AMENAZAS CIBERNÉTICAS Y SU IMPACTO EN LAS ORGANIZACIONES DEL SECTOR INDUSTRIAL Y SERVICIOS DE COLOMBIA EN LA ÚLTIMA DÉCADA

DAYRO LUIS GUTIÉRREZ TORO
84096501

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
RIOHACHA – LA GUAJIRA
2020

AMENAZAS CIBERNÉTICAS Y SU IMPACTO EN LAS ORGANIZACIONES DEL SECTOR INDUSTRIAL Y SERVICIOS DE COLOMBIA EN LA ÚLTIMA DÉCADA

DAYRO LUIS GUTIÉRREZ TORO
84096501

MONOGRAFÍA PARA OPCIÓN DE GRADO

DIRECTOR
CHRISTIAN REYNALDO ANGULO
INGENIERO DE SISTEMAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
RIOHACHA – LA GUAJIRA
2020

AGRADECIMIENTO

Primero que todo quiero agradecerle a nuestro señor que fue el que me ayudo a enfrentar las dificultades en todo este proceso de auto formación que comencé cuando entré a estudiar a la universidad nacional abierta y a distancia.

A mis padres y hermanos por los concejos, que me dieron, su cariño y compresión a todos mis compañeros que ellos también contribuyeron a que alcanzara este logro.

A todos los docentes que me ayudaron y me exigían siempre a presentar un buen trabajo para alcanzar los objetivos propuestos en cada curso académico que realicé en la universidad.

A los ingenieros de sistema Christian Reynaldo Angulo y Fernando Zambrano que fueron mis asesores de investigación para mi propuesta de grado.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

Desde la antigüedad observamos cómo los individuos de la sociedad tienden a adaptarse a los cambios que sufre la comunidad a medida que transcurre el tiempo.

Con la revolución industrial notamos como aparecen los avances científicos y tecnológicos que condicional al ser humano en el diario vivir para mejorar la calidad de vida. Cuando aparece el primer ordenador llamado “ENIAC” comienza la etapa de sistematización de datos para optimizar procesos y funcionamientos de las organizaciones a nivel empresarial, todo era utilizado de la mejor manera y el hombre jamás manejaba un pensamiento egoísta donde predominada un bien particular.

Cuando comienza a evolucionar el primer ordenador y se dan las etapas de las generaciones informáticas el pensamiento del hombre se vuelve complejo descubre nuevos conocimiento, y con la ayuda del internet WWW “WOLD, WIDE WEB” que es una red de búsqueda de la información a nivel mundial y las herramientas las TIC las personas comienzan a desarrollar modelos o estrategias para vulnerar los sistemas de información, que es lo que hoy se conoce con el nombre de ciberdelincuencia.

Este fenómeno ha causado grandes pérdidas millonarias y ha puesto en riesgo la estabilidad económica de las empresas en Colombia ya que estas no toman las medidas necesarias para implementación de una buena seguridad de red en sus sistemas de información y dejan expuesto los datos a manejo de terceras personas, por eso el estado ha decidido crear normas jurídicas que ayuden a procesar a los individuos de la sociedad que cometan el delito de ciberdelincuencia y así poder despertar conciencia para que todas estas herramientas no se usen con fines negativos que atenten contra la sociedad.

2. RESUMEN

Con la implementación de las herramientas las TIC y el internet los individuos de la sociedad viven en una dependencia total con la tecnología ya que esta se presenta prácticamente en todos los campos del conocimiento por los que están conformados una comunidad. “aspecto político, cultural, educativo, económico y organizacional por eso en la siguiente investigación se analizará cual es la magnitud del impacto que está a generado en el sector industrial y servicios de Colombia en la última década.

Además resaltaremos características de los diferentes ataques como: malware; se encarga de atentar contra el funcionamiento de los archivos que constituyen el sistema operativo de un computador, apt; consiste en captura de información de las personas que utilizan ordenadores para exponerlas a terceras personas, ransomware; que es un virus encargado de restringir archivos de un ordenador para exigir rescate, anonymos; que es un virus informático que tiene las mismas características del ransonware ,el Cross site-scripting; este ataque se caracteriza porque el delincuente se enfoca en analizar la vulnerabilidad que posee un sitio web o aplicación para usar el código fuente de portal web para su propio beneficio y defacement; que cosiste en la modificación de un portal web sin autorización de propietario etc. el cual servirá a las organizaciones a identificar las posibles fallas que existen en los sistemas de seguridad en redes que utilizan para proteger toda la información que ellos consideren relevante.

También se relacionará las leyes que fundamenta el estado para la seguridad de redes de las organizaciones en Colombia y las sanciones que ocasionan cometer delitos de tipos cibernéticos.

Finalmente, se resaltará la importancia de las nuevas normas de delitos informáticos que regirán el estado colombiano y mediante la contextualización de esta se pretende que el ciudadano tome conciencia y el índice de criminalidad disminuya un Poco.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Realizar un estudio monográfico que permita identificar las amenazas cibernéticas y su impacto en las organizaciones y sector industrial en la última década.

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Identificar cuáles han sido los ataques más relevantes que han atentado contra a estabilidad económica de las organizaciones industriales colombianas en los últimos dos años

- ✓ Analizar los diferentes tipos de ataques cibernéticos a los cuales están expuesto las organizaciones en Colombia

- ✓ Reconocer cuales son los elementos que influyen para que las organizaciones no ejecuten una buena metodología para protección de la información.

4. PLANTEAMIENTO DEL PROBLEMA

Con la globalización de las nuevas tecnologías de comunicación y la sistematización de las organizaciones los datos juegan un papel importante en el funcionamiento de las empresas ya que estas se pueden considerar como el insumo que las orientan a alcanzar los objetivos como lo establecen en su política.

Lamentablemente si las entidades no estructuran un buen plan para la protección de sus datos la información estará expuesta a dominio de terceras personas el cual buscan siempre beneficio común y esto es lo que conocemos en la actualidad con el nombre de ataque cibernético.

Este es un fenómeno que se ve a nivel mundial y atentan contra la estabilidad económica de cualquier país, nación, organización y hasta los individuos de la sociedad, un ejemplo de esto se vive en Colombia en la última década ha sufrido ataques los cuales le ha dejado muchas pérdidas millonarias.

Las principales características según Téllez Valdez para que los individuos de la sociedad cometan estas acciones pueden ser:

> conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas, acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya trabajado, acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico, Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios económicos "al hechor, 0frecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse, Son muy sofisticados y relativamente frecuentes en el ámbito militar, Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico, En su mayoría son imprudenciales y no necesariamente se cometen con intención[1]

[1] MANJARREZ BOLAÑO, Iván. JIMÉNEZ TARRIBA, Farid. Caracterización de los delitos informáticos en Colombia [en línea]. En: Pensamiento Americano. Coruniamericana. Julio – diciembre de 2012, vol. 5, no. 9, p. 71 - 87. [Consultado: 13 de febrero de 2018]. Disponible en Internet: http://coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano.ISSN: 2027-2448.

De acuerdo al informe de la comisión de regulación de telecomunicaciones (CRT) en los primeros tres meses del año 2008 los usuarios de internet aumentaron 13.6% llegando a 1.569,126 de los cuales el 55,7% tiene el servicio de internet y esto ha permitido el aumento en el uso de las herramientas TIC y a su vez la delincuencia cibernética ya que las personas ni las organizaciones toman medidas preventivas para protección de su información[2]

Los ataques comunes que utilizan para atentar contra los activos de las organizaciones o datos particulares de las personas en Colombia se destacan, aquellos que perturban el patrimonio económico, transacciones virtuales, phishing, páginas web ilegales, portales web con publicidad engañosa.

Los que explotan a los menores, mediante la publicación de imágenes, videos, y hasta salas de chat. Los orientados a propiedad intelectuales, como la manipulación y venta de software sin pagar los respectivos derechos de autor.

Los que realizan robo de información confidencial de las compañías para beneficios particular dejándolas en desventaja contra las demás empresas si están compitiendo en determinado mercado, ya que actualmente sabemos que el principio que rige este nuevo mundo tecnológico es “entidad que no implemente tecnología y sistematización de sus datos en su funcionamiento tiende a desaparecer por no optimizar sus procesos” de producción.

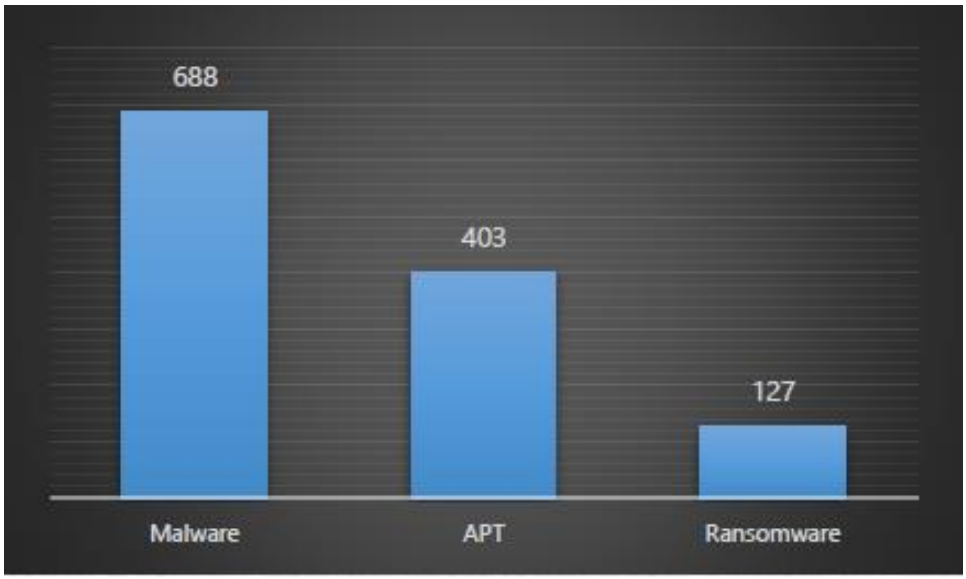
El país en el año 2015(reporto 153 incidentes y 328 para el 2016). A medida que transcurre el tiempo notamos que los ataques van aumentando y a la vez se vuelven más complejo ya que los delincuentes buscan la forma de adaptarse a los cambios por los cuales está pasando la sociedad ya que las herramientas TIC día a día van evolucionando.

[2] ibíd. Caracterización de los delitos informáticos en Colombia [en línea]. En: Pensamiento Americano. Coruniamericana. Julio – diciembre de 2012, vol. 5, no. 9, p. 71 - 87. [Consultado: 13 de febrero de 2018]. Disponible en Internet: http://coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano. ISSN: 2027-2448.

Lamentable mente cambiar el pensamiento del individuo en la sociedad para que usen la tecnología de forma correcta con respecto al conocimiento, es un reto porque no todos posen valores éticos y siempre se está buscando tener ventajas frente a los demás.

Regularmente, los delitos informáticos organizacionales son relacionados directamente a grandes corporaciones las cuales son las que más información almacena y hacen que los ataques sean más exitosos dejando mayor beneficio, según un informe del policía Nacional relacionado con delitos informáticos, durante el año 2016 hubo un incremento de 114. 4% en ataques de malware[3]

Figura 1. Ataques cibernéticos que han sufrido las organizaciones en los últimos años



Fuente: policía Nacional –Dirección de Investigación Criminal interpol. [Imagen]. Centro cibernético policía nacional. Colombia 2017.P.5. [Consultado: 10 marzo2017]. http//caivrtual.policia.gov.co/sites/default/files/informe_amenazas_de Cibercrimen:

Las amenazas persistentes avanzadas permiten al delincuente identificar sus víctimas mediante programas maliciosos para explorar falencias en los sistemas de información. En el año 2015 se hace un reporte de 45 ataques cibernéticos de los

[3] Policía Nacional –Dirección de Investigación Criminal interpol, Amenazas del Cibercrimen en Colombia 2016-2017. [EN PDF]. Análisis del Cibercrimen. Marzo Diez Del 2017, paginas 4- 5. [Consultado: 17-03-2017].Disponible internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

cuales el ransomware registra un porcentaje del 500%, para el año de 2016 aumento a 286 ataques y esta tendencia se proyecta para el periodo 2017.

Finalmente, para poder tomar medidas contra esta problemática que actualmente se está presentando en el entorno social, directamente en las empresas u organizaciones es necesario ¿identificar Cuáles son los elementos que influyen en las organizaciones colombianas para que no se haga una buena planificación en cuanto al tema de seguridad en los sistemas de datos?

5. JUSTIFICACIÓN

Indiscutiblemente los avances tecnológicos condicionan el diario vivir de las personas en la sociedad, el funcionamiento de las organizaciones públicas o privada que constituyen un estado, el desarrollo social, cultural y económico de un país.

Un ejemplo de esto es la comunicación, anteriormente notamos que el hombre para comunicarse trasmitía el mensaje mediante un texto llamado “carta” el cual demoraba hasta dos días para llegar a su destino, pero con la aparición del internet este proceso se optimizó y ahora podemos enviar documentos, mensajes, video y fotos con solo un clic y en menos de 12 hora transmitiendo la información a cualquier parte del mundo.

A pesar que las herramientas de información se crearon para optimización de procesos ya sea para aspectos personal u organizacional si no se toman las medidas necesarias para proteger los datos estos pueden quedar expuesto al dominio de terceras personas.

