CIBERSEGURIDAD EN COLOMBIA

Valoyes Mosquera Amancio.
avamostova@hotmail.com
Universidad Piloto de Colombia

***Abstract*—**The hacking of companies has been increasing as time progresses, but when it compromises confidential informa-tion, damage to infrastructure, databases, etc., it affects the core of the business, and could even lead to bankruptcy. According to an annual report from Symantec (ISTR), which performed the analysis among 157 countries. Revealed that Colombia was the sixth country in Latin America with the highest number of attacks in 2017. In all these cases, cybersecurity has become a fundamental factor for the protection of the computer infrastruc-ture and everything related to it, especially the information that circulates In the network, this article will try to explain what is cybersecurity and its different meanings, and based on Colombia because there are weaknesses in the ability to mitigate these weaknesses and therefore seeks to generate policy guide-lines in cybersecurity and cyber-defense.

***Resumen*—**El hackeo a las empresas ha ido en aumento a medida que avanza el tiempo, pero cuando compromete información confidencial, daños a la infraestructura, bases de datos, etc., afecta el core del negocio, y podría llevarlos incluso a la quiebra. Según un informe anual de Symantec (ISTR), que realizo el análisis a entre 157 países. Reveló que **Colombia fue el sexto país de Latinoamérica con el mayor número de ataques en el 2017.** Por todos estos casos la ciberseguridad se ha vuelto un factor fundamental para la protección de la infraestructura computacional y todo lo relacionado de esta, especialmente la información que circula en la red, este articulo tratara de explicar que es la ciberseguridad y sus diferentes significados, y basándose en Colombia porque se tienen debilidades en la capacidad de atenuar estas debilidades y por ello busca generar lineamientos de política en ciberseguridad y ciberdefensa.

Índice de términos—Amenaza, ataque, ciberseguridad, Ciberdefensa, ciberespacio, cifrado, conpes, ISP, TI, TIC.

I. INTRODUCCIÓN

Antes de iniciar el artículo es importante aclarar dos términos, La ciberseguridad y la seguridad informática, la ciberseguridad normalmente se puede asociar con palabras como ciberespacio, Ciberamenaza, Cibercriminales u otros más. Pero constantemente lo toman como un sinónimo de seguridad informática y pues no es del todo cierto. Según una definición de Eset, la Ciberseguridad busca proteger la información digital en los sistemas interconectado. Está comprendida dentro de la seguridad de la información. [1] Para ello se debe explicar claramente los dos ya que con una definición acertada se podrá tener la conclusión más precisa de las diferencias entre estos dos términos.

Todo esto va porque se genera siempre una confusión cuando se tiene que aplicar y expresar de manera correcta estos dos términos, si bien existen muchas definiciones de ciberseguridad y de seguridad informática. A continuación, las definiciones.

II. CIBERSEGURIDAD

Existen varias definiciones de la ciberseguridad, en una edición de bSecure conferenced, es una conferencia donde se reúnen todo el profesional de seguridad de ISACA (Information Systems Audit and Control Association), y estos comenzaron a participar para poder darla una definición sobre que es la ciberseguridad, y la conclusión de acuerdo con la asociación, puede entenderse como:

"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". [1]

La iso 27001 define el activo de información como los conocimientos que para una organización tienen un valor, mientras que los sistemas de información son las aplicaciones, servicios, activos de tecnologías de información o demás componentes el cual permiten hacer un manejo de esta. Teniendo en cuenta estos dos términos se entiende que la ciberseguridad tiene como objetivo principal la protección de la

información digital, que esta o es transmitida entre los todos los dispositivos que se encuentran interconectados, por esto, la ciberseguridad está en la seguridad informática.

III. SEGURIDAD DE LA INFORMACIÓN

La seguridad en resumen lo que busca es reducir los riesgos hasta un nivel aceptable, ya que es difícil asegurar que se apunte a una solución ideal para evitar todos los peligros, es decir en todos los ámbitos la seguridad busca reducir los riesgos y buscar actividades encaminadas a proteger algún tipo de peligro. La información se encuentra en varias maneras: digital, física, incluso en manera no representada como seria las ideas o el conocimiento de las personar. Por lo tanto, sin importar su forma o estado, la información requiere que tengan medidas para su protección, que sean adecuadas de acuerdo con la importancia y su criticidad, y esto es precisamente lo que se encarga la seguridad de la información.

Ya teniendo los conceptos más claros de ciberseguridad y seguridad informática, se podría identificar las principales diferencias. El más primordial es que la seguridad de la información tiene un alcance mayor que la ciberseguridad, puesto que la seguridad de la información busca proteger la información de todos los riesgos posibles que puedan llegar a afectarla. La ciberseguridad se encarga principalmente de la información digital y los sistemas con los que se encuentran interconectados, los cuales la procesan, almacenan o trasmiten. [1]

IV. QUE Y PARA QUE LA CIBERSEGURIDAD

En la actualidad, la incursión de las tecnologías de la información y la comunicación (TIC), referentes principalmente a la informática (uso de computadoras) y las telecomunicaciones (Internet) ha cambiado radicalmente las ocupaciones y transformado los modelos comportamentales y las relaciones sociales.

