PREVENCIÓN EN CIBERSEGURIDAD: ENFOCADA A LOS PROCESOS DE INFRAESTRUCTURA TECNOLÓGICA

CYBERSECURITY PREVENTION: FOCUSED ON TECHNOLOGICAL INFRASTRUCTURE PROCESSES

Mauricio Rodrigo Cando-Segovia
Egresado de la Maestría en Ciberseguridad
Pontificia Universidad Católica del Ecuador Sede Ambato, (Ecuador).
E-mail: mauricio.r.cando.s@pucesa.edu.ec ORCID: https://orcid.org/0000-0002-6773-5488

Patricio Medina-Chicaiza
Docente de la Escuela de Ingeniería de Sistemas, Pontificia Universidad Católica del Ecuador Sede Ambato.
Grupo de Investigación de Desarrollo Territorial, Empresa e Innovación (DeTEI),
Facultad de Ciencias Administrativas de la Universidad Técnica de Ambato, (Ecuador).
E-mail: pmedina@pucesa.edu.ec / ricardopmedina@uta.edu.ec ORCID: https://orcid.org/0000-0002-2736-8214

Recepción: 28/12/2021 **Aceptación:** 24/12/2021 **Publicación:** 29/03/2021

Citación sugerida:
Cando-Segovia, M. R., y Medina-Chicaiza, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. *3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10*(1), 17-41. https://doi.org/10.17993/3ctic.2021.101.17-41

RESUMEN

En la actualidad, crear conciencia para salvaguardar la información de toda persona o empresa es de vital importancia aun las pequeñas y medias empresas de Latinoamérica no cuentan con personal especializado o se encuentran en proceso de implementación de un departamento de ciberseguridad, El objetivo del presente trabajo es la revisión de la literatura respecto a los procesos relacionados a la prevención ante ciberataques enfocadas a las infraestructuras tecnológicas. Para la recolección de información se revisaron documentos en idioma español e inglés indizados en bases de datos como: Scopus, Scielo, Dialnet, Microsoft Academic Search. Los resultados del estudio se aglutinan en la definición y construcción de buenas prácticas tecnológicas de lo que para algunos autores son las ciberamenazas más populares, se propone acciones necesarias para la prevención de ataques y dan paso a una posible creación de ecosistemas que facilita la innovación y la adopción para las empresas y son aplicables a sus entornos tecnológicos.

PALABRAS CLAVE

Ciberseguridad, Infraestructura tecnológica, Procesos de prevención, Ataques informáticos.

https://doi.org/10.17993/3ctic.2021.101.17-41

ABSTRACT

Currently, raising awareness to safeguard the information of any person or company is of vital importance even small and medium-sized enterprises in Latin America do not have specialized personnel or are in the process of implementing a cybersecurity department, the objective of this work is to review the literature regarding the processes related to the prevention of cyberattacks focused on technological infrastructures. For the collection of information, documents in Spanish and English were reviewed indexed in databases such as: Scopus, Scielo, Dialnet, Microsoft Academic Search. The results of the study are grouped together in the definition and construction of good technological practices of what for some authors are the most popular cyberthreats, necessary actions are proposed for the prevention of attacks and give way to a possible creation of ecosystems that facilitate innovation and adoption for companies and are applicable to their technological environments.

KEYWORDS

Cybersecurity, Technological infrastructure, Prevention processes, Computer attacks.

https://doi.org/10.17993/3ctic.2021.101.17-41

1. INTRODUCCIÓN

La ciberseguridad para Urcuqui *et al.* (2018) es el área de las ciencias de la computación encargada del desarrollo y la implementación de los mecanismos de protección de la información y de la infraestructura tecnológica. En el estudio de Macancela *et al.* (2019), se menciona que los ataques cibernético como phishing o malware son el pan de cada día para los piratas informáticos (hacker), no solo en el Ecuador sino en países con grandes sistemas empresariales; debido al crecimiento que ha tenido la tecnología en la última década desencadenada por la nueva era digital y la globalización ha permitido que el tema de ciberseguridad tome una evolución sin precedentes (Sabillón y Cano, 2019). Si bien, aun es un tema en explotación, este engloba un número incalculable de técnicas y herramientas que hacen frente a los riesgos de la tecnología y la comunicación. A todo esto, se recalca la importancia de la ciberseguridad como factor a invertir y la necesidad de expertos en los que se debe fomentar su formación.

La infraestructura o equipamiento informático (servidores, equipos de red, computadores, juntamente con sus herramientas de administración), es uno de los pilares base de cualquier organización a nivel mundial; la seguridad que se aplica a esta, es un factor clave que mantiene el negocio operativo, la imagen y la integridad de las organizaciones (Chinchilla y Allende, 2017). En su análisis (Gómez y Parra, 2017), menciona que la protección de las infraestructuras tecnológicas que aseguran a los servicios esenciales se ha convertido en una prioridad para las diferentes naciones y organizaciones, se considera la dependencia que se tiene de los mismos y que incrementa exponencialmente año a año. De la misma manera, Roy (2017), señala que la ciberseguridad vela por la preservación de la disponibilidad e integridad de las redes e infraestructuras tecnológicas, y por la preservación de la confidencialidad de la información contenida en éstas.