Colombia es un país que día a día está expuesta a los ataques cibernéticos, debido que en la sociedad existen personas que no están conforme con las normas que rigen una comunidad y saben que en la actualidad todo gira en torno a las herramientas de tecnología y el éxito o fracaso en el funcionamiento de las organizaciones se obtiene dependiendo del uso de los datos ya sea a nivel organizacional o particular. Por esto para la protección de la información se han creados mecanismos de control de orden jurídicos relacionado con normas que rigen la seguridad de datos.

Por tal motivo en el país, se constituye la ley 1273 de 2009 enfocada a controlar y mitigar los delitos informáticos cambiando así el código penal formando una nueva reforma denominada “protección de la información y de datos” aunque existan programas que influyen para que los habitantes de la sociedad tomen las

respectivas precauciones para protección de datos, surge el siguiente interrogante ¿Por qué los ataques cibernéticos a medida que transcurre el tiempo van aumentando?

Es por eso que con la realización de este trabajo se analizara el impacto que estos ataques han caudado en la última década en Colombia, así como las características principales de cada amenaza y los factores que motivan a las personas a realizar los delitos que se pueden realizar por medio de internet.

También resaltaremos las medidas o procedimientos legales que se implementan en Colombia para contrarrestar la ciberdelincuencia ya que en la comunidad muchos individuos desconocen las sanciones jurídicas.

6. MARCO TEÓRICO

6.1 PERFIL CRIMINOLÓGICO CIBERNÉTICO

Antes de comenzar a dar un concepto especifico de perfil criminológico cibernéticos de los individuos que cometen delitos relacionados con los sistemas de información y la tecnología es importante analizar el término desde el ámbito psicológico para poder entenderlo del contexto tecnológico.

Como lo resalta el Doctor Cesar. M Ramírez Luna en su artículo “el perfil criminológico del delincuente informático” puede definirse como una estimación acerca de las características biográficas y del estilo de vida del responsable de una serie de hechos delictivos graves o leves y que aún no se ha identificado, estas características pueden provenir desde un contexto social, psicológico e incluso familiar[4]

La psicología siempre se ha caracterizado por estudiar el comportamiento que tienen las personas en la sociedad cuando estas están sometidas a leyes de convivencia y de acuerdo a esto se da la clasificación de los delitos dependiendo de las características físicas según el Doctor Lombroso existen dos niveles, en el primer nivel encontramos criminal nato; que son los delincuentes primitivos que van de generación en generación y a medida que trascurre el tiempo van evolucionando con el conocimiento , demente; delincuente que nace por patología mentales y los criminaloides; que no pertenecen a ninguno de los dos grupos y por circunstancias de la vida les toca cometer el delito.

[4] RAMÍREZ LUNA, Cesar. El Perfil Criminológico Del Delincuente Informático [en línea]. derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf.pag 3-5. [Consultado el día 15 de agosto 2018].Disponible en internet: http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf

En los del segundo nivel encontraremos los locos morales, epilépticos, ocasionales y pasionales. Por eso es correcto afirmar que los criminales cibernéticos los podemos identificar en el nivel uno con los criminales natos, ya que estas son personas especiales que la inteligencia la han desarrollado con la evolución del conocimiento a través que trascurre el tiempo, una de las características que poseen estos delincuentes son personas pocas sociables y a veces hasta marginados por la comunidad.

De acuerdo a las características mencionadas anteriormente los delitos informáticos se clasifican en individual, de propiedad, gubernamental y dependiendo de la intención del atacante:

- ✓ Hacker
- ✓ Piratas informáticos
- ✓ Cracker
- ✓ Lammer
- ✓ Gurus
- ✓ Phreaks
- ✓ Bucaneros
- ✓ Newbie

6.2 TIPOS DE PERFILES CIBERNÉTICOS

6.2.1 Hacker, son las personas que se dedican a atacar los sistemas de información para demostrar que ellos pueden vulnerar cualquier sistema de datos no importa la complejidad de protección que utilicen, su único objetivo es ganar reputación en una comunidad[5]

[5] MESESAN. Sergiu Open Data Securyti. Hackers-. [en línea]. Hackers-de-evolucion-tecnologica-ha-armas-gubernamentales. publicado en (3 de enero -2017). P 1-2.consultado (15 de mayo .2017) disponible internet: https://opendatasecurity.io/es/hackers-de-evolucion-tecnologica-a-armas-gubernamentales/

6.2.2 Piratas informáticos, se llaman así a las personas que no son capaces de crear aplicaciones o programas para cometer los delitos informáticos, por lo generar utilizan software creado por terceras personas sin autorización del propietario.

6.2.3 Cracker, son aquellas personas que vulneran la seguridad de los sistemas de información con el objetivo de robar o eliminar datos importantes, hacen transferencias ilegales y siempre están buscando fallas en los sistemas de seguridad de redes para cometer delitos [6]

6.2. 4 LAMMER, son aquellas personas cuyos conocimientos son limitados depende de los estudios y análisis que publican otras personas para cometer los ataques no son capaces de ir más allá del conocimiento investigado.

6.2.5 Gurus, son los maestros están encimas de lammer, Cracker, Piratas informáticos, Hacker y el demás grupo que existan porque ya son personas mayores y han adquirido sus conocimientos a través de los años.

6.2,6 PHREAKS, personas encaminadas a cometer delitos cibernéticos de tipos telefónicos, hacer llamadas gratis más que todo afectan a las empresas de telecomunicaciones

6.2.7 BUCANEROS, son las personas que se dedican a comercializar servicios que pueden ser pagado por tarjetas de créditos, como por ejemplos cuentas para canales de tv, otras como cuantas, para escuchar música, con solo el hecho de crackear el producto. No tienen conocimiento de programación, ni informática

6.2.8 NEWBIE, se les llama así a los principiantes que apenas están comenzando los primeros pasos para empezar a delinquir con los ataques cibernéticos “el

[6] GUILLEM. Alsina DEFINICIONES – ABC. Cracker. [en línea]. definicionabc.com/tecnología/cracker-phreakin-lammer. Publicado (mayo de 2017). p- 4 consultado (17 de mayo de 2019). Disponible internet: https://www.definicionabc.com/tecnologia/cracker-phreakin-lammer.php

aprendizaje es lento y se orientan por las teorías o explicaciones que comparten los individuos que realizan estas acciones”

7. MARCO LEGAL

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. Se considera violación de la ley, cuando el individuo de la sociedad accede a un sistema informático protegido sin autorización previa del propietario. Este se condenará a penas de cuarenta y ocho (48) a noventa y seis (96) meses de prisión y pagará multas de 100 a 1000 salarios mínimos legales

- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. Este se fundamente argumentando que individuo que no tenga autorización e impida el funcionamiento de un sistema de información a datos o contenido de red en telecomunicaciones será castigado con cuarenta y ocho (48) a noventa y seis (96) meses de prisión y será sancionado con multas de 100 a 1000 salarios mínimos legales

- **Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS**. Esta norma manifiesta que aquel individuo sin orden judicial intercepte datos informáticos desde su origen a destino o dentro de un ecosistema informático de transfiere datos será sancionado con treinta y seis (36) a setenta y dos (72) meses de prisión

- **Artículo 269D: DAÑO INFORMÁTICO**. Se relaciona con sancionar al individuo que sin estar autorizado destruya, elimine, altere datos de un sistema de información tendrá de cuarenta y ocho (48) a noventa y seis (96) meses de prisión con multas de 100 a 1000 salarios mínimos

- **Artículo 269E: USO DE SOFTWARE MALICIOSO**. Esta ley específica que las personas que utilicen, diseñen o fabriquen programas o link para capturas de datos en un sistema de información tendrán una sanación de cuarenta y ocho meses (48) a noventa y seis (96) meses de prisión con multas que van desde 100 salarios mínimos hasta 1000 vigentes legales.

- **Artículo 269F: VIOLACIÓN DE DATOS PERSONALES**. Esta norma manifiesta que el individuo que sin estar autorizado se apropie, ofrezca, comercialice e intercambie datos de personas que estén almacenado en un sistema de información o medios de datos tendrán una condena a prisión de cuarenta y ocho (48) a noventa y seis (96) meses de prisión con multas de 100 a 1000 salarios mínimos vigentes legales.

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. Esta ley específica que las personas que utilicen, diseñen ventanas emergentes o link para capturar datos de personas que utilicen los sistemas de información tendrán una sanción de cuarenta y ocho a noventa y seis (96) meses de prisión con multas de 100 a 1000 salarios mínimos vigentes legales.

Es importante resaltar que la norma se orienta a los delincuentes cibernéticos que utilizan el vector de ataque “phishing” que es una de las modalidades más frecuentes que se utiliza para extraer información de medios sistemáticos y correos electrónicos.

- **Artículo 269H: CIRCUNSTANCIAS PENALES PUNTUALES.** La norma se relaciona circunstancias de agravación de los artículos mencionados anteriormente como aumento de pena o disminución de las tres cuartas partes por conducta.

- ✓ Ataques a sistemas de información del estado, sector financiero, nacionales o extranjeros
- ✓ Por ser empleado del estado cumpliendo sus funciones
- ✓ Revelando información de datos para perjudica a otro
- ✓ Obteniendo ganancias para un tercero o para sí mismo
- ✓ Con fines terroristas o generando riesgo al estado

- **Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES**. El individuo que viole la seguridad que contiene una red de información y manipule un sistema de datos y suplante al usuario ante la autorización y autenticación tendrá pena de 3 a 8 años.

- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que cometa la persona con ánimo de lucro, valiéndose de métodos para procesar datos transfiriendo información sin autorización de cualquier activo para perjudicar a un tercero tendrá una pena de 48 a 120 meses de prisión y así mismo será multado con salarios mínimos vigentes entre 200 a 1500.

Esto también aplica a quienes fabriquen o tengan programas que tengan como objetivos transferencias de datos ya que esto también se considera como estafa

Ley Estatutaria 15 81 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: estas normas también la podemos relacionar con la protección de datos personales en el estado colombiano.

Decreto 2693 de 2012: esta norma se relaciona con estrategias del estado y el ministerio de las tecnologías y comunicación para apoyar las leyes 1341 de 2009 y 1450 de 2011 donde se encuentran los siguientes decretos:

Decreto 2578 de 2012: norma que reglamenta el sistema nacional de archivos entrega de documentos, los funcionarios públicos cuando estén investigando delitos informáticos tendrán que entregar documentos impresos, archivos tradicionales, equipos de cómputos y portátiles a las autoridades correspondiente.

Decreto 2609 de 2012: esta se orienta al título de ley V creada en el año 2000 el cual incluye características para adecuar archivos electrónicos.

Ley 1341 DE 2009: se orienta a definir los principios que deben tener los individuos de la sociedad con los sistemas de información y la organización de las tecnologías de información y medios de comunicación

Modelo Estándar de Control Interno MECI 1000:2005: se caracteriza porque atravez de esta se puede planificar el control para evaluar si las organizaciones pueden cumplir los objetivos con la seguridad de datos que implementa en su funcionamiento.

NTCGP1000:2004: esta ley se orienta a definir los requerimientos para implantación y calidad de un buen servicio de seguridad de información para la rama del poder público y otras entidades relacionada con esta misma

·**ISO/IEC TR 18044:2004:** es una norma orientada a asesorar para implementar o planificar una buena seguridad de información dependiendo del número de incidentes que está presente

Ley 599 DE 2000: se fundamenta por el código penal, para proteger el bien jurídico “derechos de autor” para protegerlos de los delitos informáticos como comercialización de instrumentos que se utilizan para interceptar información precisa entre dos personas cuando pongan a disposición los sistemas de información

8. MARCO CONCEPTUAL

ATAQUE DE FUERZA BRUTA, es una técnica que utilizan los delincuentes cibernéticos donde prueban códigos o ping alfa numéricos apara acceder a un sitio sin autorización vulnerando la seguridad de los sistemas de información

CRIPTOGRAFÍA, rama de la informática que se encarga de codificar información para proteger los datos de los individuos u organización en un sistema de información[7]

DENEGACIÓN DE SERVICIO, delito informático que se realiza a una red o un sistema conformado por estaciones de trabajos formados por computadores el cual hace que un recurso sea in accesible a los usuarios.

ENIAC, nombre del primer computador creado para procesar información

FICHEROS, se conoce así a el conjunto de documentos que son almacenados en dispositivos los cuales contienen la identificación, y descripción de la carpeta que los contiene

FRAUDE, se conoce al acto que utilizan los delincuentes al cometer delitos que atenten contra los principios o normas que rigen una comunidad.

INGENIERÍA SOCIAL, técnicas que se utilizan para cometer delitos informáticos mediante la utilización de programas que sirven para violar la seguridad de los sistemas de información[8]

---

[7] Kaspersky. Ingeniería social. [en línea]. kaspersky.com/resource-center/definitions/what-is-social-engineering.consultado (15 de septiembre de 2018). disponible en internet: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

[8] GARCÍA. De Mata. Criptografía básica para entender la tecnología de blockchain. [En línea]. Criptografía-básica-para-entender-la-tecnología-blockchain. Publicado (14 de marzo de 2018). P 1. Consultado (22 de mayo de 2019). Disponible el internet: https://blockchain.grantthornton.es/

PHP, lenguaje de programación que se utiliza para crear aplicaciones web mediante códigos HTML[9]

SISTEMA OPERATIVO, nombre del programa que permite manipular los recursos de una computadora.