Los beneficios que las TIC ayudan a la sociedad actualmente son muchos y muy perceptibles. Sin embargo, el desarrollo de dichas tecnologías brinda también un aspecto muy negativo: han abierto puertas a conductas antisociales y delictivas. Han aparecido nuevas maneras de atentar contra la privacidad y la propiedad de las personas y las empresas, para perpetrar agresiones cotidianas en formas no usuales.

Por ello la ciberseguridad se define como la práctica de defender los computadores y los servidores, los dispositivos móviles, sistemas electrónicos, las redes y los datos de ataques malicioso, a través de conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, métodos de gestión de riesgos, acciones y demás tecnologías que pueden utilizarse para proteger los activos de información de la organización y usuarios del Ciberespacio.

Pero que es el ciberespacio, este concepto nació en la ciencia ficción, fue William Gibson quien plantea por primera vez la idea de un “Ciberespacio”, se trata de un campo donde el ser humano puede construir un mundo donde realiza lo que desee, se proyecta de la manera que le parezca y obtiene aquello que el mundo físico le niega o le condena a no tener.

Su origen viene en la palabra griega Cibernao (pilotear una nave), y dándole un entorno más informático, se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red.

V. DELITOS INFORMÁTICOS

Hacer seguimiento al delito es una tarea compleja, y enfrentar la delincuencia transnacional y el crimen organizado en todo nivel es la tarea que se realizada por el ministerio público por mandato constitucional y por disposición legal. Pero el fenómeno que se ha visto en los últimos tiempos ha tenido un avance significativo en cuanto la masificación de esta clase de delitos y tecnificado a otra clase como son los delitos informáticos.

Como escribe albánese, citado por Carlos Resa, "el crimen organizado no existe como tipo ideal, sino como un “grado” de actividad criminal o como un punto del 'espectro de legitimidad". Esto en si define el crimen organizado, y este a través, de los años se ha ido extendiendo a un marco global, o transnacionalizando, y por ello se habla de delincuencia transnacional. [2]

Los progresos a nivel mundial de las computadoras, el aumento del almacenamiento, mejor procesamiento, miniaturización de los chips, la investigación de la inteligencia artificial, etc., ejemplifican el

término "era de la información" o era de la informática. Por tanto, las implicaciones de este aumento han resultado en nuevos escenarios y un abuso de la actividad informática y su repercusión el mundo informático, y generados grupos con comportamientos delictivos y en algunos casos difíciles de tipificar en las normas penales tradicionales, por ello el sistema ha denominado a este grupo de manera genérica delitos informáticos, criminalidad mediante las computadoras, delincuencia informática, criminalidad informática.

El aspecto más importante de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después. [3]

Julio Téllez Valdés, coordinador del observatorio 2.0 de la Unam, e investigador de tecnología, conceptualiza al delito informático en forma típica y atípica, entendiendo por típica, *"las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por la atípica "actitudes ilícitas en que se tienen a los computadores como instrumento o fin".* [4]

Parker define a los delitos informáticos como *"todo acto intencional asociado a una manera u otra a los computadores, en los cuales la victima habría podido sufrir una perdida, y cuyo autor ha o habría podido obtener un beneficio".* Paker además propone una tabla de los delitos informáticos de acuerdo con el propósito que consiguen:

1) **Propósito de investigación de la seguridad:** Abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, nycum and oura, 1973).
2) **Propósito de investigación y acusación**: Delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática (departamento de justicia de estados unidos).
3) **Propósito legal:** Delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.
4) **Otros propósitos:** Abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

La brigada de investigación tecnológica de la policía nacional española los clasifica de la siguiente manera:

1) **Ataques que se producen contra el derecho a la intimidad**: delito de descubrimiento y relevación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos (artículo del 197 al 201 del código penal).
2) **Infracciones a la propiedad intelectual a través de la protección de los derechos de autor**: especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas (artículos 270 y otros del código penal).
3) **Falsedades**: Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (artículos 386 y ss. Del código penal).
4) **Sabotajes informáticos**: Delitos de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (artículo 263 y otros del código penal).
5) **Fraudes informáticos:** Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (artículos 248 y ss. Del código penal).
6) **Amenazas:** Realizadas por cualquier medio de comunicación. (artículos 169 y ss. Del código penal).
7) **Calumnias e injurias:** Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (artículos 205 y ss. Del código penal).
8) **Pornografía infantil:** Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos. La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187). La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elabora-

ción hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189). El facilitamiento de las conductas anteriores (el que facilitare la producción, venta, distribución, exhibición...). (art 189). La posesión de dicho material para la realización de dichas conductas. (art 189). [5].