En su investigación, Almeida y Recalde (2019), mencionan que los países que son parte de la Organización de Estados Americanos frente a estas nuevas amenazas en materia de Ciberseguridad se han formulado algunas estrategias con la participación de la empresa pública, la academia y los organismos estatales crearon los Centros CERT que son Equipos de Respuesta ante Emergencias Informáticas. Según su

https://doi.org/10.17993/3ctic.2021.101.17-41

portal web, el CERT de Ecuador (EcuCERT), abrió sus puertas desde noviembre de 2013 cuyo alcance se enmarca en el ámbito de la aplicación de la Ley Orgánica de Telecomunicaciones (LOT), muestra objetiva de ello es que, tan solo en la primera mitad del 2020, este CERT había trabajado ya sobre doscientos sesenta y dos incidentes reportados sobre activos críticos de nuestro país, y así apoya a las organizaciones afectadas y a la colectividad en general.

Para Sánchez (2017), un ataque informático es la acción o conjunto de acciones ejecutadas por uno o un grupo de individuos que pretenden afectar las características de los activos de información de una organización o una persona. Según el portal de ISO 27001 en español, el riesgo asociado a la seguridad de la información se define como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información". Basado en lo mencionado, toda acción que presente una amenaza que puede ser perjudicial para una organización para lo cual se debe estar preparados con una infraestructura robusta y personal capacitado.

En el estudio realizado por Vega y Ramos (2017) recalcan que para evitar y en el mejor escenario minimizar los ataques e infiltraciones no deseadas, es indispensable implementar medidas de protección y seguridad a la infraestructura tecnológica, adoptar políticas de seguridad informática y diseñar una intranet segura, lo cual solo es posible, a través de un análisis detallado de los distintos protocolos de seguridad, herramientas tecnológicas y aplicaciones informáticas. De igual manera, Reigada (2018), señala que las técnicas de protección contra ciberataques deben proveer la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes a las infraestructuras tecnológicas.

En consecuencia, la situación problemática que se obtiene tras la revisión de la literatura respecto a la prevención en ciberseguridad enfocada en los procesos de infraestructura tecnológica resulta ser: Las pequeñas y medias empresas de Latinoamérica aun no cuentan con personal especializado o se encuentran en proceso de implementación de un departamento de ciberseguridad, lo que conlleva que las organizaciones se encuentren vulnerables ante ataques informáticos. Dado que, asegurar la información y proteger los equipos ya no es una tarea opcional, los beneficiarios directos del estudio son

https://doi.org/10.17993/3ctic.2021.101.17-41

las organizaciones y profesionales del área interesados en fortalecer y garantizar la continuidad de sus servicios, por otro lado, los beneficiarios indirectos son los estudiantes de carreras afines a las tecnologías de la información.

Con los antecedentes señalados, el objetivo de este trabajo es generar un acercamiento teórico que apoye con procesos de prevención en ciberseguridad enfocada a infraestructura tecnológica.

2. METODOLOGÍA

El aporte teórico de este proyecto se apoyó de fuentes de información acreditadas como: libros, artículos científicos (Scopus, Scielo, Dialnet, Microsoft Academic Search), donde se recopiló los documentos más destacados en idioma español e inglés, delimitados a través de palabras claves como: ciberseguridad, infraestructura tecnológica, procesos de prevención, ataques informáticos, por su relevancia y contenido actual. Para ello, se utilizó una metodología similar a la declaración PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Anayses), propuesto por Kitchenham (2004) y Okoli (2010) que sigue una guía de ocho pasos:

1. Establecer el objetivo de la revisión;
2. Protocolo y formación;
3. Indagación de la literatura;
4. Depuración de las publicaciones;
5. Valoración de la calidad;
6. Extracción de datos;
7. Síntesis de los estudios;

https://doi.org/10.17993/3ctic.2021.101.17-41

8. Escritura de los resultados.

Asimismo, el criterio empleado para la selección de artículos estaba sujeto a su aporte en las definiciones relevantes acerca de los conceptos relacionados al objeto de estudio planteado, considerándose los aspectos siguientes: resultados teóricos o empíricos sobre las temáticas principales objeto de estudio, metodología empleada para la prevención en ciberseguridad, resaltándose los enfocados en el análisis de la infraestructura tecnológica; posteriormente, se organizó coherentemente la información encontrada según el tipo de documento, título, autores y aportes destacados basados en el índice de la herramienta tecnológica Perish (Harzing, 2010) que muestra el número de citas para mayor rigurosidad y respaldo científico. Esta metodología, arrojó los siguientes datos:

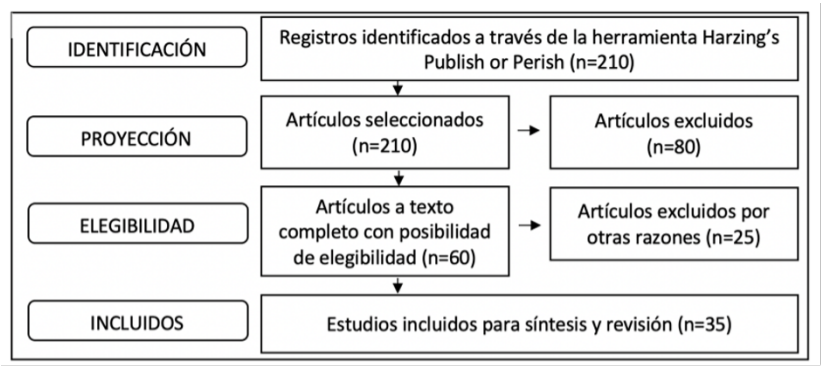

Figura 1. Diagrama de flujo PRISMA.
Fuente: elaboración propia.