SSH, mecanismo de control remoto que permiten controlar al usuario servidores a atravez de internet

VBS, es un lenguaje de programación que permite al usuario hacer aplicaciones mediante elementos en exel

VPN, topología en red de información para equipos informáticos que permite mediante una conexión segura transmitir información en una red de área local “LAN”

[9] Aprendamos a programar.com. Lenguaje de programación php [En línea]. Criptografía-. aprenderaprogramar.com. publicado (21 de junio 2018. última actualización). Consultado el (23 de mayo de 2019). Disponible en internet: https://www.aprenderaprogramar.com/

9. ATAQUES RELEVANTES QUE HAN ATENTADO CONTRA LA ESTABILIDAD ECONÓMICA DE LAS ORGANIZACIONES INDUSTRIALES COLOMBIANAS EN LOS ÚLTIMOS AÑOS

Desde el principio de la humanidad, el hombre empezó a adaptarse a los constantes cambios que pasó la sociedad para poder vivir; la minería para crear herramientas para practicar la cacería y poder alimentarse, en la etapa feudal el individuo de la comunidad se apoyaba en la tenencia de tierra para practicar la agricultura. En la revolución industrial fue la etapa donde las personas comenzaron a inventar máquinas aparece la locomotora, telégrafo y otros inventos que mostraron avances en la sociedad.

Con la aparición de la primera calculadora, creada por el señor pascal, que servía para agilizar procesos contables el individuo empieza a desarrollar un pensamiento complejo, aparece la primera computadora el cual se conocía con el nombre de ENIAC, inventada por el señor Jhon Von Neumann que era una máquina de dimensiones 2,4 metros por 0.9 metros por 30 metros que consumía 160 kW cada vez que entraba en funcionamiento y su peso era de 27 toneladas y esta se utilizaba para el procesamiento de datos.

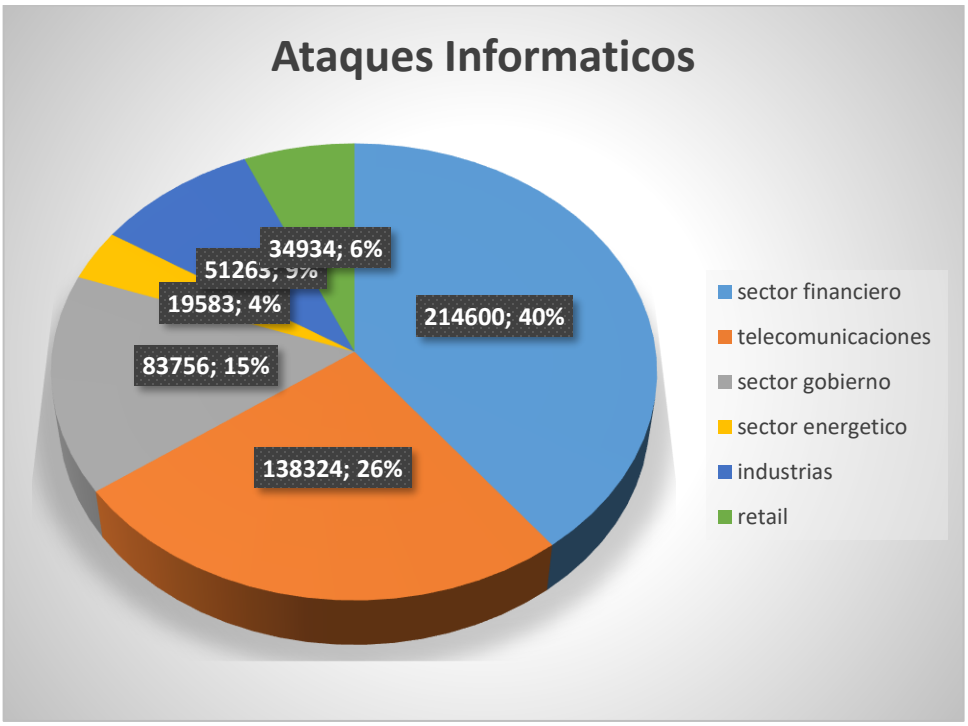
Tiempo después se da la etapa de las generaciones informáticas donde la primera computadora pasa por diversos cambios para optimizar su funcionamiento, luego entramos al siglo XXI donde el boom de la sociedad es el nuevo mundo tecnológico donde todo gira en torno al as herramientas las TIC que se utilizan mediante internet.

Con la sistematización de los datos en las organizaciones, estas pueden optimizar los diferentes procesos que presentan en su funcionamiento, lastimosamente si no se propone una buena planificación en las políticas de seguridad de datos, estas quedaran expuestas a los ataques cibernético, los cuales buscan atentar contra la

estabilidad económica de un país, estado, nación y organizaciones que constituyen una sociedad.

Un ejemplo de esto, se observa en Colombia que diariamente en él se producen aproximadamente 542.465 ataques informáticos los cuales se distribuyen de la siguiente manera como se muestra en el siguiente gráfico:

Figura 2. Sectores que han sufrido ataques cibernéticos en Colombia año 2018

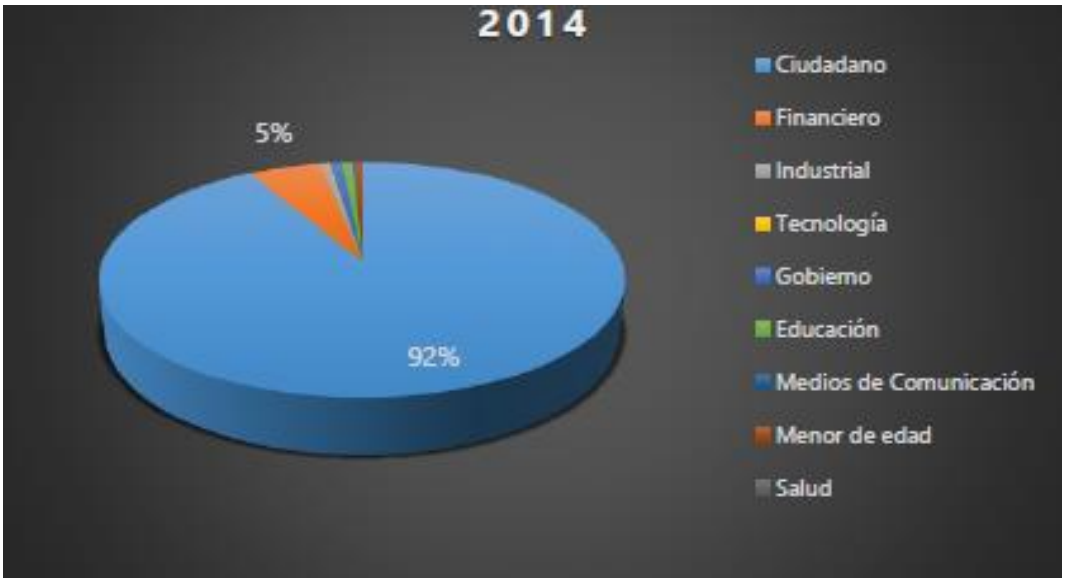


Fuente: GUTIERREZ Dayro. Ataques Cibernético año 2018 Colombia [Grafico].Sectores más vulnerables ataques cibernéticos https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Si comparamos en años anteriores los ataques cibernéticos aumentaron razonablemente en los sectores industrias, financiero, tecnológico en donde se resaltan ataques como malware, apt, ransomware.

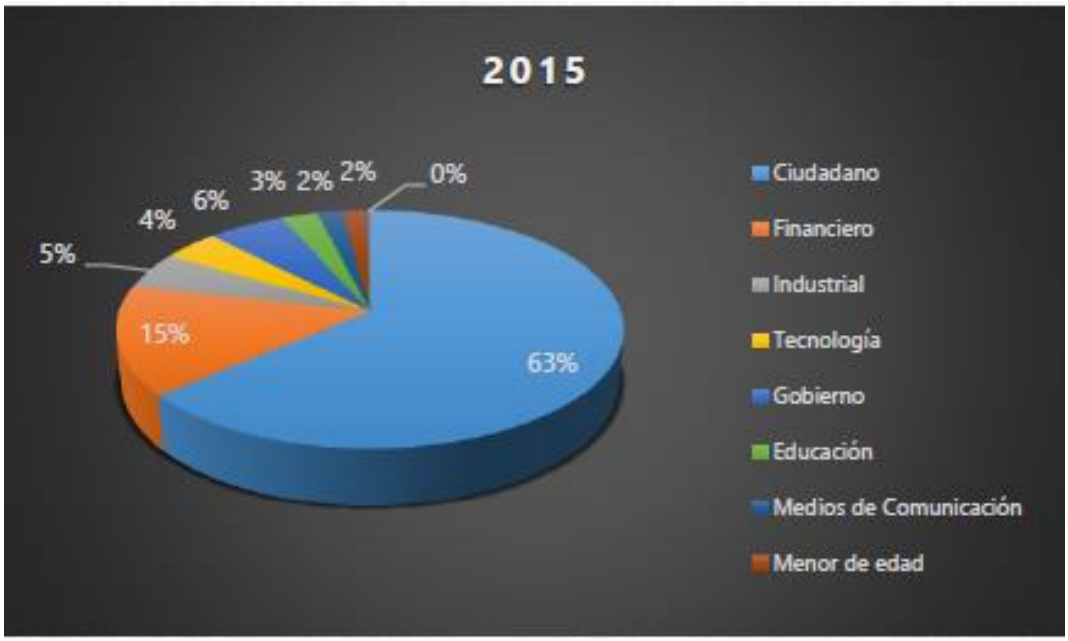
En el año 2014 un 92% de los ataques cibernéticos eran dirigidos a los ciudadanos, pero en el periodo 2015-2017 disminuyen a un 35% pero aumenta un 28% en el sector empresarial.

Figura 3. Sectores que han sufrido ataques en Colombia año 2014



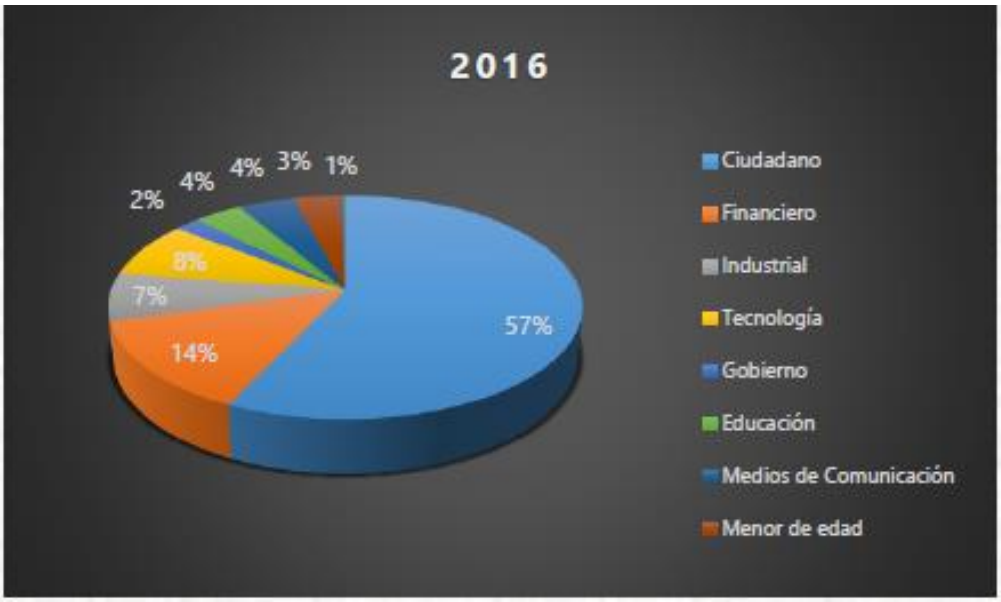
Fuente: policía Nacional – Dirección de investigación criminal interpol. [Imagen]. Centro cibernético. Policía https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Figura 4. sectores que han sufrido ataques cibernéticos en Colombia año 2015



Fuente: policía Nacional – Dirección de investigación criminal interpol. [Imagen]. Centro cibernético policía p.5 [consultado: 10 marzo 2017]. https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Figura 5. Sectores que han sufrido ataque cibernético en Colombia año 2016



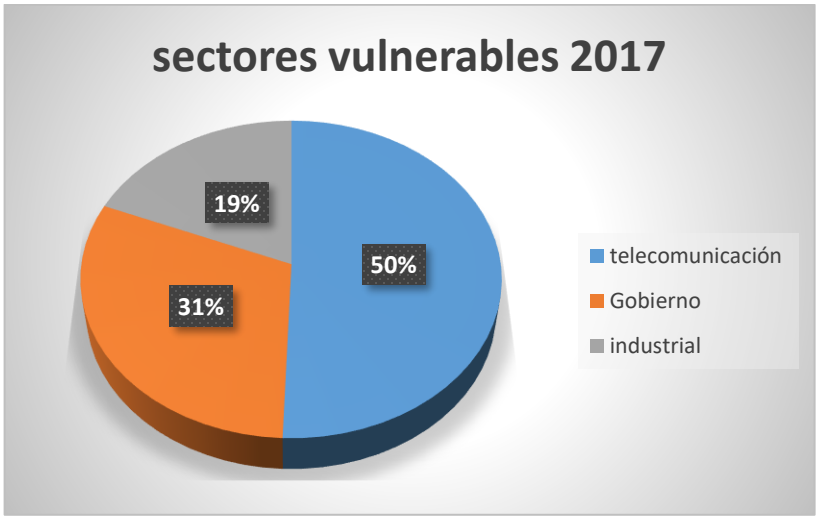
Fuente: policía nacional – Dirección de investigación criminal interpol. [Imagen].centro cibernético policía p.5 [consultado: 10 de https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

En el periodo 2014 los ataques son dirigidos al ciudadano común y registran un porcentaje de 92 % mientras que en el año 2015 se registra una disminución de 63% y así mismo para el siguiente año fue de 57 % quiere decir que hay una disminución de 35% al ciudadano común, mientras que en el sector empresarial dé un 5% aumenta a 28 % esto quiere decir, que a mayor volumen de ataques con mayor números de víctimas dirigidos a los ciudadanos comunes los beneficios económicos son bajos mientras, que si los ataques son más avanzados y dirigidos a otros sectores los beneficios económicos son mayores y para esto los delincuentes utilizan metodologías basadas en Malware, APT y Ransomware .

