v. 3, n. 16, 2023

International Journal of Human Sciences Research

CYBERSECURITY PERSPECTIVE WITH THE USE OF VIRTUAL ENVIRONMENTS IN EDUCATION

Luz María Hernández Cruz
Universidad Autónoma de Campeche
Campeche – Mexico
https://orcid.org/0000-0002-0469-5298

Charlotte Monserrat Llanes Chiquini
Universidad Autónoma de Campeche
Campeche – Mexico
https://orcid.org/0000-0001-8389-5943

Diana Concepción Mex Álvarez
Universidad Autónoma de Campeche
Campeche – Mexico
https://orcid.org/0000-0002-1142-586X

Martina Díaz Rosado
Tecnológico Nacional de Mexico,
campus Champotón
Campeche – Mexico
https://orcid.org/0000-0002-1142-586X

Abstract: Today, in today's world, the use of the Internet and information and communication technologies assist in teaching practice at all educational levels. Specifically, in the management of online technological tools, academic teaching-learning, communication, collaboration, dissemination and dissemination activities have been used to develop, to mention some of the most important. Therefore, the educational community is concerned with the imminent risk of being victims of cybercrimes. The purpose of the research is to raise awareness in the academic community of the need to identify and use cybersecurity controls that benefit the use of the Internet in a safe and reliable manner, accepting international standards that reinforce security. Likewise, act as a channel of diffusion in the student community to safeguard their privacy and integrity. The ISO/IEC 27032 Standard is a recognized and accepted international standard to guarantee the action measures provided in this study.
Keywords: Internet, education, risk, cybersecurity, ISO 27032.

INTRODUCTION

The coronavirus disease (COVID-19) pandemic has caused an unprecedented crisis across the board. In the sphere of education, this emergency has led to the massive closure of face-to-face activities of educational institutions in more than 190 countries in order to prevent the spread of the virus and mitigate its impact. According to data from the United Nations Educational, Scientific and Cultural Organization (UNESCO), by mid-May 2020, more than 1.2 billion students of all levels of education, worldwide, had stopped having face-to-face classes at school.

In the educational field, a large part of the measures that the countries of the region have adopted in the face of the crisis are related to the suspension of face-to-face classes at all levels, which has given rise to three main fields of action: the deployment of distance learning modalities, through the use of a diversity of formats and platforms; the support and mobilization of educational personnel and communities, and attention to the health and comprehensive well-being of students (ECLAC, 2020).

Security on the Internet and in cyberspace is a complex issue. There is an increasing presence in cyberspace, websites and other applications tend to take advantage of this new virtual world. Cyberspace is a complex environment resulting from the interaction of people, software and Internet services supported by hardware and communications networks (ISO 27032).

In Mexico, during the third quarter of 2020, the National Institute of Statistics and Geography (INEGI) collected the National Survey on Availability and Use of Information Technologies in Households (ENDUTIH) 2020. ENDUTIH 2020 estimates They allow characterizing the phenomenon of the availability and use of ICT at the national, urban, and rural levels, by socioeconomic stratum and federal entity. With this effort, INEGI and the institutions that support the conduct of this survey, the Federal Institute of Telecommunications (IFT) and the Ministry of Communications and Transportation (SCT), make more and better statistics available to users for decision-making. decisions. ENDUTIH estimates that in 2020 there are 84.1 million internet users, representing 72.0% of the population aged six or over. This figure reveals an increase of 1.9 percentage points compared to that registered in 2019 (70.1%).

The term "cybersecurity" has become widespread today in our society and, along with it, some others such as cybercrime, cyberterrorism, cyberattack, cyberdefense,

etc. Cybersecurity is the ability to resist, with a certain level of reliability, any action that compromises the availability, authenticity, integrity, or confidentiality of the data stored or transmitted, or of the services offered. The different types of agents that can cause a cybersecurity problem are considered to be:

- Natural agents without intention or motivation. For example, a natural disaster or human error.
- Low profile agents. Isolated or loosely organized individuals who normally act for exclusively personal purposes.
- Cybercriminals. Mafia or organized crime organizations that seek to obtain an economic benefit cause damage according to their interests.
- Cyberterrorists. Terrorist organizations in propaganda, recruitment and attacks against information systems.
- Cyberactivists. anti-system groups, of radical political or ideological extremism, which act mainly to discredit or damage institutions.
- State. When these give continuity to physical conflicts, extending them to the virtual world, ranging from simple smear campaigns, meddling in electoral processes or, more broadly, to cyberwar.

