ISSN-E: 2737-6439

Athenea Journal
Vol.3, Núm. 9, (pp. 26-37)

https://doi.org/10.47460/athenea.v3i9.43

Perspectivas sobre la ciberseguridad y ciberdefensa en América Latina

Pavón Estefanía
https://orcid.org/0000-0002-4832-1386
eesteefania@hotmail.com
Fuerza Terrestre Ecuatoriana,
Brigada de Artillería 27 Portete
Cuenca-Ecuador

Guaytarilla Luis Fernando
https://orcid.org/0000-0002-3547-1887
guaytikfer@hotmail.com
Fuerza Terrestre Ecuatoriana,
Batallón de Selva 62 Zamora
Zamora-Ecuador

Cueva Christian
https://orcid.org/0000-0002-7788-0363
chris.cueva.1993@icloud.com
Fuerza Terrestre Ecuatoriana,
Tercera División Tarqui
Cuenca-Ecuador

Durango Karla
https://orcid.org/0000-0003-4796-3245
karlysdu_1603@hotmail.com
Fuerza Terrestre Ecuatoriana,
Brigada de Artillería 1 El Oro
Machala-Ecuador

Recibido(12/05/2022), Aceptado(05/06/2022)

Resumen.-En este artículo se presenta una revisión bibliográfica que aborda el aspecto de la ciber seguridad y ciber defensa en países de Latinoamérica, se destaca el gran alcance que poseen en la actualidad los ciber ataques, las acciones que han tomado los gobiernos de naciones y las perspectivas futuras para mejorar la ciber seguridad en los países de América Latina. Este trabajo parte de una revisión sistemática de artículos relacionados con aspectos en Ciberseguridad y Ciberdefensa que se han obtenido de bases especializadas en avances de la informática y desarrollos de carácter militar. Se concluye que la gran brecha tecnológica presentada en los países de América Latina respecto de otros países de América del Norte y Europa, es un factor de alta importancia y que debe reducirse de manera urgente para evitar la exposición y riesgos de la integridad de las nacionesy sus intereses.

Palabras clave: ciberseguridad, ciberdefensa, America Latina

Latin American cybersecurity and cyber defense perspectives

Abstract.- This article presents a bibliographical review dealing with the aspect of cyber security and cyber defence in Latin American countries. It highlights the large scale that cyber-attacks currently have, the measures taken by the governments of the countries and the future prospects for improving cyber security in Latin American countries. This work is based on a systematic reviewof articles on aspects of cyber securityand cyber defence drawn from specialised databases on computer advances and military developments. It is concluded that the large technological gap of Latin American countries compared to other countries in North America and Europe is an important factor and must be urgently reduced to avoid compromising the integrity of nations and their interests

Keywords: cybersecurity,cyber defense, Latin America

.

I. INTRODUCCIÓN.

La Ciberseguridad hace referencia al gobierno, desarrollo, gestión y uso de herramientas y técnicas de seguridad de la información. Los componentes de la Ciberseguridad según su abordaje se presentan en la figura 1.

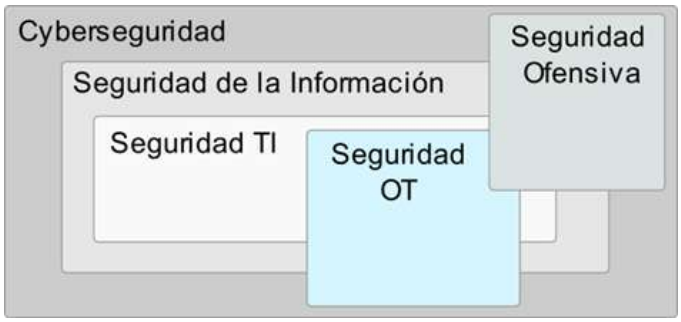

Fig. 1. Ámbitos de acción de la Ciberseguridad

La seguridad cibernética o ciberseguridad ha ganado más importancia a medida que aumentan la cantidad de ataques cibernéticos y la poblaciónemplea cada vez más dispositivos conectados a internet [1] . Las organizaciones a menudo se sienten confundidas sobre cómo administrar las actualizaciones tecnológicas y sus implicaciones con la seguridadcibernética. Debido a lo mencionado, varias organizaciones se han centrado en proteger de forma proactiva sus datos de diversos riesgos de tipo informático. Los especialistas en seguridad cibernética utilizan encriptación de grado militar para crear una plataforma impenetrable para los clientes, emplean múltiples capas de protección, servicios de autenticación y pruebas de verificación de identidad que protegen los sistemas contracualquier ataque. La seguridad de la información es la protección del flujo de información en toda una organización. Se puede hacer tanto de forma interna como externa, y ofrecen muchos beneficios, como la prevención de infracciones o ataques, la protección de datos y la identificación de la causaraíz de las fallas [1].

La seguridad en tecnologías informáticas TI, protegen la integridad de las tecnologías de la información evitando daños en ataques a sistemas informáticos, redes y datos. Las tecnologías de seguridad OT permiten cambiarlos procesos físicosa través del monitoreo y administración de dispositivos adaptándose a cada sector en el que operan. La seguridad ofensivaevita los ataquesinformáticos contraatacando con técnicas que emplean Inteligencia Artificial IA mediante lo cual en algunos casos se adelantan a las acciones de los atacantes brindadouna seguridad más avanzada, similara la humana [2]. Los humanosusan el conocimiento previo de cómo los usuarios pueden atacar un sitio web o una red y crean una estrategia o algoritmo que se puede implementar con éxito, a pesar de ello, el malware se encuentra en constante evoluciónrepresentando amenazas que conducen a la detección de falsos negativos y amenazas peligrosas que pasan por alto las estrategias defensivas. El ciberdelito siempre ha sido un problema para las empresas, pero hay evidencia de que ha tenidoefectos significativamente peoresen 2019. Las organizaciones internacionales ya han invertidoy seguirán haciéndolo en busca de recursos que son impulsados por inteligencia artificial (IA).

