Athenea

Revista en Ciencias de la Ingeniería

ISSN: 2737-6439
DOI: 10.47460/athenea
Volume 3, Issue 9
September 2022

Published by:

AutanaBooks
Engineering & Services

ATHENEA JOURNAL

JOURNAL IN ENGINEERING SCIENCES

Electronic Journal Edited By AutanaBooks.

Quarterly Periodicity

Our cover:

Engineering applications are glimpsed with a promising future, where scientific and technological developments come together to provide solutions to important problems of social life.

Volume 3 // Issue 9 // September 2022
DOI:10.47460/athenea
ISSN: 2737-6439

Viewing the Journal:
https://minerva.autanabooks.com/index.php/Minerva

TECHNICAL TEAM

Webmaster and Metadata
Ing. Ángel Lezama (Quito, Ecuador).
a2lezama@gmail.com

Graphic design and layout:
Adrián Hauser
(AutanaBooks, Ecuador).
adrian.hauser@gmail.com

Translator: Fausto Bartolotta
Via Francesco Crispi, 309/A
98028 Santa Teresa Di Riva, Provincia Messina
Italia
email: fbartolotta@gmail.com

"by the grace of God"

Publisher: Dr. Franyelit Suárez,
http://orcid.org/0000-0002-8763-5513
editorial@autanabooks.com
AutanaBooks, Quito, Ecuador

DIRECTORY OF THE ATHENEA
JOURNAL IN ENGINEERING SCIENCES

ACADEMIC COMMITTEE

Athenea Journal
Volume 3 // Issue 9 // September 2022
DOI:10.47460/athenea
ISSN: 2737-6439

Content

Editorial

Engineering has been participating actively in numerous professional areas, and the application of engineering in the development of new proposals that favor human life is increasingly necessary, from medical applications, to anti-seismic constructions, or robotic technologies for industry, as well as as developments that go unnoticed but have their foundations in engineering, such as satellite tracking, computer systems, and the many contributions to manufacturing and agriculture, to name a few.

In this way, engineering becomes the profession of the new times, and in this issue of Athenea Magazine, in Engineering Sciences, only those works that stand out for the significant contribution that engineering offers to the solution have been selected. of social problems.

Dra. Franyelit Suárez

ISSN-E: 2737-6439

Athenea Journal
Vol.3, Núm. 9, (pp. 7-14)

https://doi.org/10.47460/athenea.v3i9.41

Mecanismo de hinchamiento de óxido de hierro en procesos de metalización

Azócar Luis
https://orcid.org/0000-0002-7683-4488
azocarluisalberto@hotmail.com
UNEXPO, Vicerrectorado Puerto Ordaz
Puerto Ordaz-Venezuela

Dam Oscar
https://orcid.org/0000-0002-0594-6757
oscar.curmetals@gmail.com
UNEXPO, Vicerrectorado Puerto Ordaz
Puerto Ordaz-Venezuela

Recibido(11/11/2021), Aceptado(05/05/2022)

Resumen.-Se muestran los resultados de esfuerzos causados por la desorción de átomos de nitrógeno disueltos en defectos puntuales de las fases alotrópicas del hierro metálico obtenido mediante procesos de reducción en estado sólido. En las fases ferrita y austenita se calcularon las cantidades de nitrógeno disuelto y vacancias y se propuso la expansión del mecanismo superficial de adsorción del nitrógeno, con la absorción-desorción para determinar la cantidad de sus átomos y moléculas ajustadas al espacio de las vacancias ubicadas en el interior de las fases y obtener las presiones y esfuerzos generados por el gas confinado. Los valores calculados de los esfuerzos por la desorción de tres moléculas del nitrógeno en una vacancia de la red cristalina de la ferrita y austenita fueron 621,2 y 727,6 Kgf/mm2, y al compararse con los valores conocidos de sus resistencias a la tracción (rotura) de 28 y 105 Kgf/mm2, resultaron en 22 y 7 veces superiores respectivamente, favoreciendo su hinchamientoy agrietamiento catastrófico.

Palabras clave: Hinchamiento, nitrógeno, reducción, filamentos de hierro metálico

Mechanism of iron oxide swelling in metallization processes

Abstract.- The results of stresses caused by desorption of dissolved nitrogen atoms in point defects of allotropic phases of metallic iron obtained by solid state reduction processes are shown. In the ferrite and austenite phases, the amounts of dissolved nitrogen and vacuums were calculated and the expansion of the surface mechanism of nitrogen adsorption was proposed, with the absorption-desorption to determine the amount of its atoms and molecules adjusted to the space of the vacuums located inside the phases and to obtain the pressures and efforts generated by the confined gas. The calculated values of the efforts for the desorption of three molecules of nitrogen in a vacuum of the ferrite and austenite crystalline network were 621.2 and 727.6 Kgf/mm2, and when compared with the known values of their tensile strength (breakage) of 28 and 105 Kgf/mm2, they were 22 and 7 times higher respectively, favoring their swelling and catastrophic cracking.

Keywords: Swelling, nitrogen, reduction, whiskers.

I. Introducción.

El hinchamiento anormal de los óxidos de hierro bajo atmósfera reductora ha sido investigado desde el año 1963 cuando apareció en la industria del acero japonesa. El proceso de reducción es complejo por la cantidad de parámetros involucrados y que pueden tener efecto en el fenómeno de hinchamiento: Gases reductores como el monóxido de carbono (CO); hidrógeno (H2); mezclas reductor-oxidante (CO-CO2-COS), reductor-reductor-oxidante-inerte (CO-H2-CO2-N2) [1], en este caso el nitrógeno (N2) se utilizó como modificador de la presión parcial de los gases acompañantes. Cambios de fases del mineral de hierro: hematita (Fe2O3) -> magnetita (Fe3O4)-> wustita (FeO)-> hierro metálico (Fe°) en atmósfera 100% amoniaco (NH3) [2], además de las que ocurren en los óxidos que acompañan y/o se añaden para formar los aglomerados a reducir y sus efectos en el hinchamiento: CaO-SiO2, CaO-SiO2-Mg-Al2O3, dolomita (MgCO3-CaCO3), MnO2.

También se ha investigado la velocidad, la temperatura y el tiempo de reducción. Varios han sido los modelos propuestos para explicar el fenómeno, y en su gran mayoría se basan en la generación y crecimiento de hierro metálico en forma de hilos o fibras, llamados whiskers. En una alternativa divergente se propuso al nitrógeno como causa fundamental para explicar el hinchamiento anormal [3], y en [4] se resaltó la propuesta, sin embargo hasta la fecha no se ha realizado investigación alguna para considerarla y quizá porque se considere como un gas inerte. En este artículo se analiza la relación del nitrógeno, visto desde su lado inerte, con el fenómeno de hinchamiento de los aglomerados reducidos, para lo cual se aplicarán conocimientos asociados con la transformación alotrópica del hierro metálico (Fe°), sus defectos en la red cristalina, la adsorción-absorción-desorción del nitrógeno y determinar si las presiones y esfuerzos generados superan las propiedades de resistencia del material como para potenciar su hinchamiento.

La vía a seguir se fundamenta en calcular: a) cantidad de nitrógeno que puede disolver el hierro a las temperaturas de reducción en estado sólido y en las fases alotrópicas (Feα, Feγ), b) cantidad y volumen de espacios vacíos en la red cristalina del hierro, c) argumentar un mecanismo que lleve a la desorción de átomos de nitrógeno disueltos en las fases alotrópicas para así calcular la presión ejercida por el gas nitrógeno confinado en una vacancia y compararla con las propiedades de resistencia a la tracción (rotura) de cada fase alotrópica.

Se indican los conocimientos y ecuaciones necesarias en demostrar la potencialidad del nitrógeno para afectar la estabilidad mecánica del hierro metálico.

A. Disolución del nitrógeno

En el estado sólido los metales absorben gases del ambiente que les rodea y durante la reducción de los óxidos de hierro, el hierro metálico formado se mantiene en intimo contacto con los gases reductores y también con el nitrógeno, porque este haya sido alimentado para disminuir la presión parcial del gas reductor o porque el proceso se lleve a cabo en la atmosfera, la cual contiene 78% en volumen, bien porque se haya utilizado gas de amoniaco (NH3), o generado en etapa temprana de reducción, al utilizarse aglomerados con material carbonaceo y cuya descomposición, según (1) [5], p. 636, puede generar nitrógeno, favorecido por la presencia del Fe°, actuando como catalizador:

$$1/2\,N2\,(g) + 3/2H2\,(g) = NH3\,(g) \qquad (1)$$

De [6], [7], y [8], se resume el siguiente mecanismo para transferencia del gas (nitrógeno) desde la superficie del material (óxido-hierro) hasta su interior:

1. Moléculas de nitrógeno alcanzan la superficie del hierro y si bien no reaccionan, se pueden disociar.
2. La disociación, etapa más lenta, ocurre en sitios intersticiales y con participación de las vacancias que difunden y alcanzan la superficie de reacción.