VI. DELITOS INFORMÁTICOS EN COLOMBIA

Según las estadísticas de la comisión de regulación de telecomunicaciones (crt), en los primeros tres meses del 2008 el total de suscriptores de internet aumento 13.6%, llegando a 1.569.126, de los cuales el 55,7% cuenta con conexión de banda ancha. Por ello el acceso de usuarios a internet ha generado que los avances tecnológicos asciendan de manera exponencial, al igual que este las nuevas modalidades de robo y prácticas delincuenciales han crecido a la par. [6]

La normatividad sobre los delitos informáticos según el código penal colombiano, ley 1273 de 2009, "*por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*", define los siguientes delitos, y sus penalidades:

1) **Artículo 269a:** Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
2) **Artículo 269b** Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
3) **Artículo 269c:** Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
4) **Artículo 269d:** Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
5) **Artículo 269e:** Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca, o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
6) **Artículo 269f:** Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
7) **Artículo 269g:** Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la con-

ducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una ip diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

8) **Artículo 269h:** Circunstancias de agravación punitiva: las penas imponibles de acuerdo con los artículos descritos en este título se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
   - Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
   - Por servidor público en ejercicio de sus funciones.
   - Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
   - Revelando o dando a conocer el contenido de la información en perjuicio de otro.
   - Obteniendo provecho para sí o para un tercero.
   - Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
   - Utilizando como instrumento a un tercero de buena fe.
   - Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.
9) **Artículo 269i:** Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este código.
10) **Artículo 269j:** Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

    Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. [7]

Según un balance del cibercrimen en Colombia en 2017 del centro cibernético de la policía nacional de Colombia [8], se habían recibido 11.618 denuncias por violación a la ley 1273 de 2009 dando panorama a los delitos que más se denuncian en el país.

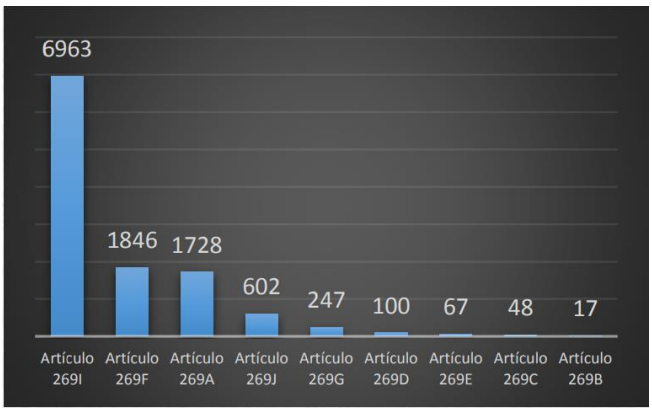

Fig. 1. Delitos por articulo [9]

Como se ve en la *figura 1*, el delito que más fue denunciado fue el artículo 269i, "hurto por medios informáticos y semejantes" esto es equivalente a 60%, seguido por el artículo 269f violación de datos personales" con el 16% y el artículo 269a,

"acceso abusivo a un sistema informático", con un 15%, como se puede apreciar en la *figura 2*.

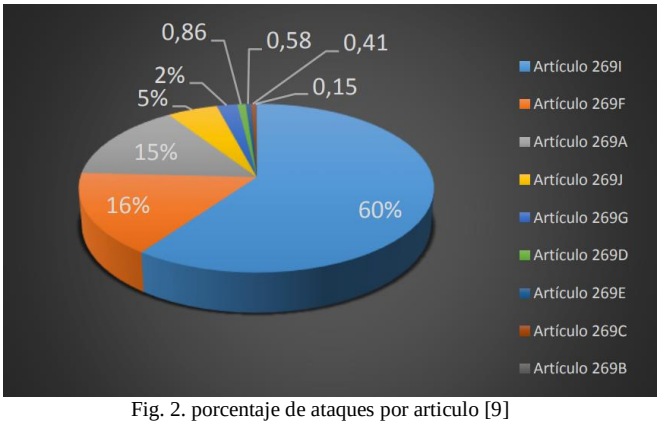

Fig. 2. porcentaje de ataques por articulo [9]

Con esto se refleja que las intenciones de los cibercriminales en Colombia están interesados principalmente a los campos comerciales y financieros, que cada vez se hacen más visibles en la cotidianidad de las personas y entidades, gracias a la masificación del uso de las tecnologías de la información y las comunicaciones a nivel nacional como se ha mencionado anteriormente, lo que proporciona una extensión de las capacidades humanas, por lo que la interacción hombre máquina adquiere gran protagonismo, sin dejar de lado tres aspectos primordiales que soportan el e-comercio (confianza, sistemas de pago y seguridad).

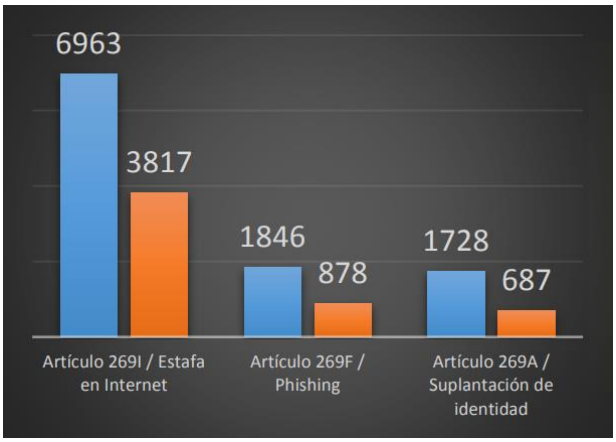

Fig. 3. Comparativa entre modalidades de incidentes informáticos [9]

En la *figura 3*, se compara 3 modalidades de incidentes informáticos, con cifras de 3 delitos que se encuentran enmarcadas dentro de las conductas punibles tipificadas en Colombia, siendo concordante el crecimiento de la denuncia de la mano con la modalidad que más se identifica en su materialización.

