Ataques informáticos en tiempos de pandemia COVID-19 en Latinoamérica: Revisión Bibliográfica

Bibliographic review of the most frequent computer attacks in times of the COVID pandemic in Latin America

Autores: Ormaza Calderón Jonathan Geovanny, López Mora Christian Israel, Muñoz Ríos Lelis Javier, Aura Dolores Zambrano Rendón.

jonathan.ormaza@espam.edu.ec,
christian.lopez@espam.edu.ec,
lelis.munoz@espam.edu.ec,
azambrano@espam.edu.ec

Resumen

Este artículo tiene como objetivo realizar una investigación sobre los ataques informáticos más frecuentes en tiempos de pandemia COVID-19 en Latinoamérica. La revisión bibliográfica sistematizada tuvo un rol importante ya que se empezó estableciendo los criterios de búsqueda, en este caso seguridad informática, ataques cibernéticos y riesgos digitales, para definir el conjunto de documentos que serían analizados, lo que permitió obtener fuentes claves, mismas en las que se logró identificar cuáles fueron estos ataques y con un oportuno análisis de la información recabada se pudo notar cómo la terrible situación por la que estaban atravesando los países influenció a que se agravaran los delitos digitales. Posteriormente, se consiguió crear esquemas en los que se muestre y explique con mayor claridad los resultados obtenidos en este trabajo, los cuales fueron una tabla en la que están los artículos y tesis seleccionados para luego en otra tabla colocar la frecuencia en la que estaban cada uno de los ataques focalizados.

Palabras clave: Seguridad informática, amenazas, ciberseguridad, pandemia.

Abstract

The objective of this article was to carry out an investigation on the most frequent computer attacks in times of the COVID-19 pandemic in Latin America. The systematized bibliographic review played an important role since it began by establishing the search criteria, in this case computer security, cyber-attacks and digital risks, to define the set of documents that would be analyzed, which allowed obtaining key sources, same in the that it was possible to identify what these attacks were and with a timely analysis of the information collected, it was possible to notice how the terrible situation that the countries were going through influenced the worsening of digital crimes. Subsequently, it was possible to create schemes in which the results obtained in this work are shown and explained more clearly, which were a table in which the selected articles and theses are, and then in another table, place the frequency in which each was found. one of the targeted attacks.

Keywords: Computer security, threats, cybersecurity, pandemic.

1. Introducción

En el mundo moderno, donde la información se transmite utilizando las computadoras y las redes, el internet se ha convertido en el principal medio del avance económico, político y social. La vida cotidiana de las personas se ha adaptado a las nuevas tecnologías de la información; así también se ha abierto un nuevo campo de ataques del tipo informático por los denominados “Piratas informáticos o ciber criminales”, que, debido al uso indebido de la tecnología, no se limitan al mismo, por lo que se ponen en alto riesgo a las sociedades de la actualidad (Alvarado, 2020).

Es importante acotar que hay momentos en los que las naciones se vuelven más vulnerables y por esta instancia pasaron los países de Latinoamérica en el tiempo de pandemia.

“La pandemia de COVID-19 creo crisis complejas y asimétricas a nivel mundial y en América Latina: sanitaria, económica y social. Por otro lado, la región presenta debilidades estructurales, lo que genera serias dificultades para enfrentar el triple desafío de contención epidemiológica, recuperación económica y mitigación de costos sociales.” (Filgueira et al., 2020).

Años de poca estabilidad económica debido a varios sectores que tienen problemas en la productividad y un modelo de mercado de trabajo segmentado, perdidas de inversión y la demanda agregada en las etapas finales del ciclo económico regional, y niveles de pobreza y desigualdad que reflejan mejoras en las primeras etapas. La década del siglo llano es irreversible, y las condiciones de habitabilidad y acceso a los servicios básicos socavan nuestra capacidad para afrontar adecuadamente estos retos. (Filgueira et al., 2020).

El COVID-19 ha supuesto un difícil contraste en la actualidad, logrando que la sociedad sea consciente de lo frágil que es y de lo rápido que puede cambiar el su ámbito, pero la pandemia y los riesgos potenciales van mucho más de lo que tenemos en mente. Los bloqueos impuestos por COVID-19 en varios países han afectado el uso de plataformas digitales, las ventas en línea, el monitoreo de la salud de empleados y terceros(Zanotti, 2020).