Se ha evidenciado un incremento del 700 % en los ataques a dispositivos que emplean internet(Internet of Things, IoT) en los últimos años. Es difícil entender qué impide que un dispositivo IoT vulnerable sea hackeado y absorbido por una red de bots [3]. Para mantenerse seguro, IBM recomienda medidas de seguridad integrales, como la gestión de políticas, la exploración técnicade las necesidades de supervisión y generación de informes, que ayudan a prevenir amenazas potenciales y automatizan la detección de anomalías para un mejor rendimiento. La seguridad de las tecnologías operativas es una preocupación cada vez mayor,especialmente cuando se operan múltiples maquinarias conectadas a la red como es el caso de automóviles con modos de piloto automático, aviones con WiFi en vuelo, computadoras portátiles y dispositivos que brindan formas convenientes para la filtración de datos, así como la información personalde

las personas. La ciberseguridad a nivel empresarial también cobra importancia debido al carácter de la información que manejan,por ello defender la información resulta ser un aspecto de alta prioridad.

El concepto IoT se ha encontrado en más y más dispositivos, y se están volviendo más inteligentes gracias a la IA. Las máquinas están conectadas entre sí con la capacidad de comunicar información en cualquier momento [4]. Sin embargo, los vehículos aéreos tienen un sistema de seguridad más débil que carecede protocolos de comunicación integrados, lo que los hace inseguros para IoT. Esta tecnología aún es nueva, pero ahora está siendo utilizada por EE. UU., Rusia, China y Corea del Norte, tanto con fines militares como comerciales.

Se ha identificado un sofisticado ataque psicológico descubierto recientemente en las conversaciones de usuarios humanos desprevenidos, los investigadores expusieron de forma anónima a grupos de personas a declaraciones repetidas que diferían solo, en una palabra. Se descubrió que los participantes terminaron ajustando su cambio de idioma de manera esperaday medible" como resultado de la presiónimpuesta [4]. Este estudio demuestra exactamente cómo las líneas maliciosas pueden generar miedo en los humanos a través de pequeñas manipulaciones: lo que pretendían ser elecciones inocuas pueden llevar a algunos usuariospor caminos que los hacen sentirviolados, dañados y acorralados.

Cuando hay un ataque cibernético en el sistemade energía, no se limita a una determinada computadora o estación de energía, sino que todo el sistemaestará bajo ataque.Las infracciones puedenocurrir de varias maneras, ya sea cuando una persona interna almacena las credenciales de inicio de sesión o utiliza un método de phishing para interceptar mensajesque contienen credenciales de inicio de sesión detalladas. Estos piratas informáticos nonecesitan ser expertosen habilidades tecnológicas avanzadas o representar amenazas sofisticadas, pero solo un motor de búsqueda en línea y su caché pueden resultar beneficiosos para este tipo de robo.Lo que es más, los piratas informáticos no tienen que robar información personal del cliente para su beneficio lo que hace que el delitosea más insidioso porque no pueden identificar a la víctima final.

Se han presentado casos en los que los ciber atacantes han afectado los sistemas de navegación dejandovulnerables los datos que rastreaban la posición de navíos, con ello han evitado que los capitanes de los barcos no conozcan el paradero de sus tripulaciones tornando innavegable el barco debido a la carencia de ayuda externa. Dentro de estas horas posteriores al ataque cibernético, el precio del crudo se incrementó considerablemente para el usuario final. El ataque condujo a la decisión de una importante compañía naviera de cerrar indefinidamente varios puertos, donde también quedaron varadas decenas de miles de millones de dólares en envíosde energía [5].

Se han observado varios casos de consecuencias de la piratería en los teléfonos inteligentes desde el año 2014 en el cual se comenzó a cobrar rescate para desbloquear teléfonos o PCs. De la misma manera los ciberataques pueden hacerse con el control de los coches autónomos y provocar accidentes. En los casos recientes, pilares de la industria mundial como Industro, Drone Racer Tech y Midwest Utilizer Company han sido víctimasde ciberataques. Las industrias son sistemas complejosque involucran muchos componentes interconectados y requieren una conectividad continua con sus socios comerciales para operar de manera efectiva [4]. El presente trabajo presenta múltiples enfoques, casos y acciones que se han efectuado en países de América Latina para promover en sus habitantes, instituciones, organizaciones y entidades nacionales, acciones que fortalezcan su ciber seguridad en vista de los alcances y afectaciones a la integridad de la sociedad que es cada vez mayor como consecuencia de los ciber ataques.

III. DESARROLLO

La creciente complejidad de la tecnología ha venido acompañada de un gran aumento en el número y la gravedad de las amenazas a la seguridad cibernética. Hace aproximadamente 10 años en Iran, se tuvo el caso de un gusano informático denominado Stuxnet el mismo que penetró en un laboratorio iraní y posteriormente se extendió a todo el mundo. El evento que comenzó en Irán hizo reflexionar al mundo sobre la vulnerabilidad de los sistemas de defensa y de cómo actos de este tipo pueden hacer colapsar ciudadesenteras, economías e incluso sistemas de red que nos mantienen a todos con vida.

A. Ciber Ataque en América Latina.

América Latina es actualmente la tercera región más afectada del mundo alcanzando los 84 millones de ciberataques según un informe de Kaspersky Lab. La mejor manera en que los países latinoamericanos pueden combatirestos ataques es actualizando las campañas de concientización y trayendo más proveedores de ciberseguridad a la región. América Central y América del Sur tienen muchas iniciativas nuevas enfocadasen el cambio, pero necesitan un apoyo continuopara lograr la transformación que tanto necesitan [6]. América Latina tiene la tasa más alta del mundo de ciber espionaje. Esta región trae consigo una grancantidad de nuevas oportunidades, pero también tiene algunos riesgos de los que todavía no puede defenderse, especialmente cuando se trata de ciberseguridad.

