REPUBLICA DE ECUADOR

UNIVERSIDAD TECNOLOGICA
EMPRESARIAL DE GUAYAQUIL

TRABAJO DE GRADO
PARA LA OBTENCIÓN DEL TITULO DE:

INGENIERO EN SISTEMAS – MENCIÓN REDES
Y COMUNICACIONES

TEMA:

ANÁLISIS DE LOS CIBERATAQUES REALIZADOS EN AMÉRICA LATINA

AUTOR:
MANUEL JESÚS GUACHO LEMA

GUAYAQUIL – ECUADOR
2018

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TECNOLÓGICA
EMPRESARIAL DE GUAYAQUIL

TRABAJO DE GRADO
PARA LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS – MENCIÓN REDES Y COMUNICACIONES

TEMA:

ANÁLISIS DE LOS CIBERATAQUES REALIZADOS EN AMÉRICA LATINA

MANUEL JESÚS GUACHO LEMA

2018

GUAYAQUIL - ECUADOR

AGRADECIMIENTO

Agradezco a Dios por darme la oportunidad de vivir este momento tan importante en la vida de todo estudiante universitario, a mis padres por la confianza y el apoyo incondicional brindado a lo largo de mi vida, y a quien debo este éxito profesional, a mis hermanos, por facilitarme su ayuda en todo momento, y siempre velar por mi bienestar.

DEDICATORIA

1. El presente trabajo de titulación va dedicado a Dios, quien supo guiar mi camino durante mi formación profesional, estando conmigo en todo momento, dándome fuerzas y esperanzas para no desistir en las adversidades presentadas a lo largo de este periodo.

2. A mis padres, Martha y Manuel quienes con sus responsabilidades, amor y sacrificio me han permitido lograr esta meta, gracias por enseñarme por medio del ejemplo a ser perseverante y nunca darme por vencido.

3. A mis hermanos, Jorge, César y Esther por alentarme a seguir el camino correcto, acompañándome durante todo este duro proceso, dándome su apoyo para poder cumplir mis objetivos.

4. A mi compañera sentimental Gladys, por ser un apoyo incondicional que con su amor, paciencia y consejos supo mantenerme firme en este camino hacia el profesionalismo.

5. A mis amigos, compañeros y profesores de aula, gracias por brindarme su paciencia y apoyo durante mi formación profesional.

La Responsabilidad de este trabajo de investigación, con sus resultados, conclusiones y recomendaciones, pertenece exclusivamente al autor

.....

FIRMA

ANÁLISIS DE LOS CIBERATAQUES REALIZADOS EN AMÉRICA LATINA

Manuel Jesús Guacho Lema

Universidad Tecnológica Empresarial de Guayaquil "UTEG"

RESUMEN

Este trabajo constituye una investigación documental sobre los ciberataques realizados en América Latina. Un ciberataque definido como un delito cibernético puede tener múltiples consecuencias cuya gravedad dependerá de cada caso y de la intención del delincuente. El objetivo del estudio es determinar el nivel de riesgo y preparación en ciberdefensa que tiene la región de tal forma que se puedan definir lineamientos para combatir futuras amenazas. En última instancia se desea conocer cómo se está preparando América Latina para ataques cibernéticos. Este estudio constituye una investigación cualitativa de tipo documental, no concluyente. Para el desarrollo se realizó una revisión exhaustiva de fuentes secundarias y discusiones en congresos para la comprensión general del tema. Se definieron también los distintos tipos de ataques cibernéticos y su nivel de daño. Como resultado se pudo obtener una descripción general de ataques cibernéticos en la región y el nivel de defensa general de los países que la integran. Como conclusión principal se obtiene las deficiencias que existen en los países de la zona con respecto a mecanismos de defensa contra ataques cibernéticos. Este estudio puede ser utilizado como punto de partida para un análisis específico de cada país y la determinación de objetivos de defensa a implementarse.

Palabras clave: Ciberataque, Ciberdefensa, Cibernauta, Malware, Ataque cibernético, América Latina.

1. INTRODUCCIÓN

Según lo señaló Sancho (2017), “la gobernabilidad de todo sistema político requiere de considerar tres factores básicos: seguridad como condición, institucionalidad como medio y desarrollo como objetivo” (p. 8). Considerando aquello, la seguridad en el ciberespacio representa una condición ineludible para las relaciones dentro de un Estado.

El concepto de ciberseguridad toma particular relevancia ante el creciente uso del ciberespacio como un lugar virtual para la interacción social, resultado de la evolución de las tecnologías. De igual manera, la gran cantidad de datos virtuales que se generan en dicho espacio posibilitan almacenar y usar gran cantidad de información con buenos o malos propósitos. Según reporte de la Unión Internacional de Telecomunicaciones, en el 2015 la cantidad de usuarios de internet se estimó en 40% de la población mundial (Sancho, 2017).

Considerando la cifra anterior, también es importante destacar que no todos los usuarios de internet realizan el mismo nivel de penetración en las redes. En este sentido, usuarios con mayor educación tienden a utilizar más servicios como comercio electrónico, pagos en línea, entre otros; mientras que usuarios con menor educación tienden a usar el internet más con fines de comunicación. Por esta razón, las autoridades deben establecer medidas que permitan a las personas adquirir las habilidades y competencias necesarias para el uso pleno de Internet, así como garantizar condiciones mínimas de seguridad para su uso debido a los riesgos que existen y que pueden observarse en la tabla 1 (Bitar, 2014).

Tabla 1: Factores de riesgo en el Ciberespacio

Autoría	**Gobierno**	**Sector privado**
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, amenazas persistentes avanzadas	Espionaje, ataques contra infraestructuras críticas, APT

Ataques patrocinados por privados	Espionaje	Espionaje
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de Internet; infección con malware; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros.	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros.
Crimen organizado	Espionaje	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Ataques de personal con accesos privilegiados (Insiders)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT.	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT.