3. RESULTADOS

Seguidamente se detallan tres epígrafes: 1.- Principales aportes teóricos en ciberseguridad, surgimiento y desarrollo; 2.- Tendencia, perspectivas y componentes de la ciberseguridad; 3.- Principales aportes de prevención en ciberseguridad enfocadas a los procesos de infraestructura tecnológica.

https://doi.org/10.17993/3ctic.2021.101.17-41

3.1. PRINCIPALES APORTES TEÓRICOS EN CIBERSEGURIDAD, SURGIMIENTO Y DESARROLLO

Con respecto al termino ciberseguridad vale la pena resaltar que la Unión Internacional de Telecomunicaciones aprobó la Resolución 181, donde propuso una definición de ciberseguridad como expresa en la Recomendación UIT-T X.1205, la misma señala que: "La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno…". Por otra parte para algunos autores como Maroto (2009), Carlini (2016), y Sancho (2017) enfatizan que la revolución tecnológica de los últimos años ha acelerado el proceso de globalización, da importancia a la seguridad en el ciberespacio, y se considerada actualmente de interés común, que percibe como mecanismos esenciales el salvaguardar los sistemas informáticos y sobre todo el prevenir las conflagraciones cibernéticas. Por esta razón, Fuentes (2020) menciona en su análisis la importancia de la ciberseguridad y resalta que debe ser tomada muy en serio, además la obligación de abordarla con conciencia y visión estratégica.

Tabla 1. Evolución de la ciberseguridad.

AÑO	SUCESO
600 a 500 ac	Inicios de la criptografía, eruditos hebreos hicieron uso de sencillos cifrados por sustitución monoalfabéticos (como el cifrado Atbash)
1903	El primer hacker de la historia fue Nevil Maskelyne. interceptó la primera transmisión de telégrafo inalámbrico, demostró las vulnerabilidades de este sistema desarrollado por Marconi.

https://doi.org/10.17993/3ctic.2021.101.17-41

1969	Inicios del internet, red por la cual se ha generado millones de ciberataques
1970	John Draper fue el primer ciberdelincuente, mejor conocido como “Captain Crunch”, podía engañar a la señal de la central telefónica y así poder realizar llamadas gratis.
1971	Apareció el primer virus de la historia: Creeper (enredadera), no era un programa malicioso, y simplemente viajaba por la red y replicaba el mensaje “soy una enredadera, atrápame si puedes”.
1980s	Auge de los software maliciosos (malware)
1980	Kevin Mitnick empezó a utilizar la ingeniería social para obtener información personal y datos privados
1986	En Estados Unidos se creó la Computer Fraud and Abuse Act. como una enmienda a la primera ley federal de fraude informático, para abordar el hacking.
1987	Inicios de antivirus, Bernd Robert Fix escribió un programa que neutralizó las capacidades infecciosas y destructivas de un virus.
1988	Surgió La primera propuesta de firewall, o filtro de paquetes, por Jeff Mogul de Digital Equipament Corp (DEC)
1900s	La industria antivirus respondió con productos como McAfee, Norton Antivirus y Kaspersky, que detectaban amenazas en los archivos de un sistema.
1995	Se formó en Europa un comité de expertos en delitos informáticos, lo que llevó a la redacción y aprobación del Convenio sobre Ciberdelincuencia, mejor conocido como Convenio de Budapest.
1995	Secure Sockets Layer (SSL) se creó para cifrar las comunicaciones entre una computadora y un servidor remoto.
2000s	Aparece como una propuesta ambiciosa el Internet de las Cosas o Internet of Things (IoT)
2001	Se aprobó y firmó el Convenio de Budapes, Enfatiza la importancia de crear mecanismos de cooperación internacional contra la cibercriminalidad.
2002	Un ataque de denegación de servicios (DDoS) afectó a 13 servidores de dominio (DNS), dejó fuera de servicio a cinco. Fue el primer intento de deshabilitar Internet.

https://doi.org/10.17993/3ctic.2021.101.17-41

2003	En Estados Unidos en el departamento de Seguridad Nacional establece la División Nacional de Seguridad Cibernética, el primer grupo de trabajo oficial dedicado a la seguridad cibernética.
2003	Aparece Anonymous (grupo más grande de hackers), a través de foros, una comunidad donde cualquier internauta puede publicar contenidos relacionados con un determinado tema.
2008	Conficker un complejo gusano se infiltra en los sistemas operativos de Windows La empresa Microsoft ofreció una suma de 250.000 dólares para quien les facilitase información
2000	ILOVEYOU, un gusano se propagó a través de un correo electrónico, La infección se extendió tan rápidamente que el Pentágono y la CIA apagaron sus sistemas de correo electrónico.
2010	El virus Stuxnet se instalaba en los sistemas, robaba su información y más tarde les ordenaba que se autodestruyeran. Este malware es catalogado como el más desarrollado e innovador hasta la fecha.
2010s	Los dispositivos móviles se vuelven un blanco ideal para los ciberdelincuentes
2013	Yahoo sufrió una violación que finalmente resultó en el robo de datos personales de 3 billones de usuarios, No reportó la infracción hasta 2016.
2014	Se acuñó el término Internet Industrial de las Cosas, en ingles Industrial Internet of Things (IIoT), Industrial Internet Consortium junto con Cisco, IBM, AT&T e Intel.
2014	El Consorcio de Internet Industrial, se centra en la creación de estándares que promueven la interoperabilidad abierta y el desarrollo de arquitecturas comunes.
2017	Equifax (empresa que almacena los historiales crediticios) anunció que los datos personales de hasta 143 millones de personas se habían visto comprometidos.
12-may-17	Sucedió el mayor ataque de la historia, denominado “Wannacry”, que afectó más de 200 mil computadores en cerca de 120 países en todo el mundo, dicho ataque fue un ramsomware, que es un secuestro de información, a través del cual, el ciberdelincuente encripta la información y solicita dinero para restaurarla.
2020	Con el teletrabajo, el uso compartido de la información en la nube y el IoT los riegos amplían su alcance, el riesgo ahora está en casa