En Colombia, la panorámica del delito informático se ve reflejada en el siguiente mapa de calor, (figura 4), donde en las principales ciudades se encuentra más del 75% de suscriptores de internet fijo y el mayor índice de habitantes por ciudad.

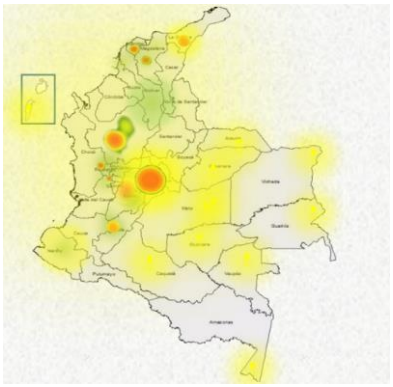

Fig. 4. Mapa de calor, panorámica del delito informático en Colombia. [9]

VII.AMENAZAS

Según informe del balance del cibercrimen en Colombia del 2017 **[8]**, el cibercrimen tuvo un aumento del 28,30% respecto al año anterior, también aclaran que "*los ciberataques sofisticados de afectación global impactaron infraestructuras digitales críticas en el mundo, en Colombia 446 empresas reportaron haber sido víctimas"*

Por ello a través del ciberpatrullaje que realiza la policía nacional, junto con los reportes de los ciudadanos (contando solo los que reportan, ya que hay muchas empresas y personas comunes que no reportan por miedo, pena o porque el nombre de su empresa tenga alguna incidencia en ante nuevos clientes), se identificaron las modalidades del Cibercrimen que más afectan en Colombia, que son las siguientes:

1) ***Ciber inducción al daño físico****:* A nivel mundial los niños y adolescentes ya están teniendo integración al mundo digital, con ello llegaron interacciones a base de retos con fines de auto lesión. Entre algunos hallazgos detectados, se identificaron 15 grupos delictivos a nivel mundial en la red de Facebook (ballena azul, reto del hada de fuego), 3 grupos eliminados en Colombia (Facebook), 4123 usuarios que se les impidió el acceso a estos grupos, 1 alerta mundial INTERPOL (circular morada), y muchos más, pero dado que las redes sociales son tan libres es muy difícil que puedan frenar este tipo

de ataques, por ello es importante el limite a los niños y adolescentes al mundo del internet desde los hogares.

2) ***Estafa por suplantación de simcard****:* esta modalidad criminal aprovecha cuando un titular de una línea telefónica está de viaje o no puede atender llamadas, se presenta en la oficina del operador y solicita una nueva simcard a partir de la suplantación. Luego sincroniza redes sociales y productos financieros vinculados al número telefónico para validar accesos que le permitan generar transferencias no consentidas. Por este método se reportaron al caivirtual 1385 casos con pérdidas que ascienden a los $ 7.690.000.000 millones.
3) ***Vishing – tráfico de datos personales:*** en este tipo de estafa los ciberdelincuentes aplican técnicas de ingeniería social vía telefónica, con el fin de tener acceso a la información personal y financiera de sus víctimas para así lucrarse económicamente. Durante la vigencia se han reportado 1055 casos con pérdidas que ascienden a los $ 2.132.000.000 estos incluyen una variedad de programas que ejecutan acciones sin que el usuario se dé cuenta, recolectando datos que son captados por los ciber criminales, y estos pueden destruir los datos, alterarlos con intenciones delictivas, causando daños a la operación normal del computador y también usando los recursos de este.
4) ***Fraude por falso WhatsApp:*** las personas inescrupulosas crean conversaciones falsas y utilizan datos públicos como fotos de perfil y el número de celular de las víctimas y pantallazos, donde de estos se tema información para cometer delitos vinculados a la afectación de la reputación de las personas, estafas, extorsión, entre otros. Se han reportado 381 casos al @caivirtual, y las principales víctimas son gerentes, a los que les llegan falsas conversaciones entre los mismos con empleados de áreas financieras, donde se evidencia la intención de materializar estafas.
5) ***Ciberpirámides:*** Los Ciberdelincuentes están aprovechando la incertidumbre que existe al respecto de las criptomonedas en cuanto a su legalidad y fluctuación, y esto capta la atención de incautos inversionistas para hacer compras de la monedas como el bitcoin, ripple o ethereum, reteniendo dineros y luego desaparecer estafando masivamente a los ciudadanos, la fiscalía general de la nación logro identificar a dos de los presuntos responsables de una está a más de 10 países entre EE.UU. y Latinoamérica, siendo el 77% de los reportes originarios de Colombia. El portal web MECOIN represento una estafa donde las cifras ascienden a 1.500 millones de pesos represen-tados en 182 personas en 11 ciudades.

A pesar de que estas estafas son las que estaban en el 2017 teniendo más fuerza según el informe de la policía, también hay unos ataques recurrentes que no dejaban de reportar victimas en Colombia, entre ellas se encuentran las siguientes:

1) ***Ransomware: WannaCry y Petya:*** entre el 12 y el 14 de mayo se registró un ataque cibernético a escala global bajo la modalidad infección de malware conocido como ransomware (los hackers utilizan esta técnica para bloquear sus dispositivos y exigir un rescate a cambio de recuperar el acceso [11]), el cual afecto infraestructura critica de medios de transporte, hospitales, energía, gas, teléfono en más de 150 países. En Colombia este ataque impacto principalmente a las pymes vinculadas al sector productivo del país. Brasil, México y como tercer lugar Colombia, encabezan los blancos de los ataques en américa latina según Kaspersky, el 98% de los equipos atacadas usaban Windows 7.

