48

Fecha de presentación: febrero, 2020
Fecha de aceptación: marzo, 2020
Fecha de publicación: mayo, 2021

ANÁLISIS DE SEGURIDAD INFORMÁTICA

EN ENTORNOS VIRTUALES DE LA UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES EXTENSIÓN QUEVEDO EN TIEMPOS DE COVID-19

ANALYSIS OF COMPUTER SECURITY IN VIRTUAL ENVIRONMENTS OF THE AUTONOMOUS REGIONAL UNIVERSITY OF THE ANDES EXTENSION QUEVEDO IN TIMES OF COVID-19

MAndrea Raquel Zuñiga Paredes[1]
E-mail: uq.andreazuniga@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-4042-1523
Edmundo José Jalón Arias[1]
E-mail: uq.edmundojalon@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-3060-736X
María Ernestina Andrade Olmedo[1]
E-mail: uq.rrhh@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-2763-8464
José Leonardo Giler Chango[1]
E-mail: joselgc.tmq@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-5649-6162
[1] Universidad Regional Autónoma de Los Andes. Ecuador.

Cita sugerida (APA, séptima edición)

Zuñiga Paredes, A. R., Jalón Arias, E., Andrade Olmedo, M. E., Giler Chango, J. L. (2021). Análisis de seguridad informática en entornos virtuales de la universidad Regional Autónoma de Los Andes extensión Quevedo en tiempos de Covid-19. *Revista Universidad y Sociedad*, 13(3), 454-459.

RESUMEN

La presente investigación se realiza con el fin de obtener el impacto de los procesos de seguridad informática en los miembros de UNIANDES-Quevedo en tiempo de COVID 19, es sabido que a nivel nacional la pandemia ha forzado a varias instituciones a cambiar su modalidad presencial por la virtual y hasta el momento no se han realizado estudios sobre los efectos en nivel de seguridad informática en la institución, razón por la que se propone el estudio, el uso de las tecnologías informáticas en todos los aspectos de la cotidianidad humana, ha conducido a que la seguridad informática no sea solo una preocupación de las grandes empresas, con la pandemia que atraviesa el mundo entero muchas empresas se han visto en la obligación de implementar el teletrabajo en sus compañías quedando vulnerables ante las faltas de controles que les permitan protegerse de instrucciones no deseadas. Con una investigación exploratoria, con manejo de información descriptiva, se aplicó una investigación de campo, con técnicas como entrevista y encuesta con la finalidad de indagar y obtener información de los sistemas implementados en UNIANDES en tiempos de pandemia; determinando el impacto de la seguridad en los procesos que ofrece UNIANDES.

Palabras clave: COVID-19, Protocolos de seguridad, ciberdelito, plataformas virtuales, teletrabajo.

ABSTRACT

This research is conducted in order to obtain the impact of computer security processes in the members of UNIANDES-Quevedo in time of COVID 19, it is known that nationally the pandemic has forced several institutions to change their face-to-face mode by the virtual and so far no studies have been conducted on the effects on the level of computer security in the institution, which is why the study is proposed, the use of the computer technologies in all the aspects of the human daily life, has led to that the computer security is not only a concern of the big companies, with the pandemic that crosses the whole world many companies have been seen in the obligation to implement the telework in their companies remaining vulnerable before the lack of controls that allow them to protect themselves of not wished instructions. With an exploratory research, with descriptive information management, a field research was applied, with techniques such as interview and survey in order to investigate and obtain information of the systems implemented in UNIANDES in times of pandemic; determining the impact of security in the processes offered by UNIANDES.

Keywords: COVID-19, Security protocols, cybercrime, virtual platforms, teleworking.

INTRODUCCIÓN

El estudio planteado aportará con información básica sobre seguridad informática en tiempos de pandemia en una institución de nivel superior; es importante porque servirá ver los puntos que le faltaría para ofrecer un mejor servicio y verificar si ha existido vulnerabilidad en los procesos logrando ser un referente en otras instituciones (Lim, 2021).

Las TICS en tiempo de pandemia se volvieron fundamentales para todas las empresas a nivel nacional los servicios incluyen difusión, venta, teletrabajo; según datos del Ministerio de telecomunicaciones al 2019 se registra al 41.05% de personas que usan computadoras; así mismo personas con acceso a internet en el 2019 registra el 182.71% (Ecuador. Instituto Nacional de Estadística y Censo, 2020), lo que indica que en la actualidad este porcentaje con los requerimientos de la pandemia de mayor.