It is considered important to create a responsible culture of cybersecurity for end users focused on prevention, given the co-responsibility of these and the State to avoid risks in cyberspace, through the implementation of awareness measures about the importance of knowing the threats in the digital environment that violate security and the importance of lines of action with unrestricted respect for human rights (Tapia Hernández, Ruiz Canizales, & Vega Páez, 2021).

The ISO/IEC 27000 family of standards establish a robust methodology for the implementation of integrated Information Security Management Systems based on risk management and iterative cycles of continuous improvement (González Inés, 2021).

In October 2012, the International Organization for Standardization (ISO) announced the creation of the ISO/IEC 27032 standard for cybersecurity. The organization explained in its official presentation that this new standard aims to guarantee the security of information exchanges on the network. Specifically, it provides a Secure framework to make processes secure. "The standard (ISO/IEC 27032) facilitates secure and trusted collaboration to protect the privacy of people around the world. Specifically, it helps to prepare for, detect, monitor, and respond to attacks from social engineering, hackers, malware, spyware, and other types of unwanted software (Joyanes Aguilar, 2021).

The ISO/IEC 27032:2012 standard (Guidelines for cybersecurity) focuses on the protection of cyberspace, covering some gaps in the field of cyber risk (Gayoso Martínez, Hernández Encinas, & Arroyo Guardeño, 2020).

The International Standard ISO/IEC 27032 aims to highlight the role of values in cyberspace, with respect to information security, network and internet security, and Critical Information Infrastructure Protection (CIIP). ISO/IEC 27032 as an international standard provides a policy framework to address trust-building, collaboration, information sharing, and technical guidance for systems integration among stakeholders in cyberspace.

(Blue Hat Corporation, n.d.)

ISO/IEC 27032 provides guidance on cyber security. Presents the guidelines to improve the state of cyber security and its dependencies with other security-related fields. It deals specifically with the security of

information, networks and the Internet and the protection of critical infrastructures that manage information. (Jean-François, 2016)

With this cybersecurity standard, a new framework has been created to improve internet security and it is totally oriented towards trying to guarantee a safe environment through security guidelines. (ACMS Consultants Group, s.f.)

Stakeholders have to play an active role in their respective use and development of Cybersecurity. From this, the analysis focuses on the role of individuals, the academy (teaching community) and the student community are indisputably identified as a permanent consumer due to the distance modality in Education in the face of confinement by COVID-19 . Hence, the importance of paying attention to cybersecurity controls for the end user in order to reduce or mitigate the risk of recurring Internet access.

METHODOLOGY

The study was kind enough to use documentary and critical research, it used the descriptive method with a cross-sectional design.

Based on this, the methodology used was divided into two main phases:

- Phase of analysis of the ISO 27032 standard and end-user security controls: this stage describes the objective of the standard and particularly the elements that are established as required controls in the end-user role to secure assets and prevent cybercrimes; and
- Phase of application of surveys in an educational context: it includes an exploratory field study that allows reflection and a perception of the knowledge and/or use of the cybersecurity controls of the ISO 27032 Standard by the academic community.

RESULTS

The stages of the cybersecurity cycle management are (Rodríguez Canfranc, 2014):

- Prevention: access control and identity management. Prevention of data leaks and network security.
- Detection: vulnerability management and continuous monitoring.
- Response: recovery system and countermeasures.
- Intelligence: data comparison and open source data.

In the first stage, prevention, the following are included (Rodríguez Canfranc, 2014):

- Control over who accesses company resources and the assignment of permissions and credentials to staff based on the roles performed.
- Establishment of technical, organizational and legal measures to prevent information leaks.
- Definition of a network security policy, which must be implemented through software and hardware tools and must be audited frequently to ensure its effectiveness.

In the second stage, the detection is understood (Rodríguez Canfranc, 2014):

- Continuous monitoring of the company's systems and networks in order to identify attempted attacks as soon as possible and limit the damage they may cause.
- The identification of weaknesses in our IT infrastructures that can leave us exposed to malicious conduct.