3. Los átomos de nitrógeno disociados se adsorben y se disuelven en la superficie del hierro.

En este mecanismo no se considera la desorción del nitrógeno y como vía para facilitar los cálculos de la los esfuerzos generados en el interior de las redes cristalinas de las fases alotrópicas, se expandió con la adición de nuevos pasos y así justificar la presencia del nitrógeno como gas en el interior de estas fases:

4. La disolución superficial de los átomos de nitrógeno migran hacia intersticios internos, favorecidos por la ley de Fick.
5. Los átomos pueden congregarse en vacancias interiores y de sorberse, formando gas.
6. El gas confinado en el espacio de la vacancia genera presión, la que se asocia con esfuerzo mecánico que potencialmente puede expandir la red cristalina del hierro.

En la Fig. 1 se visualiza el mecanismo arriba mencionado: átomos de hierro liberados en la superficie, representado por las flechas hacia arriba, aportan la energía para romper los enlaces y disociar la molécula de nitrógeno y generar los átomos que siguen a través de intersticios hasta encontrarse en vacancias interiores y regenerarse en gas, pasos indicados por las flechas hacia abajo.

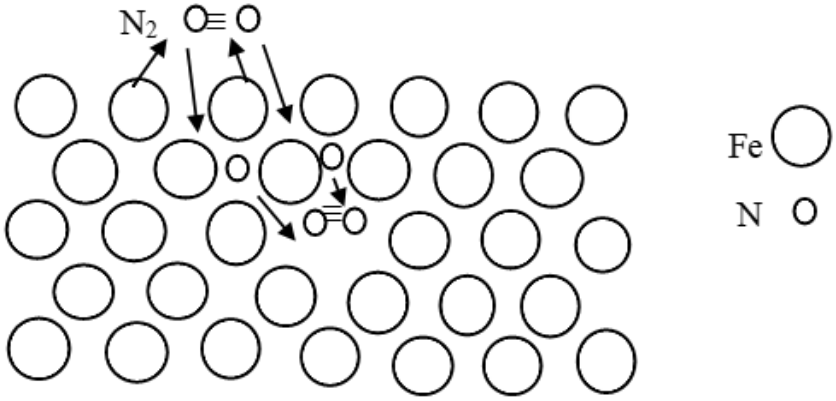


Fig. 1. Mecanismo para la disociación- adsorción desorción del N2 en hierro (Fe). Fuente Autor.

La cantidad de nitrógeno disuelto en hierro, se obtiene mediante (2), según la ley de Sievert [9],:

$$\%\,[N] = K\sqrt{pN2} \qquad (2)$$

[N] = Nitrógeno atómico en disolución.
K = Constante de equilibrio.
pN2 = Presión parcial del gas nitrógeno.

La cantidad de nitrógeno disuelto también depende de la fase alotrópica del hierro que desde bajas temperaturas hasta 911°C se mantiene como ferrita (Feα), y a temperaturas mayores cambia para austenita (Feγ) y K, en cada fase, se calcula mediante (3) y (4) determinadas experimentalmente [10], donde T = Temperatura absoluta.

$$\log. KFe\alpha = -\left(\frac{1570}{T}\right) - 1{,}02 \qquad (3)$$

$$\log. KFe\gamma = \left(\frac{450}{T}\right) - 1{,}95 \qquad (4)$$

B. Defectos en la red cristalina.

Los defectos internos pueden ser puntuales (vacancias e intersticios) y lineales (dislocaciones de borde y helicoidales), y constituyen espacios vacíos que pueden alojar átomos de nitrógeno y debido a que los primeros presentan espacios menos restrictivos, serán considerados a continuación. Las vacancias aparecen cuando un átomo de hierro de la red es transportado a otro sitio dejando un espacio vacío, este proceso es activado térmicamente y la cantidad de ellas se obtiene mediante (5) [11],

$$\mathrm{Ln}\,(n/N) = -(E/kT) \qquad (5)$$

Ln = Logaritmo neperiano.
n = Cantidad de vacancias (□).
N = Total de puntos reticulares de la red cristalina.
E = Energía para transporte de la vacancia (eV).
k = Constante de Boltzmann (8,62*10-5 eV/K).

Los intersticios son espacios entre los átomos del hierro y donde pueden alojarse átomos pequeños como los del nitrógeno. Ambas fases alotrópicas del hierro poseen intersticios octaédricos y la tendencia a ser ocupado se asocia con la relación entre los tamaños del radio atómico del soluto nitrógeno (r [N]) y solvente hierro (r Fe) en el rango de la austenita y mostrado en (6), según [12],

$$0{,}414 < r\,[N]\,/r\,Fe < 0{,}732 \qquad (6)$$

III. METODOLOGÍA

El método para la cuantificación es tipo teórico basado en el desarrollo de un mecanismo donde se asocian aspectos fisicoquímicos de adsorción- absorción-desorción del gas nitrógeno, estructura cristalina del material, datos experimentales reportados en la literatura y la ecuación de gases ideales para facilitar los cálculos matemáticos.

IV. RESULTADOS

Para determinar la cantidad de nitrógeno en disolución en la ferrita, se utilizó la temperatura de 900°C y en la austenita 1100°C, ambas en el rango de la obtención mayoritaria de hierro metálico en el proceso de reducción en estado sólido y en el cambio alotrópico de fases en el hierro; mediante (3)-(4), se obtienen los valores de las constantes de equilibrio para la disolución del nitrógeno en el hierro y estos valores se introducen en (2), asumiendo pN2= 0.78, aunque en realidad es menor por estar mezclado con los gases reductores. La cantidad de nitrógeno disuelto tanto en la fase ferrita como en austenita se presenta en Tabla I.

Tabla 1. Valores de la constante de equilibrio y nitrógeno disuelto en fases alotrópicas del hierro.

Fase alotrópica	Temperatura (K)	Constante equilibrio	Nitrógeno disuelto (%)
Ferrita (Feα)	1173	0,0044	0,004
Austenita (Feγ)	1373	0,024	0,021

Estos valores, aunque bajos, aseguran la existencia de nitrógeno en cada fase del hierro y pueden difundirse hacia los defectos puntuales de su red cristalina. La cantidad de vacancias potenciales donde pudieran terminar los átomos de nitrógeno, se puede calcular mediante (5), haciendo la corrección con la inclusión de la densidad (ρ) de cada fase, que puede obtenerse según (7) [11].

$$\rho = N° \, P.A / Vc \, NA \qquad (7)$$

N° = cantidad átomos por celdilla unitaria.
P.A = peso atómico (55,85 g/mol).
Vc = volumen de la celdilla unitaria (nm3).
NA = número de Avogadro (6,02*1023 átomos/mol).

La celdilla unitaria de la ferrita posee 2 átomos de hierro en un volumen de 0,024 nm3, mientras que en la austenita hay 4 átomos de hierro ocupando un volumen de 0,043 nm3, los resultados del cálculo de la cantidad de vacancias se presenta en la Tabla 2:

Tabla 2. Cantidad de vacancias en fases alotrópicas del hierro.

Fase alotrópica	Temperatura (K)	Densidad (g/cm^3)	Cantidad vacancias ($□/cm^3$)
Ferrita (Feα)	1173	7,93	$8,17\ 10^4$
Austenita (Feγ)	1373	8,58	$3,55\ 10^7$

En la austenita, a mayor temperatura, la cantidad de vacancias es mayor y consistente con los procesos activados térmicamente. El espacio vacío dejado por el traslado de un átomo de hierro y la cantidad de átomos de nitrógeno que potencialmente puede almacenar se asocia con sus volúmenes: 8,0 10-3 nm3 para la vacancia y 1,5 10-3 nm3 para el nitrógeno, considerando el radio atómico del hierro (rFe) = 0,124 nm y el del nitrógeno (rN) = 0,071 nm [13], Apéndice 2. La relación de volumen de vacancias a átomos de nitrógeno es: 5,3, por lo cual se puede alojar en forma ajustada hasta 6 átomos de nitrógeno y así mantener el equilibrio termo mecánico de la red cristalina. Estos átomos pudieran reaccionar entre si y formar tres moléculas de gas que confinadas en el volumen de la vacancia ejercerían una presión que se puede calcular mediante la ley de los gases ideales (8) [14], p.68, por cuanto existen las condiciones de alta temperatura y baja concentración del gas en el interior de cada fase alotrópica.

$$P\,V = n\,R\,T \qquad (8)$$

P= Presión (Atm.)
V = Volumen de vacancia □ (Lit).
n= cantidad de moles asociados a tres moléculas de gas nitrógeno (mol).
R = Constante de los gases (0.082 Atm. Lit. /mol K).
T = Temperatura absoluta (K).

Los valores de presión y su equivalencia en esfuerzos se presentan en la Tabla 3:

Tabla 3. Presión ejercida por el nitrógeno en una vacancia, según la fase alotrópica.