Varios piratas informáticos o ciber criminales han logrado identificar las vulnerabilidades que existen en el mundo tecnológico y han aprovechado la pandemia de COVID-19 para lanzar varios de los llamados ciberataques. En particular, mucho malware el cual ha estado relativamente inactivo desde que aparecieron estos han sido redescubierto y adoptado nuevas formas, sus creadores están usando COVID-19 para amplificar aún más sus tácticas de ingeniería social. (Interpol, 2020).

Se entiende por tanto que este fenómeno sobrenatural está poniendo a prueba formas de trabajo tal y como las conocíamos hace apenas unas semanas. Estamos ante una implantación a gran escala del trabajo remoto y con ella vienen una serie de cambios en los protocolos ya establecidos dentro de límites seguros. Es decir, el trabajo se monitorea desde una oficina conectada a una red segura, generalmente desde el área de sistemas u otra área controlada. Cuando se trata de ataques cibernéticos, más que nunca, las personas enfrentan escenarios extremadamente peligrosos en sus hogares y oficinas. (Zanotti, 2020).

Encontrándose a la cabeza de las búsquedas ataques como Malware, Phishing y Ransomware ya que son los más utilizados por quienes se aprovechan de la situación para atacar a los más débiles, informáticamente hablando, y con mucha más razón por el escenario en el que se han puesto gracias a la pandemia.

Por esto nace la problemática de querer cerciorarse cuantos, y cuales más fueron los ataques informáticos más frecuentes, para lo que se procederá a revisar información bibliográfica y realizar un análisis de esta con el fin de llegar a demostrar con fuentes válidas el propósito de este trabajo.

2. Materiales y Métodos

Para llevar a cabo esta indagación se implementó una revisión bibliográfica sistematizada, misma que corresponde a una serie de valores académicos que ayudan a distinguir oportunidades investigativas que posibilita hacer nuevas aportaciones o innovaciones en un cierto tema examinado.
Por medio de este método se puede obtener un banco de documentos que previamente han sido seleccionados de fuentes confiables como pueden ser las bases de datos académicas, permitiendo así obtener esquemas claros para el análisis de los mismos y logrando a la vez presentar los resultados alcanzados usando diferentes estrategias (Codina, 2020).

Para el trabajo objeto de estudio se realizó 4 fases, tal como lo expresa Codina (2020):

- Se empezó estableciendo los criterios de búsqueda para definir el conjunto de artículos a evaluar; se utilizaron los términos: seguridad informática, ataques cibernéticos y riesgos digitales, COVID-19. Como fuente confiable para extraer los documentos se utilizó Google Académico, Redalyc, Scielo, Emerald, Scopulus aplicando además un filtro desde el año 2020 hasta el presente, para delimitar la indagación al periodo de tiempo donde la pandemia afectó más a Latinoamérica.
- Luego se procedió a examinar los trabajos encontrados para decretar si los mismos eran aptos para constituirse como evidencia relevante mediante una evaluación rigurosa que detectara su validez para formar parte del banco de documentos.
- El siguiente paso fue diseñar un esquema para analizar de forma sistemática los documentos seleccionados, para lo cual se implementó una tabla explicativa.
- Por último se hizo un análisis mostrando de manera comprensiva los resultados de esta investigación.

El análisis que se obtiene con la revisión bibliográfica sistematizada mediante el uso de tablas, aporta en gran medida a que una investigación adquiera cualidades sistematizadas para cualquier tipo de revisión.

3. Resultados y Discusión

Son variados los ataques informáticos que existen hoy en día y que con la pandemia iniciada en 2019 fueron proliferando cada vez más. Conocer ampliamente las vulnerabilidades digitales a las que se expone Latinoamérica resulta vital para promover prácticas de seguridad en cualquier ámbito a futuro, por eso el centro de esta investigación no es más que conocer un poco más estos ciberataques.

Se puede divisar en la tabla 1 los trabajos que fueron buscados y posteriormente examinados para demostrar que estos sirvieron de evidencia importante y con esto obtener el discernimiento más cercano sobre los ataques informáticos dados con mayor recurrencia en Latinoamérica durante la pandemia.

Tabla 1. Trabajos encontrados para análisis.

