REVISTA CARIBEÑA DE CIENCIAS SOCIALES

Enero 2020 - ISSN: 2254-7630

IMPACTO DE LOS CIBERATAQUE EN LA SEGURIDAD INTERNACIONAL

IMPACT OF THE CIBERATAQUE ON INTERNATIONAL SECURITY

Autor: MSc. Ramón José Madrigal González.[1]

ramón@uniss.edu.cu

Para citar este artículo puede utilizar el siguiente formato:

Ramón José Madrigal González (2020): "Impacto del ciberataque en la seguridad internacional", Revista Caribeña de Ciencias Sociales (diciembre 2019). En línea: https://www.eumed.net/rev/caribe/2020/01/ciberataque-seguridad-internacional.html

RESUMEN: El auge vertiginoso experimentado por las Tecnologías Informáticas y las Comunicaciones a escala global; el ciberespacio se ha convertido en campo de batalla de muchos Estados y corporaciones, los cuales conforman estrategias de "resiliencias cibernéticas" ante ataques de hackers a infraestructurales vitales de las economías, tales como: redes eléctricas, instituciones financieras, departamentos de defensas, corporaciones fílmicas, parlamentos, sistemas electorales, redes informáticas, barcos, aviones. Gobiernos latinoamericanos y del mundo están destinando cada vez más presupuestos a la ciberseguridad y al ciberdefensa; los ciberdelicuentes no reconocen fronteras, sus propósitos es obtener el mayor lucro. El ciberataque dirigido por EE.UU. contra Venezuela es una táctica de Guerra no Convencional para acelerar conflictos internos y forzar un cambio de régimen, lo mismo ocurre contra el sistema informativo militar de Irán en respuesta del derribo de un dron, que el Pentágono habría propuestos después del ataque de un petrolero en el golfo de Omán.

Palabras clave: ciberataque, seguridad internacional, ciberespacio, resiliencias cibernéticas, hackers, ciberseguridad, ciberdefensa.

SUMMARY: The vertiginous boom experienced by Information Technology and Communications on a global scale; cyberspace has become the battlefield of many states and corporations, which form strategies of "cybernetic resilience" against attacks by hackers to vital infrastructure of economies, such as: electricity networks, financial institutions, defense departments, film corporations , parliaments, electoral systems, computer networks, ships, airplanes. Governments in Latin America and the world are increasingly allocating budgets to cybersecurity and cyberdefense; cyberdelicuentes do not recognize borders, their purposes is to obtain the greatest profit. The US-

[1] Máster en Ciencias de la Educación Superior. Profesor Asistente. Licenciado en Educación Primaria. Imparte Seguridad y Defensa Nacional en el Departamento de Enseñanza Militar de la Universidad de Sancti Spíritus "José Martí Pérez". Pertenece al Proyecto Forsat "Fortalecimiento al Sistema de Alerta Temprana para la cuenca Zaza y Agabama, Ha participado en el X Congreso Internacional de Desastre y la VI Conferencia de Bomberos en el Palacio de las Convenciones en La Habana, Cuba. Ha participado en el I, II Taller Nacional de Reducción de Riesgos.

led cyber attack against Venezuela is a non-conventional war tactic to accelerate internal conflicts and force a regime change, the same happens against the military information system of Iran in response to the demolition of a drone, which the Pentagon would have proposed after the attack of a tanker in the Gulf of Oman.

Keywords: cyber attack, international security, cyberspace, cybernetic resilience, hackers, cybersecurity, cyber defense.

Introducción

Los indicios son por demás demostrativos de la urgencia con que se está asumiendo este episodio de sabotaje a escala global. A pesar de imponerse el relato hegemónico del colapso venezolano, no cabe duda de que son más quienes asumen que se está perfilando una nueva manera de poner en práctica intervenciones, incluyendo al actual presidente de los Estados Unidos.(Cubadebate, 2019)

Más aún, el Foro Económico Mundial, que se reúne en Davos cada año, tiene desde febrero de este año advirtiendo a Estados y corporaciones conformar una estrategia de «resiliencia cibernética» en común ante ataques de hackers (independientes, contratados o gubernamentales) a infraestructuras vitales como las redes eléctricas, que podrían desencadenar efectos en cascada por lamentar. (Ob. Cit)

Hoy en día uno de los activos más importantes de las empresas después de las personas es su información. Invertimos en alarmas, vigilancia, seguros, seguridad perimetral, etc. pero ¿Cómo invertimos en proteger nuestros datos? robos, virus, ataques informáticos, fallos humanos, esto puede provocar la pérdida de datos indispensables para la empresa. (Martínez, 2019)