Fase alotrópica	Temperatura (K)	Presión (Atm.)	Esfuerzo (Kgf/mm^2)
Ferrita (Feα)	1173	$6{,}03\ 10^4$	621,2
Austenita (Feγ)	1373	$7{,}04\ 10^4$	727,6

El átomo de nitrógeno también puede difundir a los intersticios y según (6), (r[N]/rFe) = 0,573, tendrá preferencia por el intersticio octagonal, cuyo espacio vacío se calcula a través: rocth.= (√2-1)* rFe [12], igual a 0,051 nm, generando el volumen de 5,55*10 -4 nm3, que relacionado con el volumen del átomo de nitrógeno: = 1,50*10-3nm3, se obtiene: 5.55 *10 -4/1,50*10-3= 0,37 átomos, o sea solo es posible alojar en forma ajustada un átomo de nitrógeno, lo que imposibilita la formación de la molécula biatómica del nitrógeno. En función a los resultados obtenidos, es posible hacer los siguientes análisis:

Los valores calculados de las presiones causadas por la desorción de tres moléculas del nitrógeno en una vacancia de la red cristalina del hierro son muy elevados, Tabla III, y afectan la estabilidad mecánica del hierro metálico en el óxido natural o aglomerado y el comportamiento del nitrógeno como gas ideal. En cuanto al hierro, son conocidos los valores de resistencia a la tracción (rotura) a temperatura de 20°C, y establecidos en 105 Kgf/mm2 para la austenita y 28 Kgf/mm2 en la ferrita [15], pp. 187, 189 respectivamente, siendo los valores calculados de esfuerzos a la tensión 22 veces superiores a los esfuerzos de rotura en la ferrita y 7 en la austenita.

En cuanto al comportamiento del nitrógeno ante grandes presiones, del análisis del diagrama de compresibilidad del nitrógeno [14], p. 491, se determina que a la presión de 360 atmósferas el factor de compresibilidad es mayor a uno correspondiente al gas ideal, lo que pudiera contribuir al incremento de presión, al interactuar entre si las moléculas del gas.

El hierro, como todos los metales al ser sometidos a esfuerzos de estiramiento presenta respuestas elásticas y plásticas, y en especial a altas temperaturas, al enfriarse se recupera el alargamiento elástico pero no la deformación plástica obtenida. Cuando el esfuerzo de estiramiento supera el de rotura, produce grietas y alivio de los esfuerzos hasta llegar a la rotura. Los valores de resistencia a temperatura ambiente, se reducen según ésta aumenta, por lo que sería aún más probable que ocurra el colapso del material. Resultados experimentales en tratamiento de minerales de hierro con atmósfera de amoniaco [2], presentaron evidencia, Fig. 2, de ruptura mecánica del producto, lo cual puede ser asociado con la presencia del nitrógeno, al descomponerse el amoniaco, según lo indicado en (1).

Por otra parte, enlos cálculos de la presión solo se consideró una vacancia, entonces es posible estimar que dependiendo de la cantidad y agrupación de vacancias se dispondrá de más espacios para la absorción-desorción de nitrógeno, lo cual conllevaría a la generación de mayores esfuerzos y así incremento catastrófico de volumen.

Fig. 2. Aspecto de grieta en muestra de Fe2O3-Fe3O4, A 900°C-100% NH3, 29,1 % Reducción y 25,95% incremento de volumen [2].

Son pocas las investigaciones realizadas referentes al efecto de átomos de gases alojados en defectos puntuales de estructuras cristalinas de metales, en [16] se calculó, mediante teoría de elasticidad, el cambio de volumen generado por átomos de helio (He) en vacancias del cobre a temperatura muy baja y se determinó una relación con tendencia lineal entre la presión y la relación de átomos por vacancias, y en su Fig. 4, se observa el valor de ~ 1,5 106 Atm., de presión para 6 átomos de He en una vacancia,ante tan elevada presión, el investigador Baskes hace el comentario: "La muy alta presión obtenida en esta pequeña burbuja no es sorprendente", y acota: "A temperatura ambiente, un gas ideal podría tener una presión unas 50 veces menor a las presiones aquí calculadas". Convirtiendo este comentario en datos, representa unas 30 mil atmosferas a temperatura ambiente, valor que estaría en el orden de magnitud del valor de 60 mil atmósferas calculadas por el autor a temperatura de 900°C, que convertidas mediante (8), a temperatura ambiente (27 °C) equivalen a 15375 atmósferas.

CONCLUSIONES

1. Se propuso la expansión del mecanismo de adsorción del nitrógeno para incluir su desorción en el interior de defectos puntuales de la red cristalina del hierro y calcular los esfuerzos producidos.
2. Los valores de los esfuerzos causados por la desorción de tres moléculas de nitrógeno en una vacancia, al compararse con los valores conocidos de éste a 20°C, de 28 y 105 Kgf/mm2 de resistencia a la tracción (rotura) para la ferrita y austenita respectivamente, resultan en 22 veces superior en la ferrita y 7 en la austenita y favorecen su hinchamiento y agrietamiento catastrófico.
3. Los valores de los esfuerzos obtenidos dependerán de la cantidad de vacancias involucradas en un determinado clúster, según el tránsito del paso de reducción a hierro metálico naciente.
4. En el espacio intersticial octaédrico solo puede alojarse un átomo de nitrógeno, sin posibilidades de formar gas que se expanda y fracture las fases alotrópicas.

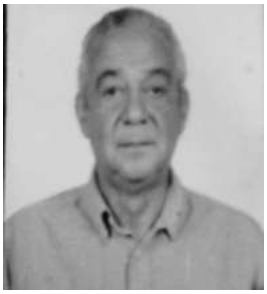
REFERENCIAS

[1]H. Wang and H. Y. Sohn. "Effects of Reducing Gas on Swelling and Iron Whisker Formation during the Reduction of Iron Oxide Compact". 2012 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim, steel research int. 83, 2012, No. 9999, pp. 1-7.
[2]G. O. Dam. "The effect of nitrogen of swelling iron ore". Thesis Doctoral Imperial College, London. 1983.
[3]G. O. Dam, "Influence of nitrogen on the swelling during reduction of Venezuelan dense hematite ore". Thesis Magister. Imperial College. London. 1977.
[4]A. A. EL-Geassy, M. l. Nasr and M. M. Hessie, "Effect of reducing gas on of volume change during reduction of oxides compact". ISIJ International, Vol. 36, nro 6. 1996, pp. 640-649.

[[5] B. H. Mahan. University Chemistry. 3°ed. Addison-Wesley Publishing Company. Philippines. 1975.
[6]C. M. Marcos. Notas: Premios Nobel 2007: Química y Física. Universidad de Sevilla, pp. 333-342.
[7] H. J Grabke. "Conclusions on the Mechanism of Ammonia-Synthesis from the Kinetics of Nitrogenation and Denitrogenation of Iron". Zeitschrift für Physikalische Chemie Neue Folge, Bd. 100, S. 185—200 (1976) © by Akademische Verlagsgesellschaft, Wiesbaden 1976, pp. 185-200.
[8] H. J Grabke and G Hortz. "Kinetics and mechanisms of gas metal interactions". Ann. Rev. Mater. Sci, 1977, pp. 155-178.
[9]S. Filippov. The theory of metallurgical processes. Moscow: MIR Publishers, 1975.
[10] W. Lankford, N. Samways; R. Craven. The making shaping and treating of steel. 10° ed., Pittsburgh: Herbick & Held, 1985.
[11]W. D. Calister, Jr. Introducción a la ciencia e ingeniería de materiales. 2° ed., México. Limusa Wiley, 2009.
[12]D. R. Askeland. Ciencia e ingeniería de los materiales. 3° ed., México. International Thomson Editores. 1998.
[13]J. F. Shackelford. Ciencia de los materiales para ingenieros. 3° ed., México. Prentice Hall Hispanoamericana. S. A. 1995.
[14]V. Wylen. Fundamentos de termodinámica. 2°ed, México. Limusa Wiley. 2012.
[15] S. H. Avner. Introducción a la metalurgia física. Madrid, España. Talleres Gráficos de Ediciones Castilla, S. A. 1966.
[16]M. I. Baskes and J. H. Holbrook. "Volume changes in copper due to point defects". Physical Review B, Vol. 17, nro. 2. 1978, pp.422-426.

LOS AUTORES:

Luis Alberto Azócar, metalúrgico de profesión en elaboración de acero vía segunda generación: hornos eléctricos de ultra alta potencia y pre reducidos. Doctorando de la Universidad Nacional Experimental Politecnica de Guayana (UNEXPO).



Oscar G Dam G, Metallurgical Engineer graduated from the Central University of Venezuela 1972 Master Science in Metallurgy and Diploma (DIC) Graduated from the Imperial College of Science and Technology 1977, England Doctor in Metallurgy graduated from the University of London in 1983. Department of Metallurgy at the Experimental Polytechnic Institute of Guayana (UNEXPO) since 1978. Postgraduate professor in materials science at the Central University of Venezuela and at the Experimental University of Guayana (UNEXPO)since 1984, external tutor for postgraduate studies at the Venezuelan Research Institute of Science (IVIC).