Las regiones que conforman América Latina poseen las áreas más ricas en recursos como también las zonas más pobres, los problemas de carácter económico dificultan obtener la cooperación necesariapara la sostenibilidad financiera en la ejecución de proyectos de ciberdefensa y otros tipos de proyectos. Los países ricos de América Latina tienen los recursos para financiar programas, pero no necesariamente tienen la motivación y la eficacia para ayudar a los países más pobres. Hay desafíos que los países latinoamericanos tratan de enfrentar sin éxito porque la pobreza impide cualquier tipo de avance y desarrollo sostenible a largo plazo. América Latina enfrenta tres desafíos en torno a la sostenibilidad y la prosperidad: necesidad de cooperación internacional, altos costos eléctricos, bajos estándares educativos. Estos desafíos se combinan y se exacerban entre sí, lo que hace que AméricaLatina logre con dificultad el progreso económico más allá del trabajo de nivel cercano a la pobreza para instituir una de las necesidades básicas que necesita sus habitantes [7].

América Latina está presenciando un crecimiento alarmante de los incidentes de fraude cibernético, siendo esta región calificada como la más propensa al fraude a escala mundial. La lentitud económica, la falta de servicios básicos(como atención médicao agua potable) o la incapacidad para crear instituciones confiables están aumentando la vulnerabilidad de las personasy aumentan sus probabilidades de vulnerabilidad al ciberdelito. El sistema financiero latinoamericano está en riesgo de ataques y de robo cibernético, a pesar de esto, existen países de América Latinaque aún no han tomadoconciencia de la gravedad del riesgo cibernético en su sector. Hay muchos factores importantes como el PIB y el nivel de desarrollo, los cuales son susceptibles a los efectos de los riesgos cibernéticos. Muchos de los países de América Latina han ampliado las lealtades a través de fronteras escasamente separadas y una diversidad de diferentes culturas e idiomas con un amplio acceso a la tecnología y por tanto a mayores riesgos cibernéticos. Un estudiode 2017 realizado por el Banco de Pagos Internacionales encontró que se realizan más de dos mil millones de transferencias bancarias todos los días,10 veces más que antes del año 1998 [7].

Un ataque cibernético en varios países de América Latina en abril del año 2019 dejó perplejos a los expertos. Se presentaron interrupciones en las telecomunicaciones, los servicios de GPS, Internet, los sistemas financieros y el sector agrícola. América Latina ha sido durante mucho tiempo un objetivo interesante para los ataques cibernéticos. Las corporaciones argentinas fueron objeto de ataques de enjambres de piratas

informáticos en 2012. Existen informes que sugieren que este hecho fue precedido por otros dos incidentes de piratería durante el año en los que se utilizaron bases de datos específicas para recopilar las credenciales de los empleados del gobierno y el uso de botnetspara lanzar DDoS. El Pentágono ha tratando de explicar el ataque cibernético que golpeó los sistemas militares en AméricaLatina que presuntamente podría haber sido causado por atacantes de Rusia o China. No se ha sido reclamado oficialmente a ninguno de esos estados pero supuestamente se ha comentado que estaban insertando un servidor ilícito y desestabilizando las redes desplegadas. Los delincuentes informáticos procuran la eliminación de datos de las reden LAN y de esta manera han obtenido información personal confidencial representando un grave problema. La tasa de ataques cibernéticos de América Latinaes la segunda más alta del mundo,con un 30 % de todas las empresas orientadas a Internet que son atacadas por piratas informáticos cada año, según NQ Computer Services. Impulsar las exportaciones de TI de Latinoamérica ha sido una parte clave del plannacional de desarrollo de países como Chile y Brasil [8].

Según Verizone Business Solutions, el 90 % de las empresas latinoamericanas no están haciendo lo suficiente para mantenerse a salvo de los ataques cibernéticos, lo que se atribuye en gran parte a la falta de especialistas en TI calificados en América Latina (esto a pesar de que el 21 % de ellas sufre un ataque dirigido conocido). Los datos revelan que el 60% en toda América Latina no protege los datos de contraseña con encriptaciones y solo el 49% usa software antivirus. Colombia es uno de los países de América Latina que ha sido bloqueado por un hackeo masivo. Se han bloqueado algunos de estos ataques, sin embargo, los atacantes provienen de todo el mundo y, por lo general, se disfrazan a través de proxies y servicios de anonimato enmascarando sus huellas y dificultando que los profesionales de seguridad los rastreen e identifiquen. Los ciberataques van en aumento en Perú, según 714 profesionales de TI que trabajan en más de 781empresas, casi la mitad de las organizaciones han sufrido ataques cibernéticos en los últimos 12 meses. Curiosamente, más de un tercio de estas organizaciones dijeron que fueronpirateadas por competidores [9]. Argentina es una bomba de tiempo de vulnerabilidades de seguridad informática. El sistema de vigilancia no está a la altura y el sistema judicial no cuenta con las herramientas adecuadas para su protección. Muchos ciberataques que ocurren en Argentina no son detectados por firewalls u otros sistemas de protección cibernética. Según Ciberdefensa, un Centro de Investigación de Seguridad en Buenos Aires, el 94 % de las empresasque fueron víctimasde un ataque y luego respondieron a una consultaidentificaron al menos una vulnerabilidad en su red antes de ser atacadas. Estas fallas en seguridad frustran a ciudadanos y empresarios que cada vez demandan más respuestas de funcionarios clave en materia de ciberseguridad, abordandopreocupaciones fundamentales sobre privacidad, infraestructura y crecimiento económico debido al complicado perfil de este país que lo convierteen un buen objetivo para los ciberhackers.

