Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Information Security Management in A Higher Education Institution Based on Standards, Legal Basis for the Optimization of Administrative Resources

Diego Andrade A.[1], Moisés Toapanta T.[2], Rodrigo Del Pozo Durango[3], Oswaldo Vanegas-Guillén[4], Pamela Toapanta Pavón[5], Zharayth Gómez D.[6], Roció Maciel A.[7], Antonio Orizaga T[8]

Abstract

Problems in managing information security for access to remote laboratories in higher education institutions are persistent worldwide. The objective of this research is to define alternatives to mitigate risks, vulnerabilities and threats in a remote laboratory for the management of information of students, teachers and administrators in a higher education institution. The deductive method and exploratory research were used with the application of seven phases defined by the authors. It resulted a simulation of the evaluation of the information security of a remote laboratory, an Architecture of a remote laboratory integrating virtual learning environments and a Model for the integration of information security in remote laboratories. It was concluded that information security analysis to mitigate risks, vulnerabilities and threats in a remote laboratory of a higher education institution is crucial to guarantee data protection, experiment management and integrity, confidentiality and availability (CIA). for information management of students, teachers and administrators; considering the optimization of administrative processes and the legal basis.

Keywords: *Legal Basis, Administrative Processes, Remote Laboratories, Security and Privacy, Virtual Education, Information Security, Virtual Environments.*

Introduction

Information security problems are persistent globally. In this research, information security for remote laboratories in higher education institutions is important and a priority for educational management to mitigate the risks, vulnerabilities, and threats in their processes. Educational remote laboratories are cyberphysical systems that offer students the opportunity to remotely access laboratory experiments through a computer network. These interconnected learning environments have the capacity to transform the way science and engineering education is delivered, thereby removing geographic and temporal barriers. Fundamentally, these laboratories are integrated into Learning Management Systems (LMS) through interoperability protocols or standards. This approach not only ensures a smooth transition between different platforms and applications, but also allows effective collaboration between various educational tools. Remote educational laboratories have learning analytics functionalities that allow the detailed monitoring and evaluation of educational processes. Learning analytics collects and analyzes student data to provide a clear view of their progress, allowing educators to personalize their teaching approaches to improve student performance. It is important to highlight that security and protection are of utmost importance in these applications. The educational nature and potential exposure to various risks and robust

[1] Centro de Estudios de Seguridad (CESEG), Universidad de Santiago de Compostela (USC), Santiago, España, Email: diegoandradea@hotmail.com.
[2] Centro de Investigación en Mecatrónica y Sistemas Interactivos (MIST), Ingeniería en Tecnologías de la Información, Universidad Tecnológica Indoamérica, Quito, 170301, Ecuador, Email: moisestoapanta@uti.edu.ec.
[3] Postgraduate Director, Universidad Estatal de Bolívar (UEB), Guaranda, Bolívar, Ecuador, Email: rdurango1973@yahoo.es.
[4] Information Technologies Department, Faculty of Mathematical and Physical Sciences, Universidad de Guayaquil, Guayaquil, 090514, Ecuador, Email: oswaldo.vanegasg@ug.edu.ec.
[5] Facultad de Ciencias administrativas, Universidad Central del Ecuador, Quito, 170129, Ecuador, Email: pamela12004@hotmail.com
[6] Research Department, Gestión de Tecnologías Para El Mundo (GTM), Quito, 170301 Ecuador and Doctorado en Ciencias de la Educación, Universidad Pedagógica Experimental Libertador, Caracas, 1014, Venezuela, Email: zharaythgomez2709@gmail.com
[7] Information Systems Department of the CUCEA University of Guadalajara (UDG), Guadalajara, México, Email: ma.maciel@academicos.udg.mx
[8] Information Systems Department of the CUCEA University of Guadalajara (UDG), Guadalajara, México, Email: jose.orizaga@academicos.udg.mx

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

security measures must be implemented to protect the confidentiality, integrity, and availability of the system with the privacy of users. Consequently, safety and security aspects must be considered from the beginning of the design and implementation of remote laboratories problems in judicial management persist regarding the applicability of artificial intelligence (AI) systems. Currently, they have become a challenge as they lack legal foundation and legitimacy, given that to date, only a minimal number of countries have laws addressing the supervision, regulation, management, and control of the applicability of artificial intelligence systems. Below, we identify possible issues, advantages, and trends of AI in relation to judicial management:

According to a National Cyber Security Center (NCSC) report, the education sector is facing an increase in cybersecurity risks, threats, and vulnerabilities(Centre, 2021). It is important to mention that Microsoft Security Intelligence mentions that the educational sector has the highest risk of malware(Microsoft, 2023). Safety and security challenges in educational remote laboratories include intrusions through remote access, sabotage, and student/employee dissatisfaction due to a lack of adequate identification, authorization, authentication, and auditing (IAAA) risk analysis and the use of standardized risk matrices that can facilitate comparisons between laboratories, security of remote laboratories, security of virtual learning environments, security in analytical tools, and security in interoperability tools(Uckelmann, Mezzogori, Esposito, Neroni, Reverberi, Ustenko, et al., 2021). The main security issues are privacy faced by virtual learning environments, unauthorized access to educational data, misuse of data by cloud storage servers, and the need for security controls(Ben Amor et al., 2020). The authors mentioned the following security problems in virtual learning management systems: unauthorized access, data theft, inadequate authentication and password security, insecure communication channels, and insufficient data protection(Faculty, 2016). They identified issues that included the potential for cheating in testing systems, concerns about authentication and data security, and issues related to technology compatibility and reliability(Butler-Henderson & Crawford, 2020). During the Covid-19 pandemic, the main privacy security problems faced by virtual learning environments have been identified, including the disclosure of data without authorization, violation of private information, lack of secure communication, and unauthorized access(Almahasees et al., 2021). The main security and privacy challenges faced by virtual learning environments include data protection, risk of data breach, and identity theft(Singh & Sisodia, 2021). The main security and privacy issues facing virtual learning environments include unauthorized access to student information, data leaks and breaches, and the collection and use of confidential student information without proper consent or transparency(Ang et al., 2020). The authors of this research determined that there are academic dishonesty, problems in privacy and confidentiality, and a need for data protection are challenges that virtual learning environments (VLE) have(Darren Turnbull, 2021). Another problem is the lack of transparency and integrity of data in online education platforms to mitigate risks, such that the security of information has confidentiality, integrity, availability, and privacy(Wang et al., 2022). Learning management systems (LMS) face several privacy implications, including the protection of student data, the use of surveillance practices, and issues with sharing data with third parties, among others(Amigud et al., 2018). Key challenges and considerations that must be addressed when developing protection policies for management systems were identified(Turnbull et al., 2022). The authors defined the security and privacy challenges facing virtual learning environments as authentication, data protection, integrity, availability, and confidentiality(Salimovna, 2019). They established that remote laboratories face the following problems related to data security, access, and hacking attacks(Emilio Werner, Jhennifer Cristine Matias, 2023). Problems identified by the authors include viruses, malware, and impersonation of users remotely, as they may allow unauthorized access to laboratory systems and resources(Rivera & Petrie, 2016). In remote laboratories integrated with learning management systems (LMS), several solutions have been identified to address the security challenges posed in trust calculation, authentication methods, data manipulation, and dynamic architecture. These solutions highlight the need for a proactive and strategic approach for security in remote laboratories(Palka & Schauer, 2015). Cyber-physical systems are subject to a series of vulnerabilities that can compromise their security and effectiveness. First, exposing insecure devices to public networks can increase their susceptibility to external attacks, and common protocols can contain inherent vulnerabilities, backdoors, and gaps in the network perimeter that can be exploited by malicious actors(Asghar et al., 2019). Regarding analytical solutions, they stated that the main security and privacy challenges faced by virtual learning environments with respect to learning analytics are data privacy and knowledge of the adversary's background(Gursoy et al., 2017). The implementation of remote laboratories

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

has not been carried out in the majority of HEIs because the technological processes linked to academic processes are not yet clearly defined. Remote laboratories are used in educational environments for several reasons: when the equipment is not available where the student is, due to unavailable physical spaces, and availability of the physical presence of the teacher or student, among others(Rivera & Larrondo-Petrie, 2016). The transformation of the education system from face-to-face to online education through the Internet provides a hands-on learning experience for online students. A remote laboratory learning system offers the flexibility to be deployed in any physical environment(El-Haleem et al., 2023). The authors state that remote laboratory management is currently the basis for online education in engineering, administration, and other fields. They propose a novel architecture that simplifies the development and management of remote experiments using a communication paradigm between publisher and subscriber to integrate WebAssembly computational notebooks in a secure and efficient manner. In their analysis, they highlight both the advantages and challenges of the proposal, with a significant emphasis on interaction, scalability, reuse, interoperability, and accessibility(Vanegas-Guillén et al., 2023). They determine that the lack of adequate models based on information technologies for the management of administrative processes has caused immense damage to public and private companies, higher education institutions, among others. They state that one of the options to improve the management of administrative processes is the generation of a conceptual model to minimize risks, a risk control prototype, a flow chart of the prototype, a process simulation with five scenarios, determination of the formula to detect the probability of a company closing, analysis and evaluation of risks; this structure can be applied in the management of remote laboratories for the optimization of administrative processes(Altamirano et al., 2024). They state that the legal basis must currently be applied in all areas of ICT that are going to be implemented. The information generated in laboratories for their management must constitute mandatory elements of the formulation of policies and the drafting of laws(Mariusz MACIEJEWSKI, Policy Department for Citizens' Rights and Constitutional Affairs, 2024). The authors mention that all digital projects must be supported by a legal basis in order to protect user profile data at all levels. A key element of such a digital profile should be a digital consent system designed to transfer data from state registries to other persons in order to receive services from them based on the legal basis of the country where it is implemented(Bundin et al., 2023). The legal framework is currently necessary to apply to all projects related to information and communications technologies. They state that in Ecuador there are no clear laws to mitigate risks and vulnerabilities in the management of information security. They recommend applying the legal basis for all administrative processes generated by the implementation of technological solutions(Armas et al., 2024). Laboratories of higher education institutions must have information security management; for this, automated administrative processes are required. The authors recommend using a data matrix algorithm to design the new strategy for scientific information security in the university administrative management system with optimized processes(Wei, 2022).

Why is it necessary to perform the analysis for Information Security Management in a higher education institution based on standards, a legal basis for the optimization of administrative resources?

To determine alternatives that allow the mitigation of risks, vulnerabilities and threats in information management through virtual learning environment architectures, information security, remote laboratories, prototypes or models.

The objective of this research is to define alternatives to mitigate risks, vulnerabilities and threats in a remote laboratory for the management of information of students, teachers and administrators in a higher education institution.

The results were a simulation of the evaluation of the information security of a remote laboratory, an architecture of a remote laboratory integrating virtual learning environments and a model for the integration of information security in remote laboratories.

It is concluded that information security analysis to mitigate risks, vulnerabilities and threats in a remote laboratory of a higher education institution is crucial to guarantee data protection, experiment management and integrity, confidentiality and availability (CIA). for information management of

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

students, teachers and administrators; considering the optimization of administrative processes and the legal basis.