ISSN-E: 2737-6439

Athenea Journal
Vol.3, Núm. 9, (pp. 15-25)

https://doi.org/10.47460/athenea.v3i9.42

Avances en sistemas de defensa antiaérea

Páliz Patricio
https://orcid.org/0000-0003-4294-116X
pxpaliz@gmail.com
Fuerza Terrestre Ecuatoriana,
Brigada de Artillería 27 Portete
Cuenca-Ecuador

Acosta Juan
https://orcid.org/ 0000-0003-1007-5076
panchoacosta01@hotmail.com
Fuerza Terrestre Ecuatoriana,
Brigada de Artillería 27 Portete
Cuenca-Ecuador

Tiuma Alexis
https://orcid.org/0000-0002-2015-2656
alexis.tiuma@hotmail.com
Fuerza Terrestre Ecuatoriana,
Brigada de Artillería 27 Portete
Cuenca-Ecuador

Bravo Marlon
https://orcid.org/0000-0002-9690-7445
marlonbrav89@gmail.com
Fuerza Terrestre Ecuatoriana,
Brigada de Artillería 27 Portete
Cuenca-Ecuador

Recibido(23/05/2022), Aceptado(17/06/2022)

Resumen.-En el presente trabajo se presentan de manera técnica los avances y características de los sistemas de defensa antiaéreos. Se recopiló información a partir de una revisión sistemática en bases de datos especializadas referentes estrictamente al ámbito de la defensa militar de amenazas aerotransportadas. Se han desarrollado múltiples avances, algunos en los que la Inteligencia Artificial IA ya juega un papel fundamental permitiendo en algunos eventos tomar decisiones con mayor probabilidad de acierto y precisión frente a las decisiones y velocidad de respuestas humanas.

Palabras clave: Sistemas de defensa, Defensa antiaérea, Aeronáutica Militar

Advances in air defense systems

Abstract.- This paper presents the advances and characteristics of air defence systems technically. The information is derived from a systematic review of technical databases dealing exclusively with military defence against airborne threats. Many advances have been developed in which Artificial Intelligence AI already plays a fundamental role, in some cases enabling decisions to be made with greater probability of success and precision than with decisions and the speed of human reactions.

Keywords: Defense Systems, Air Defense, Military Aeronautics.

I. INTRODUCCIÓN.

La defensa aérea es un componente clave en el arsenal militar de cualquier nación y tiene la capacidad de proporcionar a los líderes nacionales lo que es esencialmente un escudo para proteger a su gente, a las fuerzas terrestres y aeroespaciales, siendo la clave para una defensa exitosa una adecuada ofensiva que evite a la amenaza aerotransportada llegar a su destino.

Con el incremento del terrorismo en todo el mundo, los países y organismos de defensa están buscando nuevas formas de hacer retroceder a los atacantes a través del uso de armas de ataque aéreo. Las armas aéreas se emplean mediante el uso de aviones o misiles para atacar objetivos desde las alturas [1]. Los éxitos de los ataques con armas de ataque aéreo se basan en un cierto grado de inacción de la parte atacada como el blindaje y el apagón. Por esta razón, tales ataques no son ideales cuando los militares están operando en áreas de baja intensidad y los insurgentes tienen una inteligencia extraordinaria sobre los movimientos [1].

Las primeras armas de ataque aéreo utilizadas fueron las primeras encarnaciones de las bombas, en particular la bomba Napalm, que fue desplegada por primera vez por los Estados Unidos contra las fuerzas atrincheradas en el Lejano Oriente durante la Segunda Guerra Mundial. Con tecnología más sofisticada y capacidades de navegación más precisas, las ballestas, comenzaron a usarse para ataques aéreos con apoyo cercano de las fuerzas terrestres. Un sistema llamado "Nail" permaneció en funcionamiento hasta al menos 1946, pero la artillería nuclear comenzó a reemplazarlos a medida que se desarrollaba la tecnología de misiles. La proliferación nuclear, particularmente después de que la "Operación Buda Sonriente" de la India realizara una prueba de explosión de aire de bajo rendimiento en 1974 que tuvo un impacto significativo en la opinión pública sobre las pruebas atmosféricas, redujo considerablemente la cantidad de grupos de combate que permanecen regularmente en el aire en un momento dado [2].

Los acontecimientos mundiales recientes que han llevado a guerras también conducen indirectamente a la producción de misiles destinados al ataque. Dado que los misiles disparados en un ataque aéreo pueden causar mucho daño, siempre existen razones para explicar por qué fueron necesario su uso. El problema es que hay numerosas quejas de ciertos grupos sobre lo malo que realmente puede ser el lanzamiento de misiles contra los propios soldados del atacante y las personas dentro de las designaciones aéreas por las que están atacando.

Existe la necesidad de contrarrestar acciones hostiles en diversas áreas del país, dedicadas a la defensa, protección de las fronteras nacionales en el sentido militar y aseguramiento de la soberanía estatal en el espacio aéreo. Implementar tales tareas es más difícil con una subdivisión no sistematizada e inadecuada de los recursos humanos y su asignación entre varias subdivisiones.

La deficiencia en equipamiento militar resulta del actual nivel de desarrollo en algunos países del mundo, en otros países de mayor tamaño, los sistemas de defensa tienen trayectoria en sus desarrollos y habitualmente están constituidos por radares de largo alcance en sistemas transportables/robóticos (demostrado mediante pruebas técnicas), ametralladoras rotatorias dinámicas de fuego para vehículos oruga o blindados, pequeñas estaciones de armas con torretas, para todo tipo de despliegue rápido. vehículos o remolques separados para montajes de vehículos blindados ligeros y todo tipo de helicópteros; estaciones de armas [3].

En la sección que continua se describen los desarrollos tecnológicos implementados y teorizados según la revisión sistemática, se detallan los resultados y hallazgos de la información obtenida y finalmente se presentan las conclusiones respecto de los avances y estado actual de los sistemas de defensa antiaérea.

Los sistemas de defensa aérea son buenos para proteger los recursos terrestres y marítimos de los ataques aéreos. Según la región y el tipo de fuerzas militares que entren en conflicto, las defensas aéreas pueden variar mucho en fuerza. En un conflicto regional donde los dos bandos son similares y no se puede lograr la superioridad aérea, la importancia central de los sistemas de defensa aérea queda clara como una gran ventaja sobre el enemigo. En terrenos de combate que contienen montañas (continente o islas pequeñas), la artillería antiaérea operada por humanos o controlada por computadora puede ser muy efectiva [1]. En el campo de batalla del desierto, donde las tormentas de arena pueden ocultar los movimientos de los bombarderos y las defensas aéreas terrestres son menos efectivas, generalmente se utilizan misiles montados en helicópteros o aviones no tripulados. Las aeronaves se pueden usar para lanzar artillería en la batalla o realizar misiones de apoyo aéreo cercano con armas montadas en vehículos aéreos como ametralladoras y cañones automáticos [4].

Un importante desarrollo reciente en los sistemas integrados de defensa aérea es el empleo de sistemas cibernéticos y de interferencia para negar el acceso de las aeronaves intrusas enemigas al espacio aéreo. Estas tecnologías emplean una combinación de terminales cinéticos y no cinéticos. La Organización del Tratado del Atlántico Norte (OTAN) presentó una impresionante variedad de nuevas armas para respaldar sus compromisos en la Cumbre de Gales de septiembre de 2014. En China se ha acelerado la inversión en tecnologías anti aeroespaciales que van desde bloqueadores hasta codificadores y láseres [2].

Un grupo de trabajo naval ha desarrollado una nueva formulación para el problema de la defensa aérea de los buques de guerra. Se ha propuesto un método de solución basado en definir el problema de asignación de misiles (MAP) como la asignación óptima de un conjunto de misiles tierra-aire (SAM) de un grupo de trabajo naval a un conjunto de objetivos aéreos atacantes. El MAP es una nueva forma de abordar un problema actual frente al aumento de las capacidades de misiles antibuque (ASM), los diferentes niveles de capacidades de defensa aérea de los buques de guerra contra la amenaza ASM y la nueva tecnología que permite una defensa totalmente coordinada y colectiva. Además de asignar SAM a ASM, MAP también programa el lanzamiento de rondas SAM de acuerdo con la política de compromiso shoot-look-shoot o sus variaciones, considerando múltiples sistemas SAM y tipos de ASM. MAP se puede utilizar para la planificación de la defensa aérea en un escenario determinado [3].

La figura 1, presenta de forma gráfica los componentes y etapas mediante la cual se realiza la intercepción de los misiles enviados por un atacante.

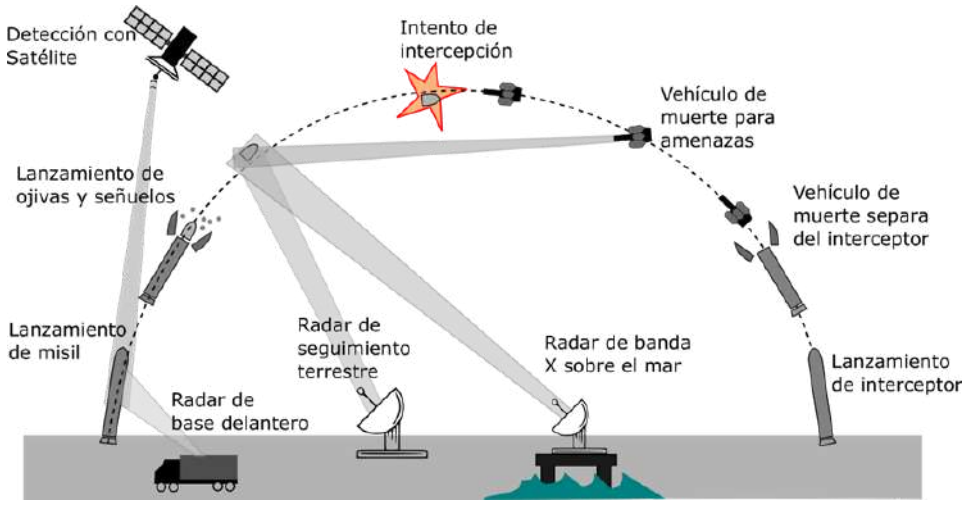


Fig 1. Esquema del proceso de intercepción de misiles de ataque en espacio aéreo.