El ataque electrónico a gran escala perpetrado contraVenezuela el 17 de mayo de 2019 cortó la conexión a Internet del país durante treinta y cinco horas. A partir del colapso el liderazgo de Venezuela culpó a gobierno de los Estados Unidos, específicamente al Comando Cibernético de los EE. UU. y la Agencia de SeguridadNacional (NSA), cuyas organizaciones negaronsu participación en estos eventos [10]. En 2016, recientes ataques cibernéticos en Brasil provocaron el incumplimiento de cuentas bancarias militares. Una brecha de seguridad de esta magnitud no debería ocurrir en un sistema actualizado como el Banco Militar BR. El Ministerio Público de Brasil durante las investigaciones dijo que estos casos no fueron causados por terceros sino por un virus maliciosoque se lanzó en sistemasmilitares anteriores. El secretario de Defensa, Nelson Jobai, afirmó que los múltiples ataques cibernéticos son calculados y presuntamente tenían un objetivo más amplio que obtener ventajas individuales específicas de clientes institucionales únicos. La sospecha es que existe algún vínculo con personas externas. Brasil ha otorgado a su Consejo de Seguridad brasileño la responsabilidad de coordinar las respuestas contra los ataques cibernéticos y se ha informado que las comunicaciones de los centros dentro de Argentina, Malta y Ucraniaapoyan a Brasilen sus esfuerzos para combatir los ataques cibernéticos de esta gravedad[10].

B.La Ciberseguridad en América Latina

Internet y un mundo sin desconexión es una aspiración de muchos países latinoamericanos, sin embargo, el problema radica en que América Latina tiene la menor protección de datos en comparación con otros países del mundo siendo propensos a los ataques cibernéticos ya que casi el 100% de los canales de comunicación satelitalestán abiertos y disponibles. Introducir la seguridadcibernética en América Latina comienza por movilizar nuevas tecnologías como si fueran escudos contra las vulnerabilidades humanas (Fig. 2)

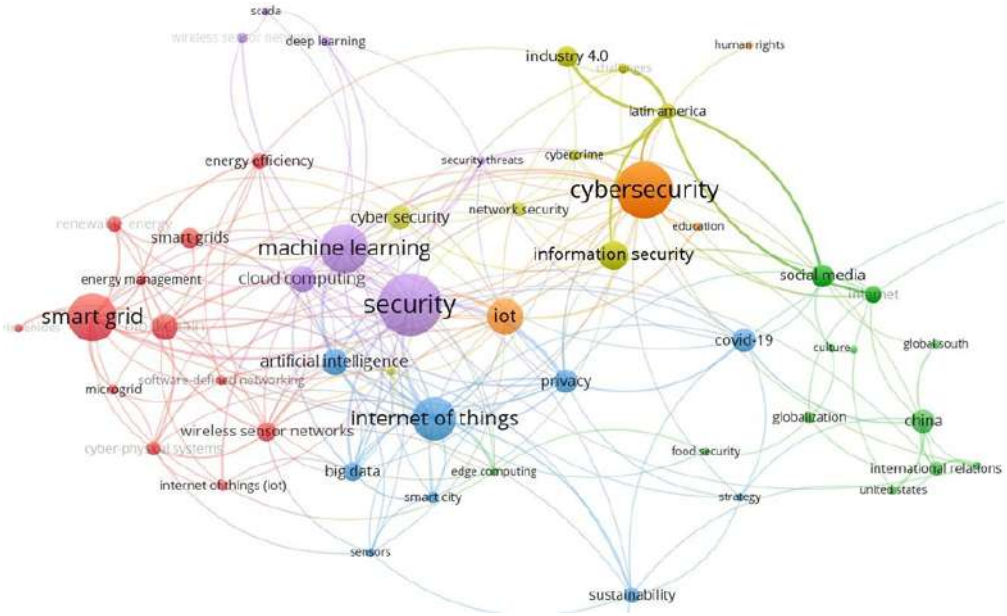

Fig2. Vista Bibliométrica de Estudios relacionados con Ciberseguridad en Latinoamérica

La representación de la figura 2, evidencia la escasa investigación bibliográfica en torno a la ciberseguridad en Latinoamérica presentándose un mayor número de estudios sobre aspectos de educación, cibercrimen, seguridad de la información. Por otra parte la mayoría de los artículoscientíficos se centranen los avances tecnológicos que son implementados y desarrollados a diariopor países desarrollados.

Se han establecido cinco niveles de madurez en aspectos de la seguridad cibernética, las naciones que recién comienzan en ello se consideran de nivel inicial,a cuyo nivel pertenecen 26 países de un total de 32. Los siguientes países están en un nivel intermedio, pero lejos de Corea o Estados Unidos: Argentina, Brasil, Chile, Colombia, México y Uruguay. Existen empresas brasileñas líderes en este campo de la ciber seguridad. A nivel Global, la mitad de los países del mundo no tienen una estrategia de respuesta coordinada a los incidentes de seguridad informática, lo que significa que no pueden reaccionar ante el ciberdelito y otros ataques. Dos de cadatres países tampoco tienen centros de comando de seguridad cibernética [11]. La agencia de seguridad cibernética de Perú analizarcualquier riesgo para la seguridadcibernética nacional y protege el ciberespacio de los delincuentes, piratas informáticos e insurgentes. Las alianzas con universidades dan soporte en capacitación a esta agencia con la participación de especialistas jubiladospara su retencióny para que aporten sus conocimientos sobre la soberanía digital de un país, lo cual es una importante apuesta del Perú para crear derecho a través de las tecnologías en consonancia con los posibles daños que se nos vienen encima a las sociedades digitalizadas que están apareciendo en todo el mundo.

El gobierno argentino está buscando intensamente identificar los nodos débiles en la seguridad cibernética del país y las mejores metodologías para cumplir con sus objetivos de incrementar su ciber seguridad. Se han propuestocampañas que tienen como objetivopromover la concienciación sobre seguridadde las cuentas en las redes socialesy otros consejosde seguridad [8].