In the response, when a cyberattack has finally been suffered, this stage begins, which entails:

- Recovery systems, which allow the state of equipment and applications to be returned to the starting point before the

problem occurred.

- The application of new security measures that prevent the situation from happening again in the future.

Intelligence is about sharing information about attacks to better understand the attack operations and make the response to cybercrime more effective.

All of the above has been summarized and To clearly describe the cybersecurity life cycle, the context of action from the perspective of the end user is presented in Figure 1.

Likewise, ISO 27032 cybersecurity controls are grouped into four categories: application, servers, end user and social engineering. In this study, the object of analysis is the end-user controls. Figure 2 shows the end user controls of ISO 27032.

All antiviruses work in the background, inspecting each file or page that is opened on the device where they are installed. Antivirus Software uses three methods to protect the system:

1. Analyze files by comparing them with a database of malicious software or programs.

2. Monitor computer files as they are being opened or created to ensure they are not infected. This is real-time protection against viruses, which can affect system performance.

3. Periodically inspect the entire system to check for corrupted files and remove any existing viruses, in case they may have entered your computer.

Personal firewalls are programs that filter traffic to and from a computer. Once installed, the user must define the security level: allow or deny the access of certain programs to the Internet (temporarily or permanently) and authorize or not access from outside. These two types of firewalls are not mutually exclusive; there are protection systems that are a combination of both: software + hardware (Veiga, 2020)

Spyware is spyware that collects information from the computer where you are working, entering and operating on it without the user noticing. The spies on the computer can enter when programs are installed and their conditions are accepted, being as a general rule not noticed by the person who installs it. There are computer programs that detect and eliminate spyware introduced into the system, called antispyware. The most popular are: SpyBot Search & Destroy and Lavasoft Ad-Aware (Beltrán, 2012)

A pop-up blocker or pop-up blocker is software that prevents pop-up windows from appearing on a website. Some popup blockers work by immediately closing the popup, while others disable the command that calls the popup. Most browser software allows the user to turn the blocker on or off. Blocking pop-ups can be done in different ways through (Marañón, 2009):

1. Your browser settings.

2. The plugin bars for navigation and search

3. Your antivirus security options

4. Specialized software for this purpose.

The phenomenon of phishing (identity theft) consists of usurping personal information from Internet users through false emails that appear to come from a trustworthy company. Once on that site, the Internet user is asked to provide confidential data, which is then collected by the usurper to use for his own benefit.

Anti-phishing filters check searched sites against a constantly updated list of sites known for phishing activity. If you find a suspicious site, the browser alerts you that you might have landed on a dedicated phishing site. Currently most web browsers include anti-phishing tools.

