la seguridad de la información ya que se mira más un gasto que una inversión por la adquisición de herramientas licenciadas y mejoras en la infraestructura.

Figura 6. Ransomware



Fuente. Mcafee Lab[65]

Esta imagen muestra el crecimiento que ha tenido el código malicioso Ransonware en el que ha afectado un gran número de organizaciones en todo

[64] KASPERSKY LAB. Ransomware: definición, prevención y eliminación. . {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://latam.kaspersky.com/resource-center/threats/ransomware

[65] MCAFEE. Informe de McAfee Labs sobre amenazas {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/reports/rp-quarterly-threats-mar-2018.pdf

el mundo, incluyendo gubernamentales, hospitales y tecnología en los cuatro trimestres entre los años 2016 y 2017 pasando de 450 000 000 a 700 000 000 ataques en tan solo 2 años.

¿Cómo evitar el Ransomware?

- Tener nuestro sistema operativo parchado.
- Instalar productos licenciados.
- No abrir correos de remitente desconocidos.
- No navegar por paginas inseguras.
- Tener backup de nuestra información.[66]

[66] PANDA SECURITY. ¿Qué es un Ransomware? {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

10. RECOMENDACIONES PARA MEJORAR LA SEGURIDAD INFORMÁTICA

10.1. SEGURIDAD PARA REDES EMPRESARIALES - LA RED COMO SENSOR

10.1.1. La Visibilidad que Necesita en Toda su Red

Cisco ofrece las herramientas que necesita para detectar flujos de tráfico sospechosos, infracciones a las políticas y dispositivos comprometidos en el entorno. ¿Sabe qué sucede en la red? No puede proteger lo que no puede ver, con las soluciones de Cisco, muchas de las tecnologías que necesita ya están integradas en la red, listas para ser activadas.

NetFlow: rastrear cada conversación
Cisco IOS Flexible NetFlow es una potente tecnología que le otorga la visibilidad que necesita para las actividades de la red. Registra cada conversación Cada registro NetFlow identifica la fuente, el destino, la hora y el protocolo, de manera muy similar a cómo la cuenta telefónica resume las actividades de llamadas. Se puede ver quiénes participaron en la conversación, dónde se produjo y cuánto duró.

Los datos de NetFlow pueden utilizarse como fuente de información de seguridad para supervisar comportamientos anormales y actividades que vulneran la seguridad. Proporciona evidencia forense para reconstruir una secuencia de eventos y puede utilizarse para ayudar a cumplir los requisitos normativos. Ayuda a proporcionar visibilidad durante toda la secuencia de ataque.

Casos de uso

- Detecta actividades de reconocimiento en la red que los atacantes inician para explorar puertos TCP y UDP en múltiples hosts.

- Vea los patrones cuando un host interno comprometido habla con un servidor de control y comando (C&C) externo.
- Reconozca el tráfico anormal cuando un host envía fragmentos deformes en ataques.
- Descubra exfiltración de datos, si se producen grandes transferencias salientes de archivos superiores al funcionamiento normal de una red.

Puede utilizar NetFlow en muchos otros casos de uso. Lo mejor de todo, NetFlow está integrado en la mayoría de los dispositivos basados en Cisco IOS que ya tiene, como routers, switches y controladores de redes LAN inalámbricas, NetFlow es el corazón del enfoque de la "red como sensor" de Cisco, que le otorga una profunda y amplia visibilidad.

Lancope StealthWatch con inteligencia contra amenazas

El sistema Lancope StealthWatch utiliza datos de NetFlow para ayudar a las organizaciones a detectar comportamientos vinculados con una amplia gama de ataques, incluidas amenazas avanzadas persistentes (APT), ataques distribuidos de denegación de servicio (DDoS) y amenazas internas. Entre los beneficios, StealthWatch:

- Le ayuda a analizar pruebas de auditoría de red integrales y a acelerar el análisis de causa raíz
- Proporciona inteligencia contra amenazas para acelerar la respuesta a incidentes y reducir el riesgo empresarial.
- Lo alerta para que vea, se prepare y responda al contexto completo de una amenaza potencial
- Mejor visibilidad e inteligencia contextual contra amenazas