Fuente: Sancho (2017)

Elaboración: El Autor

En referencia a los métodos empleados para afectar los intereses de un país, se pueden identificar dos tipos: la explotación de redes informáticas y ataques como tal. La primera comprende actividades de espionaje con el propósito de alcanzar información específica que podría servir para lucrar de dicha información o preparar futuros ataques a redes. Por su parte, los ciberataques corresponden a introducción de virus que causarán pérdida de información y afectarán el

funcionamiento normal de las redes o sitios web. La evidencia sugiere que los ataques más recurrentes están orientados a impedir el funcionamiento normal de entidades del gobierno o empresas privadas (Amigo, 2015). Los ciberataques están dirigidos a computadores de todo el mundo y su finalidad, en última instancia, es cometer delitos bancarios o probar la vulnerabilidad de algunos sistemas (Aranda, Riquelme, & Salinas, 2015).

Al referirse específicamente a la problemática que atañe a América Latina, primero se debe reconocer que la región está desigualmente conectada, por lo que unos países enfrentan un mayor riesgo que otros. Producto de esta falta de conectividad y bajos niveles de defensa de ciberataques que existen en América Latina (Anselmo, 2012; Cornaglia & Vercelli, 2017; Guzmán & Angarita, 2017; Hernández J. , 2018; Martin, 2015), este estudio tiene como objetivo general: analizar los ciberataques que se han realizado en América Latina.

Del objetivo general señalado se desprenden tres objetivos específicos: i) Resumir los ciberataques de la zona de análisis; ii) Realizar un análisis de la ciberdefensa de América Latina; y, iii) Sistematizar las estrategias de la región para defenderse de los ciberataques. En última instancia, se desea responder a la siguiente pregunta de investigación: considerando las amenazas y ciberataques suscitados, ¿Cómo se está preparando América Latina para defenderse?

Estudios de este tipo se justifican en la necesidad existente de protección de datos y soberanía digital. La no intervención de los Estados en este tópico dejaría abierta una puerta a oportunidades de espionajes, robos, estafas y delitos de usurpación de identidad.

2. MÉTODO

Para el desarrollo de este trabajo se realizó una investigación documental (Huacho, 2011) sobre los trabajos de diferentes instituciones e investigadores sobre ciberataques y ciberdefensa en América Latina. Este trabajo presenta una

sistematización de la información encontrada y su influencia en la defensa que puede tomar la región contra delitos cibernéticos.

Esta es una investigación de tipo cualitativa – documental (Hernández Sampieri, Fernández, & Baptista, 2014). La población del estudio comprende a todos los países de América Latina y como muestra se tomaron los años desde el 2009 hasta el 2017. Se realizó mayor énfasis en aquellos países que presentaron mayor nivel de ciberataques como Colombia, Venezuela, México y Argentina. Al final se presenta un cuadro de resumen con los eventos más importantes en América Latina sobre ciberataques y ciberdefensas.

El país que más reglas de juego dicta al hablar de internet es Estados Unidos. América Latina es la región que tiene la mayor cantidad de redes de comunicaciones dependientes, de manera exclusiva, de este país. En este punto es importante mencionar la disyuntiva existente entre soberanía digital e intervencionismo. Este último responde a un ideal de soberanía de los Estados que pueden afectarse por las nuevas formas de comunicación, no obstante la intervención en comunicaciones atenta contra la soberanía digital (Sierra, 2015).

Este punto es importante mencionarlo ya que las ciberdefensas deben ir enfocadas no sólo a personas naturales que pueden atentar contra entidades, personas jurídicas o la población a través del robo de información o estafas cibernéticas; sino que deben enfocarse también en actividades de espionaje que se disfracen de protección.

Reyna y Olivera (2016), en su estudio sobre amenazas cibernéticas publicado en México, realizan un resumen de los ataques más comunes que se realizan y citan ejemplos específicos. Estos ataques pueden ser a correos electrónicos, con la intención de obtener información; redes sociales, para robo de información personal o usurpación de identidad; banca en línea, para estafas a través de la manipulación a las víctimas para obtener códigos de acceso; comercio electrónico, para estafas por pagos en línea; y, juegos en línea, en los cuales se piden claves de tarjetas para acceder a dichos juegos.

Estos ataques pueden ser leves o graves, dependiendo de la intención del atacante. Por ejemplo, en el 2014 se denunció un hackeo a Yahoo en el que se

robaron más de 500 millones de cuentas que podían incluir nombres, direcciones de correo, preguntas de seguridad y teléfonos. Algunos expertos lo consideraron el hackeo más grande de la historia (Reyna & Olivera, 2016). Sin embargo, Yahoo no es la única empresa que ha sufrido hackeos, entre otras se pueden mencionar Microsoft, Google, Facebook, el proveedor PalTalk, YouTube, Skype, AOL y Apple (Aranda, Riquelme, & Salinas, 2015).

No obstante, no sería adecuado pensar que estos ataques sólo suceden en países desarrollados o con tecnologías de primer nivel. América Latina ha sido víctima en numerosas ocasiones de delitos cibernéticos. En América Latina y el Caribe, el costo de ciberataques asciende a un promedio de US$90.000 millones al año debido a la falta de una política orientada a la respuesta oportuna a incidentes (Raudales, 2017).

Acorde a los datos presentados por la International Telecommunication Union del 2013, América Latina presenta cuatro grupos de países acorde a su nivel de conectividad. En el primer grupo con conexión superior al 55% se encontraban países como Chile y Argentina; en un segundo nivel con conexión entre un 45% y un 55% se encontraban a Colombia, Venezuela, Brasil y Panamá; en tercer lugar entre el 35% y el 45% de conexión se encontraba México, Ecuador, Perú y Bolivia; y, en niveles menores al 35% se encontraban Cuba, Nicaragua y otros países de Centro América (Martin, 2015).