En un estudio que se realizó en la actualidad realizado por la empresa Kaspersky correspondiente a Rusia entre el periodo de enero del treinta y uno (31) y agosto del 2017 que en américa latina registra 677 millones de amenazas cibernético y que a cada hora se cometen 117.

También resaltan que en Colombia para el mismo año los sectores más afectados fueron el de telecomunicación con 138.329, gobierno con 83756 e industriales con 51236.

Figura 6. Sectores que han sufrido ataque cibernético en Colombia año 2017



Fuente: GUTIERREZ Dayro. Ataques Cibernético año 2017 Colombia [Grafico].Sectores más vulnerables ataques cibernéticos https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Antes de detallar las principales características de los virus que se utilizan para cometer delitos en Colombia hay que resaltar que estos virus que están utilizando para cometer delitos informáticos es la evolución del primer virus informático que fue creado por el señor John Von Neumann, el cual crea un programa capaz de auto reproducirse en ordenadores, luego con la evolución se fueron creando programas de acuerdo al contexto que se presentaba.

9.1 CARACTERÍSTICAS VIRUS MALWARE

Término que se relaciona con “softwares maliciosos” y hace referencia a los programas que se utilizan para dañar o ejecutar acciones no deseadas a los sistemas de información, este proviene del latín “malus” que significa malo y “ware” que viene de la expresión software.

Existen personas que anteriormente han definido al malware como un virus informático que utiliza una secuencia de símbolos cuando se trabaja en el contorno adecuado (ordenador) y modifica la misma secuencia de símbolos en el mismo medio mediante la inclusión realizando una copia de si mimo, estos ataques lo podemos clasificar según sus características en: virus clásico, gusano de red, caballo de Troya, spyware, phishing, adware, riskaware, bromas y spam

9.2 VIRUS CLÁSICOS

Cuando hablamos de virus nos referimos a un programa informático que es capaz de penetrar los sistemas de información para obtener datos de tipo confidencial o privada, reciben el nombre de virus clásicos porque son los primeros que se crearon cuando comenzó la revolución de las tecnologías de información, estos se clasifican según el entorno donde se esté realizando el ataque: sobre escritura, acompañante, vínculos, módulos de objetos. Librerías de compilación, códigos fuentes de aplicación y parasíticos. Sobre escritura, es un modelo de virus que no es muy complejo, se encarga de sustituir el código del archivo el de mismo atacante. Y borra el original dejando así el fichero dañado y no puede ser restaurado, estos virus son fáciles de detectar debido que el sistema y aplicaciones dejan de funcionar correctamente cuando está infectado.

Parásitos, son virus informáticos que se caracterizan porque modifican el fichero al ser infectado dejándolo parcialmente o totalmente dañado. Se clasifican de acuerdo a las secciones del fichero o código que se utilizan anexado al comienzo o al final,

Cuando hablamos de fichero anexado al comienzo; nos referimos a aquellos códigos que apuntan para dos momentos, en el primer contexto el virus desplaza el código al inicio del archivo y lo escribe en ese espacio.

En la segunda alternativa el virus lo adiciona al código del fichero a su propio código, en ambas situaciones cada vez que el fichero se esté ejecutando el código se elaborara primero con el objetivo de mantener la integridad de la aplicación.

Fichero anexado al final, los virus por lo general se clasifican en estas categorías estos siempre se escriben al final del fichero infectado. Cambiando el punto de entrada en el encabezado del archivo. Mientras que los insertos son amenazas que poseen variedad de métodos para insertarse en la mitad del fichero, los modos más utilizados son simples que se caracterizan por desplazar el código al final del fichero o crea copia del código original dejándolo al lado para abrir espacio al virus; en ellos también se incluyen los llamados virus cavidad, que son aquellos que se insertan en las secciones de los ficheros vacíos.

9.3 VIRUS ACOMPAÑANTES

Son aquellos que se caracterizan porque estos no modifican el fichero original, sino que crea una copia del archivo original y cuando se ejecuta el archivo infectado se activa el virus.

En esta categoría también encontramos virus que cambian el nombre del archivo original, graban un nuevo nombre y sobre escribe el fichero original. virus macros, son aquellos que se utilizan para atacar las diferentes aplicaciones de Microsoft como Word, Excel, y powert Point los cuales se guardan en formatos OLE2, estos virus son pocos comunes. La ubicación real de virus depende del formato del archivo y una forma de darse cuenta que está siendo atacado porque las aplicaciones no funcionan en óptimas condiciones.

Virus script, estos virus son subgrupos de archivos que se escriben en diferentes lenguajes de programación VBS, BAT, y PHP que infectan otros scripts y se utilizan para atacar las aplicaciones web. Mientas que el rootkit es un virus informático que se caracterizan por ser creados para atacar las vulnerabilidades del mismo medio y permite que el delincuente tenga acceso a las funciones y recursos del sistema, ocultan su presencia en los diferentes procesos o ficheros y por eso se dificulta la detección.

. La diferencia que existe entre las amenazas Adware y spyware, es que la primera tiene como función mostrar publicidad de datos productos y servicios en diferentes

sitios web, adicionando códigos que divulgan ventanas emergentes y la segunda fue creada principalmente para reunir información de los usuarios que usan aplicaciones o programas que almacenan sus datos para que este re direccione la información a terceras personas.

9.4 CARACTERÍSTICAS DE VIRUS APT

El termino APT se relaciona con tema como Advanced persistent threat, el cual se caracteriza porque son ataques dirigidos que utilizan vectores de intrusión para tener mayor grado de complejidad

El tiempo de duración que se utiliza para programar este ataque se basa en investigación de tipo operacional, donde se tienes aspectos tales como tamaño de proporción, probabilidad de cruce, inteligencia artificial y mutaciones ya que su objetivo es explotar el elemento más débil que constituye el sistema para no levantar sospecha. En el estudio que se hace se analizan los perfiles de los distintos usuarios para poder usar los múltiples vectores de ataques que ayudan a cometer el delito.

Entre los más comunes podemos destacar: Stuxnet, Winnta, Regin, Gauss, The mask

9.4.1 STUXNET, es un virus informático de tipo gusano que se caracteriza porque afecta a los ordenadores que utilizan sistemas operativos Windows son capaces de reprogramar los controladores lógicos y ocultar los cambios realizados.[10]

El modo de operar es identificar las vulnerabilidades conocidas con el nombre de día cero las cuales se relacionan con temas como Cplink, Scada, conficker y wincc/pcs7

[10] STUXNET, Wikipedia. [en línea]. publicado (año 2010). Consultado [10 de marzo de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Stuxnet

9.4.2 REGIN, este virus fue creado en el año 2014 por compañía de antivirus Kaspersky Lab y Symantec, en acuerdo con agencias de seguridad nacional y entidades británicas, creado para el espionaje en grandes y su objetivo es robar contraseñas para acceder a la información. [11]

9.4.3 GAUSS, virus dedicado también al espionaje y se caracteriza por interceptar ficheros cookies y contraseñas en los navegadores, recopilar información acerca de la configuración del sistema, infectar memorias USB con módulos para el robo de datos para poder utilizarlos en delitos como robos bancarios, en redes sociales, servicios de correo y mensajería instantánea. [12]

9.4.4 THE MASK, este virus fue descubierto a inicio del año 2014, se caracteriza por el uso combinado de herramientas malware entre las cuales destacamos exploits, rootkit, bootkit y keyloggers. Esta amenaza almacena información interceptando canales de comunicación en un sistema de red, capturando archivos de tipos RPD, criptográficos y SSH con configuración VPN.

9.5 CARACTERÍSTICAS DE VIRUS TIPOS RANSOMWARE

Los virus de este tipo son aquellos que utilizan técnicas para bloque de dispositivos ya sea ordenadores, celulares u otro medio informático donde se manejen datos con internet y así poder negar el acceso al usuario a su información si este no paga un rescate, entre ellos podemos encontrar: Zeus bot, amenaza cibernética creada para recuperar información bancaria ingresando a formularios a través de sitios web.

[11] Regin, wikipedia.org/wiki/Regin. [en linea]. Actualizado (10 de enero 2019). Consultado [10 de abril 2018]. Disponible en internet: https://es.wikipedia.org/wiki/Regin_(malware)

[12] Fayerwayer Kaspersky-pide-ayuda-para-descifrar-al-virus-gauss. [en linea]. publicado [14 de agosto de 2012] consultado (10 de enero 2019). Disponible en internet: https://www.fayerwayer.com/2012/08/kaspersky-pide-ayuda-para-descifrar-al-virus-gauss/

9.5.1 CONFICKER, amenaza dirigida a buscar vulnerabilidades en administradores de seguridad en redes tale como Windows server y así poder acceder a la información que se desee.

9.5.2 FREAK, amenaza cibernética descubierta y formalizada en el año 2015 caracterizada por buscar vulnerabilidades en protocolo SSL/ TLC que se usa para HTTP, el cual descifra claves con longitud menor a 512 bit.

9.5.3 PSYB0T, amenaza cibernética descubierta en el año 2008 y fue creado para atacar enrutadores y módems de alta velocidades.

9.5.4 SQL SLAMMER, amenaza cibernética que se creó con el fin de atacar bases de datos buscando vulnerabilidades en programas SQL.

9.5.5 BLASTER, amenaza cibernética que se propaga por medio de vulnerabilidades de seguridad en comando de acceso remoto, desplazándose por servidores IIS creando daños de negación de servicio.

9.6 TIPOS DE ATAQUES Y FRAUDES INFORMÁTICOS

Con la implementación de las nuevas herramientas de comunicación en la sociedad la vida cotidiana de las personas se condiciona y ellos están obligado a estar actualizados en temas relacionados con la tecnología, ya que una característica del nuevo mundo tecnológico es la innovación, por eso es importante resaltar la importancia que estas tienen en los sistemas organizacionales.

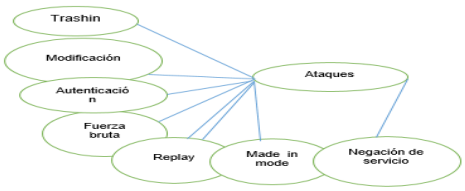
Lamentablemente el impacto que estas causan en la sociedad no es positivo en su totalidad, si las empresas no estructuran buenas políticas para la seguridad en sus sistemas de información, estas quedaran expuestas a lo que hoy se conoce con el nombre de “ataque informático”.

Que se puede definir como un método organizado que utilizan ciertos individuos de una comunidad para causar daños a los sistemas de datos, donde se aprovecha las

vulnerabilidades que presentan el hardware y software que constituyen un ambiente informático. Los daños que estos ataques pueden causar se pueden clasificar en: daños triviales, daños severos, daños menores, daños moderados, daños mayores y daños ilimitados.

El primer daño hace referencia a problemas con los sistemas de información solo causas mínimas molestias a los usuarios. El segundo se caracteriza porque son cambios mínimos que causan los virus, el usuario no se percata de las modificaciones en los datos y también puede causar molestia de funcionalidad en algunas aplicaciones. El tercero se orienta a cuásar problemas a los programas y aplicaciones en los sistemas de datos. Los moderados, son aquellos que se ocasionan directamente al disco duro de los ordenadores cambia el formato del disco FAT, o se sobre escribe sobre el mismo muchas veces esto se solucionan utilizando Backus del sistema operativo. Los daños mayores, son aquellos que los virus causan a el sistema ni la restauración los logran solucionar y toca realizar otra vez la instalación y configuración del sistema de información y por último los ilimitados**,** son aquellos ataques que le otorgan privilegios al atacante de disponer de la información del sistema. Así mismo, estos daños se relacionan con el tipo de ataque que realice el delincuente a la hora de cometer el delito.

Figura 7. Fraudes informáticos



Fuente: Gutierrez T. Dayro. Tipos de ataques fraude informático. [Grafico]. delitos informáticos. [Consultado: 6 septiembre 2018]. https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico

10. ANALIZAR LOS DIFERENTES TIPOS DE ATAQUES CIBERNÉTICOS A LOS CUALES ESTÁN EXPUESTAS LAS ORGANIZACIONES EN COLOMBIA

A medida que trascurre el tiempo observamos como en Colombia surgen las organizaciones grandes, medianas y pequeñas que están incursionando en diversos sectores tales como son industriales y bienes de servicio que mueven la economía colombiana y no tienen en cuenta los diversos problemas tecnológicos que pueden presentar la institución si en su planificación o funcionamiento no implementan una buena seguridad en su sistema de información, dejándolas así expuestas a los constantes peligros, amenazas o ataques cibernético entre los cuales destacamos el malware, apt y ransomware que son los que han afectado la economía de las entidades colombianas en los últimos años .