Cisco Identity Services Engine (ISE) ofrece mejor visibilidad e información contextual sobre las actividades de la red. Ayuda a acelerar la identificación de amenazas al compartir datos contextuales de NetFlow e ISE con Lancope StealthWatch. Puede pasar de la asignación de direcciones IP a comprender los

vectores de amenaza basado en quién, qué, dónde, cuándo y cómo los usuarios y dispositivos se conectan y cómo acceden a los recursos de la red. El uso de la infraestructura de red de Cisco como sensor de seguridad le otorga una solución poderosa y escalable para obtener una profunda visibilidad, control y análisis.[67]

10.2. LOS 5 COMPAÑEROS QUE SE NECESITAN PARA GANAR EL PARTIDO CONTRA LAS AMENAZAS INFORMÁTICAS

1 – El esfuerzo realizado a tiempo puede prevenir más trabajo en el futuro

Debido al incremento de ataques con WannaCryptor y el ataque de Equifax es importante configurar todos dispositivos hogareños de modo que realicen actualizaciones de manera automática para proteger la información sensible, no está demás que el usuario sea consciente de no divulgar datos personales a cualquier desconocido o portal web.

2 – Recortar el equipo

Para evitar ser atacados por los ciberdelincuentes se debe identificar que programas ya no se utilizan o cuales presentan vulnerabilidades en código fuente o características porque es mejor desinstalarlo y así mismo bajar los puertos de servicios para disminuir los peligros y ser objetivo de algún pirata cibernéticos con fines lucrativos.

3 – Practicar el uso de contraseñas fuertes

La mejor forma de proteger la privacidad en línea es generando contraseñas robustas las cuales deben ser largas, con caracteres especiales y que no tengan nada que ver con la vida cotidiana de esta forma será muy difícil casi imposible que un ciberdelincuente adivine una contraseña o sea adivinada en un ataque de diccionario o fuerza bruta.

[67] CISCO. Seguridad para redes empresariales - La red como sensor. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.cisco.com/c/es_mx/solutions/enterprise-networks/enterprise-network-security/net-sensor.html

4 – Observar antes de saltar

Hoy en día la ingeniera social le facilita al ciberdelincuente obtener información valiosa como contraseñas, por eso se debe ser muy cuidadoso a la hora de dar un clic porque puede ser una página falsa creada por el delincuente para obtener dicha información, así como ser muy precavidos con los correos que llegan a la bandeja de entrada.

5 – Añadir un factor

Se recomienda tener dos autenticaciones especialmente en las cuentas que contiene información y datos personales, así por más que un ciberdelincuente tenga la contraseña principal se encontrara con otra barrera que es la segunda contraseña que también debe ser robusta con mayúsculas, minúsculas alfanumérica y con caracteres especiales.[68]

10.3. COMO PREVENIR EL CIBERCRIMEN

- Usar algún conjunto de aplicaciones de seguridad en Internet que ofrezca un servicio completo, para asegurar la protección de un virus, y otras amenazas procedentes de Internet.
- Usar contraseñas robustas, no repetirlas y cambiarlas constantemente, se puede apoyar en aplicaciones que administran las contraseñas para mayor protección.
- Tener todo el software actualizado. Es importante tener actualizado el sistema operativo y el software de seguridad en Internet. Los hackers usan los puntos débiles conocidos en el software para obtener ingreso al sistema. Emplear parches a esos puntos vulnerables disminuye la probabilidad de ser una víctima.
- Administrar la configuración de las redes sociales para mantener protegida la mayoría de la información privada y personal. Los cibercriminales que usan ingeniería social normalmente pueden obtener

[68] CIBERSEGURIDAD LATAM. Los 5 compañeros que se necesitan para ganar el partido contra las amenazas informáticas. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.ciberseguridadlatam.com/2018/06/27/los-11-companeros-que-se-necesitan-para-ganar-el-partido-contra-las-amenazas-informaticas/

información personal con solo algunos puntos de referencia. Por eso, cuanta menos información se comparta en Internet, mejor.