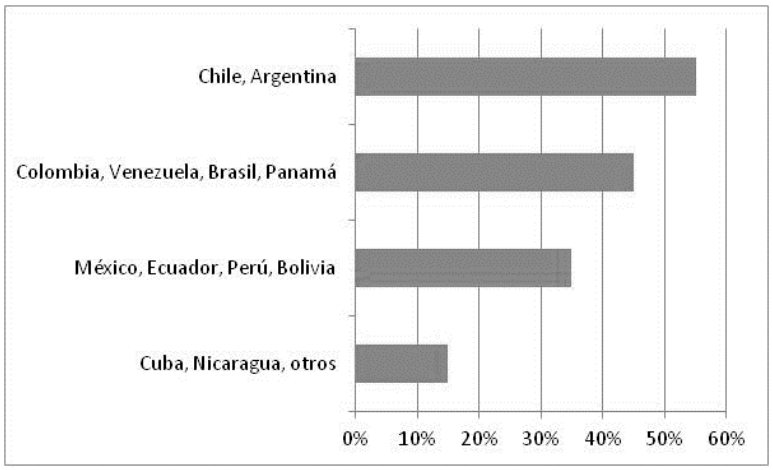


Figura 1: Nivel de penetración de internet por países

Fuente: Martin (2015)

Elaboración: El Autor

En 2013, Julián Assange indicó que el internet estaba siendo observado en todas sus escalas por la milicia estadounidense para incidir en las sociedades. Denunció también que la soberanía digital de América Latina y el Caribe se encontraban en riesgo debido al canal de comunicaciones cuya fibra óptica pasaba por Estados Unidos (Sierra, 2015).

En marzo del 2016 el Servicio de Administración Tributaria de México sufrió un hackeo que se adjudicó al Grupo Anonymous México, el cual dejó a su portal web sin atención durante un lapso de dos horas y media. La intención del hackeo fue enviar un mensaje indicando que dicho grupo estaba más fuerte que nunca. Guadalupe de la Torre, directora de daños de Lockton México estima que en ese país se gastan 24 millones de dólares anuales en ciberataques y señala que los países que reciben más ataques cibernéticos son Brasil, México y Colombia (Reyna & Olivera, 2016).

Por otra parte, la empresa Symantec (2014), citada por Rodríguez, Oduber y Mora (2017), destaca que el 4,2% de los ataques cibernéticos de América Latina y el Caribe durante el 2013, ocurrieron en Venezuela; país que tuvo una infección por malware del 23% en el total de computadoras analizadas. Así mismo registró el 5% del total de spear phishing suscitado en la región.

En lo que respecta a Colombia, varios han sido los ataques a las páginas de la Presidencia de la República y Ministerio de Defensa Nacional dejando a dichos portales sin operación durante varias horas. En el 2009, se suscitaron robos a cuentas bancarias por un monto superior a los 50 millones de dólares. En el 2012 se pudo capturar a Jorge Maximiliano Pachón, un delincuente cibernético, que poseía más de 8000 tarjetas de crédito clonadas y que poseía más de 9 millones de dólares divididos entre 5 países de América Latina en los que operaba (Riveros, 2016).

Una estadística señalada en el 2016 por la empresa PwC señala que del total de delitos económicos reportados a nivel global, el 32% correspondía a crimen cibernético y ocupaba el segundo lugar en la lista. El mismo reporte indicaba que más de un tercio de la población en Colombia reportaba haber sido víctima de

fraudes electrónicos y 6 de cada 10 personas pensaban que los defraudadores trabajaban en las mismas organizaciones (Patiño, 2017).

Uno de los delitos cibernéticos más recientes que afectó a varios países de América Latina, incluyendo en gran medida a Ecuador, fue la aplicación Pokémon GO. Se reportó que algunos usuarios por no poder descargar la aplicación oficial, instalaron otras versiones que no contaban con la seguridad adecuada. Esto implicó un número considerable de ataques cibernéticos ya que la versión oficial incluía un sistema de seguridad de información que se encuentra en la cuenta Google, mientras que las otras versiones no lo tenían. No obstante, este no fue el único delito cibernético que se cometió con este juego. Pokémon GO permitía interactuar entre el mundo real y el mundo virtual en lo que se conoce como realidad aumentada. El juego debía jugarse con el teléfono al aire libre, lo que provocó que se generaran falsos reportes de puntos o Pokémon en zonas poco transitadas donde delincuentes robaban teléfonos a los usuarios (Guzmán F. , 2017).

Uno de los factores más importantes por lo que muchos países de la región están expuestos en gran nivel a delitos cibernéticos es por la falta de educación de los usuarios ni la cultura para proteger su información, permitiendo de esta forma el acceso de delincuentes a datos personales como claves, fechas, documentos, direcciones, entre otros (Hoyos, 2015).

Considerando la problemática expuesta, la Unión de Naciones Suramericanas – UNASUR incluyó este tópico en sus planes de acción del 2012, 2013 y 2014. De la misma manera, definieron políticas, mecanismos y capacidades regionales para detener o disminuir los ataques cibernéticos. En el Plan de Acción del 2015 se incluyó la temática como Grupo de Trabajo Extra Plan de Acción, para continuar con el trabajo de defensa de ataques cibernéticos, medida que fue adoptada también por la Organización de Estados Americanos como Estrategia Interamericana Integral de Seguridad Cibernética (Cornaglia & Vercelli, 2017).

En enero del 2015, la OEA presentó el programa de seguridad cibernética para los países del Caribe y América Latina debido al crecimiento del internet en la

mencionada región. A través de esto se buscaba el desarrollo de una política integral de seguridad cibernética (Hernández, Cerquera, & Vanegas, 2015).