1. Ataque cibernético en Venezuela prende las alarmas en el mundo

Para nadie es casualidad que, días después de que se detectaran los impactos por arma electromagnética en el sistema eléctrico venezolano y se denunciara públicamente, la Casa Blanca emitiera una orden ejecutiva en el que urge a la comunidad científico-militar estadounidense a reforzar los sistemas defensivos en torno a las «tecnologías e infraestructuras críticas» de los Estados Unidos, de ser atacados por pulsos electromagnéticos que podrían «interrumpirlas, degradarlas y dañarlas» (Rusia y China, «amenazas existenciales» para el Pentágono, poseen sus propios arsenales en la materia). (Ob. Cit)

No se tiene noticia de ciberataque alguno de la magnitud registrada el 7 de marzo de 2019 a la Central Hidroeléctrica de Guri, sobre todo por las consecuencias humanas y económicas del apagón que duró poco más de 72 horas. Si llegara a ocurrir cualquier acción similar en el futuro en otro país (incluyendo los Estados Unidos), tendrá a Venezuela como precedente. (Ob. Cit)

La revista Forbes publica un artículo donde se reconoce que es «muy realista» el hecho de que la causa del blackout fuera un ciberataque dirigido por Estados Unidos. Asegura que ésta sería una táctica implicada en la aceleración de los conflictos internos de un país para forzar un cambio de régimen, ya que perjudica infraestructuras y servicios críticos de una sociedad. (Ob. Cit)

No sólo existen indicios de que los apagones en Venezuela fueron provocados por nuevas modalidades de guerra con autoría foránea (estadounidense, específicamente), también el precedente venezolano sentó las bases para que organizaciones de ascendencia occidental como Forbes y el Foro Económico Mundial advirtieran que efectivamente se están tomando de manera estratégica armas de semejantes calibres contra las líneas vitales de países y hasta corporaciones en todo el mundo. (Ob. Cit)

La guerra eléctrica sería un nuevo capítulo de la agresión que lleva adelante la extrema derecha, cumpliendo los designios de Estados Unidos, ya que solo tres minutos después del apagón, la

cuenta de Twitter de Marco Rubio anunciaba exultante el siniestro. También se pronunció Mike Pence, quien anunció además que lo siguiente sería la caída de Maduro. (Cubainformación, 2019)

El mandatario denuncia ante una marcha antimperialista del pueblo, que el país fue víctima desde el pasado jueves de una de las mayores agresiones en 200 años de soberanía nacional, pero el Gobierno en pleno trabaja para solucionar las afectaciones causadas por un sabotaje cibernético que dejó sin electricidad a 18 de los 24 estados y generó daños en las telecomunicaciones. (Ob. Cit)

La alcaldesa de la capital de Venezuela, Erika Farías, afirma a Telesur este domingo que el «pueblo ha respondido en paz y se va a mantener en paz», a lo que añade que la reanudación de la energía será progresiva. Detalla que las autoridades se encuentran desplegadas atendiendo las distintas contingencias en la ciudad capital, garantizando el suministro de agua y alimentos con prioridad para la red de hospitales públicos. (Ob. Cit)

La guerra eléctrica sería un nuevo capítulo de la agresión que lleva adelante la extrema derecha, cumpliendo los designios de Estados Unidos, ya que solo tres minutos después del apagón, la cuenta de Twitter de Marco Rubio anunciaba exultante el siniestro. También se pronunció Mike Pence, quien anunció además que lo siguiente sería la caída de Maduro. (Ob. Cit)

El Presidente cubano Miguel Díaz-Canel catalogaba de sucio hecho terrorista el ataque al sistema eléctrico nacional de Venezuela. Desde su cuenta de Twitter denuncia que el siniestro busca alentar una intervención armada en el país de Bolívar. Evo Morales, presidente de Bolivia, por su parte, lo tachaba de cobardía y advertía acerca del efecto de las sanciones injerencistas por parte de la administración Trump. (Ob. Cit)

En una conferencia de prensa de septiembre de 2018, el asesor de Seguridad Nacional John Bolton señala lo importante que es el ciberespacio para la disuasión geopolítica y militar de sus adversarios. Afirma que con ese propósito han «autorizado operaciones cibernéticas ofensivas (…) para demostrar que el costo de su participación en operaciones contra nosotros es más alto de lo que quieren soportar». (Ob. Cit)

La carrera armamentística en torno a las estrategias cibernéticas son tomadas cada vez más en cuenta, sobre todo si tomamos en cuenta que detrás de la cortina de la guerra comercial entre China y la Administración Trump se encuentra el campo de batalla de la ciberguerra y el desarrollo de las tecnologías de última generación. (Ob. Cit)