- Tener el conocimiento sobre las brechas de seguridad más importantes, si tiene una cuenta en un sitio en el que se produjo una brecha de seguridad, investigar qué información obtuvieron los hackers y cambiar la contraseña inmediatamente.
- Si se cree víctima de un cibercrimen: alertar a la policía porque de esta forma, evitara que los criminales se aprovechen de otras personas en el futuro.[69]

10.4. TIPS PARA EVITAR EL PHISHING

- Dudar de aquellos mensajes alojados en la Bandeja de Spam y que además le soliciten información confidencial.
- Comprobar cuando un mensaje redireccione a la página Web de la empresa emisora, verificar que la dirección de dominio concuerde con el de la empresa, tener en cuenta que para identificar las páginas Web seguras, se debe observar en la dirección del dominio que el sufijo sea https y no simplemente http.
- Es claro, que gracias al desarrollo de la tecnología cada vez es más común realizar compras sin salir de casa, por ello es necesario que, al usar estos servicios, los usuarios tengan los cuidados pertinentes para evitar ser víctimas de cualquier tipo de fraude.
- Si hay dudas sobre la legitimidad de un correo comunicarse a la compañía a través de un número reconocido y no de los que tiene incluido el mismo mensaje; con esto se tendrá más seguridad de la legalidad de la información y de la plataforma.[70]

[69] NORTON. De qué manera distinguir el cibercrimen y protegerse. {En línea}. {Consultado abril 23 de 2019}. Disponible en: https://mx.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

[70] ARBOLEDA MARIN, Melissa. Phishing. {En línea}. {Consultado abril 23 de 2019}. Disponible en: https://www.exus.com.co/es/no-seas-victima-de-estafas-ciberneticas-BA25

11. CONCLUSIONES

Se evidencia que con el trascurrir del tiempo las modalidades del cibercrimen han avanzado en el que el atacante ha creado nuevas técnicas y herramientas para vulnerar la seguridad de las pymes y medianas empresas estando en gran riesgo de una quiebra eminente por la poca importancia que le dan seguridad informática.

Hoy en día desde un correo hasta una llamada telefónica puede ser la estrategia que lleva el ciberdelincuente para acceder a la información sensible o confidencial. Por eso se deben tomar medidas preventivas al momento de dar información como nunca dar clic a los enlaces que llegan de un correo porque puede apuntar a una página falsa con las mismas características de una página bancaria.

Estableciendo unas políticas de seguridad y buenas prácticas además de concientizar al usuario que es el eslabón más débil en este ámbito una pyme y mediana empresa puede reducir la probabilidad de ser atacada por un cibercriminal. Internet ofrece herramientas y cursos gratuitos provenientes de fuentes confiables que pueden ser un aliado para la protección de estas organizaciones.

12. REFERENCIAS BIBLIOGRAFICAS

AGUDO, Sergio. El FBI explica cómo fue hackeado Yahoo: mediante un ataque de spear phishing {En línea}. {Consultado junio 23 de 2019}. Disponible en: https://www.genbeta.com/seguridad/el-fbi-explica-como-fue-hackeado-yahoo-mediante-un-ataque-de-spear-phishing

ARBOLEDA MARIN, Melissa. Phishing. {En línea}. {Consultado abril 23 de 2019}. Disponible en: https://www.exus.com.co/es/no-seas-victima-de-estafas-ciberneticas-BA25

AVAST. Ransomware. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.avast.com/es-es/c-ransomware

BENITEZ, Albert. ¿Qué es Wanna Cry y cómo evitarlo? {En línea}. {Consultado octubre 21 2018}. Disponible en: https://xpertix.com/que-es-wanna-cry-y-como-evitarlo/