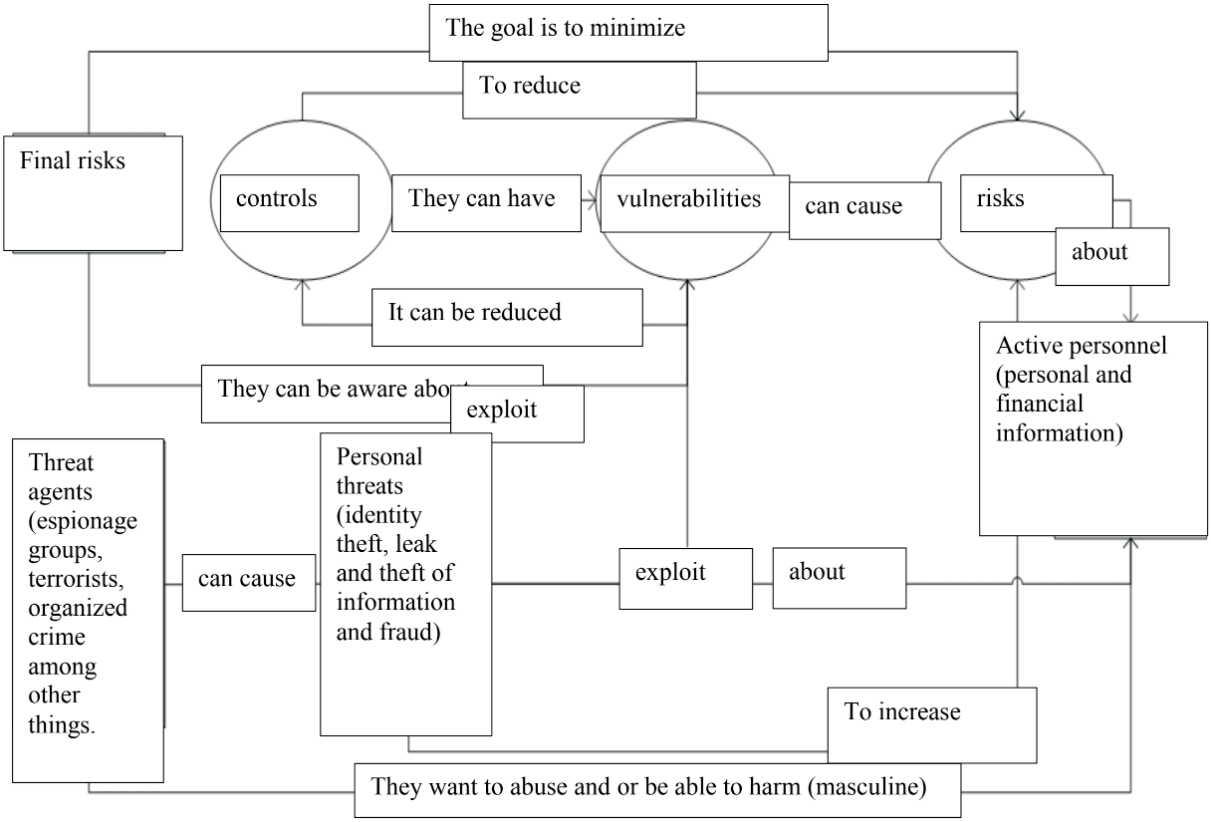

Figure 1: Cybersecurity Life Cycle. Source: Own source.

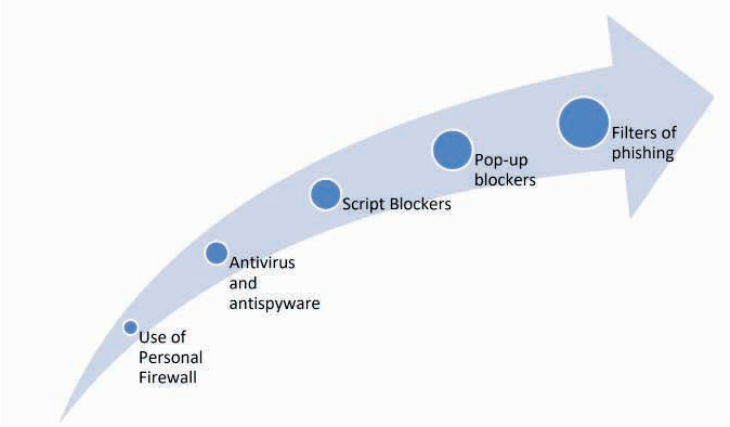

Figure 2: End User Controls of the ISO 27032 Standard. Source: Own source.

As a second contribution of this study, and acknowledging the previous analysis, an exploratory study is proposed in the student community of the Faculty of Engineering of the Autonomous University of Campeche that serves as a reflection on the knowledge and management of user controls. end of cybersecurity and the importance that they currently represent with the excessive use of the Internet as the main medium in distance or hybrid education.

Cybersecurity has become one of the ICT areas that has received the most attention and effort in recent years, both due to the need to respond to the constant growth and sophistication of attacks and risks that society faces as well as the incessant development of the technology itself. In this environment, in which the human factor is a crucial aspect, cybersecurity training and awareness activities are critical elements, which must be constantly deepened, updated and improved.

A series of fundamental measures to psycho-educate education professionals who in their daily work work with children and adolescents through virtual and offline classrooms (Mendivil Caldentey, Sanz Urquijo, & Gutierrez Almazor, 2022):