En los últimos años los distintos actores llamados a enfrentarse en una Tercera Guerra Mundial (Estados Unidos, China, Rusia) vienen preparándose en este terreno. Pero con el cibergolpe en Venezuela estamos presenciando una actitud que incluye defenderse con más ahínco de este tipo de ataques, que producen efectos cascada indeseables para cualquier población. (Ob. Cit)

Con la petición de la Casa Blanca a la comunidad científico-militar de aumentar los esfuerzos defensivos ante un ataque electromagnético, al mismo tiempo que organizaciones ligadas al corporativismo anglo-americano llama a conformar una estrategia de «resiliencia cibernética», dejan a la vista que el ataque multifactorial contra el sistema eléctrico venezolano fue un acontecimiento de alcance mundial que genera una alerta en Estados y empresas que no se toman a juego escenarios de sabotaje bajo formatos de guerra híbrida. (Ob. Cit)

Se evidencia así, que la alarma suena ante las amenazas de variada beligerancia que ponen en crisis los viejos formatos de intervención y empieza a asumirse una visión más profunda en torno a los campos de acción que competen a la ciberguerra y las nuevas armas de combate**.** (Ob. Cit)

2. Amenaza de ataques cibernéticos contra América Latina

Según Kaspersky, Brasil, México y Colombia son los países que más ataques cibernéticos han sufrido en lo que va el 2017, lo que incluye ataques realizados al estar conectados a internet y

estando fuera de conexión. En cantidad de ataques Brasil representa el 53% del total, mientras que México se ubicó en el segundo lugar con 17% y Colombia en el tercer lugar, con 9%. (CNN Expansión, 2017)

América Latina registra 746.000 ciberataques en el año 2018, reportando un crecimiento de 60% con respecto al periodo anterior y equivale a una media de 9 ataques por segundo, revela un estudio de la compañía rusa Kaspersky Lab, presentado en la Octava Cumbre de Analistas de Seguridad para América Latina realizada en Panamá. (El Comercio, 2018)

Venezuela, Bolivia y Brasil son los países que mayor número de ataques recibieron en los últimos meses, la mayoría de los cuales estaban orientados al dinero. (Ob. Cit)

Al igual que en 2017, Brasil continúa encabezando a los países latinoamericanos en términos de alojamiento de sitios maliciosos ya que 50% de los hosts ubicados en América Latina que se utilizaron en ataques a usuarios de todo el mundo está ubicado en este país. (Ob. Cit)

La investigación revela también que las empresas son más propensas a recibir ataques por medio de emails (60%) y vectores offline (43%); es decir, USB contaminados. Del mismo modo, aumentaron los ataques a través de móviles y el “phishing” fue el más común. (Ob. Cit)

Los ciberdelincuentes no conocen fronteras a la hora de lograr sus propósitos e intentar obtener el mayor lucro posible de sus actividades. Latinoamérica es un importante mercado para ellos y un objetivo cada vez más codiciado. Una de las posibles razones para explicar el fenómeno es que no siempre los países latinos suelen contar con los estándares de seguridad que se aplican, por ejemplo, a nivel europeo. A eso se suma la progresiva sofisticación y profesionalización del cibercrimen. (Heyder, 2019)

La alta dependencia tecnológica que tienen nuestros países genera que seamos vulnerables en cualquier momento a un ataque cibernético, expresa Cárdenas, oficial de operaciones del Comando Conjunto del Comando General de las Fuerzas Militares de Colombia. El creciente uso de las tecnologías para el desarrollo de actividades económicas y sociales genera "riesgos de seguridad" que deben ser tomados en cuenta. (Sputnik, 2019)

De no hacerlo se puede materializar en cualquier momento un ataque de carácter cibernético, asegura Cárdenas, quien asistió en Montevideo al seminario Ciberseguridad/ciberdelincuencia: protección en la red de menores", realizado en la capital uruguaya. (Ob. Cit)

El especialista colombiano destaca que los Gobiernos de la región están destinando cada vez más presupuesto a la ciberseguridad y la ciberdefensa, pero que no obstante eso los países latinoamericanos se encuentran lejos todavía de tener sistemas de protección igualmente de efectivos que los de potencias como Estados Unidos, Rusia e incluso España. (Ob. Cit)

Se explica que estamos en un proceso de evolución, pero nos falta muchísimo para poder estar en un nivel alto para en cualquier momento poder contrarrestar cualquier amenaza de carácter cibernético. (Ob. Cit)