Literature Review

Cloud-based educational platforms and remote laboratories (labs) enable remote access to lab equipment over the Internet and seamlessly pool and sharing resources(Crichigno et al., 2021). Remote laboratories allow the extraction of the data necessary to discover, design, acquire, and evaluate new knowledge. They defined three types of users: students, teachers, and administrators. The contribution of this study is the implementation of a remote thermal-fluid laboratory(Guillen et al., 2021). They have designed and built assets to enable physical engineering laboratories. Using this approach, they increased the capacity of the laboratory so that students could operate at their convenience and in remote locations; however, language limitations must be considered(Bolu, 2022). They offer a promising solution for integrating renewable energy and distributed generation into grids. Virtual and remote laboratories are widely accepted for conducting higher education experiments, and they have developed a web-based virtual laboratory for renewable energy microgrids that they use to teach renewable energy(Guo et al., 2022). They provide facilities that guarantee results of the same quality as physical models, reduce costs, and provide access to students who do not have access to the laboratories. They developed security and access control systems for remote laboratories using blockchain technology to standardize and update the security processes using new security technologies(Werner et al., 2021). To improve student experience, they proposed a method to integrate adaptive remote laboratories with virtual learning environments and automatically adjust experiments according to students' existing level of knowledge and experience(Rivera et al., 2017). They developed a system for student use in a remote-access mechatronics laboratory without human supervision. Students can monitor their learning in real time and receive evidence of success or failure through the gamification of their performance(MacHado et al., 2022). They built a remote control platform based on various programming languages and big data for construction, with free access to promote new teaching tools in classes(Ryan et al., 2013). They feature remote and virtual on-site laboratory models, each with its own set of advantages, and emphasize different learning objectives by using technology to simplify the design and operation of remote and virtual laboratories(Alsaleh et al., 2022). They analyzed and synthesized relevant research and studied the composition of remote laboratories. Students can visit remote laboratories. They determined a platform with tools for laboratory management to support interactions among students, teachers, and administrators(Amnuaysin et al., 2022). They evaluate the effective application model of teaching laboratories in a traditional research-oriented context but do not guarantee the quality of services in a real educational environment; remote laboratories are becoming a standard tool in educational environments(Aitor et al., 2022). They proceed with a theoretical analysis of learning with industrial automation technology and how remote laboratories are more efficient for students to obtain an innovative way to learn, even when they are not present in the classroom(Pereira & Felgueiras, 2020). Remote laboratories for engineering and instrumentation courses at the University of Edinburgh were created using the first iteration of a new open-source infrastructure. The authors concluded that skill-based and conceptualization learning interactions established for engineering laboratories are appropriate(Reid et al., 2022). The definition of a remote laboratory allows remote users to perform desired laboratory exercises and control laboratory equipment to develop and implement tools and experiments that facilitate access to competent academic training in science and engineering(Stefanovic et al., 2011). They implemented an experimental system in a remote laboratory as a resource for learning and teaching science in the future, which complements regular scientific experiments in schools(Tho & Yeung, 2018). They performed a systematic analysis and provided a reference for system implementation for the creation and development of remote laboratory systems for automated control that are suitable for remote use via the web, which is mainly concerned with teaching management concepts rather than developing software, resource sharing, and security(Leva & Donida, 2008). They describe their experience in remote laboratory control for teaching and research in the field of technology for regulation and evaluate the performance of the system using the capabilities of the remote laboratory platform they offer(Santana et al., 2013). The authors determined that remote laboratories are suitable for higher education processes that allow scalability, flexibility, and add value to educational processes. The laboratory architecture was based on a three-tier architecture (physical system, server, and client layers). The client layer was implemented using web

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

standards, such as HTML5, AJAX, and CSS. One of the results obtained by the researchers is the web interface of the classification cell(Prada et al., 2015). The authors conducted a study that included a literature review on remote laboratory security, investigated the existing requirements, and defined the operational requirements for a federated remote laboratory security guide. They then analyzed existing standardization approaches and guidelines, and proposed a guide that fits their requirements(Uckelmann, Mezzogori, Esposito, Neroni, Reverberi, & Ustenko, 2021). The authors proposed the development of a cybersecurity framework using advanced technologies such as artificial intelligence and deep learning to combat cyberattacks in remote laboratories(Vinodha et al., 2021). They designed a model to evaluate security in virtual learning environments (VLE) based on security criteria identified in manuals, norms, and standards. They focused their research on three main criteria: integrity, confidentiality, and the availability of information. They then analyzed metrics to quantify these relationships and validated their model by applying it to the Moodle and Dokeos VLE platforms, obtaining a qualitative and quantitative assessment of the security status of these environments(Callejas-Cuervo et al., 2016). The authors illustrated their analysis through a case study of the TeSLA project, evaluating how design decisions improve the efficiency and legal compliance with personal data protection. Furthermore, they proposed alternative designs that could address this issue(Kiennert et al., 2019).

Methodology

First phase

We identified problems in remote laboratories based, on a review of reference articles from the introduction phase. It is important to mention that, for the continuous improvement of remote laboratories, it is necessary to consider physical security, security of technological infrastructure, human resources, and media, among others, to mitigate risks, vulnerabilities, and threats to information management.

Below are the basic elements that should be considered in remote laboratories:

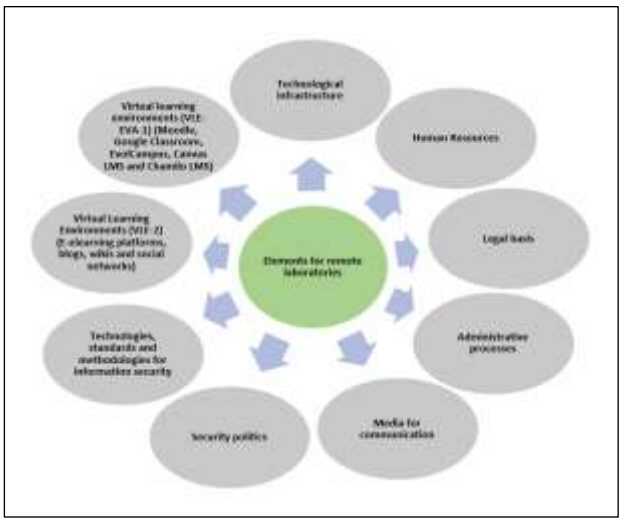

Figure 1. Basic Elements for A Remote Laboratory

In this phase, it is also important to note that the analysis of the main security and privacy problems must be conducted in virtual learning environments (VLE), remote laboratories, analytics tools, and interoperability tools.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Second phase

An analysis was performed to identify the security challenges in remote laboratories, learning management systems (LMS), virtual learning environments (VLE), cyber-physical systems, federated remote laboratories, and industrial control systems.