El actual gobierno colombiano ha tomado una posición sobre la importancia de integrar la ciberseguridad en la cultura de su país, fomentando empresas que logran avances tecnológicos y brindan a los jóvenes las habilidades necesarias para proteger la red digital de Colombia, que el gobierno cree que debería ser más segura que las de EE. UU. o el Reino Unido. El Ministerio de Educación entregó a las escuelas materialeducativo para estudiantes de 12 años en adelantesobre ciberseguridad, para se ha incorporado en la currícula escolar de Colombia desde los primeros nivelesde educación [12]. En Chile se busca fortalecer su ciberseguridad con el uso de tecnologías más avanzadas, como el uso de datos biométricos, detalles de texto y contraseñas. En este país se ha comenzado a implementar medidasdestinadas a fortalecer la seguridad, con la biometríacomo las soluciones más populares. Actualmente 4 de cada 10 chilenosutilizan algún tipo de identificación biométrica para acceder a su cuenta bancaria y realizar compras.

Nicaragua ha adquiridoinfraestructura para las tecnologías de la información y las comunicaciones que permiten un flujo adecuado de recursos generados localmente y en el exterior hacia la inversión en el desarrollo nacional. Con avancesen infraestructura e innovaciones en diversos sectores, los nicaragüenses tienen acceso a mejores sistemas de controlque mantienen la seguridad y discreción patriótica. Hay varios países en América Latina que tienen baja ciberseguridad. Venezuela encabeza esta lista seguida por República Dominicana, Argentina y México [9]. Con una actividadcriminal desenfrenada y los problemasactuales del entornosocial en la forma de vida, Venezuelaha exhibido una vulnerabilidad significativa para los piratasinformáticos que quierenejecutar sus operaciones en Venezuela sin ser detectados.

Hay varios países en América Latina que tienen baja ciberseguridad. Venezuela encabeza esta lista seguida por República Dominicana, Argentina y México [9]. Con una actividadcriminal desenfrenada y los problemasactuales del entornosocial en la forma de vida, Venezuelaha exhibido una vulnerabilidad significativa para los piratasinformáticos que quierenejecutar sus operaciones en Venezuela sin ser detectados. Las autoridades panameñas, la Secretaría General de Gobierno y los Servicios Nacionales de Protección, han avanzado recientemente en su ciberseguridad y han adoptado las últimas tecnologías disponibles para contrarrestar las amenazas de hacking. El sistema incluyefuncionalidades como un “Sistema de Alerta Permanente” que tiene como objetivo garantizar un “monitoreo y diagnóstico continuoen todo momento con algunosestándares internacionales que protegen los datos personales” a través de un software de vigilancia. Además, se está planificando un “Marco de Arquitectura de Ciberseguridad para la ImagenFutura de la Administración PúblicaPanameña”.

Bolivia es el primer país del mundoque mejoró sus estándares de ciberseguridad en materia de TICs. La tasa de alfabetización en Internet supera el 100% y existe un alto nivel de compromiso en la lucha contra el ciberdelito. La Ley de Ciberseguridad de Bolivia, la primera en América Latina,fue creada para proteger al país del ciberdelito y es la columna vertebralde los esfuerzos coordinados para eliminar los riesgos de ciberseguridad. La ley nacional también considera una reafirmación de los compromisos internacionales adquiridos por Bolivia. Brasil ha mejorado su seguridad cibernética con la introducción de la tecnología blockchain en los últimos años. Blockchain es una forma innovadora de reforzar la seguridad. La tecnología funciona descentralizando una base de datos de información y almacenándola en muchas computadoras, en lugar de almacenar datos en un lugar centralizado en un mainframe o servidor.

La iniciativa de Costa Rica de mejorar su seguridad cibernética es una decisión importante e intuitiva, teniendoen cuenta su presencia como un país basado en la información. En Costa Rica se ha logrado avances sustanciales en la mejora de su seguridad cibernética al hacer un mejor uso de las prácticasde encriptación. La importancia continuade estos esfuerzosde seguridad se está volviendo internamente más visible no solo a nivel nacional sino también dentro de la vida cotidiana de la sociedad [13]. El gobierno de Cuba ha invertido en mejorar su seguridad cibernética para lo cual protege su infraestructura de Internet y evita la intromisión de ataques en sus canales de comunicación, desplegando tecnologías 4G para mejorar su conectividad digital, su proyecto inició en 2013 y se denominó Programa de Infraestructura de Ciberseguridad (PCI). En la actualidad de usan sistemas biométricos y capacidades de cifrado de datos y se han actualizado muchos de sus sistemas críticos para protegerse contra posibles ataques.

Las autoridades de República Dominicana han aumentado su seguridad cibernética luego de la interrupción de sus sistemasde emergencia a principios del año 2018, luego de lo cual,se tomó la decisión de mejorar la seguridad cibernética. República Dominicana ha mejorado su ciber seguridad gracias a la creaciónde tres centros de ciberseguridad: El Centro Nacionalde Ciberdefensa, El eCrime Center (Centro para la Seguridad en la Red) y Los Centros Tecnológicos Estratégicos [14]. En el Salvador se ha mejorado la seguridad cibernética con la ayuda de tecnologías como algoritmos de aprendizaje automático, biometría, servicios en la nube y blockchain que se han implementado. Con estas herramientas trabajando juntas, no solo se provee de una mayor seguridad, sino incluso una mejorseguridad general de la integridad de la infraestructura. Guatemala es uno de los primeros países en crear una fuerza de policía cibernética en 2010. En la actualidad, más de la mitad de sus fuerzas del orden han recibido capacitación especializada en piratería y lucha contra el delito cibernético. Se ha implementado el software Cybersecurity EDEN de Europolque registra las firmas de ataque de datos de código malicioso permitiéndoles escanear e identificar dispositivos de alto riesgo antesde que ocurra un ataquepara evitar dañoso pérdidas de datos.