3. Los ataques cibernéticos contra los bancos

La ola de crecientes ataques tecnológicos hacia las instituciones financieras refleja una necesidad de reforzar los sistemas de ciberseguridad no sólo en México sino en toda la región latinoamericana. (Mijares, 2019)

Las problemáticas en materia de seguridad cibernética que enfrentan las entidades financieras se profundizan en la región latinoamericana. Desde el presupuesto que destinan los bancos a la ciberseguridad hasta los equipos que utilizan para operar promueven que haya mayores riesgos de sufrir ataques tecnológicos. (Ob. Cit)

La idea es lograr un sistema en capas, es decir, varios niveles que evalúen, identifiquen y mitiguen el riesgo de sufrir un ataque cibernético y esto no sólo es necesario por el impacto que podría tener en la economía del banco mismo o del sistema financiero sino porque comprometen bases de datos enormes, (Ob. Cit)

Y aunque la mayoría de los bancos importantes en países como México los procesos y técnicas en materia de seguridad cibernética no son las mismas que en donde se encuentran sus sedes. Ob. Cit)

3.1Ataque a la banca chilena

Los ciberdelincuente suelen ir a la fuente misma de lo que ellos quieren, es decir, el dinero. Es así como en Chile se han registrado diversos ataques a entidades bancarias y de crédito. (Heyder, 2019)

Según explica, Eduardo Ebensperger a mediados del 2018 una banda de hackers ataca al Banco de Chile logrando obtener un jugoso botín de cerca de 10 millones de dólares. Este banco es la segunda entidad financiera del país y fue obligado a desconectar cerca de 9 mil estaciones de trabajo en sus sucursales el para detener la propagación de un virus. (Ob. Cit)

Sin embargo, eso no fue todo. El plan de los delincuentes era bastante más sofisticado: intentar distraer al banco con el virus y al mismo tiempo los hackers iniciaban una serie de transacciones fraudulentas para robar dinero de la entidad. Al darse cuenta, el banco comenzó a cancelar las transferencias, pero cuatro de ellas fueron exitosas y hasta hace poco tiempo los montos no habían podido ser recuperados. El dinero fue a parar en gran parte a cuentas en Hong Kong, explica el gerente general al ser entrevistado por medios locales. (Ob. Cit)

4. Los retos ante los ciberataques

4.1. Adopción de marco estandarizado de mejores prácticas.

En este aspecto, el especialista enfatiza en que es necesario que la región latinoamericana refuerce la cooperación trasnacional y siga políticas alineadas con el fin de conocer más los procesos operativos del crimen cibernético y estar más preparados para hacer frente a ellos. (Mijares, 2019)

4.2. Mejorar los procesos en cómo se miden los riesgos

Otra de las áreas de oportunidad de la banca en países como México es entender mejor cómo se debe evaluar el riesgo, no sólo en términos conceptuales sino también en términos de qué agentes se encuentra involucrados en los procesos. Es decir, la evaluación de riesgo engloba desde el personal operativo del banco hasta el equipo con el que trabaja y el software que ocupa, cualquier factor puede influir en ser más o menos vulnerable a los ataques. (Ob. Cit)

4.3. Asignación de mayor presupuesto de los bancos a la ciberseguridad

Muchas entidades financieras, especialmente las medianas o pequeñas tienden a destinar pocos recursos a la seguridad cibernética. No sólo se debe ser eficiente sino también aumentar el presupuesto en este rubro. Para la banca en la región es complicado especialmente porque todavía no hay formas oficiales de medir la tasa de retorno de esas inversiones en protección, pero con la creciente ola de ataques a bancos ya se puede construir una idea de cuánto puede costarles no invertir correctamente en protección cibernética. (Ob. Cit)

4.4. Reanalizar los controles, actualizarlos a los nuevos patrones

Los ataques tecnológicos de antes no afectan ni operan igual que ahora. Por tanto, los procesos de protección deben actualizarse en todo momento. Las revisiones y evaluaciones deben estar al día con la delincuencia cibernética debido a que en la innovación financiera las técnicas se vuelven obsoletas muy pronto. (Ob. Cit)

4.5. Capacitación especializada

A escala global, pero especialmente en América Latina, persiste una brecha importante en cuanto a la especialización de los equipos destinados a proteger el sistema financiero de la delincuencia virtual. Es importante capacitar y aumentar el nivel de los agentes especializados en ciberseguridad. (Ob. Cit)