Un reciente estudio realizado por el gobierno Colombiano sobre el impacto de incidentes de seguridad digital para el año 2017 con el apoyo del ministerio de tecnología, OEA, organización de estado americano y BID banco internacional del desarrollo afirman que para que las organizaciones en Colombia puedan entender bien el tema ellas deben tener los tres conceptos básicos que se relacionan con la seguridad informática, seguridad de información y cyber seguridad empresarial, el primer término, hace referencia a la gestión que realiza la entidad para protección de sus datos orientado al monitoreo del flujo de información, el segundo se basa en estandarizar los lineamiento de seguridad de datos apoyados con las diversas matrices de riesgo que existe para comparar las vulnerabilidades en las cuales destacamos ventana de AREN, metodología octave, Margaret, y DAFP.

Por último, el concepto de seguridad empresarial que hace referencia a como las organizaciones colombianas defienden su entorno de los ataques cibernéticos a lo que están expuesto debido a los constantes cambio que sufre la sociedad por el uso de las herramientas tecnológicas enfrentándose a contextos volátil, incierto, compleja y ambiguos.

Para esto podemos analizar las vulnerabilidades ala que están expuestas las empresas dedicada al marketing en Colombia, primero partimos de observar el contexto en el cual funciona cada una, por ejemplo, las entidades que se encarga al comercio digital podrían sufrir de ataques cibernéticos relacionados con la ingeniería social como: (spear- phishing), (hole – attacks). Las variables que se pueden asociar para el delito son:

Personas = Procesos = tecnología

Figura 8. Análisis de contexto para ataque cibernético

GUTIERREZ T. Dayro. Análisis de contexto para ataque cibernético [imagen] Colombia. Encuesta global seguridad informática 2015. P. 13[consultado 10 Febrero 2019] https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015

Como podemos observar en el gráfico se enumeran las cuatro características que afectan las organizaciones que trabajan mediante el comercio electrónico. La primera relacionada con las ventas; hace referencia a la comercialización de producto por medio de E- MAIL del cual las entidades deben su funcionamiento a este atributo.

Cadenas de suministro; es la parte donde el personal maneja el sistema de pedido y pagos en línea de los productos, por eso es importante la protección de este medio atravez de él se da la comunicación entre empresa cliente.

Investigación de desarrollo; esta es la parte donde la entidad atravez de estudio previamente realizados implementa el uso de tecnología y herramientas de información para promocionar sus productos y a la vez cumplir con las necesidades a las cuales están sujetas los individuos de una comunidad por eso es importante que este atributo no esté expuesto a dominio de terceras personas porque pondría el riesgo el nivel competitivo de dicha organización.

Cuentas por pagar; es el resultado que queda de una mala planificación para la seguridad de un sistema de información que es expuesto al delito cibernético, ocasionando liberación de información, datos de privacidad.

10.1 GESTIÓN DE CIBERSEGURIDAD – ASUNTO DE LA SUPERVIVENCIA PARA LAS ORGANIZACIONES

A pesar que el estado colombiano ha crecido con relación a políticas de seguridad informática, las organizaciones siguen expuestas al peligro que estas pueden llegar a tener cuando sufren ataques cibernéticos, por eso las instituciones públicas y privadas continúan trabajando para el fortalecimiento de los sistemas de datos para lograr anticiparse a los delitos informáticos.

Las entidades financieras son las que más planifican en su presupuesto para la protección de información, han involucrado en su estructura funcional, prácticas internas relacionadas con seguridad de datos. La organización que se encarga de ejercer control “ASOBANCARIA” se encarga que las entidades financieras en su funcionamiento implementen estrategias que constituyen mejoren la seguridad cibernética.

Esta hace poco público un proyecto que tiene como objetivo dar a conocer cuáles son los requisitos mínimos para que todas las organizaciones financieras trabajen a la gestión de riesgo cibernético

- Inclusión del enfoque de riesgo frente a los temas ciberseguridad y seguridad de información

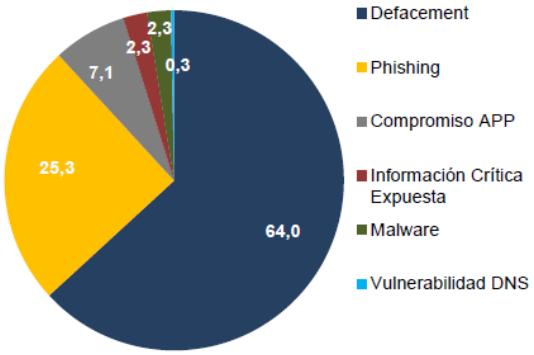
- Asenso de probabilidades de monitoreo por parte de las mayores ordenes de dirección

10.2 ATAQUES CIBERNÉTICOS UNA CRECIENTE AMENAZA

De acuerdo al informe publicado por “ASOBANCARIA” en la semana económica, el informe sobre delitos informáticos que registra el centro cibernético de la policía nacional para el año 2017 aumento un 28.3 % frente a los resultados obtenido para el año 2016, el cual destaca que el ataque cibernético que más afecto las organizaciones en Colombia fue el ransomware.

Por otra parte, el grupo colcert del centro de investigación de ASOBANCARIA, dio a conocer los ataques más comunes para el año 2017 los cuales se relacionan el siguiente gráfico

Figura 9. Tipos de incidentes cibernéticos en Colombia para el año 2017

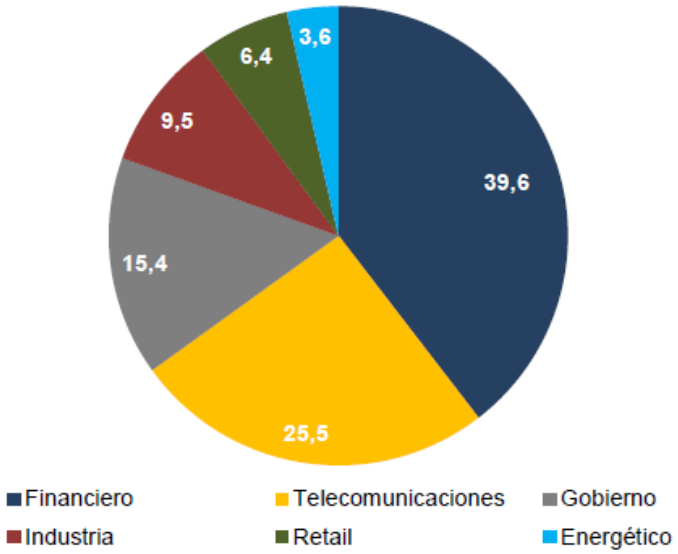


Fuente COLCERT. Asbancaria. Tipos de incidentes cibernéticos [imagen]. P.4 [consultado 14 febrero de 2019] disponible internet: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

Con referencia a los sectores afectado por los delitos informático el más sobre saliente es el financiero dado debido al tipo de información que almacenan los sistemas y los recursos que manejan [13]

La compañía de ciberseguridad digware mostro en el evento de information Security trends meeting que se realizó en Bogotá el 2017 que los sectores más afectados por ciberdelincuencia son: el financiero con 214000 ataques por día con porcentaje de 39,6 % seguido por el de telecomunicaciones con 138.329 ataques por día con porcentaje de 25,50 % como se muestra a continuación en el siguiente gráfico

Figura 10. Distribución de los ataques cibernéticos por sectores económicos en Colombia



Fuente DIGIWARE. Asbancaria. Tipos de incidentes cibernéticos [imagen]. P.4 [consultado 14 febrero de 2019] disponible internet: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

[13] Fuente COLCERT. Asbancaria. Tipos de incidentes cibernéticos [imagen]. P.4 [consultado 14 febrero de 2019] disponible internet: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

10.3 EVOLUCIÓN EN COLOMBIA SOBRES ATAQUES CIBERNÉTICOS Y APT

Analizando el contexto colombiano relacionado con pymes, se ha logrado un conjunto de acciones para mejorar la seguridad informática dentro de las instalaciones orientada bajo el concepto de APT que a su vez está ligada con los ataques de malware y ransomware y la forma de como las grandes, medianas y pequeñas organizaciones en Colombia están tomando precauciones para mejorar la seguridad en su sistema de información.

Este tipo de información se toma desde antecedentes históricos de ataques de penetración que han realizado los delincuentes y la forma de cómo evoluciona la técnica y herramientas que utiliza dependiendo de los cambios que sufra el contexto tecnológico que tenga la organización en su funcionamiento.

Es importante resaltar que dependiendo de la actividad económica por la que se caracterice las entidades y el flujo de dato que se maneje se toman las medidas de seguridad informática que satisfagan las necesidades para la protección de datos de la empresa correspondiente[14]

También se resalta que los ataques que se cometen en Colombia sino en todo el mundo son porque los hacking se percatan que ciertas entidades en su funcionamiento tienen solo un servicio de antivirus y estos no son suficientes para evitar ataques cibernéticos relacionados con malware, apt y ransonware.

Como estrategia para disminución de estos ataques se contrata el servicio de hacking el cual por medio de las matrices de riesgo informático se puede analizar las vulnerabilidades a las que están expuesto los datos de las empresas y así tomar medidas para salvaguardar y proteger la información en los sistemas.

[14] UNIPILOTO, desconocimiento de las Pymes colombianas frente a las amenazas persistentes. [en línea]. [Consultado 11 de septiembre de 2018]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2957/00002030.pdf?sequence=1

10.4 AVANCES DEL SECTOR PÚBLICO EN LA ELABORACIÓN DE POLÍTICAS PARA MEJORAR LA CIBERSEGURIDAD EN LAS ORGANIZACIONES DEL ESTADO EN COLOMBIA

Los países sud desarrollado, en este caso Colombia ha sufrido con el aumento de los ataques y amenazas cibernética dirigidas a las organizaciones por no tener una buena protección en su sistema de información. Por esta razón el estado en los últimos años viene trabajando en la creación de nuevas estrategias de seguridad de datos a nivel nacional y por eso las nuevas políticas la han orientado a tres objetivos básicos los cuales son:

- Utilizar métodos apropiados para prevenir, coordinar, atender, controlar y generar recomendaciones para controlar ataques relacionados con temas de ciberseguridad y ciberdefensa a nivel nacional.

- Ofrecer charlas especializadas en cuanto a temas de ciberseguridad y ciberdefensa

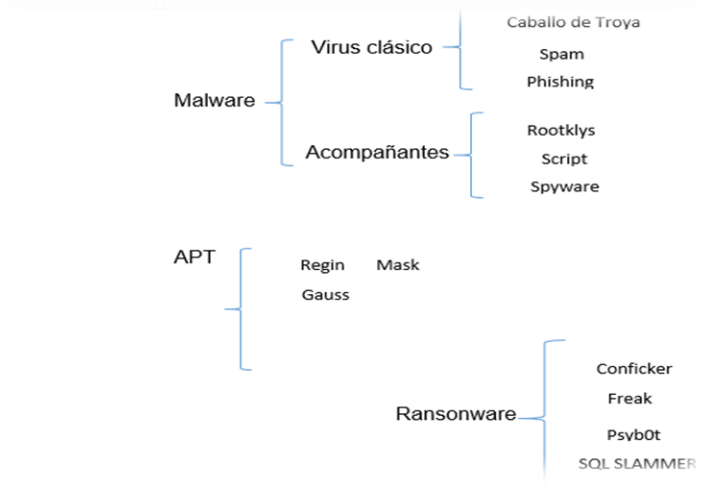
- Fortalecer las normas en cuanto a temas de seguridad y defensa de datos e incluirlas en las leyes para mejorar los instrumentos relacionado con la temática.

A pesar que el estado colombiano ha implementado las nuevas políticas para mitigar los ataques en los últimos años estos han aumentado debido a que han aparecidos nuevas modalidades y seguirán apareciendo ya que estás se van modificando debido al constante cambio que va sufriendo la sociedad con el uso de las tecnologías de información.

10.5 TIPOS DE ATAQUES

En el siguiente cuadro sinóptico resaltaremos los tipos de ataques más comunes que se pueden realizar; para luego resaltar aquellos que han causado impacto negativo en las organizaciones colombianas en los últimos años.

Figura 11. Tipos de incidentes cibernéticos en Colombia para el año 2017



Fuente: Gutierrez T. Dayro. Tipos de ataques fraude informático. [Grafico]. delitos informáticos. [Consultado: 6 septiembre 2018]. https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico

10.6 ANTECEDENTES DE ATAQUES COMETIDOS COLOMBIA

Se puede resaltar que en Colombia hasta las organizaciones del estado están expuestas a los delitos informáticos ejemplo de esto tenemos en las elecciones para el año 2010 las empresas de telecomunicaciones UNE y EPM fueron contratadas para analizar y establecer cuáles fueron las causas que ocasionaron el colapso de la plataforma virtual que se asignó para el control de la información de las elecciones para ese mismo año. El resultado de la investigación arrojo que ciertas direcciones IP realizaban consultas consecutivas y este género que dicho campo virtual quedara fuera de funcionamiento, a su vez también se obtuvo que las IP se relacionan con oficinas del DAS los cuales estos fueron contratados para ejecutar esas acciones cuando para ese entonces Carlos Ariel Sánchez que tuvo diferencia de opinión con

los miembros de gobierno cuando el estado colombiano estaba legislado por el presidente electo para ese periodo Álvaro Uribe Vélez[15]

Siguiendo en la misma linea de la investigación está también evidenció que los ataques son practicados por el ejército Nacional y ministerio de defensa nacional Este tipo de ataque se conoce como ping infinito y es muy fácil de hacer lo mismo que impedir, pero las partes encargadas no lo quisieron y por tal razón hubo manipulación en el conteo de votos y las cifras hasta el momento no son creíbles, pero igual se trabajaron con ellas y gobernaron nuestro país. Haciendo una VPN entre las ciudades y manejando esa información por un medio único como un canal de televisión evitamos este tipo de riesgo, pero no fue así. Por otro lado, tenemos el problema de la alcaldía de Bogotá

Para el mismo año en abril de 2010 la directora de asuntos disciplinarios ordeno una investigación contra el alcalde Samuel Moreno por contratar una organización de manejo de información que presentó negligencias al cumplir sus funciones. [16]

Luego en la administración de Gustavo Petro el problema se originó por qué no daban para justificar porque se perdía mucho tiempo en consultas de correos privados originados por la dependencia y despacho de la alcaldía.