Fuente: elaboración propia.

https://doi.org/10.17993/3ctic.2021.101.17-41

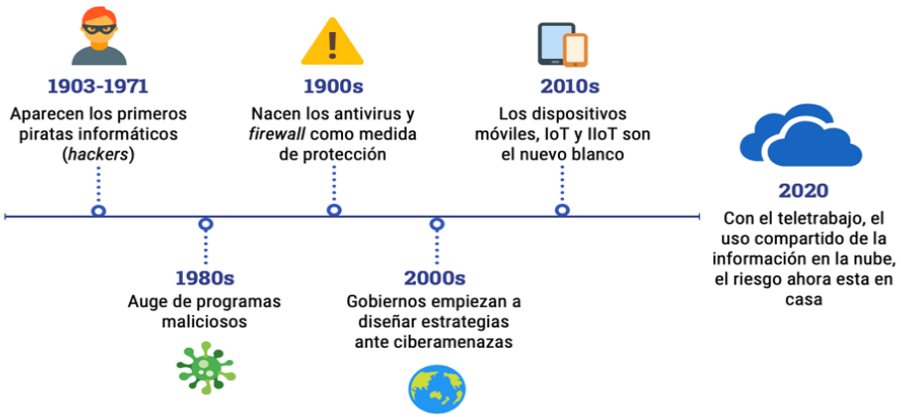

Figura 2. Línea de tiempo de la ciberseguridad.
Fuente: elaborado en infograph.venngage.com (2020).

Con respecto a que la ciberseguridad cada día va desarrollándose y abarca nuevos territorios, existen actualmente documentos de prospectiva en este campo. Cano (2020) concluye que las tendencias emergentes en este ámbito podrán ser los ecosistemas digitales, dinero digital, ciberconflictos, educación 4.0. Por esta razón, Martínez (2018), Patiño y Ramírez (2019) y Gallardo (2020) mencionan que es imprescindible mantener el mismo ritmo de innovación en ciberseguridad para poder adoptarse a las nuevas tecnologías sin superar un nivel de riesgo aceptable. La ciberseguridad está en vías de desarrollo, por ende se debe tener un crecimiento como mínimo igual al del desarrollo de nuevas tecnologías para poder adoptar estas de manera segura. Al invertir en tecnologías, las organizaciones están en el deber de realizar una inversión proporcional en ciberseguridad para los riesgos asociados a su implantación.

3.2. TENDENCIA, PERSPECTIVAS Y PRINCIPALES AMENAZAS DE LA CIBERSEGURIDAD

Es evidente que los términos ciberseguridad, ciberataques, ciberdelincuentes, entre otros se han popularizado hasta el punto de convertirse para algunos sectores en una prioridad, en sus estudios Ballestero (2020) y Vázquez (2020) coinciden que la crisis provocada por la pandemia del patógeno

https://doi.org/10.17993/3ctic.2021.101.17-41

COVID-19 ha puesto en evidencia la vulnerabilidad de nuestras sociedades y ha incitado al uso de medios digitales para realizar diversas actividades que van desde el teletrabajo, educación e incluso sesiones parlamentarias, y se confirma que el ciberespacio es el lugar más poblado del planeta, este es un entorno sin fronteras, interactuado por casi el 60% de la población (más de 4.500 millones de personas), resistiéndose a cualquier definición de una ley tradicional.

Seguidamente se integra, mediante un cuadro resumen, la definición de los ciberataques más comunes realizados a empresas e instituciones, a través del aporte de autores como: 1. Armas (2018), 2. Ballestero (2020), 3. Benavides *et al.* (2020), 4. Chesney *et al.* (2021), 5. Covarrubias y Zadamig (2020), 6. Latam Kaspersky (2020).

Tabla 2. Ciberataques más populares según varios autores.

Ciberataque	Definición	1	2	3	4	5	6	TOTAL
1.Ransomware	Es un *software* que infecta a las computadoras y muestra mensajes que exigen el pago de dinero para restablecer el acceso a la misma.	x	x	x		x	x	5
2. Ataques a dispositivos IoT	El Internet de las cosas (IoT) es todo objeto físico, vehículos, electrodomésticos entre otros que comparte datos a través de Internet.		x		x		x	3
3. Phishing e ingeniería social	Es la combinación de Ingeniería Social y exploits técnicos, diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante, atreves de una página web falsa.	X	X	X		X	X	5

https://doi.org/10.17993/3ctic.2021.101.17-41

4. Ataque a redes LAN inalámbricas	Con su traducción al inglés wireless attack, este ataque se basa en utilizar herramientas conjuntamente con ingeniera social para tratar de acceder a una red inalámbrica y muy posiblemente acceder a otros equipos.		X		X		X	3
5. Ataque de denegación de servicio (DOS o DDOS)	DoS (Denial-of-service attack) es un ataque que busca privar a los usuarios de acceso a su red o equipo. La evolución de esta amenaza son los ataques de negación de servicio distribuido (DDoS) que se provocan al generar grandes cantidades de información desde varios puntos de forma voluntaria, para que el usuario o la organización se vean privados de un recurso.		X		X			2
6. Suplantación de identidad y Sybil	Es la modalidad mediante la cual una persona suplanta a otra en la titularidad de un derecho con un fin en particular, mediante un medio electrónico.	X		X		X	X	4
7.Otros malware	El término “programa malicioso” se refiere a un software que daña dispositivo, roba datos, exististe una variedad como: virus, troyanos, spyware, backdoor y demás.	X	X	X	X	X	X	6

Fuente: elaboración propia en base a la literatura investigada.

https://doi.org/10.17993/3ctic.2021.101.17-41

Figura 3. Nube de palabras de ciberataques.
Fuente: elaboración propia.