Security challenges in remote laboratories.

Table 1. Describes The Most Relevant Challenges of Information Security in Remote Laboratories

Security issues	Potential implications	Type	Ref.
Unauthorized access, data leakage, improper authentication and passwords.	Compromise of student privacy, interruption of the learning process, loss of trust in systems	VLE	(Faculty, 2016)
Lack of secure communication channels, insufficient data protection.	Potential data breach, risk of exposure of sensitive information.	VLE	(Faculty, 2016)
Technology compatibility and reliability issues, academic dishonesty	Possible risk of data manipulation, concerns about privacy and confidentiality.	VLE	(Butler-Henderson & Crawford, 2020) (Darren Turnbull, 2021)
Data privacy (VLE, LMS), information breach (VLE), secure communication missing (VLE).	Need for data protection, risk of loss of confidential information, interruption.	VLE LMS	(Almahasees et al., 2021) (Amigud et al., 2018)
Lack of efficiency, interaction, privacy, security, transparency, integrity and data risks (VLE).	Difficulty in data analysis, challenge for data privacy and security, theft prevention, among others.	VLE	(Wang et al., 2022)
Unauthorized access (VLE) integrated into LMS), data theft (LMS), communication risks (LMS).	Risk of data breach, loss of confidential information, possible exposure of student data in (LMS).	VLE LMS	(Palka & Schauer, 2015)
Insecure devices on public networks, invasive hardware attacks, replacement of PLCs with common computers.	Increased susceptibility to external attacks, compromised physical integrity of the system and increased number of cyberattacks.	Remote laboratories and cyber-physical systems.	(Asghar et al., 2019)

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Hacking attacks, malware, data leaks, spam, malware intrusion, impersonation of users remotely, communication risks, network threats.	Interruption of services and loss of data, compromise of system integrity, unauthorized access to systems and resources, among others.	Remote Laboratories and Learning Management Systems	(Uckelmann, Mezzogori, Esposito, Neroni, Reverberi, Ustenko, et al., 2021) (Emilio Werner, Jhennifer Cristine Matias, 2023) (Rivera & Petrie, 2016)(Palka & Schauer, 2015)(Asghar et al., 2019)
Problemas de seguridad de los datos y acceso autenticado, credibilidad de acceso, robo de datos, etc.	Exposure of sensitive data and unauthorized access to resources, laboratories, etc.	Remote, federated laboratories, industrial control systems and LMS.	(Uckelmann, Mezzogori, Esposito, Neroni, Reverberi, Ustenko, et al., 2021) (Emilio Werner, Jhennifer Cristine Matias, 2023) (Rivera & Petrie, 2016)(Palka & Schauer, 2015)(Asghar et al., 2019)
Data manipulation and lack of counterattack tools.	Compromise of data integrity and degradation of the data warehouse	Remote laboratories and LMS.	(Palka & Schauer, 2015)

Third phase

In this phase, the analysis of the most relevant information was carried out, referring to the possible solutions of information security and related topics of remote laboratories, learning management systems (LMS), virtual learning environments (VLE), systems cyberphysicists, federated remote laboratories and industrial control systems carried out by the different authors.

Table 2. Analysis Of Possible Solutions Related to Remote Laboratories

Solution to the proposal	Solution category	Potential impact	Ref.
Laboratory that integrates students, teachers and administrators	Remote laboratories.	Design, acquire and evaluate new knowledge.	(Guillen et al., 2021)
Physics engineering laboratories.	Remote locations	Limitation in language.	(Bolu, 2022)
Web-based virtual laboratories	Virtual laboratories.	Conduct higher education experiment.	(Guo et al., 2022)
Using blockchain technology	Remote laboratories	Security and access control systems.	(Werner et al., 2021)

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Basic principles of pedagogy. They propose a method of integrating laboratories.	Adaptive remote laboratories with virtual learning environments.	Existing level of knowledge and experience of students.	(Rivera et al., 2017)
Remote access without human supervision.	Remote laboratories.	Real-time learning so you receive evidence of success and failure.	(MacHado et al., 2022)
Remote control platform based on programming	Remote laboratories.	Free access	(Ryan et al., 2013)
They determine a platform with tools for laboratory management.	Tools for remote laboratories.	Interactions between students, teachers and administrators	(Amnuaysin et al., 2022)
Open-source infrastructure.	Remote laboratories.	Skills and conceptualization.	(Reid et al., 2022)
Automated control that is suitable for remote use via the web.	Remote laboratories	Teaching management concepts for software development	(Leva & Donida, 2008)
The architecture is based on three levels (physical system layer, server layer and client layer).	Remote laboratories.	Scalability and flexibility	(Prada et al., 2015)
Security literature review to improve a remote laboratory	Federated remote	Security guide	(Uckelmann, Mezzogori, Esposito, Neroni, Reverberi, & Ustenko, 2021)
Design of a model to evaluate security.	Virtual learning environments (VLE).	Confidentiality, integrity and availability.	(Callejas-Cuervo et al., 2016)

Fourth Phase

We conducted an analysis of the information in Tables I and II, where it can be seen that the majority of remote laboratory solutions, including virtual learning environments, do not specify the security levels defined for the detailed management of processes and information. For mitigate risks, vulnerabilities, and threats based on confidentiality, integrity, and availability (CIA) under a scheme of identity, authenticity, authorization, audit (IAAA), and the use of new technologies.