La figura 1, presenta una primera etapa en la que hay detección cuando un misil es lanzado cuya información es obtenida por una satélite, adicionalmente existen vehículos móviles con radar para contener la ubicación del misil. El sistema también tiene un conjunto de Radares terrestres fijo o en bases marítimas sobre las aguas que permiten entre ellas ubicar la posición exacta del misil. Por otra parte, el sistema de defensa lanza un misil con un dispositivo interior que interceptará de forma directa al misil del enemigo, este vehículo transporta un sistema de seguimiento y navegación autónomo que le permitirá interceptar al misil enemigo. Las funciones del sistema de defensa antimisiles, comprende un conjunto de dispositivos interconectados para permitir el monitoreo, control y adquisición de información en tiempo real del movimiento y existencia de misiles en espacios aéreos y terrestres.

Un conjunto de sensores satelitales, radares terrestres y marítimos son usados para proveer de un sistema de monitoreo que permite la detección temprana de misiles ofensivos, adicional a esto permite la discriminación y el seguimiento para su posterior intercepción. [5]

Los sistemas interceptores lo constituyen misiles que procuran eliminar la amenaza haciendo contacto con el misil ofensivo y evitando que este llegue a su objetivo. Existen interceptores de una sola pieza como el Patriot Advanced Capability-3 (PAC-3), mientras que otros son lanzados desde silos terrestres, camiones móviles o barcos.

Los sistemas de comando y control permiten procesar la información adquirida por los sensores y de acuerdo con esta, se envía señales a los sistemas interceptores y vehículos terrestres, adicional a esto, los sistemas pueden coordinarse con la red que atiende incendios a nivel nacional.

Existen principalmente tres tipos de sistemas de defensa antimisiles: defensas de baja altitud, tecnología láser aerotransportada y sistemas de defensa aérea a nivel terrestre. Los componentes de defensa antimisiles, como el radar, están estandarizados a nivel internacional para detectar misiles entrantes, mientras que la capacidad de interceptor suele ser propiedad de los grandes fabricantes de armas de EEUU [6] .

Los sistemas avanzados como los misiles Patriot y THAAD, junto con otros sistemas de radar, detectan en promedio casi el 100% de todos los misiles entrantes, esto no significa que los misiles aún no puedan ser interceptados. Hay muchos factores disuasorios que dificultan que los ataques de los países desarrollados y en desarrollo logren atacar a otros países en primer lugar. Lo más notable a mencionar es que en cada choque singular de superpotencias hasta ahora, nadie destruyó una ciudad, esto nos indica cuán bueno es realmente estos sistemas de defensa para evitar daños.

La Iniciativa de Defensa Estratégica de los Estados Unidos (SDI) es un sistema de defensa antimisiles investigado iniciado en 1983, durante la presidencia de Ronald Reagan. El objetivo de este programa era crear un sistema que proporcionara defensas contra los misiles nucleares enemigos. Fue comúnmente conocido como el proyecto "Star Wars", que es una película de Hollywood que el presidente vio antes de su toma de posesión y soñó con el desarrollo de Estados Unidos contra los ataques con misiles en una red de defensa impenetrable. Si bien muchos políticos y expertos ven como un movimiento equivocado invertir fuertemente en el desarrollo de escudos de defensa contra misiles balísticos en lugar de armas más convencionales, también se ha opinado que estas estrategias pueden ser más rentables direccionándolas a la atención médica de primera línea [7].

Los sistemas avanzados de defensa antimisiles son un arma relativamente nueva en el arsenal militar. En los últimos años, estos sistemas antimisiles han evolucionado considerablemente gracias a los avances tecnológicos en cohetes y radares. La posibilidad de que alguien pudiera modificar uno de sus cohetes para llevar armas nucleares se identificó por primera vez al comienzo de la Guerra Fría, esto llevó a Occidente a organizar redes de defensa en capas profundas con esquemas integrados de cooperación de radar y vigilancia aérea. Los misiles modernos son interceptados por misiles que fueron disparados escondiéndose detrás de la curvatura de la Tierra. Los más antiguos ni siquiera alcanzan la velocidad de escape antes de que la atmósfera de la Tierra los detenga, mientras que los misiles balísticos más nuevos usan cargas útiles que les permiten maniobrar fuera de la atmósfera de la Tierra para que puedan volver a entrar como señuelos y alejar los misiles defensivos del objetivo.

La guerra ha sido una fuerza importante para el crecimiento de la economía estadounidense, la protección de su gente y un impulsor para la innovación tecnológica que ha beneficiado a muchas más personas e industrias. En el contexto de esta carrera armamentista en curso, las tecnologías están evolucionando no solo para superar la tecnología defensiva disponible, sino también para adoptar atributos novedosos, incluso aquellos como el sigilo y la estética, expresamente para derrotarla; ahora hay una tendencia explícitamente dirigida a derrotar las capacidades defensivas. Es evidente que los oponentes están elaborando estrategias en su carrera armamentista para hacer que la guerra sea insostenible para cualquier competidor con fronteras "cerradas" (como Corea del Norte), o adoptando tecnologías que hacen que la guerra no sea rentable en general en grandes extensiones de terreno sin tener ninguna tecnología de protección explícita [8].

Se considera que algunos sistemas antimisiles avanzados son una mejor opción que las ojivas cinéticas. Los misiles avanzados para interceptación, como los interceptores lanzados desde tierra, barcos o misiles pueden proporcionar un mayor nivel de defensa y también poseer una naturaleza menos letal para las contramedidas. Algunos opositores al uso de sistemas antimisiles avanzados plantean dudas sobre las capacidades de estos escudos y si realmente se pueden implementar en escenarios relevantes sin causar daños colaterales graves.

Los sistemas antimisiles más avanzados brindan más protección contra los misiles que provienen de varios ángulos. No solo eliminan el misil en el camino, sino que los escombros voladores protegen otros activos militares vulnerables debajo. Ejemplos de estos sistemas son: "Terminal High Altitude Area Defense (THAAD) de EE. UU., Abkonte Y y Nakotcha de Rusia y HQ-9 de China. Los sistemas antimisiles más avanzados son clave para la seguridad en numerosos frentes en la situación mundial en constante cambio de hoy. El sistema (generalmente transportado o utilizado por un vehículo) brinda protección contra los misiles que llegan al objetivo desde diferentes ángulos según el lugar del mundo en el que se lanzan: en qué formaciones geográficas ingresan, su trayectoria balística y la ubicación en la que terminan descendiendo.

A. Terminal de Defensa de Área de Gran Altitud (Terminal High Altitude Area Defense -THAAD-US)

El sistema estadounidense de defensa antimisiles denominado THAAD se emplea como apoyo en la defensa de Corea del Sur de un posible ataque por parte de Corea del Norte. Este sistema brinda protección para evadir el impacto de enemigos al disparar cohetes adversarios con un rango de protección de más de 300 millas antes de que descarguen su arsenal hacia sus puntos objetivos. En la figura 2 se aprecia un esquema de los componentes principales de este sistema que consta de radares móviles, estaciones de mando y control y vehículos de lanzamiento de dispositivos interceptores [9].

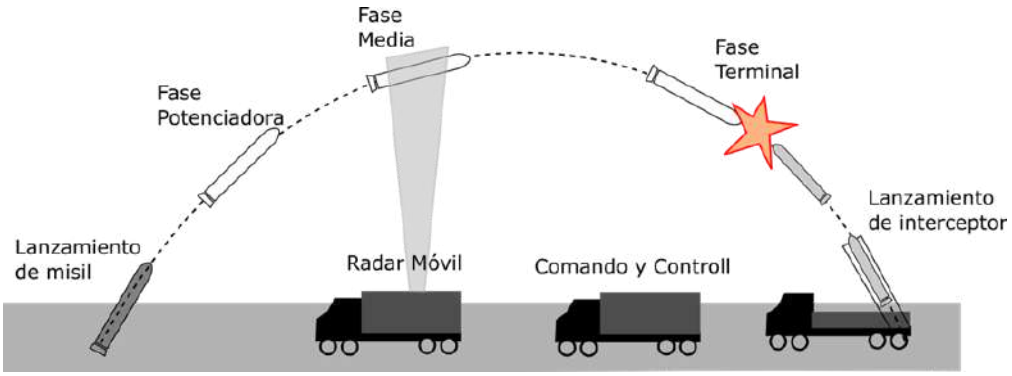


Fig 2. Esquema de la distribución y componentes del Sistema antimisiles THAAD-US.