4.6 Combinar conocimiento técnico con conocimiento empresarial y negocios

De la mano con el punto previo, también es necesario que se creen puentes entre todos los que conforman una entidad financiera. Se puede tener a los mejores hackers o responsables de protección cibernética, pero si no se combina con una perspectiva de negocios y empresas la cultura de seguridad no llegará a todos los espacios de la institución. (Ob. Cit)

4.7 Implementar nueva tecnología y equipos modernos

Es mucho más fácil sufrir de un ataque virtual cuando se opera con equipo y maquinaria obsoleta. Algunos bancos de México y el resto América Latina no invierten en mejorar sus tecnologías o equipos lo que aumenta las posibilidades de que transgredan su sistema. (Ob. Cit)

4.8 El factor cultural

Otro de los grandes retos que enfrenta la región latinoamericana en materia de ciberseguridad es la cultura, señala el especialista, Alejandro Mijares. (Ob. Cit)

Los clientes mismos no tienen la costumbre de preguntar o enterarse sobre temas de seguridad tecnológica y aunque los bancos operan bajo protocolos de protección no son suficientes para prevenir ataques cibernéticos y como consecuencia tampoco tienen alcance para saber el uso de los datos que se pierden cuando esto ocurre. (Ob. Cit)

La participación del gobierno puede ser clave en este aspecto, con iniciativas de concientización como la campaña **Ciberseguridad México 2019,** que, aunque no sólo está enfocada en el sector financiero sí puede tener influencia en el conocimiento, la información y los procesos tecnológicos en la población. (Ob. Cit)

Mijares señala que un efecto real de estos proyectos se verá sólo si se mide el alcance y el impacto que tuvieron, para que puedan mejorarse y adecuarse para cada sector. (Ob. Cit)

5. Ataque cibernéticos más importante del mundo

1999: Pirata informático ataca la NASA y el Departamento de Defensa de EE. UU.

Jonathan James tenía solo 15 años cuando se infiltra de forma repetidamente el Departamento de Defensa de Estados Unidos y la Administración Nacional de Aeronáutica y del Espacio (NASA) en 1999. Durante el ataque contra la Agencia de Reducción de Amenazas del Departamento de Defensa, una oficina encargada de contrarrestar las amenazas de armas nucleares, biológicas y químicas, robó nombres de usuario y contraseñas y más de 3.000 correos electrónicos. (El Mundo, 2019)

Debido a que cometió los delitos como menor de edad, fue sentenciado a detención de menores durante seis meses. James se suicidó en 2008 después de que el Servicio Secreto de Estados Unidos lo acusara de estar involucrado en otro ataque cibernético. (Ob. Cit)

2014: Presunto ataque de Corea del Norte a Sony

En noviembre de 2014, Sony Pictures sufre un ataque cibernético después de que un grupo de hackers que se llamaban a sí mismos Guardianes de la Paz obtuvieran acceso a la red de computadoras de la compañía. Corea del Norte negó su responsabilidad, pero describió el ataque como una "acción justa" en respuesta a la película de Sony "La entrevista", una comedia que describe la muerte violenta de Kim Jong-un de Corea del Norte. (Ob. Cit)

El Departamento de Justicia de Estados Unidos finalmente acusa al norcoreano Park Jin-hyok en septiembre de 2018 por estar detrás del ataque. El FBI dice que Park había trabajado con una compañía que operaba como fachada para el Gobierno de Corea del Norte. (Ob. Cit)

2015: Ataque a la red eléctrica de Ucrania

En diciembre de 2015, unas 230.000 personas quedaron hasta seis horas en la oscuridad después de que piratas informáticos se infiltraran en tres compañías de energía y cerraran temporalmente los generadores en tres regiones de Ucrania. (Ob. Cit)

El servicio de seguridad de Ucrania culpa al Gobierno ruso por el ataque. Por otra parte, sin nombrar a Moscú, algunas compañías privadas de seguridad de Estados Unidos que investigaron el suceso dijeron que creían que este se había originado en Rusia. Se cree que este ataque es la primera vez que piratas informáticos pueden atacar con éxito una red de distribución de electricidad. (Ob. Cit)

2016: Elecciones presidenciales en Estados Unidos

Piratas informáticos filtraron miles de correos electrónicos del Comité Nacional Demócrata (DNC), la junta directiva del Partido Demócrata, durante las elecciones presidenciales de 2016. La filtración avergonzó al liderazgo del partido, quien expresa su desdén en algunos correos electrónicos por la campaña de Bernie Sanders, un candidato que había competido con Hillary Clinton para convertirse en el candidato presidencial del partido. (Ob. Cit)