   Hoy en día los ataques de ransomware ya están apuntado a los dispositivos móviles. Otras variantes de este tipo de malware es un ejemplo hummingbad o judy. Lograron penetrar en las defensas de más de diez y ocho millones de teléfonos inteligentes. Check point es una empresa proveedora global en soluciones de seguridad , y ha recordado que los dispositivos móviles, las redes a las que se conectan y las aplicaciones “pueden robar información confidencial” como documentos, citas de calendario, mensajes de correo electrónico, textos o archivos adjuntos, además los Ciberdelincuentes utilizan el micrófono y la cámara de los dispositivos para espiar, enviar grabaciones a un servidor remoto o capturar nombre de usuario y contraseñas cuando la víctima se conecta a sistemas corporativos con datos confidenciales. [10]

En la *figura 5* se ven algunas de las cifras del ransomware en números según Kaspersky.

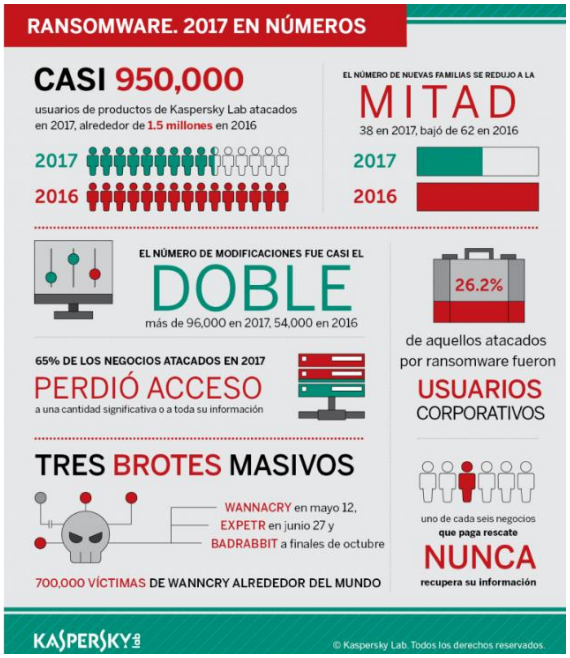

Fig. 5. Ransomware en números [11]

2) ***Ataques a entes gubernamentales:*** Las entidades fueron atacadas bajo por ataques a través de "puertas traseras" por un malware y la utilización de la técnica RAT (Remote Access Tool), con esto ejecutan software malicioso que sirve para la transferencia ilegal ya sea de dinero, información del sector público, bases de datos, etc. los costos de esta modalidad asciende a más de mil millones de pesos solo en las alcaldías a nivel nacional. En el informe de la policía dicen "*La DIJIN adelanta procesos investigativos con la fiscalía del eje temático de ciber crimen, donde se evidencia el ataque a alcaldías en diferentes zonas del país".* [8]
3) ***B.E.C (suplantación de correo corporativo):*** Estos tipos de ataque han afectado más a las empresas del sector productivo y de retail (Tipo de comercio que se caracteriza por vender al por menor), en el país como la farmacéutica, petróleos, tecnología, transporte, comercio, entre otros. Las pérdidas ascienden a los 380 millones de pesos.

   Entre los principales ataques esta la suplantación de correo cuyos objetivos primordiales son los gerentes y/o jefes de áreas Financieras, Ventas, Comercio, Exportaciones, Importación, etc. en estos correos buscan que el incauto descargue, o abra algún link desde un correo de un destinatario falso, en la *figura 6* se aprecia un ejemplo de este tipo de estafa.

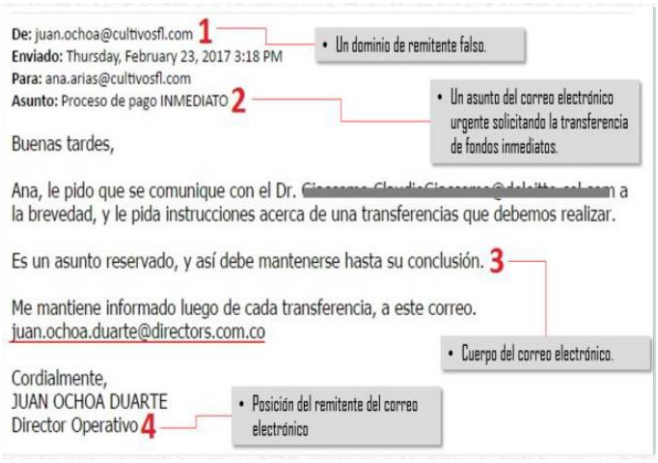

Fig. 6. Ejemplo correo fraudulento [9]

En el informe aclaran que "el FBI considera a las estafas tipo bec como el fraude de los 3 billones de dólares a partir del impacto negativo en la empresa y comercio en los estados unidos".

4) ***Carding:*** Por medio de esta modalidad los ciberdelincuentes comercializando los datos de tarjetas de crédito y débito, cuentas bancarias e información financiera. Aproximadamente este tipo de fraude deja pérdidas anuales de 60.000 millones de pesos.