In the analyses carried out in general, a lack of specification of security levels in remote laboratory solutions was identified, including in virtual learning environment laboratories. To mitigate risks, vulnerabilities, and threats, an approach based on confidentiality, integrity, and availability of information is required, supported by an identity, authenticity, authorization, and audit (IAAA) scheme. In addition, the use of new technologies must be considered for the two types of laboratories that are related, but each operates independently. Virtual learning environments (VLE), remote laboratories, analytical tools, and interoperability tools interact so that laboratories are adequate.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Fifth Phase

We analysed information directly related to the security of remote laboratories, as detailed below. An information security and physical security model for learning management in online laboratories, which considers laboratories to be cyber-physical systems (CPS) used for pedagogical purposes involving various security policies adapted to the e-learning environment with real computers on the other side of the screen, implies several potential weaknesses in the system, considering the policy-based security model. The authors proposed a security model with particularities in the educational context, seeking to preserve the security of users and equipment, and proposed a general abstraction that can be applied to different types of scenarios and technologies(Transactions, 2016). Remote laboratories are considered reliable alternatives to traditional practical laboratories and safety and security issues have become increasingly important. The authors provided guidance for evaluating the safety and security of federated laboratories by following the VDI/VDE 2182 guidelines(Uckelmann, Mezzogori, Esposito, Neroni, Reverberi, Ustenko, et al., 2021). The first level of the standard offers an online laboratory (lab) as a service (Lab as a Service or LaaS). The standard also defines methods for integrating online laboratories as intelligent learning objects into learning environments and object repositories. The authors recommend applying the EEEE Std 1876-2019 IEEE Standard for Networked Intelligent Learning Objects for Online Laboratories(IEEE Education Society, 2019).

Sixth Phase

In this phase, with the identification of problems that are persistent for remote laboratories in higher education institutions, according to the analysis of the information from the introduction and materials phase, a diagnosis is made to prepare the base architecture of a remote laboratory.

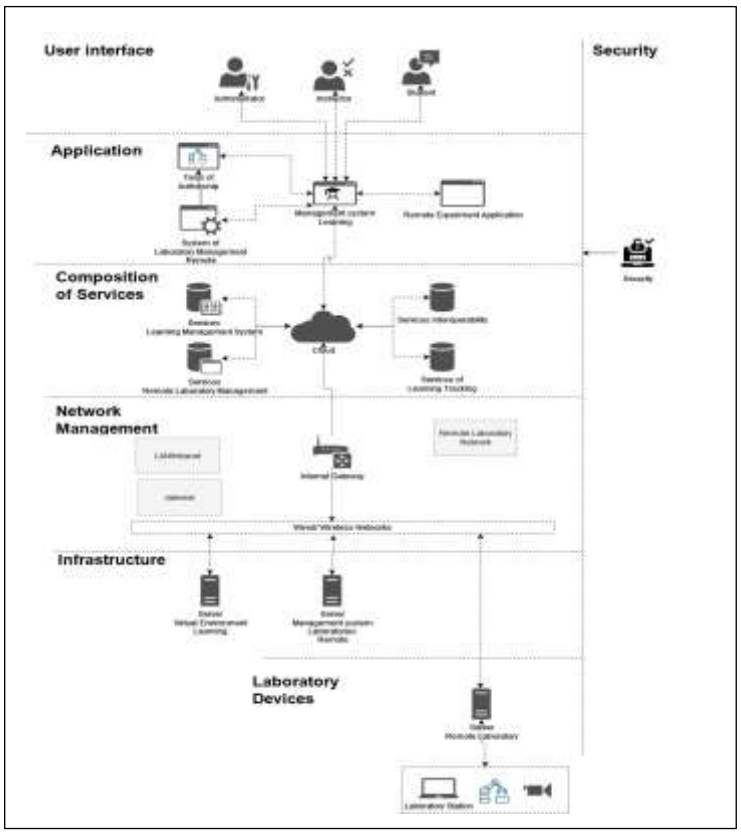

Figure 2. Definition of the Base Laboratory.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

In Figure 2, the base architecture of the security of a remote laboratory is defined by the following structure: infrastructure, network management, composition of services, application, and user interface, as described below.

The infrastructure layer is composed of a virtual learning environment server, remote laboratory management system server, and remote laboratory server with its respective devices that allow the management of the laboratories to begin. The network management layer through the Internet/gateway allows us to connect to the next layer with the network of remote laboratories. The service composition layer through the cloud allows communication with the next layer to provide the following services: learning management system, remote laboratory management, interoperability, and learning monitoring. In the application layer of the learning management system, we communicate with the next layer for the use of authoring tools, remote laboratory management systems, and remote experimental applications. The administrator, instructor, and students intervene in the user interface layer to use the defined base laboratory infrastructure.

Seventh Phase

In this phase, we define seven categories with their respective indicators, which will be used for different simulations and operations.

Table 3. Definition Of Categories with Their Indicators.

Ord.	Solution category	Indicators
1	Technical security and educational infrastructure.	Network protection, Updates, End user protection, Proper configuration, Security for integration, Definition of a TIER III, ISP Provider, Server, Bandwidth, Antivirus, Firewall, Information backup, System resilience.
2	Risk management and incident response.	Risk identification, Risk assessment, Risk mitigation, Incident preparation, Incident response, Recovery after incidents, Learning from incidents.
3	Information security and data privacy.	Personal data management, Information access controls applied by the IAAA, CIA Application, Data encryption, User consent, Privacy Impact Assessment, Learning Analytics Data Security.
4	Security and compliance management.	Governance policies, Strategic policies, Tactical policies, Operational policies, administrative policies, Compliance with security policies, Security audits, Conformity assessment, Interoperability tools, Security of learning analytics tools.
5	User participation and awareness.	Participation in security training, Understanding security policies, Compliance with security policies, Safety education, Interoperability Tools, Participation in the use of learning analytics tools, Awareness of privacy and data use in learning analytics.
6	Security of remote laboratory systems.	Secure access to equipment and systems, Security of control systems, Protection of remotely controlled physical equipment, Security in the use of interoperability tools, Data privacy and security in learning analytics.
7	Security Methodologies and Standards.	Standards Compliance, Blockchain-based security, Hyperledger Network, New technologies, ISO 27701, Cobit 2019, ISO 27001, IEEE Std 1876-2019, IEC 62443.