Diferentes sectores se vieron afectados financieramente, con pérdidas millonarias en el mercado, el mundo de la tecnología ha sufrido estragos por COVID 19, estos se han visto vulnerados por aumentando precios y escasez de productos tecnológicos; el sector más afectado es el turismo a nivel mundial como los indica la revista de Centro de investigación en política pública, el turismo es el sector más afectado por las normas de distanciamiento social, aplazando las presentaciones, reservas, disminución en restaurantes; en la presente investigación se pretende analizar el impacto de los procesos de seguridad informática en entornos virtuales, en los miembros de UNIANDES-Quevedo en tiempo de COVID 19, usando investigación exploratoria para emitir un juicio sobre la situación actual, se busca fundamentar teóricamente seguridad informática en tiempos de COVID 19, para emitir juicio sobre el estado de la seguridad en la institución.

La situación actual del teletrabajo en Ecuador y algunas empresas locales en tiempos de pandemia ha adoptado ciertas técnicas de protección de datos y las políticas más implementadas en términos de seguridad de la información (Fernández-Alemán, et al., 2015), sustentadas en documentación indexada y fuentes confiables, además de las experiencias en el campo y con la participación en procesos similares que permiten la observación y conocimiento de las herramientas utilizadas en el teletrabajo donde el empleado debe adoptar un sistema de gestión de riesgo de seguridad informática (Chaverra, et al., 2015).

Basados en algunos estudios como “Ciberseguridad en los sistemas de información de las universidades” centrado en revisar el estado del conocimiento en la ciberseguridad en los sistemas de información en el contexto universitario del Ecuador, el estudio se centra en plataformas como Sciencedirect® y Google Académico® centrada en la cultura de ciberseguridad en las instituciones universitarias (Anchundia Betancourt, 2017); también se considera toda la información sensible que produce la institución, la estructura, sistemas o aplicaciones que se comparten en la nube, muchas empresas recurren a software privados para albergar y custodiar sus datos (Álvarez Díaz, et al., 2018).

Otro elemento que intervienen en la educación son los software o plataformas que se pueden utilizar para la enseñanza virtual como Moodle, un sistema diseñado para crear y gestionar espacios de aprendizaje online, apropiados para profesores, estudiantes y administradores. Otras herramientas para la enseñanza virtual en la Suite de Google Apps for Education incluye que incluye Google Docs, Gmail, Google Calendar, Google Classroom (Fernández, et al., 2020), Suite de Microsoft incluye office 365, Outlook, OneDrive, OneNote, Teams, Stream y calendar entre otros. Además, muchos centros educativos están utilizando Telegram, App y WhatsApp; según investigaciones este proceso se puede mejorar con sistemas de e-proctoring (García-Peñalvo, et al., 2020).

La expansión del COVID 19, llegó a transformar gran parte de los sectores económicos, productivos, y empresariales, las empresas se vieron obligadas a suspender sus actividades presenciales, enviar a sus trabajadores a sus domicilios para que realicen sus actividades con un llamado teletrabajo y regirse a una serie de normas para no expandir el mismo (Sánchez-Henarejos, et al., 2014); para mantener la estabilidad de la empresa, las vinculadas a la tecnología de la información encuentran en esta coyuntura la oportunidad de posicionarse en un lugar protagónico.

El marco legal y regulaciones relacionadas con las tecnologías de la información y las comunicaciones, tratan de adecuarse a los nuevos cambios con la velocidad que esto implica (Argüelles Arellano, 2016); en cada país se están tomando varias acciones en torno a contexto actual, la Constitución del Ecuador en art. 80 (Ecuador. Asamblea Nacional Constituyente, 2008) sección novena el estado garantiza el acceso a las nuevas tecnologías, se requiere continuar con la formación y actualización de conocimientos del recurso humano de cada empresa, una opción en este sentido es hacer participar a estudiantes de las carreras de Sistemas para conducir proyectos de diagnóstico (Solarte Solarte, et al., 2015), para la implementación e implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 para su incorporación a los sectores productivos y de servicios considerados estratégicos para el desarrollo

de la economía del conocimiento y la transformación digital.

Los cambios en las telecomunicaciones es más que en otros sectores, la competencia industrial, la privacidad y protección de los datos personales, seguridad de la información, crímenes informáticos, propiedad intelectual, firmas electrónicas, certificación de documentos, protección del consumidor, acceso a la información y servicios en línea. En Ecuador son cada vez más altos los valores de participación del internet en el mercado se puede observar en la figura 1 extraída del ministerio de telecomunicaciones donde la densidad de banda ancha es alta.