CIBERSEGURIDAD LATAM. Los 5 compañeros que se necesitan para ganar el partido contra las amenazas informáticas. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.ciberseguridadlatam.com/2018/06/27/los-11-companeros-que-se-necesitan-para-ganar-el-partido-contra-las-amenazas-informaticas/

CIBERSEGURIDAD LATAM. PyMEs de América latina, más expuestas a ciberataques {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.ciberseguridadlatam.com/2018/04/27/pymes-de-america-latina-mas-expuestas-a-ciberataques/

CISCO. Cisco 2016 Informe anual de seguridad. {En línea}. {Consultado diciembre 8 de 2018}. Disponible en: https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

CISCO. Seguridad para redes empresariales - La red como sensor. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.cisco.com/c/es_mx/solutions/enterprise-networks/enterprise-network-security/net-sensor.html

COLOMBIA DIGITAL. Alto acceso a Internet en Colombia incrementa cifras de Cibercrimen {En línea}. {Consultado diciembre 9 de 2018}. Disponible en: https://colombiadigital.net/actualidad/analisis/item/10102-alto-acceso-a-internet-en-colombia-incrementa-cifras-de-cibercrimen.html

COLOMBIA DIGITAL. Colombia y América Latina en el radar de los ciberataques. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://colombiadigital.net/actualidad/bytes/item/9717-colombia-y-america-latina-en-el-radar-de-los-ciberataques.html

COLOMBIA DIGITAL. Estudio de EY: Organizaciones colombianas son vulnerables a ciberataques. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://colombiadigital.net/actualidad/bytes/item/10031-estudio-de-ey-organizaciones-colombianas-son-vulnerables-a-ciberataques.html

COLOMBIA DIGITAL. Los ciberataques mantienen en jaque a las compañías colombianas. {En línea}. {Consultado noviembre 01 2018}. Disponible en:

https://colombiadigital.net/actualidad/articulos-informativos/item/8589-los-ciberataques-mantienen-en-jaque-a-las-companias-colombianas.html

CONCEPTODEFINICION. Definición de Mediana Empresa. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://conceptodefinicion.de/mediana-empresa/

CONCEPTO. Servicio. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://concepto.de/servicio/

CONSULTHINK. Qué es y en qué consiste un ataque informático. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://www.consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/

DEBITOOR. ¿Qué es una empresa? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://debitoor.es/glosario/definicion-empresa

DEFINICION. Concepto de Seguridad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/seguridad/

DEFINICION. Confidencialidad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/confidencialidad/

DEFINICION. Definición de Prioridad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/prioridad/

DEFINICION. Eficacia: {En línea}. {Consultado 14 de mayo de 2019}. Disponible en: https://definicion.de/eficacia/

DEFINICION. Prevención. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://definicion.de/prevencion/

DEFINICION ABC. Cisco. {En línea}. {Consultado 17 de octubre de 2019}. Disponible en: https://www.definicionabc.com/tecnologia/cisco.php

DEFINICION ABC. Que es ARPANET. {En línea}. {Consultado 17 de octubre de 2019}. Disponible en: DEFINICION ABC. Que es ARPANET. {En línea}. {Consultado 17 de octubre de 2019}. Disponible en: https://www.definicionabc.com/tecnologia/arpanet.php

DIARIO OFICIAL. LEY 1273 DE 2009. {En línea}. {Consultado octubre 21 2018}. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

ECURED. Router. {En línea}. {Consultado junio 16 de 2019}. Disponible en: https://www.ecured.cu/Router

EL Significado. Significado de integridad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://elsignificadode.com/integridad/

ELLISON, Kyle. Las empresas no se preparan bien y el cibercrimen sigue creciendo. {En línea}. {Consultado noviembre 01 2018}. Disponible en:

https://www.welivesecurity.com/la-es/2016/03/11/empresas-no-se-preparan-cibercrimen/

EMPRENDE PYME.NET. Políticas de seguridad. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.emprendepyme.net/politicas-de-seguridad.html

GCFGLOBAL. ¿Qué es un computador? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://edu.gcfglobal.org/es/informatica-basica/que-es-un-computador/1/