#	Título	País	Referencias bibliográficas
1	Delitos informáticos en tiempos de COVID: Revisión literaria Ecuador	Ecuador	(Zambrano et al., s. f.)
2	Análisis de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador	Ecuador	(Vélez, 2022)
3	An Approach to Cybersecurity, Cyberbullying in Social Networks and Information Security in Public Organizations during a Pandemic: Study case COVID-19 Ecuador	Ecuador	(Toapanta et al., 2020)
4	Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá	Colombia	(Estrada-Esponda et al., 2021)
5	Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19	Ecuador	(Suastegui, 2022)
6	Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional	Ecuador, Chile, Colombia	(Mosquera-Chere, 2021)
7	Mecanismos de ciberseguridad basados en honeypots	Ecuador	(Gilces et al., 2021)
8	Mejoramiento de la seguridad de la información para reducir los ciberataques del tipo phishing en una entidad financiera	Perú	(Jancachagua, 2021)
9	Ciberseguridad: el impacto más allá de las fronteras	Ecuador	(Torres, 2020)

10	Una triple amenaza en las Américas	Brasil, Argentina, México	(KPMG, 2022)
11	¿Cómo Evitar Ciberataques En Las Mipymes colombianas?	Colombia	(Londoño Pamplona et al., 2021)
12	Incidencia del Covid-19 en el cibercrimen del 2020 y futuros retos	Colombia	(Bautista, 2020)
13	Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense	Argentina, Brasil, Bolivia, Ecuador, Chile, Colombia, Perú, Paraguay y México	(Arévalo & Hernández, 2021)
14	Los intentos de phishing en tiempos de COVID-19	Venezuela, Brasil, Colombia, México	(Pasquali, 2020)
15	Aplicación del “NIST CYBERSECURITY FRAMEWORK” en el Instituto Superior Tecnológico “Sucre”	Ecuador	(Yánez, 2022)
16	Impacto de la pandemia del covid-19 en la digitalización de la política exterior colombiana: Caso embajada de Colombia en Brasil	Colombia, Brasil	(Bravo, s. f.)
17	Acoso por medio de las tecnologías en las redes sociales durante tiempos de pandemia en Ecuador, una revisión sistemática	Ecuador	(Tacuri, 2021)
18	Panorama mundial de la ciberamenaza relacionada con la covid-19	Mundial	(Interpol, 2020)
19	Sociedad Digital en Latinoamérica 2020-2021. Un futuro posible de Colombia como sociedad digital. Una visión tecnoantropológica	Colombia	(Cardeno, 2021)
20	Seguro de riesgos cibernéticos: enfoque y perspectivas en la nueva normalidad	Argentina	(Pérez, 2021)

Es posible percatarse que fueron veinte los temas encontrados, entre ellos están artículos, tesis, informes, entre otros; estudiados por medio de la revisión bibliográfica sistematizada, mismos que servirán de base para así saber dónde fue encontrada la información necesitada. La tabla 2 expone un análisis de lo obtenido mediante esta investigación, en los cuales se tiene de un lado el nombre de los ataques y en otro la frecuencia con la que fueron encontrados puede ser esta alta, media o baja.

Tabla 2. Frecuencia de ataques informáticos en Latinoamérica durante la pandemia.

Ataques informáticos	Frecuencia encontrada en los documentos consultados
Malware	Alta
Phishing	Alta
Ransomware	Alta
Robo de información	Media
Acceso no autorizado	Media
Ingeniería social	Media
Acoso cibernético	Media
Scamming (estafa)	Media
Sniffing	Baja
Minería pirata de criptomonedas	Baja
Códigos de captación	Baja
Dominios maliciosos	Media
Insider	Baja
Defacement	Baja
Violación de políticas de escritorio limpio	Baja
Ataque DoS	Baja
Ataques a sistemas IoT	Baja

Como es bien sabido, la pandemia atribuida al COVID vino a cambiar la vida de la humanidad, moviendo casi todo a un entorno virtual y es ahí donde la delincuencia tuvo un gran auge aprovechándose de esto, lo que aumentó repentinamente los ataques informáticos y Latinoamérica no fue la excepción. Con una alta frecuencia se tiene el malware, el phishing y el ransomware, a los que se destacan por hacer daño a los usuarios y engañarlos sin su conocimiento. En frecuencia media se puede citar al acoso cibernético, robo de información, ingeniería social y demás; mientras que con frecuencia baja cabe mencionar la minería pirata de criptomonedas, ataque DoS, sniffing entre otros.

El sitio web Statista es muy reconocido por los buenos datos en los que se basan para la generación de sus gráficas para así llegar a demostrar algo. Como se puede notar en la figura 1, que es en base a los ataques phishing, cuatro de los ocho países que se divisan ahí son de Latinoamérica y en especial es uno de esos cuatro, es decir Venezuela, que contiene el índice más alto, seguido por Brasil, es decir otro país latinoamericano. Si bien los de ambos son valores elevados, pero el tema venezolano se aleja de los demás porcentajes (Pasquali, 2020).