En la Tabla 2, se evidencia la definición de los ataques informáticos más populares y se concuerda con los autores antes enunciados, pues se recomienda dichos eventos a ser considerados para su prevención por las organizaciones o el personal; conviene resaltar que las amenazas mediante programas maliciosos son las que más sobresalen en dichas investigaciones.

En conclusión, las ciberamenazas han llegado a ser el mayor reto para la sociedad moderna, hasta el punto de que ninguna empresa o persona está a salvo en su totalidad, cada día existen nuevas e innovadoras formas de vulneración. Para McIntosh *et al.* (2021) los ataques se deben en parte a la falta de un control de acceso adecuado a nivel de los sistemas, equipos tecnológicos y de la información, por otra parte, los estudios de Ben-Yaakov *et al.* (2020) y Fitni y Ramli (2020) defienden la idea de contar con buenas políticas en los equipos perimetrales (firewall), antivirus, sistemas de detección de intrusos (IDS) y juntamente con una buena capacitación al personal son el arma ideal para minimizar el riesgo de un evento malicioso.

https://doi.org/10.17993/3ctic.2021.101.17-41

3.3. PRINCIPALES APORTES DE PREVENCIÓN EN CIBERSEGURIDAD ENFOCADAS A LOS PROCESOS DE INFRAESTRUCTURA TECNOLÓGICA

A lo largo de los tiempos se han generado algunas técnicas, desarrollo de herramientas y fabricación de equipos para evitar que eventos maliciosos ocurran, mucho se menciona que ninguna red es segura en su totalidad, siempre puede existir fuga de información e incluso si se posee los equipos más sofisticas; en conclusión los atacantes utilizan cualquier método que este a su alcance para materializar la agresión, el papel que actúa todo el personal de una organización es vital, y por eso se recalca su capacitación constante en el ámbito de seguridad informática.

A continuación, mediante tablas se muestran los aportes de prevención en ciberseguridad de los ataques mencionados en la Tabla 2 según autores como: Hwang *et al.* (2008), Suriya *et al.* (2009), Chinchilla y Allende (2017), Caro *et al.* (2019), Dahan (2020), Baumann *et al.* (2021), Chesney *et al.* (2021), Han *et al.* (2021), Liu *et al.* (2021), Satapathy *et al.* (2021), Somani *et al.* (2017), y Yang *et al.* (2021):

Tabla 3. Aportes de prevención en ciberseguridad.

Ataque informático 1: *Ransomware* (programa de secuestro)
Afectados: Equipos de cómputos, servidores, información, organizaciones, aplicaciones, servicios.
Factores relevantes: El atacante solicita un rescate económico (bitcoins) a cambio de devolver el acceso a información o liberación de equipos bloqueados. La forma más común de trasmisión es a través de un correo electrónico, suele venir camuflado en un archivo ordinario o un enlace a un sitio malicioso.

https://doi.org/10.17993/3ctic.2021.101.17-41

Aportes de prevención:
Para contrarrestar este tipo de ataques la mejor solución es contar con un proceso de respaldo frecuente de la información, las técnicas de encriptación de la mayoría de los ransomware son muy complejas, a menos que se realice el pago, los datos no se recuperaran e incluso si la victima opta por desembolsar el dinero, no se garantiza su recuperación, A pesar de que actualmente existen aplicaciones anti-ransomware que detecta, detiene y elimina estas amenazas de un sistema informático, y muy probable sean una de las mejores opciones si queremos invertir en seguridad para nuestra organización, estas no cubren la gran variedad de programas maliciosos que salen a la luz cada día.
En conclusión, negociar con el atacante no es una opción recomendada, la mejor herramienta siempre será la prevención.

Ataque informático 2:
Ataques a dispositivos a Internet de las cosas (IoT)

Afectados:
Dispositivos móviles, hogares, organizaciones, servicios, información.

Factores relevantes:
Más de 25 mil millones de dispositivos IoT conectados en el 2020.
A la fecha el IoT ha llegado a la industria, agricultura, transporte, entre otros.

Aportes de prevención:
Con el objetivo de dar una propuesta para proteger los dispositivos IoT, se detalla cinco factores claves:
Autenticación robusta: brinda una mayor seguridad a los dispositivos y determina las fuentes de comunicación, de esta manera se reduce la variedad de ataques y así enfocarse en los basados en la identidad (suplantación de identidad y ataques *Sybil*).
Control de acceso físico: evitar que usuarios no autorizados accedan a los recursos de IoT.
Descarga segura: permitir que los dispositivos IoT utilicen únicamente los recursos informáticos indispensables, acceso únicamente a servidor de red troncal y limitar el recurso a la red externa.
Detección de *malware*: proteger el dispositivo de virus que pueden agotar la energía, inhibir el rendimiento de la red y provocar fugas de datos, en el mercado existe una variedad de antivirus de como son Kaspersky, ESET NOD32, McAfee, Norton, entre otros.
Actualización del software: La mayoría de los ataques exitosos tiene mucho que ver con la falta de actualización de los productos de software de los equipos, estas actualizaciones son liberadas periódicamente por los fabricantes de los dispositivos.