INFOLAFT. Lo que debe saber sobre el cibercrimen en Colombia. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

KARPERSKY LAB. Ciberamenazas Mapa en Tiempo Real. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://cybermap.kaspersky.com/es/subsystems/

KARPERSKY LAB. Evolución de los métodos de distribución de los virus informáticos y el malware. {En línea}. {Consultado octubre 21 2018}. Disponible en: https://latam.kaspersky.com/resource-center/threats/virus-delivery-methods

KARPERSKY LAB. Kaspersky: Boletín De Seguridad Estadísticas Generales de 2017 {En línea}. {Consultado octubre 21 2018}. Disponible en: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164544/KSB_statistics_2017_SP_final.pdf

KARPERSKY LAB. Qué es el cibercrimen - Definición. {En línea}. {Consultado noviembre 06 2018}. Disponible en: https://www.kaspersky.es/resource-center/threats/cybercrime

KASPERSKY LAB. Más información sobre el malware y cómo proteger todos tus dispositivos. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

KASPERSKY LAB. Ransomware: definición, prevención y eliminación. . {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://latam.kaspersky.com/resource-center/threats/ransomware

MALDONADO, Diego. ¿Qué es Infraestructura de TI y cuáles son sus componentes? {En línea}. {Consultado noviembre 06 2018}. Disponible en: http://www.icorp.com.mx/blog/infraestructura-de-ti-componentes/

MCAFEE. Informe de McAfee Labs sobre amenazas {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/reports/rp-quarterly-threats-mar-2018.pdf

MCAFEE. Informe sobre Criminología Virtual de McAfee amenazas {En línea}. {Consultado marzo 19 2019}. Disponible en: https://www.estudiocriminal.eu/wp-content/uploads/2017/03/Informe-sobre-criminologia-virtual-de-McAfee.pdf

MALWARE BYTES. Malware. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://es.malwarebytes.com/malware/

MASADELANTE. ¿Qué es un servidor? - Definición de servidor. {En línea}. {Consultado junio 16 2019}. Disponible en: https://www.masadelante.com/faqs/servidor

MENDOZA, Miguel Angel. El modelo de negocio del cibercrimen y su cadena de valor. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.welivesecurity.com/la-es/2016/11/03/modelo-de-negocio-del-cibercrimen/

MENDOZA, Miguel Angel. Países latinoamericanos, poco preparados contra el cibercrimen según nuevo informe. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.welivesecurity.com/la-es/2016/04/05/paises-latinoamericanos-poco-preparados-cibercrimen/

MOVISTAR. La importancia de la seguridad informática en un negocio. {En línea}. {Consultado junio 05 2019}. Disponible en: https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/la-seguridad-informatica/

NORTON. De qué manera distinguir el cibercrimen y protegerse. {En línea}. {Consultado abril 23 de 2019}. Disponible en: https://mx.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

NORTON. ¿Qué es un virus informático? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://co.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

PANDA. ¿Qué es un Firewall? {En línea}. {Consultado junio 16 2019}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/que-es-un-firewall/

PANDA SECURITY. ¿Qué es un Ransomware? {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

PANDA SECURITY. Las estafas BEC causan las mayores pérdidas económicas en empresas. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/estafas-bec/

PANDA SECURITY. Phishing. {En línea}. {Consultado abril 22 de 2019}. Disponible en: https://www.pandasecurity.com/es/security-info/cybercrime/phishing/

POLICIA NACIONAL. Informe: Amenazas del Cibercrimen en Colombia 2016-2017. {En línea}. {Consultado diciembre 9 de 2018}. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

PURBA, Narinder. El crecimiento del cibercrimen es “despiadado” según Europol. {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://www.welivesecurity.com/la-es/2016/09/28/crecimiento-del-cibercrimen-despiadado/

RODRIGUEZ MERINO, Cristina. ¿Qué es E-commerce o comercio electrónico? {En línea}. {Consultado 14 de mayo de 2019}. Disponible en: https://marketingdigital.bsm.upf.edu/e-commerce-comercio-electronico/