Tiempo después se realizó una sustitución en la alcaldía y dirección de asuntos disciplinarios en Bogotá dejando a cargo a él abogado Augusto campo en la dirección distrital luego lo primero que hizo fue rechazar la defensa contra la empresa que se contrató para manejar los sistemas de información activando nuevamente las investigaciones encontró que se realizaron 8000 consultas en los sistemas de datos en áreas ajenas a la dependencia de la alcaldía, después de hacer un cruce entre los

[15] MOGOLLÓN M. Felipe. Hacker atacaron Registraduría [EN LÍNEA] el espectador (21 de mayo 2011). Párrafos 3-9 (15 de septiembre 2018) https://www.elespectador.com/content/los-hackers-que-atacaron-la-registradur%C3%ADa

[16] QUEVEDO. Norbey investigación/una-hacker-alcaldia-de-Bogóta-articulo-388664 [En línea]. Un hacker en la alcaldía de Bogotá. Publicado (22 de noviembre 2012).consultado (11 de diciembre de 2018).Disponible en internet: https://www.elespectador.com/noticias/investigacion/una-hacker-alcaldia-de-bogota-articulo-388664

correos de los funcionarios y los jefes se pudo concluir que se estaba cubriendo información de posible acoso laboral de los jefes a los empleados.

10.7 VECTORES DE ATAQUES

Se conoce como vector de ataque a cualquier acción que realiza un delincuente a la hora de golpear una superficie que está constituida por elementos de información o herramientas tecnológicas. Una vez analizado el espacio se identifica un *vector de ataque*, que es la ruta que el atacante puede utilizar para sacar provecho del dispositivo, lo que permite que el atacante utilice el dispositivo para algo diferente a su propósito

En la actualidad existen dos tipos de vectores los que se conocen con el nombre de ataques pasivos y los activos, los primeros son aquellos que están relacionados con los ataques: Spoofing delito informático que consiste en suplantación de identidad fundamentado en modificar los datos en de un router para provocar atraso en los sistemas

DDoS**,** delio informático que se caracteriza por mantener ocupada el ancho de banda de una red mediante mensajes que alteran el funcionamiento normal del sistema.

En el segundo delito también se puede realizar un estudio del tráfico de datos en una red de información, donde el delincuente intercepta la ruta de comunicación y puede encontrar la cantidad de datos que se están transfiriendo por el mismo canal de comunicación.

Escuchas furtivas, son aquellas que se producen en las redes móviles de tipo ad- hoc y esta se orienta a descifrar e investigar información confidencial.

10. 8 CARACTERÍSTICAS DE VECTOR DE ATAQUE MALWARE

Algo que se debe tener en cuenta son las características fundamentales de cada vector esta depende del tipo de superficie que estén atacando por ejemplo las características para el malware podemos resaltar:

- ✓ Desencriptar información flexible del usuario
- ✓ Almacenar datos personales y financieros
- ✓ Atacar y acceder a sistemas de información
- ✓ Almacenar password y datos confidenciales de las organizaciones
- ✓ Dañar dispositivos lógicos e informáticos

10.9 ATAQUES IOT (INTERNET DE LAS COSAS)

Los ataques de denegación del servicio están orientados para atacar los hostings mediante envíos de tráfico a protocolos HTTP con el fin de bloquear o detener el acceso a internet a los sistemas de información. Los ataques de denegación de servicios por IOT por lo general se realizan a un conjunto de ordenadores que funcionan con servidores.

Por otra parte, los bots de spam, son delitos cibernéticos que se caracterizan por alimentar la industria del spam. Este medio mueve mucho dinero. Los administradores de sistemas gastan enormes cantidades de tiempo y energía para poner en listas negras los relés de spam conocidos, esperando que tan sólo una fracción de los emails de los spammers llegue a la bandeja de entrada

Otras características que podemos resaltar son las contraseñas débiles, este proceso se da con el fin de facilitar el manejo de los dispositivos a los usuarios, los fabricantes quieren que sus dispositivos se puedan configurar y utilizar fácilmente. Por eso los fabricantes saben que muchos de los usuarios finales de los dispositivos de IoT a menudo son personas con pocos conocimientos técnicos. Para que el dispositivo sea fácil de configurar y de utilizar, el fabricante hace que haya una forma fácil de iniciar

sesión en el dispositivo, como una única combinación de identificación de usuario/contraseña.

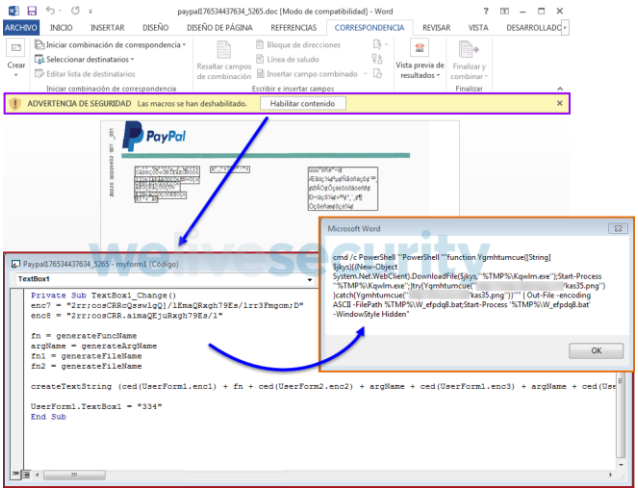
Finalmente, la falta de cifrado en la seguridad a menudo es un pensamiento tardío que en el ciclo de vida de desarrollo de los dispositivos de IoT, las funciones de seguridad, como el cifrado, son a menudo desechadas o ni siquiera se consideran. La industria solicita la criptografía incorporada, como los coprocesadores criptográficos que pueden manejar el cifrado y la autenticación en dispositivos de IoT

10.10 VECTOR DE ATAQUES PARA MACROS

La característica principal d este vector de ataque es que utiliza código de visual Basic para aplicaciones de tipos VBA las cuales se conocen con el nombre de macro. Para poder realizar este delito el usuario necesita autorizar el virus para poder activar su funcionamiento

Algunas veces se puede eliminar la infección de los documentos, pero en otros archivos se dificultad porque vienen protegidas con password creados por los atacantes

Figura 12. Vector ataque macro

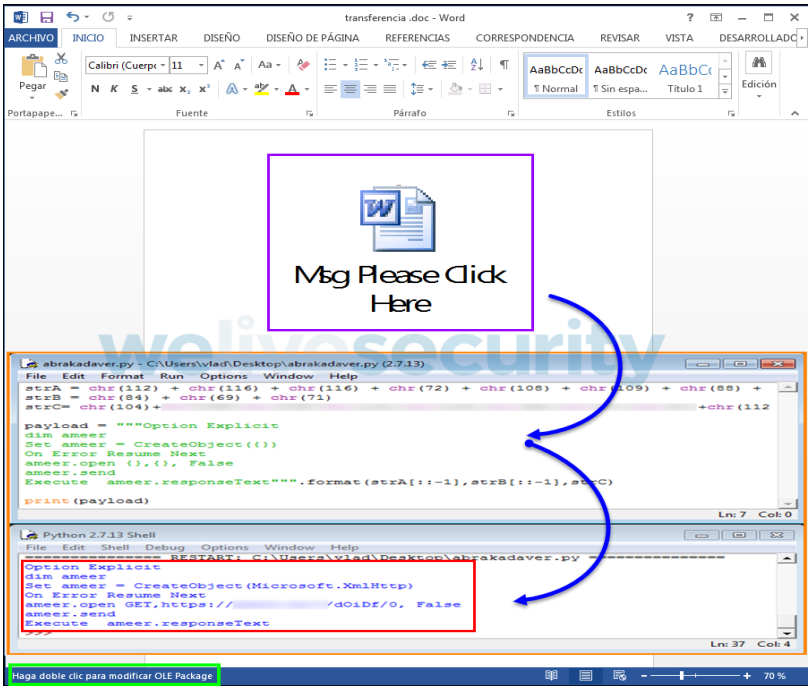


Fuente: PÉREZ Diego. Vectores – Documento de ataques [imágenes] vector macro disponible en internet: https://www.welivesecurity.com/la-es/2017/11/17/vectores-ataque-documentos-de-office/

10.11 VECTOR DE ATAQUE 2: DOCUMENTOS CON OLE

Vector de ataque que involucra archivos maliciosos con objet link (OLE) mediante esta modalidad se puede introducir archivos con scripts y para que este se pueda ejecutar igual que al de las macros el usuario tiene que dales permiso para ejecutarlo para poder infectarse

Figura 13. Vector ataque OLE

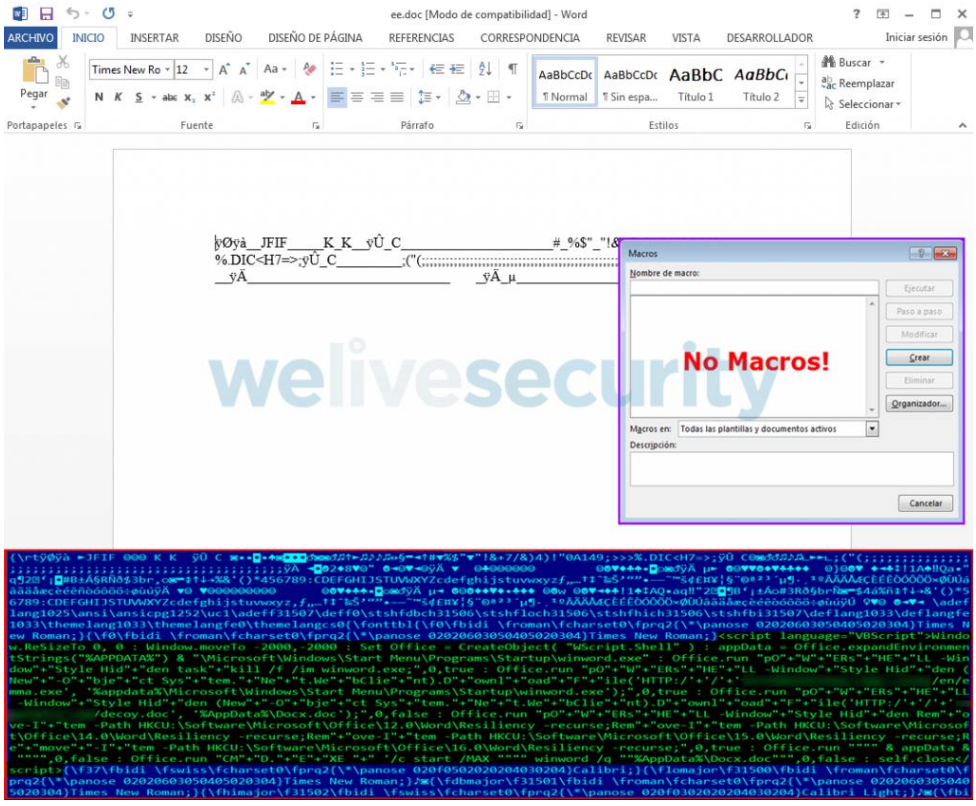


Fuente: Pérez Diego, Dayro. Vectores – Documento de ataques [imágenes] vector macro disponible en internet: https://www.welivesecurity.com/la-es/2017/11/17/vectores-ataque-documentos-de-office/

10. 12 VECTOR DE ATAQUE 3: DOCUMENTOS QUE EXPLOTAN VULNERABILIDADES

Este tipo de vector tiene como principios fundamentales vulnerar documentos creados con aplicaciones ofimáticas Microsoft Word, exel, Power point. A diferencia de los demás vectores que mencionamos anterior mente el virus se ejecutara al momento de abrir cualquier documento de tipo ofimático, ya que esta no necesita autorización del usuario para dispersarse

Figura 14. Vector ataque vulnerabilidades



Fuente: PÉREZ, Diego. Vectores – Documento de ataques [imágenes] vector macro disponible en internet: https://www.welivesecurity.com/la-es/2017/11/17/vectores-ataque-documentos-de-office/

10.13 VECTOR DE ATAQUE CONTRA APT

La protección de datos ha trascendido a valorar los activos involucrados para su funcionalidad en las organizaciones, identificar los diversos ataques que han sufrido las instituciones que constituyen una sociedad puede ayudar a planificar nuevas estrategias para mejorarla seguridad de informaciones para los sistemas de las ciudades tecnológicas ya que su funcionamiento se basa en os principios de eficiencia, sostenibilidad y gestión de recurso

10.14 RECURSOS AFECTADOS POR AMENAZAS TIPOS APT

Figura 15. Sectores afectados APT

Fuente: GUTIERREZ, Dayro. Vectores – Documento de ataques [imágenes] amenazas a sectores disponible en internet: https://www.blog.andaluciaesdigital.es/ciberataques-y-amenazas-contra-la-smart-city/#Recursos_afecta

Dentro de las características principales que existe dentro de este tipo de sociedad se da mucho la interoperabilidad de los sistemas en cuanto a las amenazas cibernéticas las más comunes podemos destacar la falsificación, denegación de servicios , intercepción de comunicación, modificación de código malicioso etc las cuales apuntan contra los pilares de la información por eso independiente del tipo de ataque o vector que esté utilizando para atentar contra la estabilidad de seguridad de datos es necesariamente implementar controles cibernéticos para prever estas acciones.