Ataque informático 3:
Phishing e ingeniería social

Afectados:
Datos personales, organizaciones, hogares, entidades bancarias.

Factores relevantes:
Está técnica esta dirigida al usuario final enfocada en recursos web.
El agresor publica una versión falsificada del sitio, que, de ser visitado por el usuario este comprometa su identidad.
Un 70% de páginas falsas son de entidades bancarias, que cuesta a las víctimas miles de millones de dólares cada año

https://doi.org/10.17993/3ctic.2021.101.17-41

Aportes de prevención:
Este ataque es muy popular y no es necesario tener muchos conocimientos informáticos para prevenirlo, verificar la barra de navegación del explorador de internet es la forma más sencilla de confirmar la veracidad del sitio, una página web de una institución confiable posee un certificado digital, el cual debemos verificar y esta ha de empezar con https:// y un pequeño candado cerrado que debe aparecer en la barra de estado de nuestro navegador. Hoy en día es obligación de toda institución, en especial de una entidad financiera brindar a sus clientes este servicio y es obligación del cibernauta verificarlo antes de la entrega de cualquier información.
Por otra parte, también es importante recalcar que ninguna entidad solicita datos personales mediante correo electrónico, en caso de sospechar que fue víctima de phishing, cambie inmediatamente todas sus contraseñas y póngase en contacto con la empresa o entidad financiera para reportar esta novedad.

Ataque informático 4:
Ataque a redes LAN inalámbricas

Afectados:
Equipos de cómputos, redes inalámbricas, información, organizaciones, hogares.

Factores relevantes:
La mayoría de las redes domésticas y empresariales posean una red inalámbrica en sus infraestructuras.

Aportes de prevención:
El factor para considerar en este ataque radica en la vulnerabilidad de administración de claves por lo que da paso a los ataques de rastreo, suplantación de identidad, DoS o hombre en el medio, no muy diferente a las redes LAN cableada, para mejorar las fallas de seguridad del protocolo de autenticación / cifrado de redes inalámbricas se sugiere la adopción del estándar 802.1x, TKIP (Protocolo de integridad de clave temporal), estándares de cifrado avanzado.
En caso de que las contraseñas y protocolo de encriptación sean débil, para los ataques se convierte en un juego de niños lograr vulnerarlas, una vez dentro de la red, la tarea se vuelve más fácil para acceder a la información.

Ataque informático 5:
Ataque de denegación de servicio (DoS o DDoS)

Afectados:
Equipos de cómputos, servidores, información, organizaciones, aplicaciones, servicios.

Factores relevantes:
DoS ataca desde un origen, mientras que los DDoS son varios botnets situados en diferentes lugares que intentan colapsar equipos o servicios.
Los ataques DoS o DDoS pueden atacar vectores como TCP, HTTP, HTTPS y SSL.

https://doi.org/10.17993/3ctic.2021.101.17-41

Aportes de prevención:
Se puede resaltar que existen varios mecanismos para la detección y prevención de este tipo de ataques, los principales son los sistemas de detección de intrusiones (IDS) y el sistema de prevención de intrusiones (IPS). IDS está correlacionado con *hardware* y *software* estos ayudan a detectar y recodificar actividades anómalas. Las funciones de IPS son similares a las de IDS; aunque es más sofisticadas, están diseñados para tomar las acciones necesarias para prevenir las actividades maliciosas.
Por otra parte, si el objetivo es salvaguardar algún sistema web, un *CAPTCHA* es una buena opción, esta es una especie de barrera que desafía mediante una identificación de imágenes o textos, con el fin de confirmar que el acceso sea de personas y mas no de los programas de software automatizados.

Ataque informático 6:
Suplantación de identidad (*spoofing attack y Sybil*)

Afectados:
Equipos de cómputos, servidores, información, organizaciones, aplicaciones, servicios.

Factores relevantes:
Los ataques de suplantación de identidad representan la amenaza más grave para los sistemas de verificación automática.
Existen variaciones de este ataque tales como: email *spoofing, sybil, ip spoofing*.

Aportes de prevención:
Para algunas empresas o entidades bancarias para acceder a sus sistemas es necesario ingresar el tradicional usuario y clave, como segundo factor de autentificación se suele enviar un correo electrónico o un *sms*, esta práctica ha permitido que la suplantación de identidad o en inglés *spoofing attack* haya evolucionado.
La biometría se usa a menudo en los sistemas de autenticación y está en muchas aplicaciones informáticas, en algunos casos no se garantiza que pueda ser eficiente o seguras, la implementación de sistemas con más de un rasgo biométrico se ha popularizado y se convertirte en una propuesta para solventar este problema.
El sistema de autenticación más utilizado es el reconocimiento facial, debido a sus complejos algoritmos para detección de rostros, especialmente en los nuevos dispositivos móviles.

Ataque informático 7:
Otros malware

Afectados:
Equipos de cómputos, servidores, información, organizaciones, aplicaciones, servicios, dispositivos móviles.

https://doi.org/10.17993/3ctic.2021.101.17-41

Factores relevantes: Algún virus, troyano, *botnet*, entre otros ha afectado en algún momento a todos los cibernautas. Existe variedad de *malware* para la mayoría de los sistemas informáticos.
Aportes de prevención: Se han realizado estudios considerables sobre la detección de *malware* debido a sus crecientes desafíos para la seguridad del ciberespacio, la mejor opción contra un programa malicioso es una protección de antivirus eficaz, incluso puede identificar y advertir amenazas previamente desconocidas en función de las técnicas típicas del virus, por ejemplo, intentar esconderse en la computadora, estos programas se ejecutan en tiempo real para detectar cualquier proceso sospecho. La detección de ataques se debe basar incluso en un análisis de tráfico, detección basada en asociación de eventos de seguridad y detección basada en minería de inteligencia de amenazas, este trabajo la puede realizar equipos como los IDS, IPS o *firewalls*. Se evidencia que los piratas informáticos observan las vulnerabilidades de los procesos de aprendizaje automático de los *softwares* antivirus para crear programas maliciosos mejorados.