México ha actuado de manera más dedicada en su intento de mejorar la ciber seguridad, han dado un paso para asegurar sus fronteras y mejorar el nivel de seguridad cibernética con su población. En los últimosaños, varios legisladores de seguridad cibernética se han asegurado de brindarles a los piratas informáticos menos oportunidades para perjudicar la presencia en línea de los habitantes. México está contribuyendo a ese esfuerzo mediante la implementación de nuevos proyectos de ley que establecen que todos los ciudadanos estarán obligados por ley a realizar ciertas actualizaciones en las redes sociales y también es obligatorio para futuros clientes/usuarios [14]. Paraguay ha lanzadoel programa Portal Web para que ciudadanos y empresas cuiden la seguridad de sus datos. Paraguay ha sido reconocido como uno de los países más seguros del mundo para navegar por Internet durante muchos años, ubicándose en segundo lugar después de los Emiratos Árabes Unidos. Se ha difundidouna campaña que brinda consejose instrucciones útiles sobre cómo evitar el delito cibernético, mantenerse seguro en las redes sociales, qué hacer si alguien es pirateado, cómo proteger una cuenta de correo electrónico: descubrirquién está detrás de este programa.

C.*El Futurode la Ciber Seguridad en América Latina*

En el futuro de América Latina, la ciberseguridad dará un giro muy complejo. La región se transformará gradualmente para responder a los desafíos que se hicieron evidentes con el surgimiento de lo que se denomina“ciberespacio”. El ciberespacio prometía nuevas oportunidades, pero también nuevos peligros. Hacia este futuro, la prevención y la preparación son factores clave. os países de América Latina en este momento utilizan diferentes estrategias y tecnologías para llevar a cabo la ciberdefensa. En particular, esta región se apoya en un pequeño número de países que producen productos de seguridad cibernética: algunos aliados militares como Rusia o Israel y en otros casos China. La discusión sobre esta nueva amenaza para América Latina nunca se materializará hasta que investiguemos cómo cambiará la ciberdefensa en este entorno cambiante. En la actualidad, algunos estudios han proyectado lo que podría suceder en el futuro de la ciberdefensa internacional y presentaron tres escenarios diferentes: Cooperación y alianzas regionales, Desarrollo de capacidades entre instituciones autosostenibles, Inversión recurrente en sistema de investigación, desarrollo e innovación. América Latina, como muchas otras regiones del mundo, se está quedando peligrosamente rezagada en materia de ciberseguridad global.Cuando piensas en América Latina,puede que no sea uno de los países que te viene a la mente cuando piensas en las altas tasas de ciberdelincuencia, pero en realidad, está clasificado como uno de los más bajos de su región en términos de seguridad. Es probable que los ataquesde ciberware se vuelvan más sofisticados y, en este caso, serán muy difíciles de prevenir. Con anticipación, las fuerzas militares de la región Latinoamericana han estado tomando medidaspara desarrollar su capacidad para enfrentar esta amenaza y fortalecer su posición de negociación con respecto a su propia soberanía de datos. Las fuerzas militaresde la región han estadotomando medidas para desarrollar su capacidad para enfrentar esta amenaza y fortalecer su posición de negociación con respecto a su propia soberanía de datos [15].

A medida que la digitalización avanza más rápido que en cualquier otra área, la necesidad de ciberseguridad se vuelve más apremiante. El énfasis dado por las fuerzas militareslatinoamericanas a travésde conferencias, feriase iniciativas de otros países es un buen augurio para el manejo transparente de datos que provocan estas tendencias. Estos hechos hacen que muchos latinoamericanos quieranapreciar lo que IA tiene para ofrecery cómo puede protegerlos mejor a ellos y a los datos de su empresa. La IA permitirá a los latinoamericanos acceder a niveles de protección sin precedentes que habríansido imposibles sin ella.

En Ecuador de acuerdo a su Política Nacional de Ciberseguridad publicada 2021 se conoce esteescenario como el quinto dominio convirtiéndose en tema de seguridad del estado. En orden general Nro. 071 de fecha 11 de mayo de 2021 el Ministerio de Defensa Nacional de Ecuador acuerda expedir la política de ciberdefensa para el sector Militar con niveles político-estratégico, estratégico-militar y operacional. En el nivel operacional el General de Brigada Henry Delgado Presidente del Comité del Arma de Comunicaciones en la parte directiva aprueba iniciativas y proyectos como generación de doctrina y capacitación en ciberdefensa [1].

III. METODOLOGÍA

En la figura 3, se aprecia la búsqueda realizada en bases de artículos científicos de las que pudieron obtenerse 67 documentos que luego del proceso de revisión, y elegibilidad, se consideraron 14 para realizar este documento.