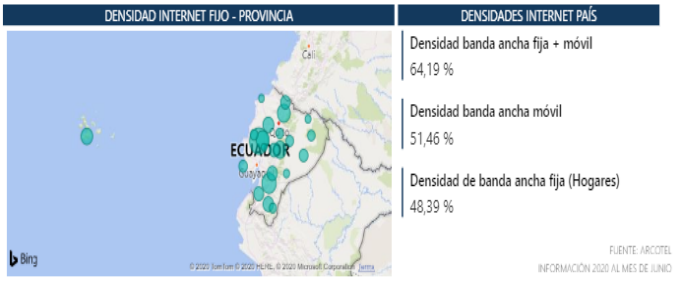

Figura 1. Densidad de Internet Fijo.

Según estudio titulado "Sector software y la situación respecto de la pandemia de COVID-19" por Ventrici, et al. (2020), empresas como Amazon, Microsoft, Google, Globant, Red Hat y Mercado Libre, para planificar la utilización de inteligencia artificial y big data para el control del despliegue del COVID 19 en Argentina mencionaron algunas iniciativas que aplicadas en tiempos de pandemia, que fueron la creación de un tablero interactivo para conocer camas y respiradores disponibles en 1400 hospitales en tiempo real y la aplicación CUIDAR, que permite el autodiagnóstico, rastreo de contagios y accesos a permisos de circulación.

Algunas de las empresas más afectadas por estragos de COVID 19 se podría mencionar: Apple y Foxconn por cierre de planta de Foxconn en Wuhan; Cancelación de eventos: Mobile Word Congress y Game Developers Conference: los organizadores deciden cancelar el evento ante la gran cantidad de grandes empresas que cancelaron su asistencia al evento por el coronavirus; Samsung ya que prevé un aumento en el precio de las memorias RAM DDR4 y los SSD; ESA: Los organizadores del evento del E3, uno de los más importantes en el mundo de los videojuegos, ha sido cancelado por el coronavirus.

Basados en informes de Kaspersky Security Network (2020), refleja que lograron neutralizar 726 536 269 ataques lanzados desde recursos de Internet ubicados en 203 países de todo el mundo; se registraron 442 039 230 URLs únicas que provocaron reacciones del antivirus web, en los equipos de 249 748 usuarios se neutralizaron intentos de ejecución de programas maliciosos diseñados para robar dinero mediante el acceso en línea a cuentas bancarias, además se neutralizaron ataques de malware cifrado en los equipos de 178 922 usuarios, detectando 164 653 290 programas maliciosos y potencialmente indeseables únicos.

Según informes de líder mundial en ciberseguridad doméstica "Kaspersky", los acontecimientos del primer trimestre del 2020, los cibercriminales explotan este tema en particular la nueva modificación en troyano como Ginp, Coronavirus FinderCookiethief, Dropper. Android OS. Shopper, robar estos datos el troyano permanece en el dispositivo.

En el primer trimestre de 2020, los productos y tecnologías móviles de Kaspersky Lab detectaron 1 152 662 paquetes de instalación maliciosa, 171 669 más que en el trimestre anterior; Kaspersky desde el segundo trimestre de 2019, ha visto un aumento constante más en amenazas móviles, dado que según sus reportes comparados con el 2019 es alto.

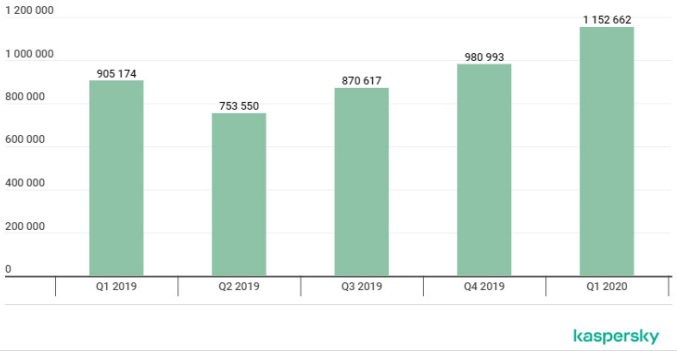

Figure 2. Informe de Kaspersky Security Network (2020).