En América Latina, inicialmente, el problema de ciberataques se abordó desde el ámbito penal y el análisis de regulaciones que favorecieran las condiciones de desarrollo y garanticen la continuidad de inversiones ante eventuales ataques cibernéticos. Es decir, se buscaba castigar al culpable más que detenerlo. De esta manera, algunos países de forma gradual, empezaron un proceso de modificaciones legales para contemplar los crímenes del ciberespacio o ciber ataques. Inicialmente estos países fueron Argentina, Costa Rica, México, Bolivia, Guatemala, Paraguay y Perú; seguidos por otros países que desarrollaron leyes específicas como Colombia, Chile, Brasil y Venezuela. Ecuador ha usado la ley civil y comercial para introducir sanciones penales y Uruguay se ha limitado al análisis de protección de derechos de autor (Aranda, Riquelme, & Salinas, 2015).

3. RESULTADOS

A continuación se presenta un cuadro de resumen con los eventos más importantes en América Latina sobre ciberataques y ciberdefensas desde el 2009 hasta el 2017.

Tabla 2: Sucesos relevantes de ciberataques y ciberdefensa en América Latina

Año	Suceso
2009	Robos cibernéticos a cuentas bancarias en Colombia superaron los 50 millones de dólares.
2011	UNASUR incluye en sus planes de acción del 2012, 2013 y 2014 tópicos concernientes a defensa contra ataques cibernéticos.
2012	Jorge Maximiliano Pachón es capturado con más de 8000 tarjetas de crédito clonadas y un monto superior a 9 millones de dólares repartido entre 5 países de América Latina.
2013	Assange advierte de espionaje de Estados Unidos a América Latina y el Caribe. El 4.2% de los ataques cibernéticos a América Latina y el Caribe corresponden a Venezuela. El 23% de las computadoras de Venezuela tuvieron infección por malware.

2014	Hackeo de más de 500 millones de cuentas en Yahoo. Hackeo de cuentas de Microsoft, Facebook, Google.
2015	OEA presenta su programa de seguridad cibernética para los países del Caribe y América Latina.
2016	Grupo Anonymous México hackea la página del Sistema de Administración Tributaria de ese país. Más de un tercio de la población de Colombia reporta haber sido víctima de fraude electrónico en distintas organizaciones. Pokémon GO deja sus primeras víctimas por aplicaciones no originales.
2017	Los usuarios de Pokémon GO dejan de ser víctimas exclusivamente por delitos cibernéticos, sino que se pasa al modelo de robo de equipos.

Fuente y elaboración: El autor

En resumen, la mayoría de los países latinoamericanos tienen o están trabajando en algún tipo de autoridad de protección de datos y privacidad, pero no cuentan con los recursos necesarios para atender ciberataques antes de que se produzcan (Anselmo, 2012).

4. CONCLUSIONES

Según los sucesos analizados en los resultados de investigación, América Latina tiene mucho trabajo por delante en temas de seguridad informática. Por ejemplo en la mayoría de países no existe una codificación general y sistemática sobre ciberdefensa y está pendiente la definición de objetivos y responsabilidades de los distintos organismos del Estado en referencia a puntos como: definir qué significa la ciberdefensa nacional; contribuir al diseño de tecnologías que sirvan para defender intereses locales y regionales; desarrollar leyes orientadas a regular sectores público y privados en actividades cibernéticas; trabajar en conjunto con actividades de ciberdefensa regionales; y enriquecer las discusiones sobre delitos cibernéticos y su forma de detenerlos (Cornaglia & Vercelli, 2017).

No obstante, es importante reconocer el esfuerzo que están realizando los gobiernos, no sólo en lo que comprende a infraestructura y centros de protección a

través de universidades, empresas especializadas y leyes; sino también en lo que comprende a capacitaciones a la población para concientizarla sobre esta problemática. Un ejemplo de ello son los videos que se pueden observar en los bancos donde se recuerda que las claves o códigos no deben compartirse y que las entidades no solicitan información a través de correos (Hoyos, 2015).

Según lo Espinoza (2015), una Estrategia Nacional de Ciberseguridad que permita la disminución o eliminación total de ataques cibernéticos, debe tener cinco ejes claves: 1) La definición de un marco jurídico robusto; 2) La difusión de información y culturización a la población sobre temas de ciberseguridad y protección de datos; 3) La capacitación de personal en la temática; 4) El trabajo conjunto entre gobierno y sector privado, y 5) El fortalecimiento de la ciberdefensa. Esta receta ya ha sido adoptada por varios países a nivel mundial con mayor o menor desarrollo entre los que se pueden mencionar a Estados Unidos, Alemania y Reino Unidos; y de manera más reciente: Corea del Sur, Argentina, Francia, Colombia, Suiza, Bélgica, Panamá, Noruega, España, Kenia, entre otros.

Finalmente, es importante destacar como conclusión que gran parte del problema de ciberataques radica en la poca información o educación de los usuarios. Ante esto, se recomienda que los ordenadores cuenten con herramientas que mantengan niveles moderados de protección. En este sentido Guzmán y Angarita (2017) señalan a *Panda Protection*, *Avast free antivirus* y *AVG antivirus free* como antivirus que son amigables en su uso, gratuitos y protegen los dispositivos conectados a la red. De la misma forma recomiendan a CCleaner como herramienta para mantener limpio el ordenador, eliminar basura del sistema y mejorar el rendimiento de las aplicaciones. Como herramienta de detección de malwares, recomiendan *Malewarebytes Anti-Malware Free.* Y por último, señalan también a *Spybot* para identificar y eliminar software malicioso.

Las mencionadas recomendaciones, sumadas a una cultura de atención y prevención de crímenes cibernéticos y protección de datos personales; podrá ayudar a mitigar los efectos de los ciberataques a los que se enfrenta la región.

5. REFERENCIAS BIBLIOGRÁFICAS

Amigo, A. (2015). Consideraciones sobre la ciberamenaza a la seguridad nacional. *Revista Política y Estrategia Nº 125*, 83 - 96.

Anselmo, A. (2012). Asecho del derecho a la privacidad en América Latina. *Revista Internacional de Protección de Datos Personales*, 1 - 17.