Table 3. Shows in general terms the categories and indicators based on the judgment of experts and information technology infrastructure, which must be considered to mitigate risks, vulnerabilities, and threats in information management, the same ones that can be used in the results phase for their respective simulation.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Results

The results obtained in this research are:

- Simulation of the evaluation of the information security of a remote laboratory
- Architecture of a remote laboratory integrating virtual learning environments.
- Model for the integration of information security in remote laboratories.

Simulation of the evaluation of the information security of a remote laboratory

The evaluation of the information security of a remote laboratory integrated into a virtual learning environment was carried out using interoperability and learning analysis tools applying the indicators defined in this research. These indicators cover areas such as technical security and educational infrastructure, risk management and incident response, information security and data privacy, security governance and compliance, user participation and awareness, and systems security, methodologies and standards for re-mote laboratories.

For the evaluation, three key dimensions were considered: the security of the indica-tor (S), probability of a security incident (p), and impact of a security incident (A). S rates the effectiveness of the security measures from 1 (indicating very poor security) to 5 (indicating excellent security). P estimates the probability of an incident occurring on the same scale, with 1 being very unlikely and 5 very likely.

Finally, (A) measures the possible consequences of an incident, with one representing minimal impact and five representing severe impact. Together, these indicators allow for a comprehensive and nuanced assessment of security, highlighting both the robust areas and those that require further attention.

Quantify laboratory safety

To quantify laboratory safety, we propose a "loss" function L(S, p, A) that reflects the negative impact of a safety incident. This function considers the rating of the indicator (S), probability of an incident (p), and impact of the incident (A). A possible model for the loss function is the product of p, A, and the difference between the six and S:

$$L(S, p, A) = p * A * (6 - S) \quad (1)$$

Evaluate the Projected Average Loss

To evaluate the projected average loss, labeled E[L], resulting from security incidents in the system, we incorporated the values assigned to each of the three indicators: security (S), probability of an incident (P), and impact of an incident (A). This procedure is formulated as follows:

$$[L] \approx \frac{1}{N} * \sum_{i=1}^{N} L(S_i, p_i, A_i) \quad (2)$$

Where N represents the total count of indicators in each security category and the sum operation is performed for all indicators. This metric, E[L], predicts the average loss expected owing to security incidents, thus providing an accurate quantitative assessment of the security level. A smaller value of E[L] denotes a higher level of security, implying a more robust and effective security implementation.

$$\mathbb{E}[L]_{normalized} = \frac{\mathbb{E}[L] - L_{min}}{L_{max} - L_{min}} \quad (3)$$

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Below is a simulation of the evaluation that was carried out in excel, integrating all the categories and indicators, in graphic mode in order to visualize the entire process that was carried out to determine its applicability in the future.

Figure 3 presents the simulation evaluation of security indicators, expressed as normalized E, in the two prominent education institutions. This assessment is conducted by experts in the field, for compares the effectiveness of the security policies and practices implemented at each institution. Additionally, the minimum required values for E for each indicator are provided to ensure an adequate level of safety. This quantitative analysis allowed for an accurate assessment of the strengths and weaknesses of security measures implemented at each institution.

A quantitative study of information security in remote laboratories has revealed robust implementation across multiple domains. In particular, areas such as " educational technical, infrastructure security, and "security of remote laboratory systems" show acceptable levels of protection. However, "Security Methodologies and Standards" register slightly higher values, indicating the need for constant review and update. The obtained data, supported by empirical and verified data, are crucial for the design and implementation of effective security strategies in remote laboratory environments.

It was determined that in institution 1, all the indicators of the category "security methodologies and standards" exceeded the minimum with a score of 0.35. In institution 2, the sum of all the indicators of the category “security of remote laboratory systems” exceeds the minimum with a score of 0.32. After performing the respective evaluations of all categories with their respective indicators, it is recommended that for a laboratory to be adequate, the general average must be in the minimum range of 0.3, equivalent to 3.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Figure 3. Evaluation Simulation Results

Architecture of a remote laboratory integrating virtual learning environments

We represent various elements and categories in a remote laboratory architecture that integrates virtual learning environments:

Communications

The communications are transverse and contain the following elements: Internet, Internet/Lan, firewall and network security, API, interoperability tools, learning tracking, web services, video tools, data synchronization services, and remote laboratory communication, which allow the interoperability of a remote laboratory.

Security

Security must be transversal for remote laboratories and include the following categories: security methodologies and standards, user participation and awareness, security management and compliance, information security and data privacy, risk management and response to incidents, security of remote laboratory systems, technical and educational infrastructure security, and mitigation of information management in a remote laboratory.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Infrastructure

The infrastructure, data, platform, services, processes, and user interface have a transversal interface of administrators, instructors, and students, where everything de-pends on the communication elements and security processes. These components work together to allow students to access content, participate in learning activities, and connect with friends and teachers. For remote laboratories, diagrams can show the different com-ponents and their relationships. In either case, diagrams can be useful for understanding the overall system architecture, identifying key interactions between components, and visualizing the flow of information in a virtual learning environment or remote lab experience.

Architecture

The architecture of a remote laboratory integrating virtual environments for learning is an alternative to identify possible improvements in the performance, security, accessibility and usability of these environments in a higher education institution.