MATERIALES Y MÉTODOS

El presente trabajo es considerado exploratoria dado que incluye un nivel investigativo "explicativo" (causa – efecto) y prospectivos, con manejo de información descriptiva. Se aplicó una investigación de campo, con técnicas como entrevista y encuesta con la finalidad de indagar y obtener información de los sistemas implementados en UNIANDES en tiempos de pandemia con respecto a seguridad informática. Finalmente, se procedió al análisis y a la interpretación de los datos obtenidos en la investigación de campo. Considerando los resultados, se realizó la interpretación de estos.

Además, se utilizó otros métodos que ayudaron en el proceso de investigación como son:

Investigación descriptiva: Fue empleada al momento de dar a conocer del porqué de la situación, mediante la explicación de las causas y el efecto que debió asumir UNIANDES tras enfrentar una pandemia, los servicios, productos y estrategias para enfrentar la situación.

Investigación bibliográfica: Este tipo de investigación se empleó para fundamentar el trabajo realizado, a nivel del tema abordado de seguridad informática en tiempos de pandemia que ayudaron en el sustento bibliográfico del presente trabajo.

Investigación de campo: La presente investigación se la aplicó en la comunica de UNIANDES a través de formas de office: docentes, estudiantes y administrativos con el fin de recolectar datos de estrategias, situaciones, procesos aplicados para seguir con el buen funcionamiento de la empresa.

Se realizó el cálculo de la muestra poblacional de estudiantes, aplicando un margen de error del 10% y un nivel de confianza de 95%; en docentes y administrativos por ser cantidades menores a 100 se mantiene la cantidad (Tabla 1).

Tabla 1 Población y muestra.

Detalle	Población	Muestra
Docentes	24	24
Estudiantes	435	79
Administrativo	29	29
Total	488	132

En la presente investigación se propuso 3 tipos de encuestas, enfocados en la comunidad UNIANDES, estudiantes, docentes y personal administrativo, con la indagación se logró obtener datos concretos sobre efectos de procesos virtuales como teletrabajo, plataformas virtuales y se pretende diagnosticar los casos de vulnerabilidad que ha sufrido la empresa en tiempos de COVID-19.

RESULTADOS Y DISCUSIÓN

Para dar un enfoque de las actividades virtuales se indaga en los estudiantes sobre el internet como herramienta didáctica, obteniendo al 46% que seleccionaron siempre y un 39% casi siempre su importancia por las actividades que realizan.

Otro resultado que se puede mencionar es las respuestas que dieron los estudiantes es sobre los recursos recibidos para el proceso de educación online, el 60% aplicaron recurso tecnológico propio (figura 2), pero en la misma pregunta se logró analizar que muchos respondieron recursos didácticos ofrecidos por docentes; en el análisis de docentes el 96% ha realizado teletrabajo con recurso propio.

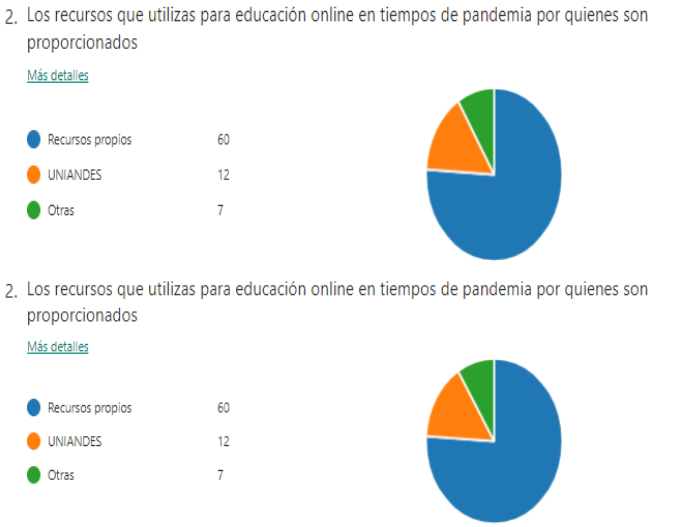

Figura 2. Recursos para educación online en estudiantes.

Indagando sobre la seguridad informática en equipos de cómputo en estudiantes se obtuvo que solo el 63% mantienen antivirus instalados y el 37% restante no cuenta con antivirus o desconoce si lo tiene; también existe una afinidad del 27.5% por Windows defender y 23.8 con Avast en programas antivirus. En antispyware el 72.5% desconoce si existe en sus equipos.

En docentes la misma pregunta reflejó que un 25% no tiene o no conoce sobre el antivirus en sus PC; entre los antivirus más usados, en ellos está el Avast con 25% y Eset Nod32 con 20.8%; lo que corresponde en Antispyware el 22% no utilizan, con un porcentaje de 30% el más utilizado es McAfee Internet Security.