El Terminal High Altitude Area Defense es un sistema de misiles antibalísticos que el gobierno de EE. UU. despliega en varios países para defenderlos de las crecientes amenazas de misiles, como el programa de misiles de Corea del Norte. THAAD es un sistema de interceptación de misiles que está diseñado para atacar y destruir misiles balísticos dentro o fuera de la atmósfera terrestre durante su fase terminal de vuelo. El alcance del radar AN/TPY-2 tiene un módulo de transmisión/recepción del tamaño de una pelota de golf montado en la parte superior de un pedestal de 30 pies que puede volar hasta 200 pies en el aire.

Los interceptores THAAD utilizan energía cinética o un vehículo exterminador exoatmosférico para destruir los misiles balísticos tácticos entrantes en el espacio durante su fase final, o terminal, después de que hayan dejado la atmósfera y hayan comenzado a caer de regreso a la Tierra [8].

B. Sistema antimisiles Abkonte Y y Nakotcha de Rusia

Junto con grandes proyectos para la defensa civil y militar, Rusia ha desarrollado sus operaciones militares en Crimea y en Siria empleando estaciones de radar. Estas estaciones han inquietado a otros países debido a las amenazas de misiles en sus fronteras.

Numerosos contratistas ofrecen soluciones innovadoras en el ámbito de los sistemas de defensa antiaérea y de misiles, protección contra minas o equipos de barrido de minas y diversas soluciones de software para el centro de mando y operaciones. Algunos de los proveedores de sistemas más avanzados incluyen el sistema Abkonte Y. Nakotcha, basados en las líneas de montaje de la planta AvtoVAZ, que producen vehículos de transporte y cuyo sistema Krizantema-P es uno de los equipos antimisiles más nuevos desarrollados por Almaz Central Design Bureau [10].

La ciencia de datos y el aprendizaje automático son el núcleo de la inteligencia detrás del reciente sistema antimisiles ruso Abkonte Y. Abkonteh que Rusia se creó como un "sistema de misiles antiaéreos compuesto por una serie de instalaciones de combate y baterías de radar que forman colectivamente una base de defensa aérea. Este caso de uso explica cómo se puede usar la recopilación de datos en grandes sistemas estratégicos para demostrar el éxito .

C. Sistema antimisiles HQ-9 de China

El sistema HQ-9 fue diseñado y fabricado en China por un consorcio que incluía el Instituto de Investigación 716, el Instituto 601, la Academia 047 y China Avionics Engineering Co. El punto de ensamblaje final para el HQ-9 probablemente fue Shanghai según la evidencia circunstancial de que el radar en la base de Pingshan con un radio de 80 kilómetros a su alrededor podría proporcionar cobertura para la adquisición de objetivos para tales radares.

El HQ-9 está armado con seis misiles en lugar de solo cuatro que se encuentran en los equivalentes occidentales como los sistemas israelíes Barak o los sistemas American Patriot. El despliegue de estas armas implica cargar dos misiles en un bote montado en un remolque permitiendo reducir la vulnerabilidad al ataque [11].

El sistema HQ-9 es uno de los sistemas más desarrollados en China, posee una autonomía de 400 kilómetros, tiene tres versiones. Un sistema antimisiles efectivo se puede resumir mediante tres factores: distancia, tiempo de reacción y rango de destrucción. Con estas características, HQ-9 forma una cadena de combate confiable y fluida para durabilidad y capacidad de ataque a misiles enemigos con una mejor precisión. Cuanto mayor sea el alcance de destrucción de un sistema antimisiles, menos vulnerable será su área de despliegue a los ataques enemigos. A largas distancias, las contramedidas o los cohetes no detectan un misil en absoluto, por lo que las posibilidades de intercepción se reducen significativamente.

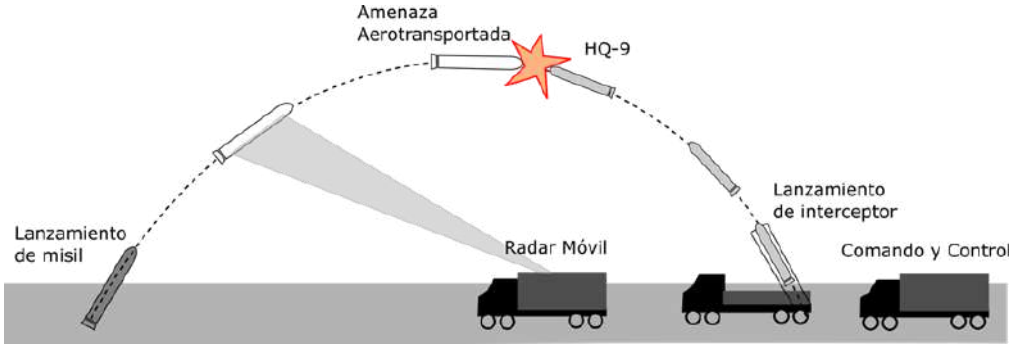


Fig 3. Esquema de la distribución y componentes del Sistema antimisiles HQ-9 -China.

D. Nuevos Avances Tecnológicos para sistemas antimisiles

Los militares y los presupuestos se han centrado en dispositivos de energía dirigida (DEW) durante años, pero la tecnología ahora está haciéndolas más asequibles. Si bien no está claro qué tan fácil será desplegar completamente esta tecnología en el combate, las últimas pruebas del prototipo DEW han demostrado que ha ido más allá de una idea abstracta. A medida que la tecnología se desarrolla y se somete a pruebas fuera de los laboratorios, es probable que atraiga una mayor atención de los militares y los gobiernos que buscan establecer una superioridad técnica sobre los adversarios [12].

El principio de funcionamiento de las armas de energía dirigida se analiza actualmente en la implementación de los sistemas antimisiles dado que una de las características de estos dispositivos es generar haz de láseres con capacidad de inhabilitar aviones o misiles, adicional a esto puede generar ondas electromagnéticas de longitudes cortas (milimétricas o microondas) o haces de partículas que pueden deteriorar estructuras moleculares o atómicas del misil, inhabilitándolo para llegar a su objetivo. En la figura 4 se aprecia un esquema de los dispositivos de alta energía y potencia en microondas.

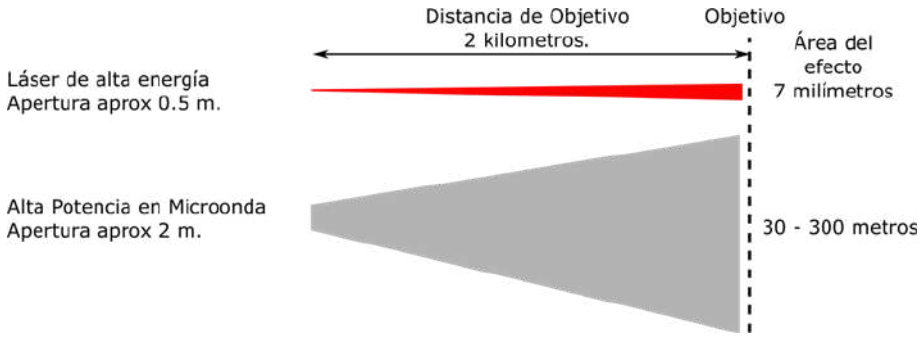


Fig 4. Alcances de los dispositivos de energía dirigida en alta energía (láser) y alta potencia en microondas.

Para la destrucción de los misiles enemigos en etapas tempranas de lanzamiento y cuando este aún se encuentra en la atmósfera terrestre. Esta tecnología permite discriminar si se trata de una ojiva letal o pedazos del misil una vez que ha lanzado señuelos. Interceptar al misil en su impulso es mucho más fácil de detectar que cuando esta ha pasado a fases avanzadas de vuelo. Esta alternativa de defensa se apoya del uso de los dispositivos de energía dirigida.

Una alternativa para interceptar a los misiles en su etapa temprana es el uso de drones que transportan un sistema de láser de alta energía con capacidad de desactivar misiles balísticos. Otra tecnología moderna es el EM Railgun que consiste en dispositivo de largo alcance y que dispara proyectiles mediante electricidad en forma de propulsión electromagnética. Los campos magnéticos se lanzan pasando de 0 a 6 machs en aproximadamente 10 milisegundos. Los proyectiles utilizados poseen una masa de 23 libras y buscan impactar evitando su detonación en el campo de batalla, el alcance de este dispositivo alcanza las 100 millas náuticas [12].

Para cuestiones de monitoreo se analiza la posibilidad de incorporar los sistemas Global Hawk de origen estadounidense, los cuales han sido desplegados para mantener vigilada la actividad bélica que pueda afectar contra las naciones. Este sistema emplea una serie de aviones de alta capacidad que evita el despliegue de tropas en varios lugares del mundo y puede alimentar con su información a los sistemas antimisiles desplegados en tierra [13]. En etapa de pruebas, se están realizando pruebas de un cañón activado con pólvora denominado Hyper-Velocity (HVP) que tiene un diámetro de 5 mm de pulgadas y que se pretende incorporar al arsenal de defensa de misiles balísticos de los Estados Unidos.