- There is no ideal chronological age to administer an electronic device to a child. It is more related to the degree of maturity of the minor and with parental control that parents should always monitor.
- Personal data and information should never be provided.
- Make use of the "private" setting. When you publish content in the public sphere, you are automatically allowing all people, including those who do not have a social network account, to access and "use" the information provided.
- Safeguard the information held on external storage devices by encryption or password and not provide these passwords to anyone.
- Carry out backups daily or with relative frequency.
- Scan email attachments using an antivirus.
- Periodically update the operating system software of the devices to reduce their vulnerability.
- Use strong passwords and change them once every three months.
- Install antivirus and antimalware applications.
- Always close sessions when leaving social networks.
- Activate the system Firewall to block unauthorized access.
- Disconnect from the Internet when not in use to prevent intruders from connecting to the network and computers.
- Protect the WIFI network with strong passwords.
- Do not share the user account with anyone. On the mobile you can install App Lock to create passwords in the applications.
- Consult information security experts in case the personal device has geolocators, spy applications or similar.
- Whenever an e-mail or a pop-up (pop-up window) is received with a message in which personal financial information or of any other nature is requested, it is important that it never be answered, but, in addition, it will not be necessary to do click on the links that may appear in the message.

These measures, provided by the authors, add to the end user controls of the ISO 27032

Cybersecurity Standard and its practice in the academic community is recommended.

In the last security meeting, held in 2020, of the ANUIES Security Commission, it was mentioned that 76% of the affiliated Higher Education Institutions have defined their security policy, but a very small percentage are those that have a specific information security plan compared to the number of these (IES 213 to 2020). There are only isolated actions such as courses, diplomas, specialties and postgraduates, for which it was proposed to prepare a catalog in the country with universities that have security programs, actions or plans.

From recent studies, it is essential to highlight the current panorama by Educational Institutions in the face of security risks and what is their action against them. Thus, the perspective of the exploratory study carried out at the Autonomous University of Campeche shown in the results of this study is complemented.

The latest results (ANUIES-TIC 2020) reflect the current educational panorama of Higher Education Institutions in terms of security in the operation of academic programs, and in the strategies and actions of training, dissemination and updating on security issues of the information, on the other hand, emphasizes the importance of having a security policy and the regulations applicable to it, which is disseminated so that compliance is given in this regard.

The analysis of information presented allows detecting the needs, and defining the areas of opportunity to propose actions, in order to strengthen the information security of all universities. The main results presented were (Salazar Mata, Cruz Navarro, Balderas Sánchez, & Díaz Uribe, 2022):

- Regarding the budget and the origin of the resources for information security, they refer that 48% of universities do not have an identifiable budget in terms of security, 21% do not have an assigned budget.
- 76% of universities have a defined security policy, but of these, only 30% have a policy that includes objectives aligned with the institutional ones.
- Regarding the responsibility for security, 52% of Universities report that the person responsible for ICTs in the Institution is the one who is in charge of security.
- 50% of the Universities surveyed use some current reference framework related to information security, implemented throughout the organization, however, of these, only 23% refer to the ISO/IEC 27001 standard and 16% to MAAGTICSI.

.

- Regarding security review, 49% of Universities do not carry out information security audits/assessments.
- And, only 7% of the institutions have current ISO/IEC 27001 certification.
- However, almost 70% of the Universities surveyed have confidentiality agreements as a security strategy.
- Regarding the responsibility of security actions, it refers that 88% of Universities have IT personnel in the areas of networks and telecommunications who additionally work in information security.
- In addition to this, they state that only 7% of Universities have personnel certified in ISO/IEC 27001.
- Regarding whether there is an information security risk treatment plan, 54 of the Universities surveyed have an information security risk treatment plan.
- Finally, 51% of Universities report

having compulsory subjects in their academic programs on information security and 16% elective subjects.

- In addition, 77% of them do not have information security researchers.

CONCLUSIONS

The ISO/IEC 27032 standard or standard provides a secure framework for the exchange of information facilitating secure and reliable collaboration to protect the privacy of people around the world. This standard aims to guarantee the security of information exchanges on the Internet in order to deal more effectively with cyberattacks. One of the main objectives of this standard is to improve security on the Internet. Specifically, this document addresses the controls applicable by end users that are necessary and sufficient to maintain security. Let's not forget that every person connected to the Internet is vulnerable to various threats that, in less experienced end users, are likely to become attacks and/or cybercrimes. In the educational or academic environment, young people have greater empathy for applying tools that allow them to protect their integrity, confidentiality, security and any of their own assets. The study specifies a proposed security model aligned to the end-user controls expected by ISO 27032 Standard, specifying specific technological tools for the environments that have been identified as most used in the student community in Mexico. Finally, it is concluded by highlighting the high need to take protection actions against cybercrimes, emphasizing the vulnerabilities to which the student community is exposed due to the excessive use of the Internet and the technological tools used in the educational field. Not only in the task of academic activities, but also in research and communication of the learning process.