El Departamento de Justicia de Estados Unidos acusa más tarde a 12 rusos –que se cree son agentes de la agencia de inteligencia militar de Rusia, el GRU– por llevar a cabo el ataque cibernético. Los cargos fueron emitidos por el abogado especial Robert Mueller, quien está investigando las denuncias de que el Gobierno ruso intervino en la votación presidencial para ayudar a elegir al entonces candidato del Partido Republicano, Donald Trump. (Ob. Cit)

2017: WannaCry

Un ataque con un ransomware conocido como WannaCry infecta a unas 300.000 computadoras en 150 países en mayo de 2017. El software cifra los archivos y exige a los usuarios entregar cientos de dólares a cambio de claves para descifrar los archivos. (Ob. Cit)

El ataque afecta a hospitales, incluidos muchos pertenecientes al Servicio Nacional de Salud (NHS) del Reino Unido, bancos y otras empresas. La compañía FedEx dice que había perdido cientos de millones de dólares como resultado del ataque. Estados Unidos y Reino Unido culparon a Corea del Norte, una acusación que Pyongyang negó y que califica de "grave provocación política". (El Mundo, 2019)

2019: Ataque del Bundestag alemán

En enero de 2019, la Oficina Federal de Seguridad de la Información de Alemania (BSI) dice que estaba investigando un ataque cibernético contra cientos de políticos, incluida la canciller alemana, Ángela Merkel. El ataque cibernético se dirige a todos los partidos en el Parlamento alemán, excepto al partido de extrema derecha Alternativa para Alemania (AfD). (Ob. Cit)

Información financiera, tarjetas de identificación y chats privados se encontraban entre los datos que los hackers publicaron posteriormente en línea. El número de fax de Merkel, la dirección de correo electrónico y varias de sus cartas también fueron publicados. El Gobierno aún no ha nombrado ningún sospechoso o no ha divulgado posibles motivos para el ataque. (Ob. Cit)

6. Tendencias en seguridad informática para el 2019

Se plantea en el reporte de ESET "Tendencias 2019" reflexiona sobre la importancia y responsabilidad que recae en las compañías a la hora de proteger los grandes volúmenes de datos que han recopilado a lo largo de los años. El 2018 se destaca en la historia de la privacidad de los datos, debido a que la Unión Europea (UE) hizo efectivo el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), el cual tiene implicaciones para cualquier organización (independientemente de su ubicación) que maneja información personal de ciudadanos de la UE. Según el informe de ESET, otras partes del mundo tomarán el camino de la UE, y analizan también la posibilidad de la existencia de una ley global. (Vida y Éxito, 2019)

Por otro lado, se destaca el rol de los hogares inteligentes a partir del uso de los asistentes de voz. Las posibilidades existentes de que los criminales pueden aprovecharse de los dispositivos IoT interconectados en el hogar y de esta manera invadir la privacidad, además se resalta el rol de los usuarios vinculado a la cantidad y el tipo de datos que se comparte con estos artefactos. (Ob. Cit)

En este contexto, el informe cuenta con un apartado dedicado a Machine Learning (ML). Esta tecnología que se basa en la generación de información a partir del análisis automatizado de grandes volúmenes de datos, también gana espacio en el campo de la ciberseguridad. Si bien los algoritmos utilizados podrían permitirle a desarrolladores identificar amenazas actuales de una manera más eficiente, también puede ser utilizada por actores malintencionados, para desarrollar tareas automatizadas y obtener información de blancos vulnerables. En el reporte de ESET se explica el potencial que tiene esta tecnología tanto para atacantes como para quienes se encargan de la seguridad. (Ob. Cit)

7. El Ministerio de Defensa de España ante los ataques cibernéticos

El Ministerio de Defensa atribuye a una "potencia extranjera" el ciberataque contra su red interna descubierto a primeros de marzo. Los responsables de la investigación se basan en la complejidad del ciberataque para descartar la autoría de *hackers* o ciberactivistas y sostener que "hay un Estado detrás". El *Informe Anual de Seguridad Nacional,* aprobado el pasado día 15 y al que ha tenido acceso EL PAÍS, no recoge aún ese incidente, pero alerta del "incremento en la agresividad de algunos servicios de inteligencia extranjeros" y califica al ciberespionaje de "grave amenaza" para la seguridad nacional. (González, 2019)

La investigación sobre el ciberataque sufrido por Defensa aún no ha terminado, pero a medida que avanza, según fuentes del ministerio, se tienen ya algunas ideas claras: es mucho más grave de lo que inicialmente se había pensado y se descarta al 90% que la intrusión procediera de dentro; es decir, de alguno de los operadores de la red de propósito general (WAN PG). Una cabo del Centro de Sistemas y Tecnologías de la Información y las Telecomunicaciones (Cestic) descubrió esa intromisión, pero el virus llevaba muchos meses (más de un trimestre, como al principio se creyó) infectando la red del Ministerio de Defensa sin que nadie lo advirtiese. (Ob. Cit)