Aranda, G., Riquelme, J., & Salinas, S. (2015). La ciberdefensa como parte de la agenda de integración sudamericana. 100 - 116.

Berdeja, A., & Olivares, I. (2016). Panorama General de la Ciberseguridad Internacional y Nacional. *REVISTA ELECTRÓNICA DE INVESTIGACIÓN DE LA UNIVERSIDAD DE XALAPA. Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico.* , 108 - 119.

Bitar, S. (2014). Las tendencias mundiales y el futuro de América Latina. *CEPAL - Serie Gestión Pública N° 78*, 3 - 58.

Bitar, S. (2015). Pensar el futuro para gobernar mejor. *PRISMA*, 45 - 48.

Congreso Internacional: Crimen económico y fraude financiero y contable (1.º: 2016: Medellín). Corporación Universitaria Remington. (2017). Memorias: Segundo Congreso Internacional: Crimen económico y fraude financiero y.

Cornaglia, S., & Vercelli, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *Revista Latinoamericana de Estudios de Seguridad*, 49 - 62.

Espinosa, E. (2015). Hacia una estrategia nacional de ciberseguridad en México. *Revista de Administración Pública Volumen L*, 115 - 146.

Guzmán, C., & Angarita, C. (2017). PROTOCOLOS PARA LA MITIGACION DE CIBERATAQUES EN EL HOGAR. CASO DE ESTUDIO: ESTRATOS 3 Y 4 DE LA CIUDAD DE BOGOTÁ. *UNIVERSIDAD CATÓLICA DE COLOMBIA. PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN*, 1 - 79.

Guzmán, F. (2017). Impacto del cibercrimen: bajo la realidad aumentada. *Congreso Internacional: Crimen económico y fraude financiero y contable*, 67 - 79.

Hernández Sampieri, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación.* McGraw-Hill.

Hernández, J. (29 de 05 de 2018). *ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN AMÉRICA LATINA.* Obtenido de http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

Hernández, L., Cerquera, J., & Vanegas, J. (2015). RIESGOS PRESENTES EN LOS CIBERATAQUES:UN ANÁLISIS A PARTIR DE AUDITORIA FORENSE. *Pensamiento Republicano. Bogotá, D.C. Nº 3*, 57 - 76.

Hoyos, V. (2015). ¿QUÉ TAL ESTA COLOMBIA EN CUESTIÓN DE CIBERSEGURIDAD? *UNIVERSIDAD MILITAR NUEVA GRANADA*, 1 - 19.

Huacho. (2011). *Metodología de la Investigación. Módulo I: Tipos de Estudios - Niveles de Investigación.*

Mantilla, C. (2018). *ANÁLISIS DE ALGORITMOS CRIPTOGRÁFICOS CLÁSICOS VS ALGORITMOS CUÁNTICOS.* Riobamba: Escuela Superior Politécnica del Chimborazo.

Martin, P.-E. (2015). INSEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA: LÍNEAS DE REFLEXIÓN PARA LA EVALUACIÓN DE RIESGOS. *Instituto Español de Estudios Estratégicos*, 1 - 17.

Montero, R., & Ybarra, K. (2016). De la Ciberseguridad a la Ciberpolítica. *REVISTA ELECTRÓNICA DE INVESTIGACIÓN DE LA UNIVERSIDAD DE XALAPA. Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico.* , 23 - 34.

Patiño, R. (2017). Afectación del cibercrimen en las pymes. *Congreso Internacional: Crimen económico y fraude financiero y contable*, 59 - 66.

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamerica de Estudios de Seguridad Número 20*, 80 - 93.

Raudales, C. (2017). LA BRECHA EXISTENTE EN LA CIBERSEGURIDAD EN HONDURAS. *Innovare Ciencia y Tecnología*, 58 - 73.

Reyna, D., & Olivera, D. (2016). Las Amenazas Cibernéticas. *REVISTA ELECTRÓNICA DE INVESTIGACIÓN DE LA UNIVERSIDAD DE XALAPA. Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico.* , 35 - 55.

Riveros, F. (2016). ADMINISTRACION DEL RIESGO CIBERNETICO UN ENFOQUE DESDE LA ALTA GERENCIA EMPRESARIAL EN COLOMBIA. *UNIVERSIDAD MILITAR NUEVA GRANADA*, 1 - 24.

Rodríguez, J., Oduber, J., & Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. *Revista Latinoamericana de Estudios de Seguridad N° 20*, 63 - 79.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier. *Revista Latinoamerica de Estudios de Seguridad Número 20*, 8 - 15.

Sierra, H. (2015). EL DERECHO A LA PRIVACIDAD Y EL INTERVENCIONISMO DE ESTADO EN LA ERA DIGITAL. *Red Universitaria sobre Derechos Humanos y Democratización para América Latina*, 73 - 93.

Valdieso, A., & otros, y. (2016). Política exterior colombiana: escenarios y desafíos en el posconflicto. *Pontificia Universidad Javeriana : Fundación Konrad Adenauer*, 1 - 688.

“ANÁLISIS DE LOS CIBERATAQUES REALIZADOS EN AMÉRICA LATINA”

Manuel Jesús Guacho Lema

Universidad Tecnológica Empresarial de Guayaquil
Facultad de Ciencias Empresariales

Guayaquil, 2018

Contenido

INTRODUCCIÓN

La presente investigación determina el nivel de riesgo y preparación en ciberdefensa que tiene la región de tal forma que se puedan definir lineamientos para combatir futuras amenazas.

OBJETIVO GENERAL

Analizar los ciberataques que se han realizado en América Latina

OBJETIVOS ESPECÍFICOS

OBJETIVO I

Res[illegible]ir los ciberataques de la zona de análisis.