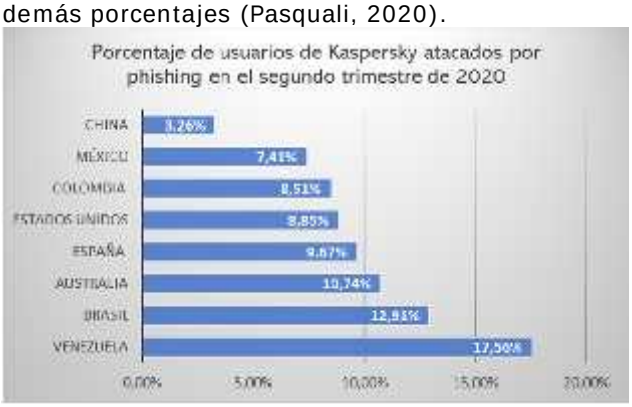

Figura 1. Los intentos de phishing en tiempos de COVID.

4. Conclusiones

En Latinoamérica se debe priorizar la seguridad informática sobre todo a raíz de la emergencia sanitaria declarada por la pandemia de COVID, donde los delincuentes se ganaron la confianza de las víctimas aplicando técnicas de phishing, que es uno de los ataques altamente frecuentes, muchas veces haciéndose pasar por entidades financieras para así obtener datos valiosos y posterior robo de información donde entra en juego el malware, así como también el ransomware. Existen otros ataques que se dan con menos frecuencia, pero no por eso se debe descuidarlos, como el acoso cibernético mediante la divulgación de información falsa o el scamming que trata sobre estafar a personas con poca experiencia cibernética; se tiene también el sniffing o el defacement que ocurren con menos frecuencia. Es conveniente preparar a las personas en temas de amenazas informáticas, generar en ellos conciencia sobre lo peligroso que resulta para así anular los impactos que estas provocan en la información digital que se maneja.

El levantamiento formado por su irrupción en la rutina de la población, administraciones y empresas ha establecido una ventana de oportunidad por la que se han creado también nuevos riesgos entre las preocupaciones de los que velan por la ciberseguridad. En particular, desde el inicio del brote se han vuelto a detectar varios malware que se encontraban en una fase relativamente latente y que han adoptado nuevas formas, ya que sus autores han utilizado la COVID-19 para dar un nuevo impulso a sus tácticas de ingeniería social. Es por esto que el malware es encontrado con una frecuencia alta en la tabla 2.

Mientras se suscitaba el estudio de los ejemplares indagados fue posible apreciar sectores dentro de Latinoamérica que se han visto afectados en mayor medida por este tipo de ataques en cuestión. El tema de Venezuela es que su nivel de pobreza es tan grande que desencadena su alta tasa de vulnerabilidad frente a los ciber atacantes y por esta razón se vuelve una de las que más han atacado. Le sigue Brasil en donde si se habla de economía no es tan malo su estado, en comparativa con la de su vecino país, pero sí tuvo uno de los índices más altos de contagios a nivel continental y mundial.

5. Referencias

Arévalo, M., & Hernández, D. (2021). Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense.

Bautista, F. (2020). Incidencia del Covid-19 en el cibercrimen del 2020 y futuros retos. Perspectivas en ciberseguridad. https://www.asobancaria.com/wp-content/uploads/2020/12/CIBERSEGURIDAD-REVISTA.pdf

Bravo, Z. (s. f.). IMPACTO DE LA PANDEMIA DEL COVID-19 EN LA DIGITALIZACIÓN DE LA POLITICA EXTERIOR COLOMBIANA: CASO EMBAJADA DE COLOMBIA EN BRASIL.

Cardeno, J. (2021). Sociedad Digital en Latinoamérica 2020-2021: Un futuro posible de Colombia comosociedad digital. Una visión tecnoantropológica. Penguin Random House Grupo Editorial.