El temor es que el virus —que al parecer se introdujo con un correo electrónico— haya colonizado otras redes. El objetivo de los ciberespías, según las fuentes consultadas, podrían ser secretos tecnológicos de la industria militar. Los investigadores no se atreven aún a señalar a los autores de la intrusión pero, por sus características técnicas, no dudan en afirmar: "Hay un Estado detrás". (Ob. Cit)

"El espionaje industrial de información clasificada en poder de empresas que participan en programas del Ministerio de Defensa supone una amenaza de primera magnitud para la Seguridad Nacional", describe el *Informe Anual de Seguridad Nacional 2018*. (Ob. Cit)

En cualquier caso, el ciberespacio se ha convertido ya, según el documento, en un “nuevo campo de batalla” en el que operan Estados, espías, empresas, grupos terroristas o ciberdelincuentes, entre otros actores. (Ob. Cit)

La batalla de la desinformación. Junto a los ciberataques, “cada vez más sofisticados”, medios de información en Internet y redes sociales pueden convertirse en “armas de persuasión masiva”, susceptibles de actuar como “elementos de desestabilización de la sociedad en momentos relevantes, como en los periodos electorales”, señala el informe. Sin mencionar casos concretos, el documento advierte de que, junto con el ciberespionaje, las “operaciones híbridas de terceros Estados”, que combinan la fuerza militar o la diplomacia con la manipulación de la información a través de la red constituyen las “amenazas más críticas”. (Ob. Cit)

La amenaza para España se asocia a su pertenencia a la coalición internacional. El mayor riesgo de atentado “proviene de terroristas individuales autorradicalizados o de quienes se integran en células autónomas”, como la que perpetró los atentados de Barcelona y Cambrils. También ese caso demuestra la “preocupante capacidad” de estos grupos “para fabricar medios explosivos de alta potencia recurriendo a materiales fácilmente disponibles”. (Ob. Cit)

8. EE. UU. lanza un ciberataque a Irán

El comando cibernético del Ejército de Estados Unidos lanza un ataque digital contra el sistema informático militar de Irán, aprobado por el presidente Donald Trump, al mismo tiempo que el presidente ordenaba abortar un ataque más convencional con misiles en respuesta al derribo de un dron de vigilancia estadounidense, según ha informado en primicia Yahoo News. (Guimón, 2019)

Los ciberataques llevaban semanas, si no meses, planeándose, según mandos militares anónimos citados por Associated Press. El Pentágono, de hecho, habría propuesto lanzarlos después del ataque contra dos petroleros en el golfo de Omán, hace casi dos semanas, que EE UU atribuye a Teherán. (Ob. Cit)

Las intrusiones dejaron supuestamente sin funcionar los sistemas utilizados para controlar los lanzamientos de misiles por la Guardia Revolucionaria, fuerza de élite iraní considerada por Washington una organización terrorista. La efectividad de un ataque así solo podría verificarse si Teherán tratara de lanzar un misil. Aunque, según Associated Press, Irán desconecta de Internet parte de su infraestructura militar después de un ataque a finales de la década pasada con un virus que aseguran fue una creación conjunta de EE UU e Israel. (Ob. Cit)

También fue atacado, según las mismas fuentes, el *software* utilizado por un grupo de la inteligencia iraní que supuestamente participa en la planificación de los ataques a los dos petroleros. La operación no habría causado ninguna víctima, civil o militar, en contraste con el ataque con misiles que Trump ordena detener, según él mismo dijo, por el “desproporcionado” coste en vidas que habría implicado. "No quiero matar a 150 iraníes. No quiero matar 150 de nada ni nadie excepto si es absolutamente necesario", explica Trump. (Ob. Cit)

El ciberataque fue autorizado, según *The New York Times,* porque se encuentra por debajo de lo que se entiende por el umbral del conflicto armado, la misma táctica empleada por Irán en sus recientes agresiones. En los últimos tiempos, los mandos militares estadounidenses han optado más a menudo por batirse con sus enemigos en el ciberespacio, donde cuentan con una capacidad militar cada vez más sólida, en vez de emprender acciones militares más ofensivas y costosas. Las operaciones *online* pretenden disuadir a Irán de cometer más agresiones dentro de esta guerra en la sombra que empiezan a librar ambos países. (Ob. Cit)