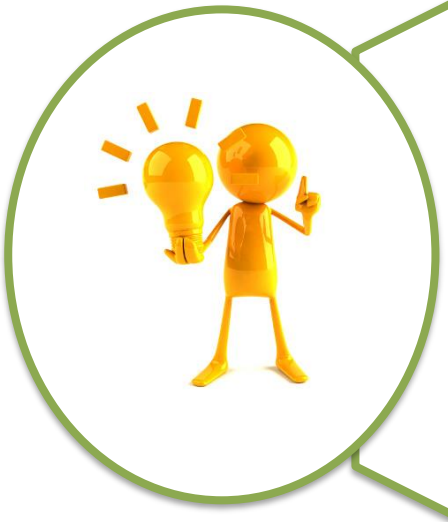
OBJETIVO II

Rea[illegible]ar un análisis de la ciberdefensa de América Latina.

OBJETIVO III

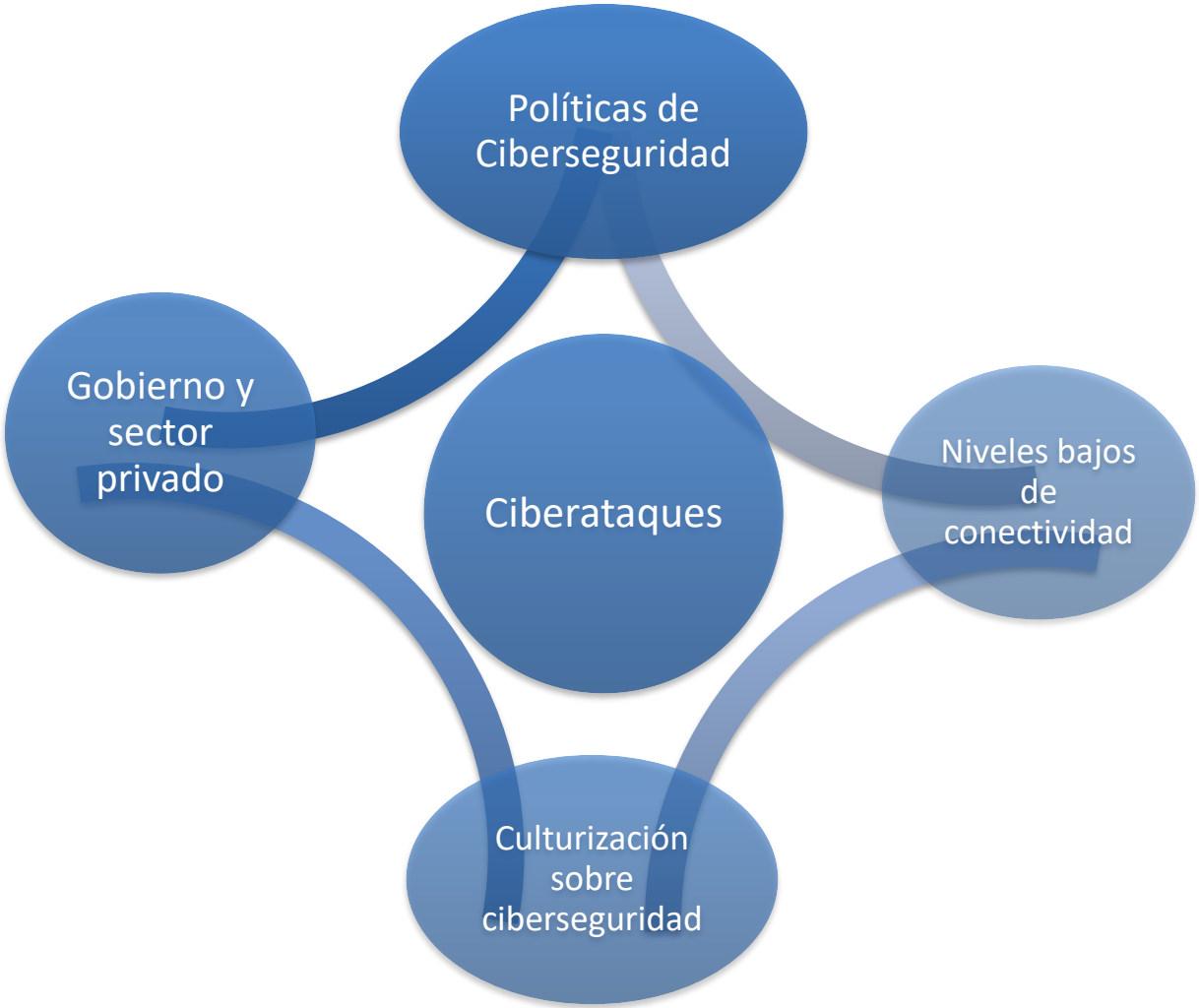
Siste[illegible]atizar las estrategias de la región para defenderse de los ciberataques.