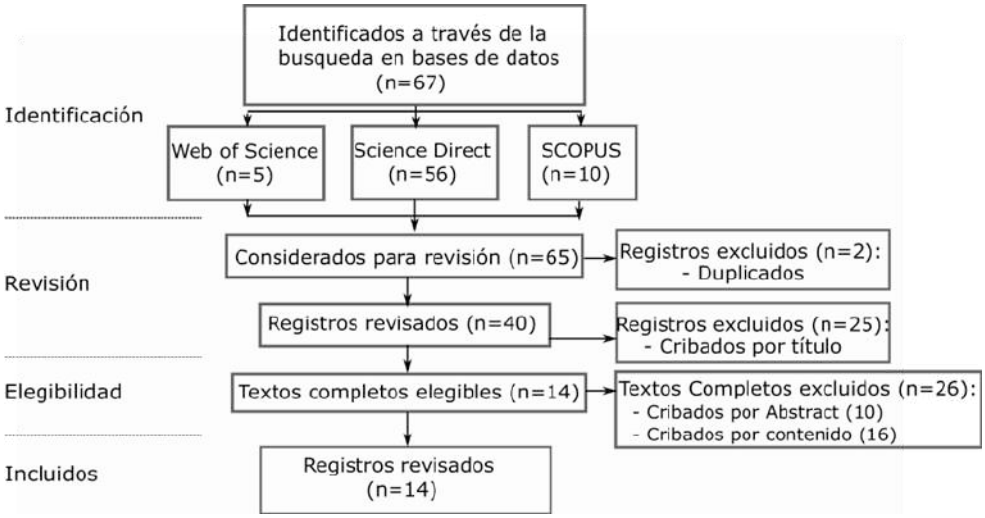

Fig 3. Esquema del proceso de revisión sistemática realizado

No existe una legislación adecuada para las nuevas tecnologías en varios países de América Latina, razón por la cual, se reducen las oportunidades de implementar tecnología más innovadora que les ayude a muchos países a defenderse de los ciberataques. La situación actual de la seguridad cibernética en América Latina ha creado un entorno donde las empresas y las personas se han incentivado con ganancias económicas y han aprovechado las brechas técnicas para delinquir o interrumpir servicios y recursos apuntando a instituciones gubernamentales o privadas con impactos en algunas ocasiones duraderos. Se destacan dos problemas principales para introducir y mejorar la seguridad cibernética en los países latinoamericanos: la falta de conciencia y la falta de iniciativa. La banca, los servicios públicos y los sistemas de control de carácter militar han sido los mas afectados en los países latinoamericanos, presentándose algunos colapsos de horas debido a ataques cibernéticos. América Latina alberga algunos países tecnológicamente muy avanzados, pero también hay países que tienen implementaciones mínimas de seguridad cibernética debido a sus bajos límites presupuestarios. Se ha afirmado que los riesgos cibernéticos globales y potenciales para las corporaciones aún no son nada comparados con el caos que los piratas informáticos podrían causar al hundir a los gobiernos latinos.

Hay muchas obstrucciones para establecer medidaseficientes, incluida la falta de conocimiento tecnológico adecuado, un alto costo de la tecnología, falta de recursosfinancieros para implementar programas, vandalismo o accidentes debido a implementaciones ineficaces. América Latina enfrenta un desafío sustancial en el sentido de que debe competir con piratas informáticos que están muy avanzados y mejoran continuamente sus habilidades para operar por delante de las medidas de seguridad locales, lo que los ha llevado a tomar medidas más cautelosas y seguir regulaciones más estrictas. América Latina es una región atractiva para los ciber atacantes. Las organizaciones de esta regiónse enfrentan a más riesgosque las empresas europeas y norteamericanas, ya que los ciberdelincuentes suelen identificar y aprovechar las oportunidades y vulnerabilidades de la escasezde seguridad cibernética que agobia a países latinoamericanos. Actualmente, se utilizan muchas soluciones de seguridad en la región: firewalls administrados, protección DDoS, administración de vulnerabilidades, pero estas soluciones brindan cierto nivel de cobertura limitada, por tanto, se requiere una estrategia de seguridad integral. Ya algunos países como Brasil, Colombiay México han ido avanzandoen el área de ciberseguridad estableciendo acciones que les permiten reducir las intrusiones cibernéticas.

La Presidencia de la República de Brasil lanzó su "Plan de Transformación Digital Segura", con características tales como más campañas de concientización, más proyectos de I + D y en colaboración de socios gubernamentales. En Colombia se aprobó una nueva ley destinada a mejorarla ciberseguridad en el país a través de la promoción de la cooperación bilateral y el aumento de los servicios tecnológicos en el extranjero. México ha creado una Estrategia Nacional de Seguridad Cibernética en 2017 centradaen el desarrollo tecnológico relevante.

CONCLUSIONES

La seguridad cibernética ha cambiado y evolucionado enormemente en los últimosaños. Si bien no hay un país sin infraestructura técnica que esté expuesto a amenazas cibernéticas potenciales, al mismo tiempo hay tendencias florecientes y esfuerzos globales que intentan aumentar la capacidad de los países de América Latina para protegerse contra las amenazas cibernéticas.

Se concluye que la seguridad cibernética en América Latina aún tiene muchas desventajas respecto de países desarrollados, se requiere de mayor atencióne inversión de los gobiernos de estos países, no se deben ignorar estas vulnerabilidades ya que afectan a sus actividades económicas y a la calidad de vida. El creciente flujo de comercio e inversiones a través de las fronteras también requiere un pensamiento conjunto para asegurar la comunicación a nivel estatal y proporcionar estándares rigurosos para los proveedores que brindan servicios críticos a las redes nacionales de computadoras interconectadas, lo que hasta ahora se ha señalado como iniciativas de la mayor parte de los países de la región.

REFERENCIAS

[1] L.-C. Herrera y O. Maennel,«A comprehensive instrument for identifying criticalinformation infrastructure services», Int. J. Crit. Infrastruct. Prot., vol. 25, pp. 50-61, jun. 2019, doi:https://doi.org/10.1016/j.ijcip.2019.02.001.
[2] Z. Bauman et al.,«After Snowden: Rethinking the Impact of Surveillance», Int. Polit. Sociol., vol. 8, n.o 2, pp. 121-144, jun. 2014, doi: 10.1111/ips.12048.
[3] J. Aguilar-Antonio, «Cyber-physical Facts: A Proposed Analysis for Cyber Threats in the National Cybersecurity Strategies», URVIO-Rev. Latinoam. Estud. Segur., n.o 25, pp. 24-40, dic. 2019,doi: 10.17141/urvio.25.2019.4007.
[4] G. L. E. M. Toapanta S.M.T. Jaramillo J. M. E., «Cybersecurity analysis to determine the impact on the social area in Latin Americaand the caribbean», ene. 2019, doi: 10.1145/3375900.3375911.
[5] M. J. O'Grady,D. Langton, y G. M. P. O'Hare,«Edge computing: A tractable model for smartagriculture?», Artif. Intell. Agric., vol. 3, pp. 42-51, sep. 2019, doi: https://doi.org/10.1016/j.aiia.2019.12.001.