   Los primordiales tipos de ataques de carding son skimming (clonación de tarjetas), **intercambio de tarjetas** (cambiazo), ataques en atm, **phishing** (suplantación de sitios web para capturar datos personales) y **vishing** (falsos call center)**.**
   Según la policía por medio de @caivirtual en 2017, se recibieron 328 incidentes por carding, siendo las zonas de interacción como las hoteleras, comercio, turismo y pago de servicios las más afectadas.
5) ***Estafas por internet:*** según la policía el 55.3% de incidentes atendidos por el @caivirtual fueron estafas en internet, siendo el de mayor afectación a los colombianos, entre las modalidades que más se impactó generaron se destacan compra y venta de productos en internet, estafas a través de llamadas telefónicas, smishing (estafas a través de mensajes de texto SMS o chats de WhatsApp), cartas nigerianas (promesas de herencias o recompensas a través de correos electrónicos y

paquetes turísticos (engaños en el alquiler de sitios de esparcimiento, generalmente en temporada de vacaciones).

Estas estafas oscilan entre 500.000 y 20 millones de pesos, y a la fecha asciende a 15 mil millones de pesos la cuantía en estafa. Se han reportado 6372 fraudes de los cuales están divididos como se muestra en la figura 7.

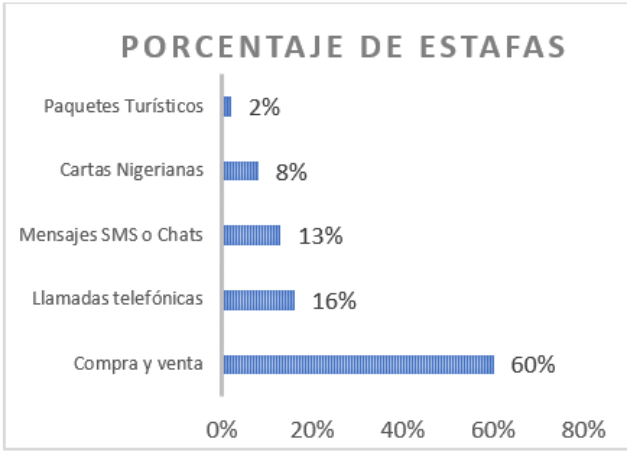

Fig. 7. Porcentaje por tipo de estafa

Hay miles de ataques que se podrían poner como ejemplo, pero solo tomando como muestra uno de los más actuales, lo pasado mundial de Rusia donde el presidente Vladimir Putin pronuncio estas palabras, "*durante el mundial de Rusia 2018, fueron neutralizados casi 25 millones de ciberataques y otras acciones delictivas contra infraestructuras informativas rusas relacionadas con el campeonato*". Esto fue detectado por las autoridades rusas encargadas de velar la seguridad durante la celebración del mundial. Por ello el mandatario agradeció a las fuerzas rusas y extranjeras por su valiosa labor conjunta durante este gran certa-men, participaron en ella 126 representantes de 55 servicios especiales y cuerpos de seguridad de 34 países.

"G*racias a este trabajo",* añadió el presidente *"quienes llegaron a Rusia se sentían realmente a salvo, podían moverse cómodamente entre las ciudades y el resto del territorio nacional, ver partidos de sus selecciones favoritas en los estadios y en las fans zone, sin que los ciudadanos respetuosos con la ley y nuestros huéspedes tropezaran con barreras o restricciones innecesarias".* [11]. Esto hace pensar lo complica.

Para dar otro ejemplo, uno de los ataques más recientes fue la que encontró una firma de seguridad que indago sobre el sucedo con la página web y aplicaciones de la aerolínea británica British Airways. En las últimas semanas esta compañía tuvo una brecha de seguridad al descubrirse que los datos de 380.000 tarjetas de crédito habían sido robados durante el periodo de tres semanas, así lo confirmó la propia aerolínea.

La firma de seguridad ha estado investigando los hechos y asegura que el robo de datos se produjo por un malware instalado hace meses en la página web de British Airways, el cual se compartía también con la aplicación de la compañía, permitiendo así duplicar el alcance. El ataque consistía en recolectar datos de del cliente como su nombre, dirección de facturación, dirección de correo electrónico y los detalles de la tarjeta de crédito, y cuando se abra la pasarela de pago del sitio web, este se enviaban la información a un servidor de los delincuentes ubicados en Rumania. La aerolínea ha puesto a disposición de los clientes un acceso en su página web donde consultar la información relacionada con el ataque, y las implicaciones que tiene y resolver la dudas al respecto [12]. El link es el siguiente: https://hipertextual.com/2018/09/british-airways-hackeo-malware-clonacion-tarjetas

El mayor problema de todos estos ataques siguen aumentando con rapidez, ya que los creadores de los malware, sobre todo de los ransomware, están utilizando una especie de mercado libre, donde venden el producto en este caso el malware, y todo esto se hace en lo que se conoce la Deep web (la Deep web es aquella parte de la red que contiene material, información y páginas web que no están indexadas en ninguno de los buscadores existentes como pueden ser Bing, Google, Yahoo!, etc.), y la demanda esta tan alta que prácticamente triplica la oferta, por esto los ciberdelincuentes se han interesado en el uso de nuevas herramientas para crear malware y así poder comercializarlo.