FORMULACIÓN DEL PROBLEMA

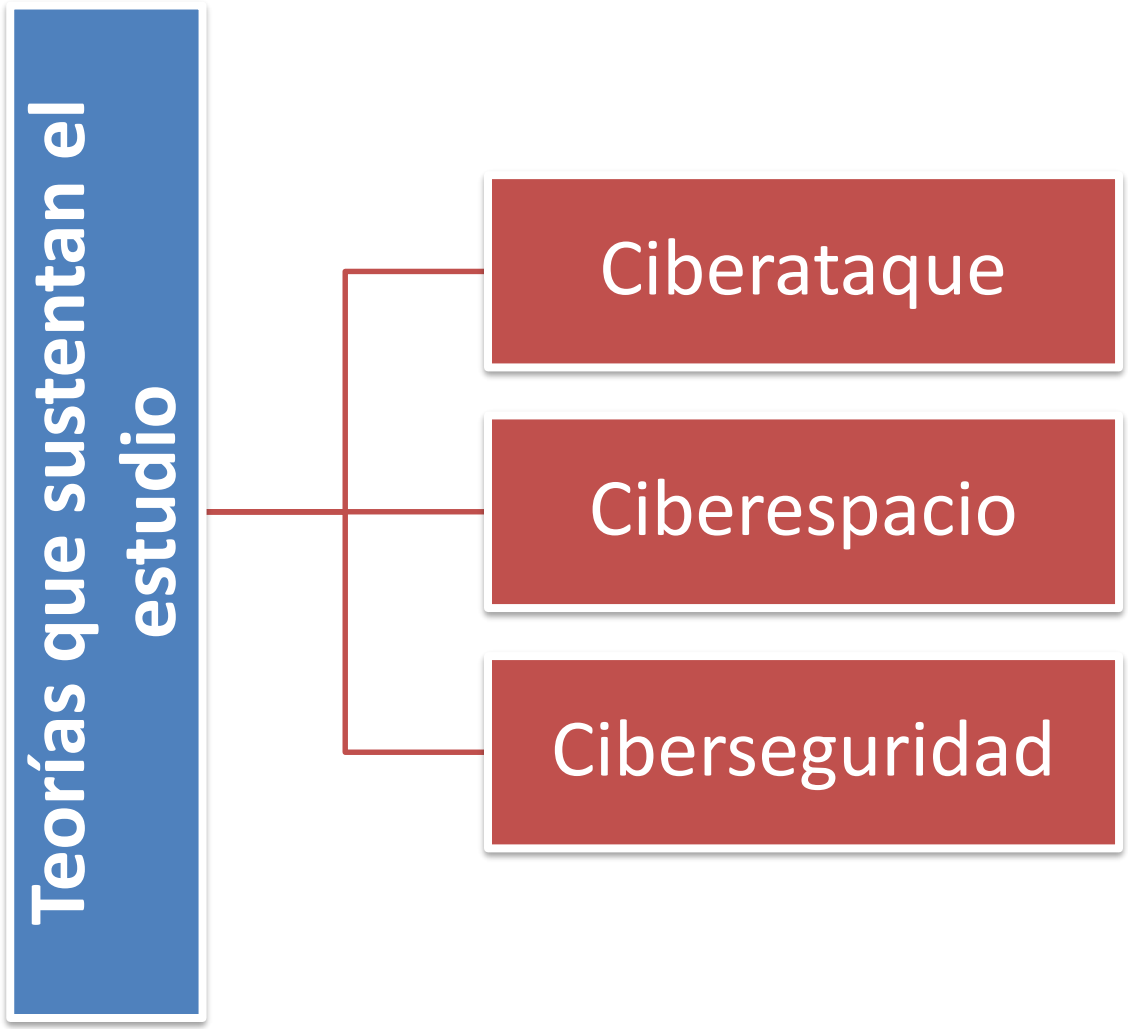


¿Cómo se está preparando América Latina para defenderse?