Codina, L. (2020). Cómo llevar a cabo revisiones bibliográficas tradicionales o sistematizadas en trabajos de final de máster y tesis doctorales. Universitat Pompeu Fabra, Departamento de Comunicación, Máster Universitario en Investigación en Comunicación Social (MUCS), 1-18. https://repositori.upf.edu/bitstream/handle/10230/45509/Codina_Revisiones.pdf?sequence=1&isAllowed=y

Estrada-Esponda, R., Unás-Gómez, J., & Flórez-Rincón, O. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos Ciencia & Tecnología, 13(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

Gilces, A., Demera, V., & Vaca-Cárdenas, L. (2021). Mecanismos de ciberseguridad basados en honeypots. Revista de tecnologías de la informática y las telecomunicaciones, 1-17. https://190.15.136.223/index.php/Informaticaysistemas/article/download/3708/3958

Interpol. (2020). Panorama Mundial de la Ciberamenaza relacionada con la COVID-19. INTERPOL General Secretariat, 2. https://www.interpol.int/es/content/download/15217/file/20COM0312-Cyberthreats-Campain_ProjectSheet - SP -2020-05.pdf

Jancachagua, J. (2021). MEJORAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN PARA REDUCIR LOS CIBERATAQUES DEL TIPO PHISHING EN UNA ENTIDAD FINANCIERA. Universidad tecnológica del Perú, 1-80. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4401/Jou_Jancachagua_Trabajo_de_investigacion_Titulo_Profesional_2021.pdf?sequence=1&isAllowed=y

KPMG. (2022). Una triple amenaza en las Américas. KPMG.

Londoño Pamplona, A., Quintero, C., & Medina Fonseca, K. (2021). ¿Cómo Evitar Ciberataques En Las Mipymes Colombianas? Revista MODUM, 3(1), 144-150.

Mosquera-Chere, S. (2021). Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional. Polo del Conocimiento, 6(3), 1251-1273. https://doi.org/10.23857/pc.v6i3.2432

Pasquali, M. (2020, septiembre 1). Gráfico: Los intentos de phishing en tiempos de COVID-19 | Statista. Statista. https://es.statista.com/grafico/18427/intentos-de-phishing-durante-la-pandemia/

Pérez, H. (2021). Seguro de riesgos cibernéticos: enfoque y perspectivas en la nueva normalidad. Revista de la Facultad de Derecho y Ciencias Sociales de la Universidad Católica de Córdoba, 4, 127-148. https://doi.org/10.22529/rfd.2021(7)04

Suastegui, L. (2022). Estudio y análisis de ataques informáticos en Ecuador durante el estado de

pandemia de COVID-19. Corporativo Edwards Deming Enero-Marzo, 6. http://201.159.223.180/bitstream/3317/18016/1/T-UCSG-PRE-TEC-ITEL-421.pdf

Tacuri, I. (2021). Acoso por medio de las tecnologías en las redes sociales durante tiempos de pandemia en Ecuador, una revisión sistemática [Universidad Politécnica Salesiana]. En Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/20242/1/UPS-GT003203.pdf

Toapanta, S., Espinoza, J., & Mafla, L. (2020). An Approach to Cybersecurity, Cyberbullying in Social Networks and Information Security in Public Organizations during a Pandemic: Study case COVID-19 Ecuador. 2020 Congreso Internacional de Innovacion y Tendencias en Ingenieria, CONIITI 2020 - Conference Proceedings. https://doi.org/10.1109/CONIITI51147.2020.9240375

Torres, G. (2020). Ciberseguridad: el impacto más allá de las fronteras. Perspectiva Económica, 10-13. https://perspectiva.ide.edu.ec/investiga/wp-content/uploads/2020/10/Perspectiva-2020-10-2.pdf

Vélez, E. (2022). Análisis de ciberseguridad en redes de telecomunicaciones y sistemas informáticos para Educación 4.0 como respuesta a la Industria 4.0 en el Ecuador [Universidad Católica de Santiago de Guayaquil]. En Universidad Católica de Santiago de Guayaquil. http://201.159.223.180/bitstream/3317/18017/1/T-UCSG-PRE-TEC-ITEL-422.pdf

Yánez, J. (2022). APLICACIÓN DEL “NIST CYBERSECURITY FRAMEWORK” EN EL INSTITUTO SUPERIOR TECNOLÓGICO “SUCRE”. https://repositorio.pucesa.edu.ec/bitstream/123456789/3693/1/77978.pdf

Zambrano, A., Loor, F., Zambrano, W., & Párraga, R. (s. f.). DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR. espam.edu.ec. Recuperado 27 de julio de 2022, de http://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf

Zanotti, M. (2020). ¿Cómo pasar de una seguridad aislada a una integrada? 39-39. https://assets.ey.com/content/dam/ey-sites/ey-com/es_pe/topics/cybersecurity/ey-giss-como-pasar-seguridad-aislada-integrada.pdf