VIII. CONPES 3701

En el 2011 se realizó el consejo nacional de política económica y social, *conpes 3701*, este documento busca generar lineamientos de la política de la ciberseguridad y la ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

La problemática central se fundamenta en la capacidad actual del estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el gobierno nacional al incluir este tema en el plan nacional de desarrollo 2010-2014 "prosperidad para todos",

Según el conpes 3701, se identificaron tres ejes problemáticos:

1) ***Las iniciativas y operaciones en ciberseguridad y ciberdefensa no están coordinadas adecuadamente:*** a pesar de existir algunos esfuerzos institucionales (tanto privados como públicos), se ha identificado que no existen organismos a nivel nacional constituidos para coordinar y desarrollar operaciones de ciberseguridad y ciberdefensa. Por tanto, no ha sido posible implementar los mecanismos suficientes y adecuados para contrarrestar ataques cibernéticos y proteger los intereses del estado en el ciberespacio. Se evidencia una debilidad en la difusión, concienciación, generación de una cultura de prevención y acción segura en ciberseguridad, dirigida tanto al sector público como al privado, así como a la sociedad civil.
2) ***Debilidad en la oferta y cobertura de capacitación especializada en ciberseguridad y ciberdefensa:***
   el conocimiento en el área de ciberseguridad y ciberdefensa tanto en el sector público como en el privado es limitado. Si bien en el país existen algunas instituciones de educación superior que ofrecen especializaciones en seguridad informática y derecho informático, se ha identificado que la oferta académica en programas especializados en estas áreas es reducida. En consecuencia, un número significativo de personas que acceden a algún tipo de formación en el área de seguridad de la información, lo hacen mediante programas ofrecidos por instituciones extranjeras, en los que no se profundiza sobre la realidad colombiana.

   El entrenamiento y formación de los funcionarios públicos y privados para reaccionar como primeros respondientes ante la comisión de los delitos informáticos es deficiente. En muchas ocasiones se pierde la cadena de custodia de la evidencia digital y se generan dificultades en la realización de las investigaciones forenses. Así mismo, existe una oferta limitada de programas de capacitación para entidades que realizan funciones de policía judicial en el tema.
3) ***Debilidad en regulación y legislación de la protección de la información y de los datos:*** pese a que existen instrumentos legales y regulatorios en seguridad de la información, persisten falencias que impiden responder oportunamente a incidentes y delitos cibernéticos. Recientemente el congreso de la república aprobó la ley de inteligencia y contrainteligencia, estableciendo mecanismos de vigilancia y control para estas actividades. A pesar de ello, ésta es una regulación que requiere particularizarse para el ejercicio de la ciberseguridad y la ciberdefensa, sobre el cual existe muy poco en términos de alcance y operatividad.

   En cuanto a normatividad internacional, dentro de los instrumentos que le permitirían al país integrarse a la comunidad mundial está la convención del consejo de Europa en delito cibernético, que requiere cumplir con aspectos como el establecimiento de mecanismos de cooperación judicial como la extradición, la creación de puntos de contacto localizables las 24 horas del día los 7 días a la semana para facilitar la investigación y el mantenimiento de los logs por parte de los ISP (Internet Service Provider), durante el tiempo necesario.

   Casos puntuales como el de la regulación de los ISP, en los que la normatividad tuvo un avance importante a finales del año 2009. De acuerdo con las características y necesidades propias de su red, se creó para dichas empresas la obligación de implementar modelos de seguridad, con el fin de contribuir a mejorar la seguridad de sus redes de acceso, cumpliendo los principios de confidencialidad e integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio, y obligaciones relaciona-

das con la inviolabilidad de las comunicaciones y la seguridad de la información. Sin embargo, se ha identificado, por ejemplo, que, en lo relacionado a la seguridad de las redes de los isp's, los logs no son almacenados por el tiempo adecuado para que sirvan en determinado momento como prueba o contribuyan en las investigaciones de ciberdelitos.

Por ello el documento conpes 3701 planteo un objetivo central y unos objetivos específicos.

A. Objetivo central.

Según el conpes el objetivo central se basa en **fortalecer las capacidades del estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.** Para ello se necesita involucrar a todos los sectores del estado con responsabilidad en el campo de la ciberseguridad y la ciberdefensa, creando un ambiente participativo donde todos los actores de la a sociedad actúen con propósitos comunes, estrategias concertadas y esfuerzos coordinados. Igualmente, es de vital importancia crear conciencia y sensibilizar a la población en todo lo referente a la seguridad de la información; fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.

B. Objetivos específicos.

Según el conpes 3701 tiene planteado 3 objetivos específicos que son los siguientes:

- Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y la ciberdefensa nacional.
- Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y Ciberseguridad.
- Fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

Para más información leer el documento conpes 3701 en la página del ministerio de las tics. [13]

IX. CONCLUSIONES

Los ciberdelincuentes están utilizando técnicas cada vez más avanzadas para generar ataques vulnerando los sistemas de las empresas, ya sean públicas o privadas, actualmente se está viviendo una oleada de ciberataques que están afectando no solo a la compañía, sino también a los que rodean el ámbito laboral, como proveedores, usuarios, incluso puede llegar a afectar la seguridad nacional o regional.