En tiempos de pandemia la empresa tuvo que realizar varios procesos online de los cuales los estudiantes mencionan que sólo el 18% presentó inconvenientes a través de algún servicio, donde el 29% sufrió pérdida de información; sin embargo, UNIANDES obtuvo un 76. % en atención a fallas técnicas en el proceso educativo con eficiencia, entre los accidentes mencionados con mayor frecuencia están servicio de internet inestable, problemas técnicos en PC y plataforma lenta.

En las preguntas dirigidas hacia los docentes, se indagaba sobre inconvenientes presentados con la seguridad de su PC en el transcurso del teletrabajo obteniendo el 33% con afirmaciones, de los cuales 25% sufrieron pérdida de información.

Entre los inconvenientes presentados por los docentes respecto con la seguridad de su PC fueron: pérdida de

información, intermitencia en redacción de archivos, bloque de funciones en office inestables, virus en archivos, plataforma inestable y fallas de hardware; sin embargo, los mismos 76% aducen haber tenido atención a fallas técnicas atendidas de manera eficiente por miembros de UNIANDES.

Sobre temas de capacitación en seguridad informática y actividades de concientización en entornos digitales se obtuvo que el 67% de los docentes han participado.

En la obtención de datos del área administrativa se obtuvo que existe un porcentaje del 52% donde UNIANDES les provee de recursos en teletrabajo, así mismo según resultados, el encargado de ofrecer servicio técnico a sus equipos es el técnico de la empresa 55%, indicando el 91% asistencias a capacitación de seguridad informática y el 95% sin problemas ni pérdida de información.

Se consultó a los docentes sobre los responsables de mantener e instalar software de seguridad en sus equipos y las respuestas obtenidas se dieron en un 67% en técnicos privados, 5% otros que incluyen los mismos docentes o algún familiar; lo mismo se indagó en el sector administrativo de la institución y ahí el 55% lo realiza los técnicos de la institución.

A través del dpto. técnico se obtuvieron datos de actividades realizadas por la institución para enfrentar la pandemia se menciona:

» En infraestructura se instalaron routers ruckus y switch
» En plataforma EVA-Moodle se implementaron módulos interactivos, para mejorar el proceso enseñanza – aprendizaje virtual
» Implementación de botón de pagos y solicitudes para estudiantes
» En seguridad informática se implementó filtro de red Fortinet, con enlaces VPN
» El personal de tics recibió capacitaciones de soporte técnico, VPN y líneas telefónicas.
» Una de las políticas más implementadas es solventar los problemas que presentan los miembros de UNIANDES en tiempo real.

Realizando un mayor énfasis en peticiones se ha logrado una buena participación de los estudiantes en la presente investigación, obteniendo con resumen de resultado el problema que más se mencionó por los participantes fue el de conexión y actualización de software; aunque el tiempo para muchos es limitado por las tantas solicitudes laborales, UNIANDES en todas las sucursales han realizaron capacitación sobre Socialización de Ingeniería Social (figure 4), donde se logró percibir las asistencias de UNIANDES a nivel nacional, más sin embargo en la presente investigación con un porcentaje alto en docentes se encuentra el bajo conocimiento del mismo y el desconocimiento de ciertas políticas de seguridad contra los llamados Phishing que se abordará en una posterior investigación, pero en la actualidad existen muchos estudios que indican que este tipo de ataque es uno de los más frecuente y afecta a muchas empresas (Gangavarapu, et al., 2020).

Dicho lo anterior en una institución no puede contemplar porcentajes mínimos de inseguridad, porque basta un descuido y la empresa podría ir a la ruina por la pérdida o filtrado de sus datos, en ese proceso se contempla los docentes que buscan un técnico privado para soporte en sus dispositivos según la investigación realizada 67% lo realiza, de ahí se puede generar un incidente de seguridad que da lugar a la violación de la confidencialidad, disponibilidad o integridad de los datos, en tiempos de pandemia es recomendable que la empresa que la empresa maneje un estándar de seguridad para todos sus empleados aplicar apps empresariales con seguridad informática y monitorización constante de software de seguridad, antivirus y cortafuegos estos con las debidas licencias con garantías de seguridad (Figura 3).

Figura 3. Captura del evento.

Toda empresa y en especial las de educación deben estar preparados para enfrentar nuevos riesgos de fraude que surgirán de la secuela del COVID-19, es necesario estar al día con investigaciones y fortalecer áreas de riesgo (León, 2020).