En la Tabla 3 se evidencia que al igual que existen una variedad de ataques, las técnicas de prevención son variadas y robustas, es importante mencionar que todos autores recalcan que el mejor método de prevención ante cualquier amenaza es la prevención; de igual manera los antivirus, equipos de protección como IDS, IPS, equipos perimetrales, estrategias como monitoreo constante de nuestro equipamiento tecnológico, cambio frecuente de contraseñas ayudan a minimizar posibles vulnerabilidades, cuantificar la efectividad de nuestras infraestructuras contra ciberamenazas es un trabajo obligatorio para cada empresa o persona en la actualidad.

4. CONCLUSIONES

El análisis de la literatura permitió desarrollar el marco teórico que sustenta fundamentos, evolución y desarrollo del campo de la ciberseguridad, cabe mencionar que este tema ha sido objeto de estudio a nivel mundial por la trascendencia e importancia que ha alcanzado, esto confirma que su adopción aun esta en desarrollo.

De los múltiples ciberataques existentes hoy en día, se abordaron para su estudio los siguientes: ataques ransomware, ataques a dispositivos IoT, phishing e ingeniería social, ataque a redes LAN inalámbricas,

https://doi.org/10.17993/3ctic.2021.101.17-41

ataque de denegación de servicio (DOS o DDOS), suplantación de identidad y Sybil y otros malware, debido a la ocurrencia en ciberespacio, frecuencia y relevancia que los autores dan a los mismos. En este sentido, se realizó algunas sugerencias que dan paso a una posible creación de ecosistemas que facilita la innovación y la adopción por parte de las empresas a las tecnologías propuestas.

Las técnicas de prevención ante ciberamenazas surgen como una alternativa para contrarrestar eventos maliciosos y además brindar a los usuarios herramientas que otorgan confianza para navegar en el ciberespacio. Como consecuencia, se propuso acciones necesarias para la lucha de los ataques mencionados. Finalmente, la necesidad de un esfuerzo multidisciplinario de todas las personas de una organización es relevante, ya que existe un surgimiento continuo de ciberatacantes y ciberamenazas.

REFERENCIAS BIBLIOGRÁFICAS

Almeida, C. A. T., y Recalde, L. (2019). La ciberseguridad en el ecuador, una propuesta de organización. *Revista de Ciencias de Seguridad y Defensa, IV*(7), 156-169. http://geo1.espe.edu.ec/wp-content/uploads/2019/03/7art12.pdf

Armas, J. A. (2018). Ciberseguridad: Como adoptar medidas para proteger sus activos de información. *Review of Global Management,* 4(2), 20-21. https://doi.org/10.19083/rgm.v4i2.1127

Ballestero, F. (2020). La ciberseguridad en tiempos difíciles. *Boletín Económico de ICE, 3122*, Article 3122. https://doi.org/10.32796/bice.2020.3122.6993

Baumann, R., Malik, K. M., Javed, A., Ball, A., Kujawa, B., y Malik, H. (2021). Voice spoofing detection corpus for single and multi-order audio replays. *Computer Speech & Language, 65*, 101132. https://doi.org/10.1016/j.csl.2020.101132

https://doi.org/10.17993/3ctic.2021.101.17-41

Benavides, E., Fuertes, W., y Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: Una revisión sistemática de la literatura. *Ciencia y Tecnología, 13*(1), 97-104. https://doi.org/10.18779/cyt.v13i1.357

Ben-Yaakov, Y., Meyer, J., Wang, X., y An, B. (2020). User detection of threats with different security measures. *2020 IEEE International Conference on Human-Machine Systems (ICHMS)*, 1-6. https://doi.org/10.1109/ICHMS49158.2020.9209426

Cano, J. J. (2020). Retos de seguridad/ciberseguridad en el 2030 : *Sistemas, 154,* 68-79. https://doi.org/10.29236/sistemas.n154a7

Carlini, A. (2016). Ciberseguridad: Un nuevo desafío para la comunidad internacional. *bie3: Boletín IEEE, 2 (Abril-junio),* 950-966.

Caro, A., García, L. J., y Sandoval, A. L. (2019). *Actas de las V Jornadas Nacionales de Ciberseguridad Junio 5-7, 2019, Cáceres, España*. Universidad de Extremadura, Servicio de Publicaciones. http://dehesa.unex.es/handle/10662/9443

Chesney, S., Roy, K., y Khorsandroo, S. (2021). Machine Learning Algorithms for Preventing IoT Cybersecurity Attacks. En K. Arai, S. Kapoor, y R. Bhatia (Eds.), *Intelligent Systems and Applications* (Vol. 1252, pp. 679-686). Springer International Publishing. https://doi.org/10.1007/978-3-030-55190-2_53

Chinchilla, E. J. S., y Allende, J. S. (2017). Riesgos de ciberseguridad en las Empresas. *Tecnología y desarrollo, 15*(0), Article 0. https://revistas.uax.es/index.php/tec_des/article/view/1174