Los ataques se han vuelto tan lucrativos que se ha generado un negocio muy bien pagado en internet, sobre todo por la Deep web o también conocida como la web profunda (para aprender un poco más sobre este tema se puede leer un especial de la página www.dinero.com sobre el acceso a ella [14]), aplicaciones para crear tu propio ransomware, donde deja ganancia tanto para el ciberdelincuente que programo la aplicación, como para el que lo adquirió, y ya que las empresas colombianas no tienen aún la conciencia de tener una gestión de riesgo correcta que le permita seguir adelanta a pesar de caer bajo un ataque o algún desastres natural como inundaciones, incendios o terremotos.

Para mantener seguros los datos es necesario que se cumplan los tres pilares de la seguridad de la información, *la disponibilidad* lo cual significa que la información siempre debe estar disponible a quienes necesitan acceder a ella, es decir por el personal que está autorizado a usar esta información ya sea para modificación o solo lectura, *la integridad* la cual significa que la información se debe tener sin modificación, es decir que se pueda mantener con exactitud tal cual fue generada, sin que esta allá sido manipulada ni alterada por alguna persona o proceso implicado y por último *la confidencialidad* que significa que se asegura el acceso a la información solo a las personas que cuentan con el acceso a ella, estos pueden ser personas, procesos o aplicaciones.

Los ciberdelincuentes vulneran estos tres pilares para robar los datos de las empresas, como sus bases de datos y datos confidenciales, etc. El problema es que el estado tiene debilidades en cuanto al seguimiento y los lineamientos a tomar para este tipo de sucesos, por ello es primordial que las empresas comiences a concientizarte se la problemática que da los

ataques cibernéticos, y piensen en invertir más en la seguridad de sus redes con profesionales en seguridad informática.

Contar con un oficial de seguridad informática podría ahorrar muchos dolores de cabeza, porque este podrá proteger la información de las empresas que son el activo más valioso, y analiza los sistemas en busca de posibles amenazas y vulnerabilidades que pudieran ser explotadas por algún pirata informático. En muchas ocasiones se alega por el costo de estos expertos, pero es importante comparar el costo que le generaría si existiera un ataque vs el costo que genera tener al oficial que le proteja este activo.

REFERENCIAS

[1] Eset, «We live Security,» Miguel Angel Mendoza, 16 06 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/.

[2] R. N. CARLOS, Crimen Organizado Transnacional: Definición, Causas, Astrea, 2005.

[3] M. M. C. Paúl, Delincuencia y Fraude Informático, Jurídica de Chile, 1999.

[4] J. TELLEZ VALDÉS, Los Delitos informáticos. Situación en México, 1996.

[5] RECOVERY LABS © 2015 -Departamento de Peritaje Informático, «TIPOS DE DELITOS INFORMÁTICOS,» Recovery Labs, [En línea]. Available: http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html. [Último acceso: 28 07 2018].

[6] I. &. J. F. Manjarrés, «Caracterización de los delitos informaticos en Colombia,» *Pensamiento Americano*, pp. 71-82, 2012.

[7] C. d. Colombia, *Ley 1273 de 2009*, Colombia, 20019.

[8] Cai Virtual Policia Nacional de Colombia, «Centro Cibernético Policial,» 2017. [En línea]. Available: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf. [Último acceso: 28 07 2018].

[9] P. Nacional, «https://caivirtual.policia.gov.co,» 2017. [En línea]. Available: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf.

[10] «El 'malware' móvil genera más dinero que el 'ransomware' en 2017, según Check Point,» Europapress, [En línea]. Available: http://www.europapress.es/portaltic/ciberseguridad/noticia-malware-movil-genera-mas-dinero-ransomware-2017-check-point-20180222164727.html.

[11] Kaspersky, «https://www.kaspersky.com/,» 2017. [En línea]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2018/03/12102102/KSB_Story_of_the_Year_Ransomware_FINAL_ES.pdf. [Último acceso: 2018].

[12] Sputnik, «ciberataques contra las infraestructuras del Mundial 2018,» 2018. [En línea]. Available: https://mundo.sputniknews.com/worldcup-2018-archive/201807161080449381-seguridad-informatica-campeonato-mundo-futbol-rusia/. [Último acceso: 2018].

[13] L. d. Barco, «El hackeo a British Airways fue provocado por un ‘malware’ de clonación de tarjetas,» Hipertextual, 11 09 2018. [En línea]. Available: https://hipertextual.com/2018/09/british-airways-hackeo-malware-clonacion-tarjetas. [Último acceso: 28 8 2018].

[14] Departamento Nacional de Planeación, «Conpes 3701,» 2011. [En línea]. Available: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

[15] Dinero, «Nos metimos en la Deep Web, la parte oscura del internet, y esto fue lo que vimos,» Dinero, 15 16 2017. [En línea]. Available: https://www.dinero.com/empresas/articulo/que-es-la-deep-web-y-que-se-encuentra-ahi/246582. [Último acceso: 25 08 2018].

[16] Kaspersky , «Ransonware. 2017 en numeros,» Kaspersky, 2017. [En línea]. Available: http://www.pcworldenespanol.com/2017/12/05/2017-kaspersky-mas-25-ataques-ransomware-fue-dirigido-empresas/. [Último acceso: 28 07 2018].