Diagram

The block diagram made it possible to clearly identify the transversality for the management of learning of virtual environments and remote laboratories to mitigate risks, vulnerabilities and threats to information management in remote laboratories

Remote laboratory project

To define a remote laboratory project in higher education institutions, it is first necessary to carry out an "Information Security Analysis for a remote laboratory" to clearly identify its infrastructure and requirements prior to its execution and implementation.

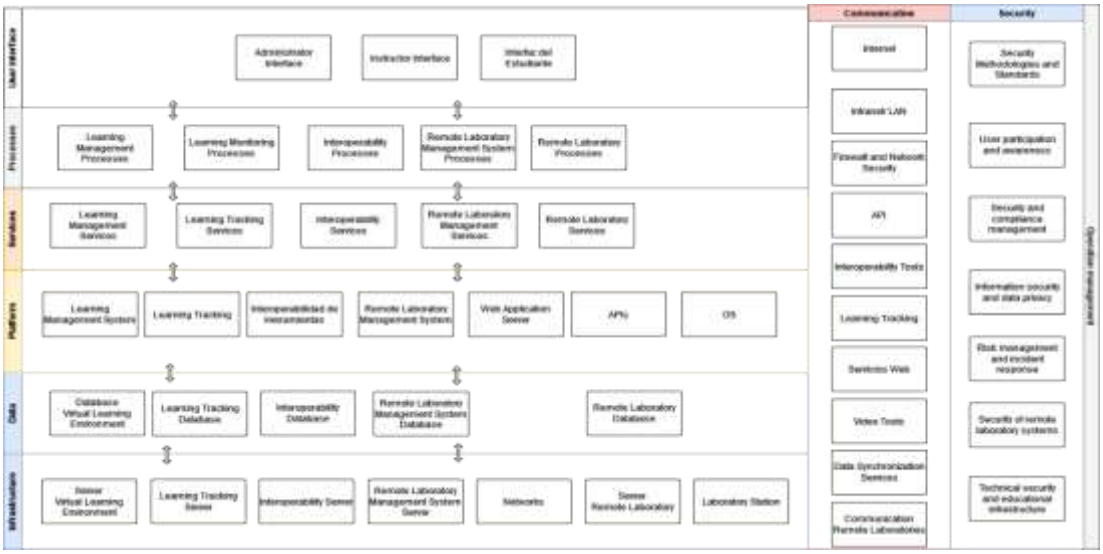

Figure 4. Block Diagram of The VLE And Remote Laboratories

Model for the integration of information security in remote laboratories

Technical Security and Educational Infrastructure

Technical security and educational infrastructure, along with their respective indica-tors, allowed us to analyze the security of the networks, systems, and requirements of an information technology infrastructure to access the remote laboratory and determine the necessary and appropriate elements for this category.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Risk Management and Incident Response

Risk management and response to incidents that allow the evaluation of possible risks, threats, and vulnerabilities of a remote laboratory and a learning management system (LMS) for the development of a security and contingency plan that will allow for responses to incidents.

Information Security and Data Privacy

Information security and data privacy are aimed at protecting the personnel of students, administrators, teachers, and any confidential information associated with remote laboratory learning management systems (LMS) so that the management process of the information is with integrity.

Security and Compliance Management

The definition of security and compliance management allows the determination of security policies, application of regulations, tools to carry out the respective analyses, and execution of audits in compliance with international standards to guarantee the processes of a laboratory.

User Participation and Awareness

Participation and awareness of users such as students, administrators, and professors in the training programs defined by the higher education institution regarding remote laboratories and their entire environment to understand and comply with security policies and procedures are considered good practices.

Security of Remote Laboratory Systems

Security of remote laboratory systems: access, use of equipment, remote laboratory system control of systems, among others.

Security Methodologies and Standards

Security methodologies and standards: In this phase, security methodologies and standards directly related to remote laboratories, LMS, and VLE, among others, are de-fined through indicators.

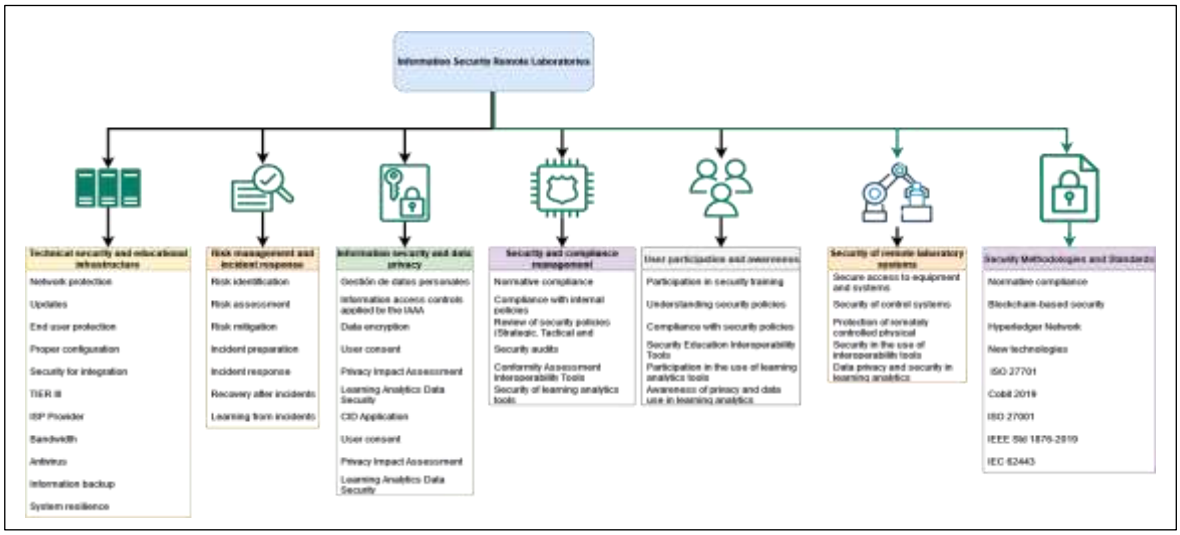

Figure. 5. Model For the Integration of Information Security of Remote Laboratories

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

In figure 5. The Model for the integration of information security in remote laboratories allowed us to clearly identify seven categories with their respective indicators directly related to information security.