SANCHEZ IGLESIAS, Angel Luis. ¿Qué es un switch? {En línea}. {Consultado junio 11 2019}. Disponible en: https://www.aboutespanol.com/que-es-un-switch-841388

SASSONE, Santiago. Video: 5 consejos de seguridad para PyMEs. {En línea}. {Consultado diciembre 9 de 2018}. Disponible en: https://www.welivesecurity.com/la-es/2017/05/25/consejos-seguridad-para-pymes/

SEGURIDAD Informatica. Objetivos de la seguridad informática. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://infosegur.wordpress.com/tag/disponibilidad/

SIGNIFCADOS. Significado de Amenaza. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://www.significados.com/amenaza/

SIGNIFCADOS. Significado de Seguridad informática. {En línea}. {Consultado noviembre 06 2018}. Disponible en: https://www.significados.com/seguridad-informatica/

SIGNIFICADOS. Significado de Vulnerabilidad. {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://www.significados.com/vulnerabilidad/

SISTEMAS. Definición de Infraestructura. {En línea}. {Consultado noviembre 06 2018}. Disponible en: https://sistemas.com/infraestructura.php

SYSTEMATIC. Informe Sobre las Amenazas para la Seguridad en Internet {En línea}. {Consultado noviembre 01 2018}. Disponible en: https://tecno.com.mx/site1/wp-content/uploads/2018/06/ISTR23-FINAL_ES.pdf

TECNOLOGIA E INFORMATICA. Vulnerabilidades informáticas {En línea}. {Consultado octubre 21 2018}. Disponible en: https://tecnologia-informatica.com/vulnerabilidades-informaticas/

TECNOLOGIA FACIL. ¿QUÉ ES MICROSOFT? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://tecnologia-facil.com/que-es/que-es-microsoft/

TOLEDANO, Bruno. Hackean la red interna de Telefónica y de otras grandes empresas españolas. {En línea}. {Consultado junio 25 de 2019}. Disponible en: https://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html

TUS FACTURAS ONLINE. ¿Qué son las empresas PYME? ¿Qué significa PYME? {En línea}. {Consultado 13 de mayo de 2019}. Disponible en: https://tusfacturasonline.com/que-son-empresas-pyme-significado-pyme-tipos/

UNIVERSIDAD LIBRE. Las nuevas aplicaciones y los cibercriminales. {En línea}. {Consultado octubre 21 2018}. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/517-las-nuevas-aplicaciones-y-los-cibercriminales

VALDERRAMA, Álvaro. ¿Quién causó realmente el ataque a Sony? {En línea}. {Consultado junio 23 de 2019}. Disponible en: https://cnnespanol.cnn.com/2014/12/25/quien-causo-realmente-el-ataque-a-sony/

VALOR TOP. ¿Qué es un virus informático? Definición y tipos. {En línea}. {Consultado abril 22 de 2019}. Disponible en: http://www.valortop.com/blog/virus-informatico-definicion-tipos

ANEXOS

ANEXO A: 5 CONSEJOS DE SEGURIDAD PARA las PYMES

1 antivirus

Para evitar un ataque en las organizaciones es necesario contar con un software robusto de seguridad que es la piedra angular para cualquier plan de seguridad y evitara la filtración de algún software malicioso en la red que solo ocasiona estragos como perdida de activos, denegación de servicios, perdidas económicas, etc.

2 correo electrónico

Este medio de comunicación es el más utilizado en las organizaciones y usuarios comunes por eso nunca pasara de moda. Por ello los ciberdelincuentes utilizan esta herramienta para generar ataques debido a que se puede realizar masivamente y es económico. Por esta razón es necesario tener un control tecnológico como maximizar la seguridad de los servidores y soluciones antispam, así como políticas de seguridad que le permitan al usuario o empresa reconocer un correo sospechoso.

3 actualizaciones de software

El área de tecnología debe garantizar que los equipos de cómputo y servidores se encuentren con las actualizaciones al día así se garantiza mejor funcionamiento y correcciones de vulnerabilidades o código. Esto trae muchos beneficios a las organizaciones garantizando a los clientes mas seguridad en el manejo de la información.