In short, the end-user controls embodied in the ISO 27032 standard in the world of cybersecurity are not enough at all. However, if it is a valuable strategy and by raising awareness among end users, cybercrime will not be as frequent.

As an end user, the responsibility of managing the use of ICTs in the excessive world of Internet and cyberspace must be made aware of effectively and efficiently. In the educational field, all actors, including the educational institution itself, must collaborate in protecting the safety of their own community.

Security is a utopia, however, it is everyone's commitment to reduce the risks and vulnerabilities of cyberspace.

Future lines of research are very diverse, from considering other international standards or norms for the prevention and treatment of vulnerabilities or risk agents to the use and application of own tools for the different stages of the cybersecurity life cycle. In the same way, specific field studies can be carried out that allow the establishment of strategies and control mechanisms in specific contexts of action.

THANKS

We thank Dr. José Alberto Abud Flores, Rector of the Autonomous University of Campeche for the provision and funding granted for the publication of this article. In the same way, attention is extended to the MAC. Francisco Javier Barrera Lao, Director of the Faculty of Engineering for the empathy of promoting, managing and supporting scientific research studies in the area of Education and Information and Communication Technologies. Finally, to recognize MTE Nancy Georgina Ortiz Cuevas, Coordinator of the Computer Systems Engineer Educational Program, for promoting academic and disciplinary research work that leads to professional advancement of the university academic community.

REFERENCES

Aguilar, J., Armando, A., Álvarez González, F. J., Amador Bautista, R., & Barrón Tirado, M. (2020). *Educación y pandemia. Una visión académica.* Mexico: Universidad Nacional Autónoma de Mexico. Instituto de Investigaciones sobre la Universidad y la Educación.

Aguirre Romero, J. (2010). *Ciberespacio y Comunicación: Nuevas formas de vertebración social en el siglo XXI.* Madrid: Biblioteca Virtual Universal.

Almagro, L. (2020). *EDUCACIÓN EN CIBERSEGURIDAD. Planificación del futuro mediante el desarrollo de la fuerza laboral.* Organización de los Estados Americanos (OEA).

Bao, W. (2020). COVID -19 y la enseñanza en línea en la educación superior: un estudio de caso de la Universidad de Pekín. *Human Behavior and Emerging Technologies, 2*(2), 113 - 115.

Blue Hat Corporation. (s.f.). *Introducción a la ISO 27032*. Obtenido de https://www.bluehatcorp.com/iso-27032-ciberseguridad-inicio/

Cano, J. (2008). Cibercrimen y ciberterrorismo. Dos amenazas emergentes. *ISACA Information Control and Audit Journal, 6.*

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Revista Sistemas. Asociación Colombiana de Ingenieros de Sistemas*(119).

Cayón Peña, J., & García Segura, L. A. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. *Estudios en Seguridad y Defensa, 9*(18), 5-13.

CCN-CERT IA-09/18. (2018). *Ciberamenazas y tendencias.*

CEPAL-UNESCO, N. (2020). *La educación en tiempos de la pandemia de COVID-19.* CEPAL, UNESCO.

CISCO. (2014). *Informe anual de seguridad.* San José, CA: Cisco Systems, Inc.

Corletti Estrada, A. (2017). *Ciberseguridad. Una Estrategia Informático/ Militar.* Madrid: Alejandro Corletti Estrada.

Cuevas Ruíz, J. L. (2021). *El papel de la Ciberseguridad en el proceso de la transformación digital en Mexico.* Instituto Federal de Telecomunicaciones.

Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital.* España: Editorial Ariel, S.A.

Garces Giraldo, L. F., Quiroz-Fabra, J., Camilo Patiño, J., & Bermeo Giraldo, M. C. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 225-239.

García Aretio, L. (2021). COVID-19 y educación a distancia digital: preconfinamiento, confinamiento y posconfinamiento. *Revista Iberoamericana de Educación a Distancia, 24*(1).

García Dobarganes, P. C. (s.f.). *Educación en pandemia: los riesgos de las clases a distancia.* Instituto Mexicano para la Competitividad A. C.