CONCLUSIONES

La pandemia del COVID-19, en el mundo ha generado cambios, en la educación ha logrado la inserción de competencias digitales para la comunicación y elaboración de los contenidos que cada docente debe planificar para cumplir con un plan de estudios con estrategias diferentes explorando las habilidades digitales del siglo XXI (Van

Laar, et al., 2017), el sílabo debió estar adherido al logro de competencias, proceso que debió contemplar seguridad de la información.

UNIANDES y su comunidad también se acogieron al teletrabajo o home office, con el fin de precautelar la salud de quienes lo conforman; como empresa de servicio presentó una importante participación de recurso humano con el que cuenta, optó por la capacitación en varios temas, los más importantes: soporte técnico, asistencia técnica en líneas telefónicas y VPN en niveles técnicos.

Demostró como centro de estudios de nivel superior estar a la vanguardia de tecnologías, con las soluciones que implementó para mejorar sus servicios en tiempos de pandemia y los resultados en la extensión Quevedo fueron favorables dado que, aunque falte capacitar a gran porcentaje de su población o estudiantes los problemas suscitados fueron atendidos con rapidez y eficiencia como se puede observar en el apartado de resultados.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez Díaz, J. A., Duro, E. A., Gubert, I. C., Cardozo de Martínez, C. A., Sotomayor, M. A., López, L., Duro, A., Niño Moya, R., & Sorokin, P. (2018). Entre Huxley y Orwell: Big Data y salud. Revista Latina de Sociología, 8(2), 23–33.

Anchundia Betancourt, C. (2017). Ciberseguridad en los sistemas de información de las universidades. Dominio de Las Ciencias, 3(3), 200–217.

Argüelles Arellano, M. C. (2016). Retos de la legislación informática en México. Computación y Sistemas, 20(4), 827–831.

Chaverra Mojica, J. J., Restrepo Vélez, H. J., & Pérez García, J. F. (2015). El teletrabajo y la seguridad de la información empresarial. Revista CINTEX, 20(1), 111–121.

Ecuador. Asamblea Nacional Constituyente. (2008). Constitución de la República. Registro Oficial N. 449. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Ecuador. Instituto Nacional de Estadística y Censo. (2019). Encuesta de Seguimiento al Plan Nacional de Desarrollo. Instituto Nacional de Estadística y Censo. INEC.https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2019/201912_Boletin_Multiproposito_TIC.pdf

Fernández, N. G., Moreno, M. L. R., & Guerra, J. R. (2020). Brecha digital en tiempo del COVID-19. ***Hekademos: revista educativa digital***, (28), 76-85.

Fernández-Alemán, J. L., Sánchez-Henarejos, A., García-Amicis, V. M., Toval, A., Sánchez-García, A. B., & Hernández-Hernández, I. (2015). Estudio sobre la importancia y la seguridad de uso de las contraseñas en el ámbito laboral sanitario. Gaceta Sanitaria, 29(1), 72–79.

Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. Artificial Intelligence Review,4, 1-63.

García-Peñalvo, F. J., Corell, A., Abella-García, V., & Grande, M. (2020). La evaluación online en la educación superior en tiempos de la COVID-19. Education in the Knowledge Society (EKS), 21(0), 26-37.

Kaspersky Security Network. (2020). Desarrollo de las amenazas informáticas en el primer trimestre de 2020 Estadísticas. https://securelist.lat/it-threat-evolution-q1-2020-statistics/90344/

León, C. E. (2020). El fraude en tiempos de pandemia. Revista Fasecolda, 178, 64-67.

Lim, H. I. (2021). An Approach to Improving Software Security Through Access Control for Data in Programs. Springer Singapore.

Sánchez-Henarejos, A., Fernández-Alemán, J. L., Toval, A., Hernández-Hernández, I., Sánchez-García, A. B., & Carrillo De Gea, J. M. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. Atención Primaria, 46(4), 214–222.

Solarte Solarte, F. N., Enríquez Rosero, E. R., & Benavides Ruano, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5), 492–507.

Van Laar, E., Van Deursen, A. J. A. M., Van Dijk, J., & De Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. Computers in Human Behavior, 72, 577–588.

Ventrici, P., Krepki, D., & Palermo, H. (2020). Sector software y la situación respecto de la pandemia de COVID-19. Conicet. 1-19. https://www.clacso.org/wp-content/uploads/2020/07/t02-Software.pdf