Entre estos ataques a las ciudades Smart destacamos:

- Malware
- Exploit kits
- Phishing
- Ataque de denegación de servicio (DDoS)
- Interceptación, robo o sabotaje de datos

11. RECONOCER CUALES SON LOS ELEMENTOS QUE INFLUYEN PARA QUE LAS ORGANIZACIONES NO IMPLEMENTEN UNA BUENA METODOLOGÍA PARA LA PROTECCIÓN DE INFORMACIÓN.

En la actualidad cuando se habla de tecnologías, enseguida el término se relaciona con herramientas las tic, internet e información esta característica es fundamental para el funcionamiento de las organizaciones, por eso cuando las empresas invierten en un modelo de seguridad de información es necesario que no lo consideren como un gasto innecesario, sino como una forma de mantener su funcionamiento en la sociedad, ya que en esta época todo se está globalizando al uso de las tecnologías y manejo de información.

Existen ciertos criterios que se consideran relevantes a la hora de realizar una planeación de seguridad informática entre estos resalta el factor humano, como un material que da un valor agregado a la inversión. se debe tener en cuenta el consto de la inversión del recurso humano, ya que este varía dependiendo de numero de empleado que estén laborando en la entidad, en Colombia esto se estipula en la ley 590 para el fomento de las micro, pequeñas y medianas empresas que quieran organizarse con MI PyMEs.

se debe tener en cuenta el consto de la inversión del recurso humano, ya que este varía dependiendo de numero de empleado que estén laborando en la entidad, en Colombia esto se estipula en la ley 590 para el fomento de las micro, pequeñas y medianas empresas que quieran organizarse con MI PyMEs.

Las micro empresas con nomina no menor a 10 trabajadores, con activos totales excluidos la vivienda por valor inferior a 500 salarios mínimos
Las pequeñas empresas con una nómina entre 11 y 50 trabajadores con activos mayores a 501 5001 salarios mínimos vigentes.

Por ultimo las medianas empresas con nominas entre 51 y 200 empleado con activos mayores deberán pagar entre 5001 y 30.000 salarios mínimos vigentes legales.

Con relación al costo que deben tener las grandes empresas en los diversos sectores y las categorías de las empresas según Mi PyMEs la tecnología que se utilizara dependerá del tipo de información y flujo de dato que tenga la entidad; por eso los factores que se consideran para este proceso serán:

- ✓ Capacitación
- ✓ Hardware
- ✓ Asesoría
- ✓ Fuerza de implementación
- ✓ Sostenimiento de seguridad
- ✓ Licencias renovadas
- ✓ Soporte
- ✓ Empleados
- ✓ Disminución de proadtividad

Capacitación, este proceso hay que analizarlo desde dos puntos de vista el primero hace referencia al cliente explicarle porque es importante el proceso de sistematización de la entidad. El segundo el empleado capacitar al trabajador para que pueda realizar su trabajo.

Hardware, algunas veces la implantación del nuevo sistema requiere inversiones de hardware, compras de nuevos pc y armar la infraestructura de red dependiendo de las necesidades de la entidad.

Asesoría, debe existir acompañamiento de una persona profesional o especialista en el área de sistemas que haga seguimiento al proceso de sistematización para asegurase el sistema cumple con los requerimientos de la entidad.

Sostenimiento de seguridad, esta etapa es importante porque atravez de esta se garantiza que los elementos que conforman el sistema no presenten desgaste y causen fallas al funcionamiento.

Renovación Licencia, en la utilización de vida útil del software existen costos adicionales del programa algunos pueden ser de renovación, periódicamente, o actualización de aplicaciones a versiones más recientes.

Para entender la problemática que se vive en Colombia con los ataques cibernéticos a las industrias, organizaciones privadas, financieras, y los demás sectores es necesario hacer un análisis utilizando la ingeniería social.

Un informe recién publicado en computerword afirma que la falta de implementación de programas en seguridad de datos para capacitar a los trabajadores y junta directiva contra ataques cibernéticos pone en riesgo la estabilidad de cualquier entidad que use herramientas tecnológicas es su funcionamiento.

Este artículo pone como ejemplo a Colombia, un país que en la actualidad se presentan situaciones donde los ciudadanos, sin tener propósito son víctimas de los delitos informáticos relacionado con la ingeniería social, el cual es un ataque que se realiza mediante la manipulación o sugestión por un tercero que hace al usuario compartir información confidencial. Esta es una de la modalidad que lleva más de 15 años extrayendo información personal y organizacional del individuo de la sociedad.

Patricia Gaviria directora de la educación ETEK internacional afirma: que el resultado de la investigación que se realizó da como respuesta que las organizaciones deben complementar su planificación en seguridad de datos con empresas que brinden el servicio de seguridad y concientizar a los empleados sobre las precauciones que deben tener a la hora de manejar información que están almacenado a diario[17] en dichos sistemas.

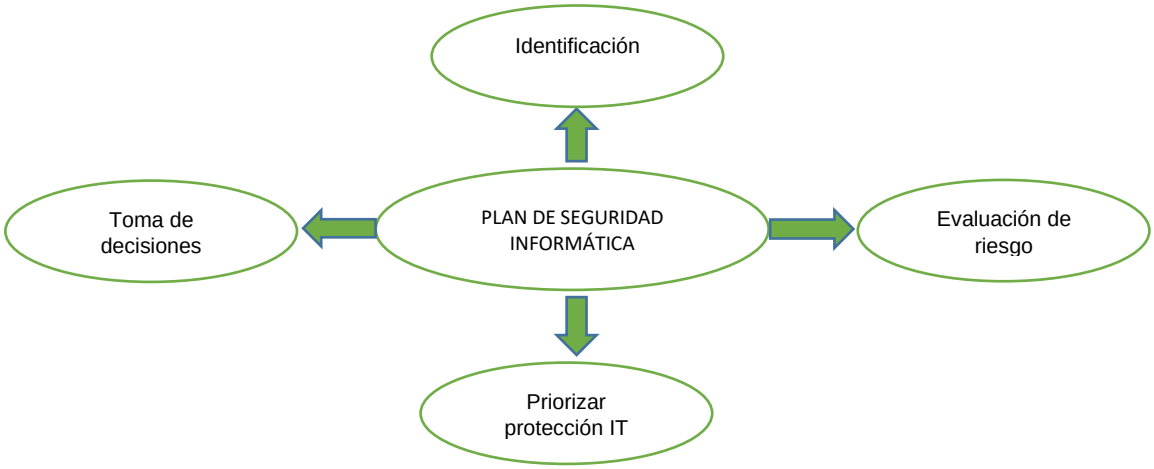
[17] Computer-world, Ingeniería social al servicio del ciber Cibercrimen. [EN LÍNEA]. Publicado (18-11-2018).párrafos 4-5 disponible en internet: https://computerworld.co/la-ingenieria-social-al-servicio-del-cibercrimen/

Un informe publica que desde el año 2013 al 2016 los elementos que influyen en la vulnerabilidad de las organizaciones pueden ser falta de conocimiento de los individuos en las entidades para manipular herramientas tecnológicas, la misma falta por parte de los trabajadores al no cumplir con las políticas interna de la misma empresa.

Los ataques cibernéticos que ocurren en las grandes, medianas y pequeñas entidades ya sea privada o públicas se dan por la carencia de un buen plan de seguridad informática, que es aquel que nos permite encontrar los riesgos a los que están expuestos las entidades cuando implementan tecnología de información al funcionamiento de la entidad.

Por eso en la elaboración del plan se debe realizar las siguientes etapas, como podemos observar en el siguiente gráfico.

Figuran 16 etapas para implementación de seguridad informática



FUENTE: GUTIERREZ T. Dayro. etapas para implementación de seguridad informática. [Grafico]. Etapas ITL. [Consultado 2 de marzo de 2019]. disponible https://www.universidadviu.com/crear-plan-seguridad-informatica-facilmente/

11.1 ¿FACTORES QUE SE DEBEN CONSIDERAR PARA FORTALECER LOS SISTEMAS DE DATOS DE LAS ORGANIZACIONES EN COLOMBIA?

Algunas organizaciones en Colombia no se preocupan por implementar estrategias de seguridad para la protección de su información, o si lo hacen no tienen en cuenta los riesgos que pueden presentar en su mismo funcionamiento. Por eso es importante que las instituciones realicen una planificación a largo plazo, no tomar medidas de prevención cada vez que estás sufra ataques cibernéticos.

Por eso cuando se esté realizando dicha planificación es necesario tener en cuenta la inversión recursos económicos, tecnológicos y talento humano

Una vez considerado el plan de seguridad de información, con sus respectivas etapas se estudia la manera de cómo fortalecer los sistemas de datos dependiendo del vector de ataque a los que estén expuesto dichas organizaciones; ya que no todos los ataques cibernéticos tienen el mismo comportamiento y estos van evolucionando dependiendo de los cambios que se presenten en la sociedad con relación a la tecnología, y manejo de herramientas las TIC.

Entre los factores que podemos fortalecer tenemos: las normas ciberseguridad CE007**,** en esta se plasman tres artículos de ley 0,29 – 0,42 y 0,52 los cuales fueron fundamentados por la superintendencia financiera, esta resalta normas como:

- ✓ Supervisión constante de los canales web, foro, redes sociales que prevenga organizaciones contra amenazas digitales.

- ✓ Utilizar mecanismo de cifrados complejos extremo a extremo para el envío y recepción de información confidencial

- ✓ Llevar el registro de los hábitos transaccionales legítimos de las que se hacen con normalidad.

Datos personales 1581 2012, la cual establece que la información es el activo más importante de las organizaciones, por eso el 17 de octubre de 2012 la Corte constitucional incluye esta ley para el manejo de cualquier tipo de información; donde en ella se regula el derecho fundamental habes data y se señala la importancia de la misma para su tratamiento.

La nueva norma busca proteger los datos personales registrado en los sistemas de bases de datos y que permiten realizar operaciones tales como recolección, almacenamiento y uso de circulación por parte de las entidades públicas y privadas.

Transformación digital (personas, procesos y tecnologías)

Las organizaciones deben gestionar un proceso que orienten estrategias, cultura y capacidades de la institución para aprovechar la innovación creada por un entorno digital para alcanzar sus objetivos planeados en sus políticas para su funcionamiento.

Por esos algunos retos que pueden presentar estas en su implantación serian:

- ✓ Cambio de pensamiento altas gerencias; estas deben estar comprometidas a iniciativas innovadoras
- ✓ Creación de una cultura empresarial
- ✓ Metodología fundamentada al conocimiento por los clientes, análisis y mediación de datos
- ✓ Desarrollo tecnológico factor competitivo
- ✓ Análisis canales de ventas
- ✓ Definición recursos financieros que apoyen proyectos de cambios

Es importante que las instituciones implementen como una herramienta de análisis la tecnología porque atravez de ella podrá tomar decisiones en tiempo real, teniendo como principio y final el uso de datos para estrategia de comunicación los cuales son

relevantes para la innovación de productos, servicios, y efectividad en campañas publicitarias.

En los sistemas de información, los ajustes de configuración son la parte más importante; porque atravez de ellos indicamos los parámetros y atributos por las cuales se fundamentan los sistemas partiendo desde los servidores a los dispositivos de red e información para las aplicaciones de escritorio.

Hay que tener en cuenta que cuando se implementa un sistema de información la perspectiva no va encaminada desde el punto de vista de la seguridad, sino desde la operatividad convirtiendo los sistemas de datos más inseguros.

También hay que tener en cuenta la configuración de los dispositivos de red, los cuales pueden tener diversas líneas de códigos para cada recurso relacionado con protocolos IP y tecnologías para complementar su funcionamiento.

Actualizar el sistema operativo, firmware y aplicaciones para mantenerlas a la vanguardia de los exploits que busquen atacar fallos en el código subyacente, mantener actualizado estos elementos optimizan el rendimiento de los sistemas de información, ya que los exploits siempre buscan identificar brechas de seguridad.

11. 2 TENDENCIAS DE LOS VECTORES DE ATAQUE CONTRA LA SMART CITY

Partiendo del análisis que se hace desde el punto de vista informático los ataques dirigidos APT en su estructura también incluye los famosos malware y ransomware estos tienden a aumentar si no se toman medidas contras las modalidades de ataques. Entre los aspectos podemos resaltar: existe más preparación por parte de los delincuentes a la hora de planificar los ataques informáticos. Ellos se están capacitando a la hora lanzar virus maliciosos a entidades clandestinas, estatales o agencia para espionaje. Para poder atentar contra la funcionalidad de infractucturas tecnológicas y así aumentar las amenazas contra los Dispositivos loT.

Modalidad para delito APT encaminada a la detección de nuevo malware que simulan trabajos normales del usuario.

Mientras tanto el ransomware aumenta su capacidad para infectar recursos de internet y lo podemos considerar unas de las potentes amenazas para las ciudades inteligentes. Ya que las estructuras están comprometidas si por ciertas razones se producen las guerras cibernéticas entre los países.

Finalmente, las herramientas especializadas van orientadas a las instalaciones relacionadas con cloud, ya que tiene una evolución que cualquier falla que presente el hardware y el firmware comprometen los datos del usuario que están en el sistema de información sin poder anular o cancelar la operación.