[6] I. A. Valdovinos, J. A. Pérez-Díaz, K.-K. R. Choo, y J. F. Botero, «Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions», J. Netw. Comput. Appl., vol. 187, p. 103093, ago. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103093.
[7] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, y J. Szymanski, «Modelling the malwarepropagation in mobile computer devices», Comput. Secur., vol. 79, pp. 80-93, nov. 2018, doi: https://doi.org/10.1016/j.cose.2018.08.004.
[8] T. B, «OAS report examines cybersecurity trends in the Americas», vol. 92, n.o 8, ene. 2013.
[9] J. Antonio, «The Cyber Security Gap in Latin America Against the Global Context of Cyber Threats», Rev. Estud.EN Segur. Int.-RESI, vol. 6, n.o 2, pp. 17-43,2020, doi: 10.18847/1.12.2.
[10] A. Karale, «The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws», Internet Things, vol. 15, p. 100420, sep. 2021, doi: https://doi.org/10.1016/j.iot.2021.100420.
[11] A. Younesi, H. Shayeghi, Z. Wang, P. Siano, A. Mehrizi-Sani, y A. Safari, «Trends in modern power systems resilience: State-of-the-art review», Renew. Sustain. Energy Rev., vol. 162, p. 112397, jul. 2022, doi: https://doi.org/10.1016/j.rser.2022.112397.
[12] W. Xiong y R. Lagerström, «Threat modeling – A systematic literature review», Comput. Secur., vol. 84, pp. 53-69, jul. 2019, doi: https://doi.org/10.1016/j.cose.2019.03.010.
[13] Banco Interamericano de Desarrollo, «Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe», Banco interamericano de Desarrollo, jul. 2020. doi: 10.18235/0002513.
[14] L. Parraguez Kobek y E. Caldera, «Cyber Security and Habeas Data: The Latin American response to information security and data protection», OASIS, n.o 24, p. 109, nov. 2016, doi: 10.18601/16577558.n24.07.
[15] J. M. Aguilar Antonio, «Retos y oportunidades en materia de ciberseguridad de América Latina frente al contextoglobal de ciberamenazas a la seguridadnacional y políticaexterior», Estud. Int., vol. 53, n.o 198, p. 169, abr. 2021, doi: 10.5354/0719- 3769.2021.57067.

LOS AUTORES

Capitán de Comunicaciones Estefanía del Pilar Pavón Unda Ejército Ecuatoriano, Comandante de la Compañía de Comunicaciones Nro. 27 "PORTETE". eesteefania@hotmail.com. Licenciado en Ciencias Militares Escuela Militar Bernardo O Higgins (Chile). Diplomado en Historia Militar de América (Chile). Diplomado de la Guerra del Pacifico (Chile). Curso de Liderazgo (EEUU). Instructor de la Escuela de Comunicaciones - Escuela de Selva y Contrainsurgencia del Ejercito del Ecuador desde 2012-2015. CCNA CyberOps Associate Universidad San Francisco de Quito (Ecuador). Área de investigación: sistemas de comunicaciones militares, pedagogía, idiomas y recursos humanos

Teniente de Comunicaciones Guaytarilla Fernando Ejército Ecuatoriano. Comandante del pelotón de Comunicaciones del Batallón de Selva No. 62 "ZAMORA". guaytikfer@hotmail.com. Licenciado en Ciencias Militares Escuela Superior Militar Eloy Alfaro (Ecuador). Curso Cisco CCNA 1 Fundamentos de Networking para Redes IP, CCNA 2 Switching, Routing, and Wireless Essentials, CCNA 3 Redes Empresariales, Seguridad y Automatización, en la Universidad de FuerzasArmas UFA-ESPE, Maestríaen Ciberseguridad en la Universidad Internacional del Ecuador. Oficial de Seguridad de la información digital en el Batallón de Selva 62 "ZAMORA" desde 2021-2022. Áreas de Investigación: Tecnologías de la información y ciberseguridad.

Teniente de Comunicaciones Christian Cueva Ejército Ecuatoriano. Comandante del pelotón sistemas informáticos de la Compañía de Comunicaciones de la TerceraDivisión de Ejército"TARQUI". Chris.cueva.1993@icloud.com. Licenciado en Ciencias Militares Escuela Superior Militar Eloy Alfaro (Ecuador). Curso del Manejo de TIC aplicada a la educación en la Universidad Técnica Particular de Loja (Ecuador). Estudiante de ingeniería en Tecnologías de la Información en la Universidad Técnica Particular de Loja (Ecuador). Curso de operadores del sistema de mando y control del Comando Conjunto de Fuerzas Armadas (Ecuador). Curso fundamentos de ciberseguridad en la Academia CISCO de la Universidad Técnica Particular de Loja (Ecuador). Oficial de Seguridadde la información digital en la Tercera División de Ejército "TARQUI"desde 2020-2022. Áreas de Investigación: Tecnologías de la información y ciberseguridad.

Subteniente de Comunicaciones Karla Cinthya Durango Flores Ejército Ecuatoriano, Oficial de Seguridadde la Información de la Compañía de Comunicaciones Nro. 1 "El Oro". karlysdu_1603@hotmail.com. Licenciado en Ciencias Militares Escuela Militar "Eloy Alfaro" (Ecuador). Curso de operadores del sistema de mando y control del Comando Conjunto de Fuerzas Armadas (Ecuador). Áreas de Investigación: Tecnologías de la información y ciberseguridad.