4 BYOD

Bring Your Own Device es el uso de terminales personales para usos corporativos y se evidencia que esta modalidad la llevan más acabo las Pymes por falta de presupuesto por ende es importante educar a los colaboradores sobre la utilización correcta de estos dispositivos, para disminuir una posible fuga de información o vulnerabilidad.

5 preocuparse por la seguridad

Dentro de una empresa es muy importante concientizar y capacitar a los colaboradores ya que dentro de la cadena de un ciberataque el eslabón más débil es el usuario por su poco conocimiento frente a estos temas que cada día van teniendo más fuerza porque si una organización quiere ser competente en el mercado debe estar globalizada.[71]

ANEXO B: RESUMEN ANALITICO ESPECIALIZADO

Tema	Seguridad informática en pymes y medianas empresas.
Título	Casos de estudio de cibercrimen para el mejoramiento de la seguridad Informática en pymes y medianas empresas.
Autor	Camila Trujillo Chávarro
Fecha	Mayo / 2019
Fuentes	Contiene 67 citaciones de fuentes bibliográficas de tipos científicas y periodistas utilizadas por el autor en este proyecto, las que se relacionan a continuación son las más sobresalientes: MCAFEE. Informe de McAfee Labs sobre amenazas {En línea}. {Consultado octubre 21 2018}. Disponible en: https://www.mcafee.com/enterprise/es-mx/assets/reports/rp-quarterly-threats-mar-2018.pdf DIARIO OFICIAL. LEY 1273 DE 2009. {En línea}. {Consultado octubre 21 2018}. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[71] SASSONE, Santiago. Video: 5 consejos de seguridad para PyMEs. {En línea}. {Consultado diciembre 9 de 2018}. Disponible en: https://www.welivesecurity.com/la-es/2017/05/25/consejos-seguridad-para-pymes/

	UNIVERSIDAD LIBRE. Las nuevas aplicaciones y los cibercriminales. {En línea}. {Consultado octubre 21 2018}. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/517-las-nuevas-aplicaciones-y-los-cibercriminales UNIVERSIDAD LIBRE. Las nuevas aplicaciones y los cibercriminales. {En línea}. {Consultado octubre 21 2018}. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/517-las-nuevas-aplicaciones-y-los-cibercriminales MCAFEE. Informe sobre Criminología Virtual de McAfee amenazas {En línea}. {Consultado marzo 19 2019}. Disponible en: https://www.estudiocriminal.eu/wp-content/uploads/2017/03/Informe-sobre-criminologia-virtual-de-McAfee.pdf SIGNIFCADOS. Significado de Seguridad informática. {En línea}. {Consultado noviembre 06 2018}. Disponible en: https://www.significados.com/seguridad-informatica/ MALDONADO, Diego. ¿Qué es Infraestructura de TI y cuáles son sus componentes? {En línea}. {Consultado noviembre 06 2018}. Disponible en: http://www.icorp.com.mx/blog/infraestructura-de-ti-componentes/
Resumen	La presente nomografía consiste en el estudio de casos de cibercrímenes presentados a nivel mundial para proponer pautas de mejoramiento de la seguridad informática en pymes y medianas empresas de Colombia. Estas organizaciones están siendo muy afectadas por sus escasos controles y consideran que tener un antivirus evita un ataque