El presidente Trump advierte de que la opción militar "está siempre sobre la mesa hasta que esto se solucione", y anuncia que impondrá “sanciones adicionales” a Teherán. “Confía en que Irán sea listo y se preocupe por su gente”, dice el presidente republicano, antes de partir a su residencia de descanso en Camp David, Maryland, para “trabajar en muchas cosas, incluido Irán”. (Ob. Cit)

Conclusiones

Se ha demostrado que el impacto generado por la violación de seguridad informática, ha creado preocupación desde el mundo privado y estatal sobre la correcta forma de protección de datos y en general del nivel de seguridad, si los protocolos son los adecuados, y si la inversión está al día comparada con otros mercados. (Martínez, 2018)

Se ha concluido que cada año, los usuarios de dispositivos digitales tales como PC, computadoras portátiles, teléfonos celulares y tabletas se convierten en víctimas de robo tanto físico como digital. Mientras que los dispositivos robados en sí, presentan una pérdida financiera para el usuario, también crean una gran amenaza a la seguridad. Los datos almacenados en esta clase de dispositivos se vuelven susceptibles no solo a criminales comunes, pero también a ciber criminales y hackers, y para las empresas, una falta de implementación de estándares adecuados en la protección de la seguridad de datos puede ser extremadamente perjudicial. Violaciones de seguridad ocurren con más frecuencia de lo esperado o pensado y son los mejores ejemplos de por qué la implementación de una política de encriptación debe ser una prioridad principal. (Ob. Cit)

Esto destapa una discusión mucho más general en torno a la protección de datos en todas sus formas, y una de las más efectivas hasta el momento es la encriptación basada en *hardware*. (Ob. Cit)

Referencias bibliográficas

Mijares, A. (2019). Seguridad Contra Ataques Cibernéticos a Bancos, con Problemas en ... Disponible en: https://kaufmanrossin.com › News. Consultado el 25 de junio de 2019

Cubainformación (2019).Venezuela bajo ataque – Cubainformación. Disponible en: www.cubainformacion.tv/.../america.../80875-venezuela-bajo-ataque-todo-sobre-el-sh... Consultado el 25 de junio de 2019

Cubadebate (2019). Ataque cibernético en Venezuela prende las alarmas en el mundo... Disponible en: www.cubadebate.cu/.../ataque-cibernetico-en-venezuela-prende-las-alarmas-en-el-mu... Consultado el 25 de junio de 2019

Sputnik (2019). La amenaza de un ataque cibernético en América Latina está "latente... Disponible en: https://mundo.sputniknews.com/.../201706031069672580-ciberataque-america-latina/ Consultado el 25 de junio de 2019.

El Mundo (2019). Seis ataques cibernéticos que sacudieron el mundo – DW. Disponible en: https://www.dw.com/es/seis-ataques-cibernéticos-que...el-mundo/a-46967214 Consultado el 25 de junio de 2019.

Vida y éxito (2019). Información de ataques cibernéticos en América Latina - Vida y Éxito. Disponible en: https://www.vidayexito.net/tags/ataques-ciberneticos/ Consultado el 25 de junio de 2019.

Heyder, C. (2019). Mapa de los ataques cibernéticos en Latinoamérica 2018 - F-Secure... Disponible en: https://blog.f-secure.com/es/mapa-de-los-ataques-ciberneticos-en-latinoamerica-2018/ .Consultado el 25 de junio de 2019.

CNN Expansión, (2017). Cada 33 segundos hay un ataque cibernético en América Latina | CNN. Disponible en: https://cnnespanol.cnn.com/.../cada-33-segundos-hay-un-ataque-cibernetico-en-ameri... Consultado el 25 de junio de 2019.

El Comercio (2018). Ataques cibernéticos crecieron 60% en América Latina, revela informe... Disponible en: https://elcomercio.pe › Tecnologia › Actualidad. Consultado el 25 de junio de 2019.

González, M. (2019). Una “potencia extranjera” atacó los ordenadores de Defensa. Disponible en:

" https://elpais.com › España. Consultado el 1de julio de 2019.

Guimón, P. (2019). EE UU lanzó este jueves un ciberataque a Irán autorizado por Trump. Disponible en:

" https://elpais.com › Estados Unidos. Consultado el 1de julio de 2019.

Martínez, O. (2018) Encriptación basada en hardware: la solución al crimen informático. Disponible en:

" https://lasverdadesdemiguel.tv/encriptacion-basada-en-hardware-la-solucion-al-crimen...
https://elpais.com › Estados Unidos. Consultado el 1de julio de 2019.