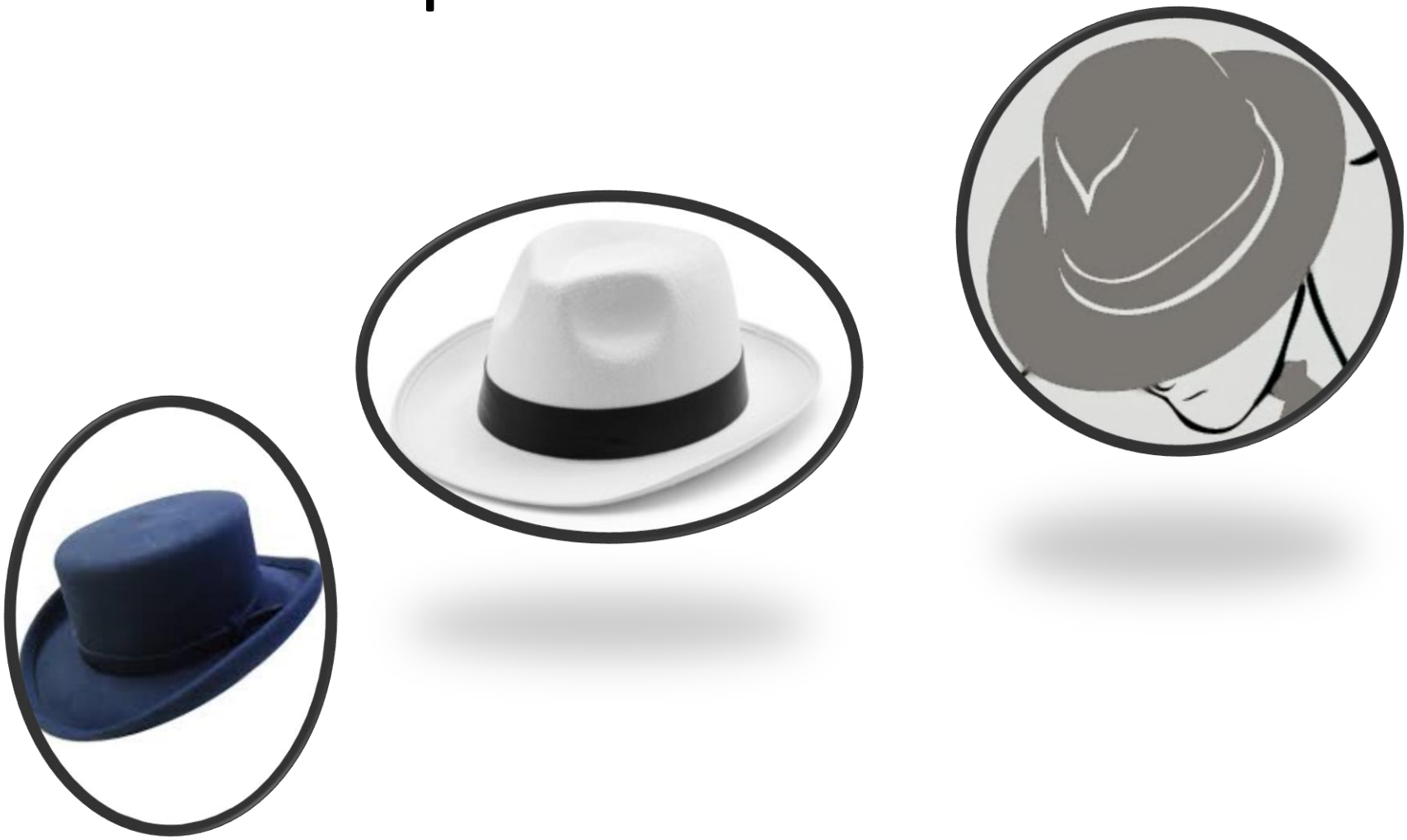
DESCRIPCIÓN DEL PROBLEMA



MARCO TEÓRICO



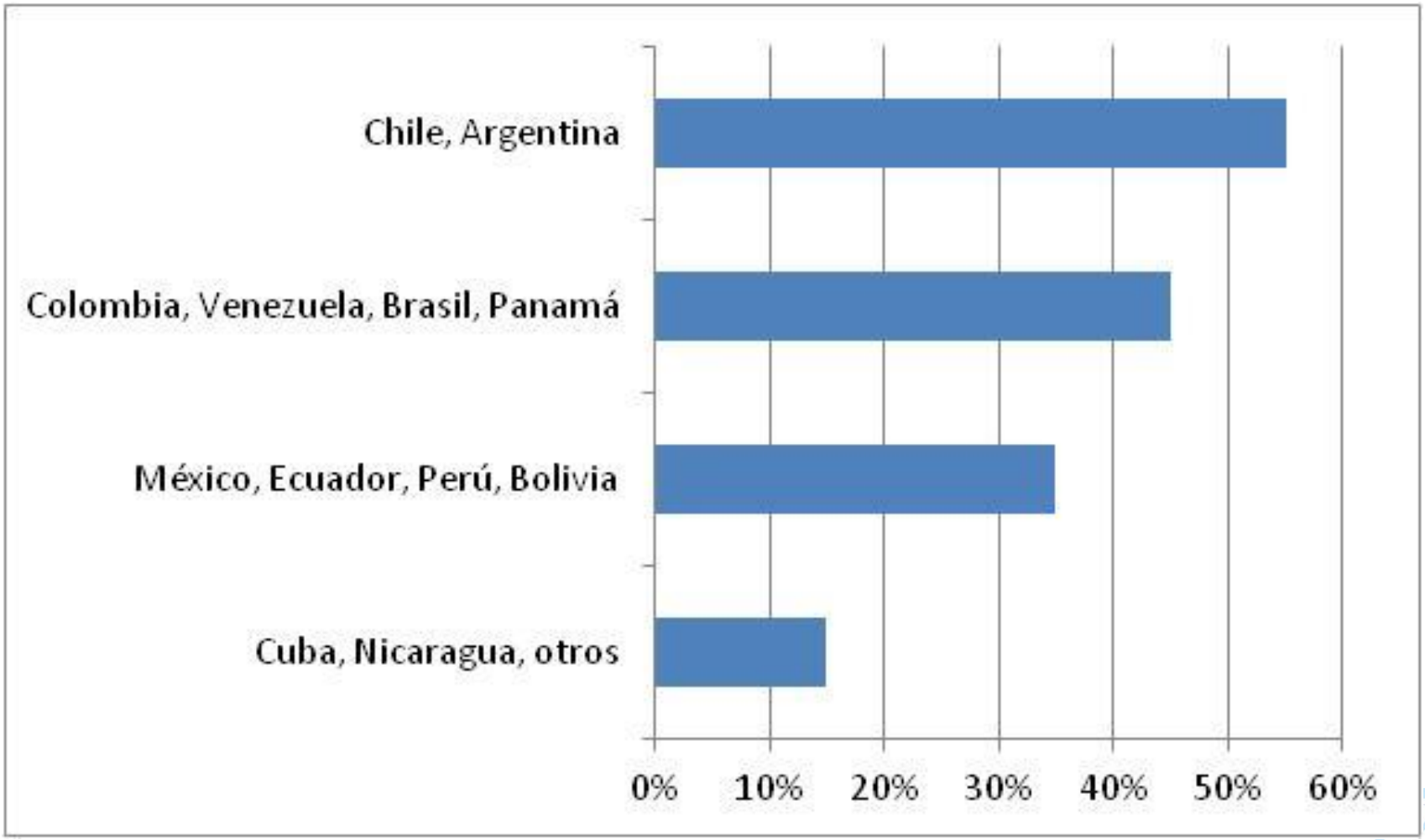
Tipos de hackers



METODOLOGÍA

Tipo de Investigación	• Documental, con características cualitativas
Población	• 20 países
Muestra	• 2009 hasta el 2017

Resultados



Nivel de penetración de internet por países

Sucesos relevantes de ciberataques y ciberdefensa en América Latina

2009

2011

UNASUR

del 2012, 2013 y 2014

2012

2013

2014

YAHOO! facebook Microsoft

2015

CSIRT EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

2016

Pokémon GO

2017

Pokémon GO

WannaCry Ransomware Attack

Conclusión

- Según lo que pudo observarse en los resultados de la investigación, América Latina tiene mucho trabajo por delante en temas de seguridad informática. Por ejemplo en la mayoría de países no existe una codificación general y sistemática sobre ciberdefensa.

- Gran parte del problema de ciberataques radica en la poca información o educación.

Recomendación

Países como Panamá, Noruega, España

Han implementado una Estrategia Nacional de Ciberseguridad que permita la disminución o eliminación total de ataques cibernéticos.

1) La definición de un marco jurídico robusto.

2) La difusión de información y culturización a la población. sobre temas de ciberseguridad y protección de datos.

3) La capacitación de personal en la temática.

4) El trabajo conjunto entre gobierno y sector privado, y

5) El fortalecimiento de la ciberdefensa.

GRACIAS POR SU ATENCIÓN