	cibernético que se ha visto en crecimiento por su gran rentabilidad y fácil ejecución. También hay que recordar que detrás de este delito no solo se encuentra un hacker aficionado en busca de probar sus conocimientos si no que ahora es un crimen organizado que mejora los malvares antiguos haciéndolos eficientes y menos detectables. La monografía tiene como función principal informar sobre un tema puntual basado en documentos periodísticos y/o científicos de interés para la comunidad por ende se estudiarán los casos de cibercrímenes sucedidos en el mundo con el fin de proponer un mejoramiento en la seguridad informática en pymes y medianas empresas por el gran riesgo que tienen de perder su información a causa de ciberataques que pueden ser ocasionados por vulnerabilidades en la infraestructura y el usuario, responsable de ejecutar un ciberataque sin ser consciente de ello.
Palabras Claves	Amenaza, Ataque informático, Confidencialidad, Disponibilidad, Empresa, Integridad, Mediana empresa, Prioridad, PYME, Seguridad, Servicio, Virus informático, Vulnerabilidad, Seguridad informática, Políticas de seguridad, Cortafuegos, Servidores, Cibercrimen, Ransomware, Wannacry, Exploits, Web.
Contenidos	El documento cuenta con una primera fase comprendida en introducción que contextualiza al usuario en que consistirá el trabajo, un planteamiento del problema indicando la problemática que se está presentado con una pregunta que se debe ser solucionada en el desarrollo del proyecto, una justificación indicando porque es necesario desarrollar el proyecto a corto, mediano y largo plazo, y que beneficios traerá. El objetivo general y específicos indican que se quiere lograr con el desarrollo de la monografía.

	El siguiente contenido guía al lector sobre los temas, teorías y leyes que soportan el documento y que son pieza clave para el desarrollo de la propuesta como el marco teórico que fundamenta el trabajo con base a lo indicado en el planteamiento del problema, el marco conceptual muestra los argumentos académicos que conforma el documento y finalmente se encuentra el marco legal en que se indican las leyes que soportan el desarrollo del proyecto. Después se puede evidenciar el contenido de la investigación realizada en el proyecto y muestra los diferentes temas que soportan y dan respuesta a los objetivos específicos del proyecto resolviendo el objetivo general, se divide en cuatro fases la primera trata de las modalidades del cibercrimen, la segunda trata de las vulnerabilidades que tienen las pymes y medianas empresas que probablemente son las más expuestas por su poco presupuesto, la tercera indica las estrategias más utilizadas por los ciberdelincuentes para atacar estas organizaciones y la cuartar da unas recomendaciones para mejorar la seguridad informática y así no estar tan expuestas ante este tipo de delito, para finalizar se encuentra las conclusiones y los anexos del proyecto.
	¿Cómo se puede mejorar la seguridad informática en las pymes y medianas empresas que están siendo afectadas por el crecimiento y rápida adaptación del cibercrimen?
Objetivo general	Realizar un estado del arte que permita el diagnóstico del estado actual de la seguridad informática en las Pequeñas y medianas empresas.
Objetivos específicos	Levantar información sobre las modalidades de cibercrímenes identificando metodologías, herramientas y técnicas con las que se realizan los ciberataques.

	Determinar las estrategias utilizadas por los ciberdelincuentes que vulneran la seguridad de las pymes y medianas empresas. Generar recomendaciones que mejoren la seguridad informática de las pymes y medianas empresas.
Metodología	Esta nomografía está basada en la investigación de documentos científicos y periodísticos para dar solución a un problema enfocado en la seguridad informática.
Conclusiones	Se evidencia que con el trascurrir del tiempo las modalidades del cibercrimen han avanzado en el que el atacante ha creado nuevas técnicas y herramientas para vulnerar la seguridad de las pymes y medianas empresas llevándolas a la quiebra eminente por la poca importancia que le dan seguridad informática. Hoy en día desde un correo hasta una llamada telefónica puede ser la estrategia que lleva el ciberdelincuente para acceder a la información sensible o confidencial. Por eso se deben tomar medidas preventivas al momento de dar información como nunca dar clic a los enlaces que llegan de un correo porque puede apuntar a una página falsa con las mismas características de una página bancaria. Estableciendo unas políticas de seguridad y buenas prácticas además de concientizar al usuario que es el eslabón más débil en este ámbito una pyme y mediana empresa puede reducir la probabilidad de ser atacada por un cibercriminal. Internet ofrece herramientas y cursos gratuitos provenientes de fuentes confiables que pueden ser un aliado para la protección de estas organizaciones.