Covarrubias, L., y Zadamig, J. (2020). *Las tres "C" de los Estados Contemporáneos: Ciberespacio, Ciberseguridad y Contrainteligencia. (The Three «c» of the Contemporary States: Cyberspace, Cybersecurity and Counterintelligence)* (SSRN Scholarly Paper ID 3649221). Social Science Research Network. https://doi.org/10.2139/ssrn.3649221

Dahan, A. (2020). *System and method for blocking ransomware infections* (United States Patent N.o US10607009B2). https://patents.google.com/patent/US10607009B2/en

Fitni, Q. R. S., y Ramli, K. (2020). Implementation of Ensemble Learning and Feature Selection for Performance Improvements in Anomaly-Based Intrusion Detection Systems. En *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, 118-124. https://doi.org/10.1109/IAICT50021.2020.9172014

Fuentes, E. M. (2020). Ciberseguridad y su Importancia en el Sector Salud: La experiencia de Madrid digital. *I+S: Revista de la Sociedad Española de Informática y Salud, 139*, 13-15.

Gallardo, S. (2020). Diez años más tarde: Retos y amenazas a la seguridad y ciberseguridad en 2030. *Sistemas, 155,* 61-80. https://doi.org/10.29236/sistemas.n155a5

Gómez, F. S., y Parra, J. L. (2017). Cooperación público-privada en la protección de infraestructuras críticas. *Cuadernos de estrategia, 185,* 171-216.

Han, W., Xue, J., Wang, Y., Zhang, F., y Gao, X. (2021). APTMalInsight: Identify and cognize APT malware based on system call information and ontology knowledge framework. *Information Sciences, 546,* 633-664. https://doi.org/10.1016/j.ins.2020.08.095

Hwang, H., Jung, G., Sohn, K., y Park, S. (2008). A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP. En 2*008 International Conference on Information Science and Security (ICISS 2008),* 164-170. https://doi.org/10.1109/ICISS.2008.10

Latam Kaspersky. (2020). *Karspersky daily.* https://latam.kaspersky.com/blog/

Liu, M., Wang, L., Dang, J., Lee, K. A., y Nakagawa, S. (2021). Replay attack detection using variable-frequency resolution phase and magnitude features. *Computer Speech & Language, 66,* 101161. https://doi.org/10.1016/j.csl.2020.101161

Macancela, E. R. Z., Ramírez, Á. A. A., Berrones, W. J. R., y Baque, C. J. S. (2019). Análisis de la seguridad de la información en las Pymes de la ciudad de Milagro. *Universidad y Sociedad, 11*(4), 487-492.

Maroto, J. P. (2009). *El ciberespionaje y la ciberseguridad.* La violencia del siglo XXI. Nuevas dimensiones de la guerra, pp. 45-76. https://dialnet.unirioja.es/servlet/articulo?codigo=4549946

Martínez, J. G. (2018). Innovación en ciberseguridad. Estrategias y tendencias. *Economía industrial, 410,* 47-56.

Patiño, A. M. S., y Ramírez, D. P. G. (2019). Análisis de la capacidad de ciberseguridad para la dimensión tecnológica en Colombia: *Ingeniería Solidaria, 15*(2), 1-30. https://doi.org/10.16925/2357-6014.2019.02.07

Reigada, A. T. (2018). Del principio de seguridad de los datos al derecho a la seguridad digital. *Economía industrial, 410,* 127-151.

Roy, A. M. (2017). La ciberseguridad, el auditor externo y los OCEX. *Auditoría pública: revista de los Organos Autónomos de Control Externo, 70,* 27-38.

Sabillón, R., y Cano, J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. RISTI - *Revista Ibérica de Sistemas e Tecnologias de Informação, 32,* 33-48. https://doi.org/10.17013/risti.32.33-48

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

Satapathy, S. C., Bhateja, V., Janakiramaiah, B., y Chen, Y.-W. (Eds.). (2021). *Intelligent System Design: Proceedings of Intelligent System Design: INDIA 2019* (Vol. 1171). Springer Singapore. https://doi.org/10.1007/978-981-15-5400-1

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., y Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications, 107,* 30-48. https://doi.org/10.1016/j.comcom.2017.03.010

Suriya, R., Saravanan, K., y Thangavelu, A. (2009). An integrated approach to detect phishing mail attacks: A case study. Proceedings of the *2nd International Conference on Security of Information and Networks - SIN '09*, 193. https://doi.org/10.1145/1626195.1626244

Urcuqui, C. C., Navarro, A., Osorio, J. L., y García, M. (2018). *Ciberseguridad: Un enfoque desde la ciencia de datos.* Editorial Universidad Icesi. https://repository.icesi.edu.co/biblioteca_digital/handle/10906/84046

Vázquez, F. M. (2020). Ciberseguridad y Estado autonómico. icade. *Revista de la Facultad de Derecho, 109*, 1-19. https://doi.org/10.14422/icade.i109.y2020.001

Vega, G., y Ramos, R. A. (2017). Vulnerabilidades y amenazas a los servicios web de la intranet de la Universidad Técnica de Babahoyo. *3C Tecnología.Glosas de innovación aplicadas a la pyme, 6*(1), 53-66. https://doi.org/10.17993/3ctecno.2016.v5n4e20.53-66

Yang, X.-S., Sherratt, S., Dey, N., y Joshi, A. (Eds.). (2021). *Proceedings of Fifth International Congress on Information and Communication Technology: ICICT 2020,* London, Volume 2 (Vol. 1184). Springer Singapore. https://doi.org/10.1007/978-981-15-5859-7

https://doi.org/10.17993/3ctic.2021.101.17-41