Existe un sensor hipersónico y balístico que puede proporcionar seguimiento desde el lanzamiento hasta el impacto de un misil enemigo, que inclusive puede discriminar si es arsenal propio o de otras procedencias. La Agencia de Desarrollo Espacial (SDA) ha empleado este tipo de sensores HBTSS para su monitoreo de defensa en órbita baja (LEO). Este sensor se basa en el funcionamiento de una red de satélites y trabajar de forma colaborativa detectando misiles hipersónicos sobre toda la superficie terrestre. Existe una iniciativa denominada Join All-Domain Command & Control (JADC2) con la que se propone reemplazar los sistemas actuales de dominio y control por uno que unifique las acciones de comunicación en los dominios de mar, aire, tierra, cibernética y espacio, fuerzas comandadas por el ejército de los Estados Unidos. La iniciativa propuesta busca incorporar todos los datos y usarlos a tiempo para garantizar una mejor respuesta de defensa incluyendo los ataques con misiles que pudieran ocurrir [14].

Uno de los aportes más significativos en la eficiencia de los sistemas antimisiles es el desarrollo de los sistemas de radares de largo alcance de estado sólido (LRDR). Este sistema constituye una base fundamental y soporte para la defensa antimisiles de Estados Unidos. Este tipo de radar permite búsqueda, rastreo y discriminación, siendo esta última capacidad, un aspecto crítico de la defensa antimisiles ya que una de las tareas más complejas es distinguir los objetos letales de los escombros y señuelos alrededor del objeto letal. El LTAMDS es un sensor de 360 grados que se utiliza para una variedad de propósitos, incluida la defensa antimisiles, su modularidad y funcionalidad cruzada aseguran que sea cómodo de implementar y ha sido diseñado para defenderse contra las amenazas de seguridad más avanzadas, incluidos misiles balísticos tácticos, aviones y misiles. LTAMDS tiene una detección de largo alcance de más de 360 grados de espacio de batalla y la capacidad de detectar y rastrear objetivos de maniobra de alta velocidad y proporcionar datos a la red [14].

El sistema Multi-Object Kill Vehicle (MOKV) permite que se lance más de un vehículo de destrucción (antimisiles) desde un solo propulsor. Este sistema consta del vehículo de transporte con sensores a bordo y una serie de vehículos destructores simples y más pequeños que lo habitual. La carga útil integrada está diseñada para adaptarse a los propulsores interceptores existentes. Esta estrategia ayuda a mejorar la intercepción de los misiles incrementando la probabilidad de éxito en la operación [15].

III. METODOLOGÍA

Se realizó una búsqueda de los sistemas antimisiles con las palabras claves anti-misile system defense, a partir de esto se hallaron documentos en las bases de Web of Sciences, Science Direct y SCOPUS. La figura 5 presenta el flujo de trabajo de la revisión realizada, de la cual eliminando los documentos duplicados y cribando los trabajos según sus títulos, abstract y contenido se obtuvieron 15 documentos relevantes que dieron soporte al desarrollo de este documento.

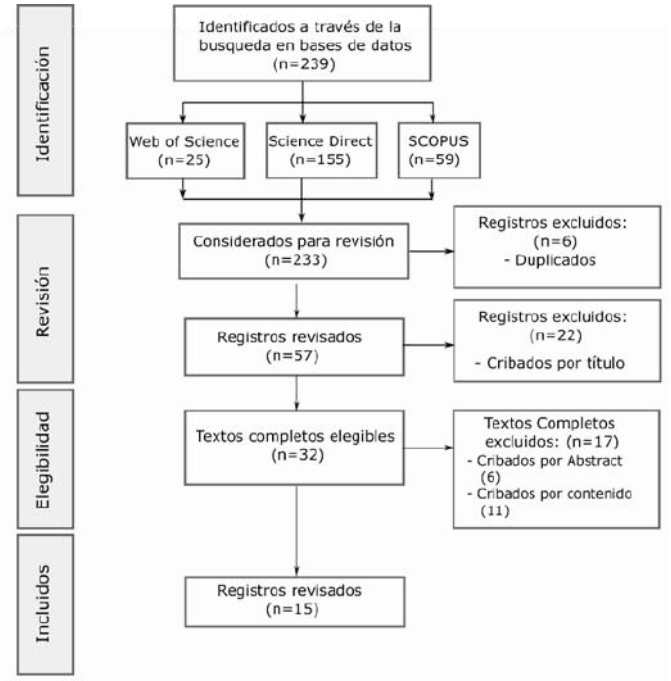


Fig 5. Flujo de trabajo de la Revisión Sistemática realizada con las palabras clave: Anti-misile, System, Defense

IV. RESULTADOS

Se han evidenciado múltiples desarrollos a partir de la revisión sistemática realizada, a pesar de que existen documentos en revistas científicas, la información técnica de operación de estos sistemas no se especifica por motivos de seguridad ya que el gobierno y uso de estas tecnologías son de carácter militar y confidencial.

La tecnología ha implementado en los sistemas antimisiles, técnicas nuevas como el uso de energía directa para inhabilitar el funcionamiento del sistema de navegación de los misiles y evitar que lleguen a sus objetivos. Adicional a esto, se han mejorado notablemente el alcance, cobertura de detección, tiempos de respuesta y técnicas para una mejor discriminación entre el arsenal aerotransportado y los señuelos disparados, lo cual implica una gran ventaja para mejorar la defensa.

Los desarrollos de estos sistemas implican cuantiosas sumas de dinero para los países, este gasto ha sido motivo de debates en torno a que estas inversiones pueden dirigirse a atender a los afectados causando mayor impacto y brindando mayor bienestar que desarrollando tecnologías antimisiles.

CONCLUSIONES

El sector militar ha conseguido un gran apoyo por parte de las naciones para la implementación y desarrollo de nuevas tecnologías antimisiles, aspecto que requiere además del aporte de grandes cantidades de dinero para la inversión de estos sistemas, siendo Estados Unidos uno de los países que más ha desarrollado estos proyectos y que posee múltiples puntos del planeta para dar apoyo en la defensa de países aliados.

Los avances en sistemas antimisiles incorporan técnicas de Machine Learning e Inteligencia Artificial, lo cual les permite obtener respuestas mucho más rápidas y eficientes en las decisiones respecto de las capacidades humanas y frente a ataques de misiles. Los desarrollos tecnológicos deben continuamente someterse a programas de mejora debido a que los sistemas de ataque enemigos también desarrollan proyectos con dispositivos más difíciles de rastrear y que incluyen el lanzamiento de señuelos que confunden en ocasiones a los sistemas de detección.

La incorporación y uso de satélites para fines de defensa representa una gran ventaja técnica a la hora de detectar el lanzamiento de misiles de largo alcance, lo que permite una mejor y rápida respuesta Adicional a esto, el uso de drones aéreos de ataque con energía directa que invalidan los sistemas de navegación de los misiles, permiten una actuación más temprana y objetiva ante estas amenazas.

REFERENCIAS

[1] J.-U. Kim y M. Kuk-Heug, «A Research on China's ballistic missile modernization and the Terminal High Altitude Area Defense(THAAD) system in Korea", J. China Stud., vol. 21, n.o 4, pp. 139-153, 2018, doi: 10.20288/JCS.2018.21.4.139.
[2] H.-Y. Kim, «A Study on the Effects of Non-Tariff Barriers after THAAD Dispute between Korea and China, KOREA Int. Commer. Rev. vol. 32, n.o 3, pp. 211-230, 2017.
[3] J. Zhang, J. Jiang, y Y. Chen, «Air defense and anti-missile weapons allocation in hierarchical systems under multi-objectives and multi decision-makers condition», Guofang Keji Daxue XuebaoJournal Natl. Univ. Def. Technol., vol. 37, n.o 1, pp. 171-178, 2015, doi: 10.11887/j.cn.201501029.
[4] D. Li, Q. Zhang, X. Li, Y. Xu, y J. Yang, «Architecture modeling for equipment of airborne anti-missile based on DoDAF», Xi Tong Gong Cheng Yu Dian Zi Ji ShuSystems Eng. Electron., vol. 39, n.o 5, pp. 1036-1041, 2017, doi: 10.3969/j.issn.1001-506X.2017.05.14.
[5] J. Yan, W. Pu, H. Liu, S. Zhou, y Z. Bao, «Cooperative target assignment and dwell allocation for multiple target tracking in phased array radar network», SIGNAL Process., vol. 141, pp. 74-83, dic. 2017, doi: 10.1016/j.sigpro.2017.05.014.
[6] E. Blanche, «EI AI to fit anti-SAM system», Janes Missiles Rockets, 2004, [En línea]. Disponible en: https://www.scopus.com/inward/record.uri?eid=2-s2.0-23844544671&partnerID=40&md5=063a401d1853b1bbc442375032cd9f2b
[7] B. Lara, «Europe and the anti-missile defenses», UNISCI Discuss. Pap., vol. 30, pp. 93-109, 2012.
[8] J. Lee, «Korea's THAAD Deployment and China's Retaliation - Implication for China's Obligation under the GATS -", "THAAD, Korean J. Int. Econ. Law, vol. 15, n.o 2, pp. 7-42, 2017, doi: 10.46271/KJIEL.2017.07.15.2.7.
[9] L.-X. Zhao y K. Changgyeong, «["China's Cognition on THAAD Deployment and Improvement of Sino-ROK Relationship", Chin. Stud., vol. 61, pp. 413-424, 2017, doi: 10.14378/KACS.2017.61.61.24.
[10] S. J. Cimbala, «Missile Defenses and Mother Russia: Scarecrow or Showstopper?», Eur. Secur., vol. 16, n.o 3-4, pp. 289-306, sep. 2007, doi: 10.1080/09662830701751133.
[11] A. Sheldon-Duplaix, «Russia-China Naval Partnership and Its Significance», en Russia-China Relations, S. Kirchberger, S. Sinjen, y N. Wörmer, Eds. Cham: Springer International Publishing, 2022, pp. 101-120. doi: 10.1007/978-3-030-97012-3_6.
[12] H. Obering, «Directed Energy Weapons Are Real . . . And Disruptive», Dir. ENERGY WEAPONS, n.o 3, p. 10.
[13] M. N. Mirza, I. H. Qaisrani, L. A. Ali, y A. A. Naqvi, «Unmanned Aerial Vehicles: A Revolution in the Making», South Asian Stud., p. 15.
[14] «SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf». Accedido: 13 de agosto de 2022. [En línea]. Disponible en: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF
[15] «Multi-Object Kill Vehicle (MOKV) – Missile Defense Advocacy Alliance». https://missiledefenseadvocacy.org/defense-systems/multiple-kill-vehicle-mkv/ (accedido 13 de agosto de 2022).