12. RECOMENDACIONES

- ✓ Para poder disminuir el efecto negativo que causa la implementación de las herramientas de información y las tecnologías en las organizaciones colombianas, es necesario concientizar a todos los empleados en las diferentes áreas administrativas que cuando se hace la transformación es con el objetivo de sobrevivir al nuevo mundo tecnológico y si no se logra una buena planificación cuando se sistematizan los datos de las entidades, se pueden enfrentar a una series de delitos informáticos que tienden a poner en riesgo la estabilidad económica de las empresas; esto lo podemos analizar en los últimos años donde los sectores más vulnerables en Colombia son las entidades financieras, industriales, telecomunicación. Gubernamental y la energética.

- ✓ Frente a los diferentes ataques que se presentan contra las organizaciones colombianas, es necesario buscar soluciones que puedan neutralizar los vectores de ataques que utilizan los ciberdelincuentes, entre ellas podemos aplicar realizar un patrón de seguridad más complejo; con leyes y estrategias de seguridad que relacionan de forma individual los recursos infractucturas que soportan las operaciones de la organización , con el marco de seguridad para la información se deberá implantar metodologías para actualización , hacer auditorias mensuales de seguridad para la parte física hardware y lógica del software dando respuesta inmediata alas incidencia que se pueden presentar con la manipulación de datos en la institución.

- ✓ Finalmente, las organizaciones necesitan definir la dirección de los programas en seguridad de información, ya que al final estos tendrán como objetivo especificar el tipo de tecnología necesaria para proteger de la mejor manera el flujo de datos de las empresas estos controles de seguridad tecnológicos necesitan revisarse y tratar de lograr una mejora continua, e innovadora"; del mismo modo en la misma planificación se debe considerar una seguridad de múltiples capas en cada uno de los dispositivos y la red, incorporar cifrado y monitoreo en los datos más sensitivos, y pensar en cómo agregar autenticación de múltiples factores para reducir el riesgo a los vectores más

comunes de ataques a las empresas: el usuario y la contraseña. “Podemos tener todos los procesos y tecnologías en su lugar, pero el atacante siempre va ir por el eslabón más débil para tratar de engañarlo y ser exitoso en el ataque: el usuario de los riesgos actuales, cómo reconocerlos y reportarlos. Esta es la mejor arma para mejorar el comportamiento del usuario frente a los ciberataques de hoy en día que utilizan ingeniería social. Regularmente, el programa debe evaluar el conocimiento de los empleados y de los equipos de seguridad para asegurarse que se encuentran en el nivel indicado”.

13. CONCLUSIÓN

- ✓ Con la realización de esta investigación acerca de las amenazas cibernéticas en las organizaciones del sector industrial y servicio, se ha logrado identificar que los ataques más comunes en los últimos años en el estado colombiano están relacionados con las amenazas de tipos Malware, APT y Ransomware y por los constantes cambios o evolución de las tecnologías en las diferentes etapas que vive la sociedad estos ataques están evolucionando y han aparecidos delitos que se derivan de las tres amenazas principales mencionadas anteriormente. Mientras que las organizaciones no implementen buenas estrategias para vencer el paradigma que existe con el ecosistema informático “medio volátil, inseguro e incierto” las empresas siempre van estar expuesta a los ataques cibernéticos. hoy en día las instituciones deben orientar su atencion a las vulnerabilidades y mecanismos de seguridad para evitar posibles delitos informáticos que puedan atentar contra su propia estabilidad económica, no es suficiente la implementación del firewalls, antivirus o una VPN que implica inversiones considerables, sino que el plan de seguridad informática este marcada por las áreas de las organizaciones que estén sistematizada, los empleados que son los que tienen las herramientas tecnológicas a su disposición Y los usuarios finales que son las personas que van a utilizar los servicios que ofrezcan las entidades.

- ✓ Otro punto relevante que hay que tener en cuenta para la investigación es que la ingeniería social influye también para que las categorías de ataques que constituyen las amenazas Malware, APT y Ransonware cumplan con sus objetivos utilizando los vectores de ataque para vulnerar los sistemas de información. Cada medio de propagación depende de ciertos factores como el comportamiento de los empleados y hasta los mismos usuarios si no toman las medidas preventivas adecuada, en este caso los delincuentes van hacer uso del vector de ataque adecuado, “Malware”; qué por utilizar modo de tipo Drive-by download, Homogeneidad, vulnerabilidad y puerta trasera se convierte en una de las amenazas preferidas para atacar las entidades

financieras. Las amenazas de tipo APT son ataques dirigíos el cien por ciento a las ciudades que están sistematizadas o las que conocemos con el nombre de Smart-city, las cuales también incluyen amenazas que están estructurada de la misma forma que Malware y Ransomware

- ✓ Finalmente, las organizaciones colombianas tienen que entender que la planificación, diseño e implementación de mecanismo de control son características fundamentales que deben estar contempladas en una buena propuesta para el plan de seguridad de información. Los empleados de las organizaciones se pueden considerar como unos de los eslabones débiles que tienen las empresas para el proceso de sistematización de información. Mientras que los trabajadores no se adapten a los ecosistemas informáticos que en la actualidad se está viviendo en las instituciones públicas o privada que constituyen la sociedad ellas estarán expuestas a los delitos informáticos que día a día sufren las empresas. El cambio en los modos de ataques y las estrategias que aprovechan al comportamiento humano frente a las falencias en uso de tecnología y seguridad de información deben ser el punto de partida para implantar estrategias que conlleven a sistemas de seguridad más robustos.

14. BIBLIOGRAFÍA

Aprendamos a programar.com. Lenguaje de programación php [En línea]. Criptografía-. aprenderaprogramar.com. publicado (21 de junio 2018. última actualización). Consultado el (23 de mayo de 2019). Disponible en internet: https://www.aprenderaprogramar.com/

ANDALUCÍA ES DIGITAL. Vectores de ataques y amenazas contra Smart city. [En línea]. Publicado (31 de mayo 2017). Consultado (15 de septiembre 2018).Disponible en internet: https://www.blog.andaluciaesdigital.es/ciberataques-y-amenazas-contra-la-smart-city/

AVAST. Software. Ransomware. [En línea]. [Consultado 2 de diciembre 2018]. Disponible en internet: https://www.avast.com/es-es/c-ransomware

BUSTAMANTE. Rubén. Seguridad en redes. [En línea] para obtener título de ingeniero electrónico y telecomunicaciones. Universidad Autónoma de estado de Hidalgo. Facultad de ingeniería. capitulo II – p -32 consultado (22 de mayo 2017). Disponible en internet en la página.

https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

CAIVIRTUAL. Policía. Informe amenazas cibernéticas Colombia [en línea]. (Publicado marzo 2017). [Consultado 17 de marzo 2017]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

COMPUTERWORD. Primer encuentro de expertos: antonimia, retrospección y Primer Encuentro de Expertos: Anatomía, retrospección y análisis de malware. [En línea] publicado (17 de mayo 2017). Consultado [10 de noviembre de 2017]. Disponible en internet: https://computerworld.co/primer-encuentro-de-expertos-anatomia-retrospeccion-y-analisis-de-malware/

CRAI-BIBLIOTECA –UAO. Uaolibguides. [en linea]. uao.libguides.com/c.php? g. actualizado (26 de noviembre 2018). consultado (15 de diciembre de 2018). Disponible en internet: https://uao.libguides.com/c.php?g=529806&p=4412778

DINERO, Los sectores económicos más impactados por el Cibercrimen en Colombia [en línea]. publicado (26 de septiembre de 2017). Disponible en internet: https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

DINERO, Los sectores económicos más impactados por el Cibercrimen en Colombia [en línea]. publicado (26 de septiembre de 2017). Disponible en internet: https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

EDICIÓN NORMAS APA 2016. 2017. normasapa.net. [En línea] abril de 2017. Disponible en internet http://normasapa.net/normas-apa-2016/.

EL PAÍS. 2017. *Google Docs. Sufre un ataque de 'phishing'.* [En línea] 5 de mayo de 2017. [Citado el: 26 de noviembre de 2017]. Disponible internet: https://elpais.com/tecnologia/2017/05/04/actualidad/1493887324_006575.html.

EL TIEMPO, informe sobre ataques cibernéticos en el sector financiero en Colombia. [En línea] publicado (27 septiembre de 2017). [Consultado 9 de mayo de 2018]. Disponible en internet: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

GARCÍA. De Mata. Criptografía básica para entender la tecnología de blockchain. [En línea]. Criptografía-básica-para-entender-la-tecnología-blockchain. Publicado (14 de marzo de 2018). P 1. Consultado (22 de mayo de 2019). Disponible el internet: https://blockchain.grantthornton.es/

GUILLEM. Alsina DEFINICIONES – ABC. Cracker. [en línea]. definicionabc.com/tecnología/cracker-phreakin-lammer. Publicado (mayo de 2017). p- 4 consultado (17 de mayo de 2019). Disponible internet: https://www.definicionabc.com/tecnologia/cracker-phreakin-lammer.php

GAVIRIA, Paricia. 2017. Phishing, el método de robo por internet más utilizado en el país. *NOTICIAS RCN.* Bogotá: RCN, 11 de octubre de 2017.

IBM. STEVEN. Perry, Anatomía de un ataque de malware a IoT. [En línea]. Publicado, (4 de marzo de 2017).consultado [20 de septiembre de 2017].Disponible en internet https://www.ibm.com/developerworks/ssa/library/iot-anatomy-iot-malware-attack/index.html

KASPERSKY, tipos de amenazas conocidas. [en línea]. publicado (11 de diciembre de 2018). [Consultado enero 3 de 2019]. Disponible en ihttps://support.kaspersky.com/mx/614nternet

MESESAN. Sergiu Open Data Securyti. Hackers-. [en línea]. Hackers-de-evolución-tecnologica-ha-armas-gubernamentales. publicado en (3 de enero -2017). P 1-2.consultado (15 de mayo .2017) disponible internet: https://opendatasecurity.io/es/hackers-de-evolucion-tecnologica-a-armas-gubernamentales/

Ministerio de educación. Colombia. Manual y normas de seguridad informática. [en linea]. Publicado (26 de septiembre de 2014). consultado (25 de mayo de 2019). Disponible en internet: https://www2.sgc.gov.co/ControlYRendicion/TransparenciasYAccesoAlaInformacion/CircularesManuales/MO-TEC-001-I.pdf

PAUS, Lucas. Similitudes y diferencia apt-avt [en línea]. Publicado (3 de marzo de año 2015). [Consultado 16 de mayo 2017]. Disponible en internet: https://www.welivesecurity.com/la-es/2015/03/31/similitudes-diferencias-apt-avt/

PORTAFOLIO, Colombia principal fuente de ciberataque en Latinoamérica [en línea]. Publicado (18 octubre de 2014). [Consultado 15 de febrero 2018].Disponible en internet: https://www.portafolio.co/negocios/empresas/colombia-principal-fuente-ciberataques-latinoamerica-50768

QUEVEDO. Norbey investigación/una-hacker-alcaldia-de-Bogóta-articulo-388664 [En línea]. Un hacker en la alcaldía de Bogotá. Publicado (22 de noviembre 2012).consultado (11 de diciembre de 2018).Disponible en internet: https://www.elespectador.com/noticias/investigacion/una-hacker-alcaldia-de-bogota-articulo-388664

RAMÍREZ. M, Cesar. El perfil criminológico del delincuente informático [en línea]. Publicado (el año 2013). [Consultado 15 de agosto de 2018]. Disponible en internet: http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf

REYES. Bernardo. Como citar y hacer referencias bibliográficas. [Video]. www.youtube.com/watch?v. publicado (5 de junio de 2016). Duración 12:34. consultado (30 de julio 2018). Disponible en internet: https://www.youtube.com/watch?v=RKkQKyNcfnA&t=82s

STUXNET, Wikipedia. [en línea]. publicado (año 2010). Consultado [10 de marzo de 2017]. Disponible en internet: https://es.wikipedia.org/wiki/Stuxnet

SUPINFO, virus informáticos [en línea]. Publicado (31 de noviembre 2016). [Consultado 3 de marzo 2017].Disponible en internet: https://www.supinfo.com/articles/single/3621-27-virus-informatique-ayant-marque-l-histoire

UNI-Colombia. Phreaking. [en línea]. informática forense. Publicado (6 de noviembre de 2017). consultado (20 de mayo de 2019) disponible en internet: https://www.informaticaforense.com.co/phreaking/

UNIPILOTO, desconocimiento de las Pymes colombianas frente a las amenazas persistentes. [en línea]. [Consultado 11 de septiembre de 2018]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2957/00002030.pdf?sequence=1

UROSARIO. Colombia no está preparada ante un ataque Ciberataque. [en línea]. Consultado (10 octubre 2018). Disponible en internet: http://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

WELIVESECURITY. Vectores que atacan documentos de office. [En línea]. Publicado (17 de Noviembre de 2017).consultado [3 de enero 2018].Disponible en internet: https://www.welivesecurity.com/la-es/2017/11/17/vectores-ataque-documentos-de-office/

XATACA- COLOMBIA, JUAN, Tamayo. Que tan preparado está el gobierno colombiano para enfrentar ataques cibernéticos [en línea]. Publicado el (25 de junio 2015).Disponible en: https://www.xataka.com.co/privacidad/que-tan-preparado-esta-el-gobierno-colombiano-contra-ataques-ciberneticos

ZENTOLOS, Los primeros virus informáticos [en línea]. publicado (13 de marzo de 2008). [Consultado 10 febrero 2019]. Disponible en internet: https://www.zentolos.com/?p=560