Gayoso Martínez, V., Hernández Encinas, L., & Arroyo Guardeño, D. (2020). *Ciberseguridad.* España: Consejo Superior de Investigaciones Cientificas.

González Inés, M. (2021). *El gobierno de la función legal en las organizaciones: Operaciones Legales, Innovación y Digitalización* . España: ARANZADI.

Grupo ACMS Consultores. (s.f.). *Norma ISO 27032 Gestión de la Ciberseguridad*. Obtenido de https://www.grupoacms.com/norma-iso-27032

Hodges, C., Moore, S., Lockee, B., Trust, T., & Bond, A. (2020). La diferencia entre la enseñanza remota de emergencia y el aprendizaje en línea. *Educause Review*.

IESALC-UNESCO. (2020). *El coronavirus-19 y la educación superior: impacto y recomendaciones*. Obtenido de http://www.iesalc.unesco.org/2020/04/02/el-coronavirus-covid-19-y-la-educacion-superior-impacto-y-recomendaciones/

INEN. (2014). *Tecnología de la información - Técnicas de seguridad - Directrices para ciberseguridad (ISO/IEC 27032:2012, IDT)*. Quito: NORMA TÉCNICA ECUATORIANA.

INNOVACIÓN EDUCATIVA. (s.f.). CIBERSEGURIDAD Y COMPETENCIA DIGITAL. *GAPTAIN*.

Instituto Español de Estudios Estratégicos . (2010). *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacios.* Madrid: Ministerio de Defensa.

ISO 27032. (2012). *Ciberseguridad utilizando la norma ISO 27032:2012.* Bogotá.

Jean-François, C. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* España: Ediciones Eni.

Joyanes Aguilar, L. (2021). *Internet de las cosas. Un futuro hiperconectado: 5G, inteligencia artificial, Big Data, Cloud, Blockcha.* España: MARCOMBO, S.L.

Lozano-Díaz, A., Fernández-Prados, J. S., Figueredo Canosa, V., & Martínez Martínez, A. M. (2020). Impactos del confinamiento por el COVID-19 entre universitarios: Satisfacción Vital, Resiliencia y Capital Social Online. *International Journal of Sociology of Education, Special Issue: COVID-19 Crisis and Socioeducative Inequalities and Strategies to Overcome them*, 79 -104.

Mariano Díaz, R. (2020). La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. *CEPAL*(6).

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Píxel-Bit. Revista de Medios y Educación.*, 197-226.

Oficina de seguridad de internauta. (s.f.). *Guía de ciberataques.* INSTITUTO NACIONAL DE CIBERSEGURIDAD.

Parra Cárdenas, H., Fernández Lorenzo, A., & Recalde Herrera, L. (2017). Directrices para la gestión de la Ciberseguridad utilizando el estándar ISO/ECT 27032. *Estudios en Seguridad y Defensa, 12*(24), 99-111.

Pedró , F. (2020). COVID-19 y educación superior en América Latina y el Caribe: efectos, impactos y recomendaciones políticas. *Análisis Carolina*.

Petar, J., Knox, J., Besley, T., Ryberg, T., Suoranta, J., & Hayes, S. (2018). Ciencia y educación postdigital. *Educational Philosophy and Theory, 50*(10), 893-899.

Ribagorda Garnacho, A. (s.f.). *PANORAMA ACTUAL DE LA CIBERSEGURIDAD.* Madrid: Universidad Carlos III de Madrid.

Rodríguez Canfranc, P. (2014). *Ciberseguridad: Protegiendo la información vulnerable.* Telefonica Fundación.

Salazar Mata, J. M., Cruz Navarro, C., Balderas Sánchez, A. V., & Díaz Uribe, H. F. (2022). La Seguridad Informática en las Instituciones de Educación Superior. *Pixel-BIT. Revista de Medios y Educación*, 197-225 .

Secretaría de comunicaciones y transporte. (2020). *Guía de ciberseguridad para el uso de redes y dispositivos de telecomunicaciones en apoyo a la educación.*

Tapia Hernández, E. F., Ruiz Canizales, R., & Vega Páez, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Revista Misión Jurídica, 14*(20), 142-158.

Urueña Centeno, F. J. (2015). CIBERATAQUES, LA MAYOR AMENAZA ACTUAL. *Documento Opinión*.

Valencia Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas iso/iec 27000*. Bógota: Universidad Nacional de Colombia.