LOS AUTORES

Mayor de Artillería Patricio Xavier Páliz Ochoa, perteneciente al Ejército Ecuatoriano, Jefe de seguridad Integrada de la Brigada de Artillería Nro.27 "PORTETE", pxpaliz@gmail.com, Licenciado en Ciencias Militares de la Escuela politécnica de Fuerzas Armadas "ESPE", Magister en Gerencia y Liderazgo Educacional de la Universidad Técnica Particular de Loja, Jefe de Seguridad en la destrucción de la munición desmilitarizada de la Fuerza Terrestre (2013), Instructor de cadetes en la Escuela Superior Militar "Eloy Alfaro" (2016-2019), Capacitación en Análisis y Gestión de Riesgos para la Seguridad.

Mayor de Material de Guerra Juan Francisco Acosta Bedon del Ejército Ecuatoriano, Comando de Apoyo Logístico Nro. 27 "PORTETE". panchoacosta01@hotmail.com. Maestría en Dirección Logística UNIR (España). Diplomado en Planificación y Gestión de Riesgos y desastres (Chile). Jefe de equipo de inspección y certificación del Ejército de munición calibre mayor y menor desde 2007-2009. Oficial de Material de Guerra del Grupo de Artillería Nro. 7 "CABO MINACHO" desde 2011–2013. Capacitación Logística en la empresa IMI Systems Ltda. 2019 (Israel). Sub comandante del Comando de Apoyo Logístico Nro. 27 "PORTETE". Área de investigación: Sistemas de defensa antiaérea, sistemas logísticos militares, gestión de riesgos y logística humanitaria.

Capitán de Artillería Alexis Tiuma, Ejército Ecuatoriano Oficial de Logística del Grupo de Artillería Lanzadores Múltiples Nro. 80 "CALDERÓN", alexis.tiuma@hotmail.com, Licenciado en Ciencias Militares en la Escuela Politécnica del Ejército, Ingeniero en Mecatrónica en la Universidad de las Fuerzas Armadas – ESPE. (Ecuador) .

Capitán de Artillería Marlon Ricardo Bravo Espinel, Ejército Ecuatoriano, Comando y Estado Mayor de la Brigada de Artillería Nro. 27 "PORTETE". Marlonbrav89@gmail.com.Licenciado en Ciencias Militares Escuela Superior Militar "Eloy Alfaro", Sub comandante de Batería del Grupo de Artillería Nro. 1 "BOLIVAR" (2014-2016), Curso de Centro Director de Tiro Experto de Artillería (Ecuador), Licenciado en Pedagogía de la Actividad Física y Deporte Universidad de Fuerzas Armadas ESPE (Ecuador), Curso de Pedagogía mediado por TIC, Diplomado en Aprendizaje basado en proyectos universidad Politécnica (Colombia), Abogado Universidad Técnica Particular de Loja (Ecuador), Oficial de Cultura física y miembro de la plana mayor especial de la Brigada de Artillería Nro27 "PORTETE".

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.

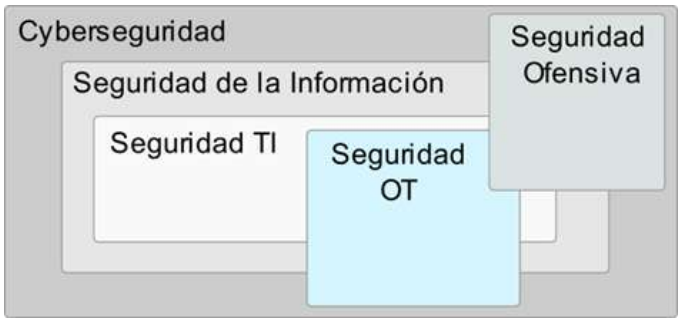


Fig. 1. Ámbitos de acción de la Ciberseguridad

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)

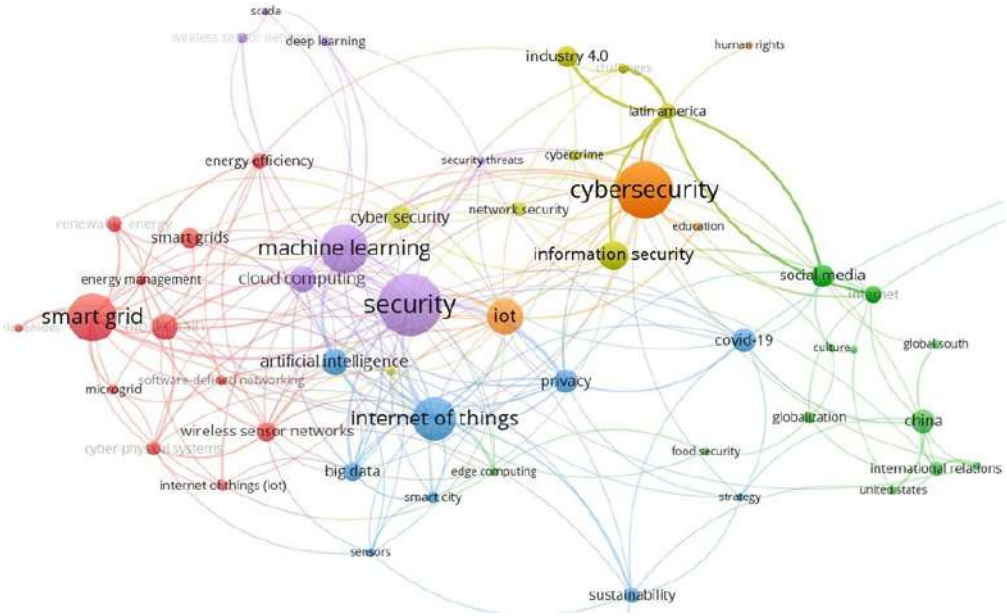


Fig2. Vista Bibliométrica de Estudios relacionados con Ciberseguridad en Latinoamérica

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.

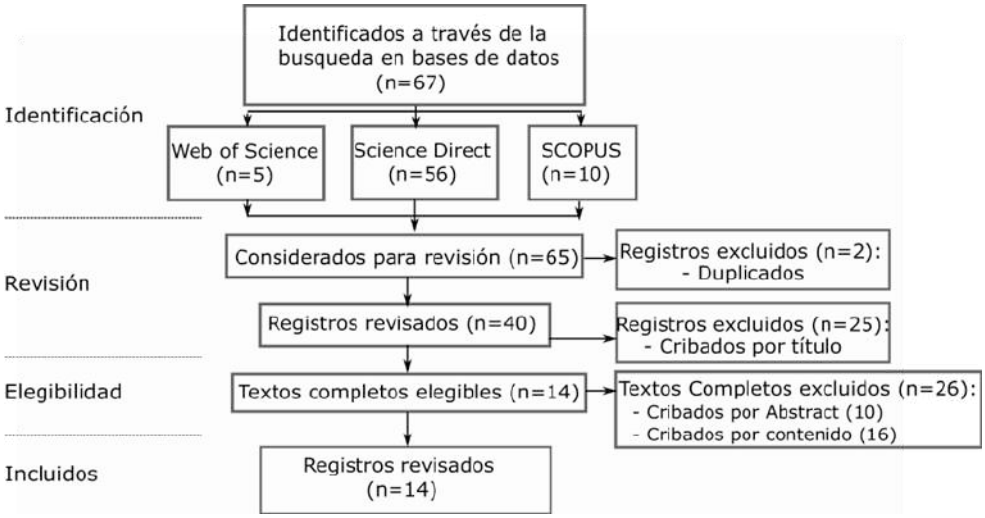


Fig 3. Esquema del proceso de revisión sistemática realizado

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.

$$(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k}$$

$$(1+x)^n = 1 + \frac{nx}{1!} + \frac{n(n-1)x^2}{2!} + \cdots$$

Published by:

AutanaBooks
Engineering & Services