Discussion

The results obtained in this research are as follows: Simulation of the evaluation of the information security of a remote laboratory, Architecture of a remote laboratory integrating virtual learning environments and a Model for the integration of information security in remote laboratories, which allows us to consider educational institutions as an alternative to carry out the "Information Security Analysis for a remote laboratory' in the planning and development phases of the project.

In this phase, a simulation was carried out for the evaluation of two higher education institutions using the categories with their respective indicators, however, their implementation has not taken place.

According to the research carried out by the authors of the references, the related works all make general contributions to the field of information security management and operations in virtual environments and remote laboratories. Our contribution in this research can be seen in the generation of a prior evaluation, definition of an architecture and a model for the security of remote laboratories integrated with virtual environments and the consideration that it is necessary to optimize the administrative processes and the legal basis.

The results obtained in this research are an alternative that can be used in the analysis phase and as a model and prototype for any higher education institution in Ecuador, Latin America, or the world, with similar implementation characteristics in remote laboratories and Management Systems. Learning environments (LMS) and Virtual Learning Environments (VLE) allow us to mitigate the risks, vulnerabilities, and threats in the management of information of students, teachers, and administrators.

Authors should discuss the results and how they can be interpreted from the perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

Future Work and Conclusions

In the immediate future, research must continue so that the results obtained in this research can be used for the planning phase, definition of remote laboratory projects, and their respective implementation and validation of a remote laboratory supported by the optimization of administrative processes and the legal basis.

From the simulation of the evaluation carried out on two higher education institutions applying expert judgment and the Likert scale, it was concluded that they partially exceeded the minimum score defined at 0.3; only in two categories. In the category "security methodologies and standards" with a score of 0.35 the first institution (S1) and the second institution (S2) with a score of 0.30 considering all indicators. In the category "security of remote laboratory systems" the second institution (S2) with a score of 0.32, while the first institution (S1) with 0.20. With the results obtained in this evaluation, it can be seen that it is necessary for higher education institutions to implement all the categories with their respective indicators defined in this research to mitigate the risks, vulnerabilities and threats in information management.

That, the model for the integration of information security in remote laboratories obtained in this research is an alternative for the integration of the seven categories with their respective indicators that allow the mitigation of risks, vulnerability and threats so that management of the information of students, teachers and administrators is with confidentiality, integrity and availability (CIA) in compliance with the IAAA.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

It was concluded that information security analysis to mitigate risks, vulnerabilities and threats in a remote laboratory of a higher education institution is crucial to guarantee data protection, experiment management and integrity, confidentiality and availability (CIA). for information management of students, teachers and administrators; considering the optimization of administrative processes and the legal basis

From the research carried out by other researchers based on the references noted in this article, none of the authors presented results similar to those obtained in our research; therefore, it is concluded that our contributions are new and different; the same ones are detailed below: Simulation of the evaluation of the information security of a remote laboratory, Architecture of a remote laboratory integrating virtual learning environments, and Model for the integration of information security in remote laboratories.

Finally, we conclude that for the technological infrastructure of a remote laboratory to function properly, it must additionally be supported by the optimization of administrative processes and a legal basis for its execution.

Authors' Contributions

All authors collaborated in the process of elaboration of the article. Diego Andrade, Moises Toapanta and Pamela Toapanta Pavón worked mainly in the Introduction, Analysis of the administrative processes, legal basis, Summary and Review of all phases of the article and the Literature. Rodrigo Del Pozo Durango, Oswaldo Vanegas-Guillén and Zharayth Gómez mainly in the methodology, search for information and results and Roció Maciel A., Antonio Orizaga T., mainly in the selection of the validation scales, discussion and conclusions.

Author Ethical Declarations

We confirm that the work has not been published elsewhere in any form or language

Funding Information: No funding was received for conducting this study.

Conflict of Interest: The authors state no conflict of interest.

Declaration of Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Aitor, V. M., Garcia-Zubia, J., Angulo, I., & Rodriguez-Gil, L. (2022). Toward Widespread Remote Laboratories: Evaluating the Effectiveness of a Replication-Based Architecture for Real-World Multiinstitutional Usage. IEEE Access, 10(June), 86298–86317. https://doi.org/10.1109/ACCESS.2022.3198961

Almahasees, Z., Mohsen, K., & Amin, M. O. (2021). Faculty's and Students' Perceptions of Online Learning During COVID-19. Frontiers in Education, 6(May), 1–10. https://doi.org/10.3389/feduc.2021.638470

Alsaleh, S., Tepljakov, A., Kose, A., Belikov, J., & Petlenkov, E. (2022). ReImagine Lab: Bridging the Gap Between Hands-On, Virtual and Remote Control Engineering Laboratories Using Digital Twins and Extended Reality. IEEE Access, 10(July), 89924–89943. https://doi.org/10.1109/ACCESS.2022.3199371

Altamirano, W. a., Moisés, T. T., Altamirano, L., Durango, R. D. P., Antonio Orizaga, T., & Roció, M. a. (2024). Prototype to Mitigate Risks for the Closure of a Company with the Support of Information Technologies. Journal of Ecohumanism, 3(7), 3176–3191. https://doi.org/10.62754/joe.v3i7.4449

Amigud, A., Arnedo-Moreno, J., Daradoumis, T., & Guerrero-Roldan, A. E. (2018). An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives. Computers and Security, 76, 50–70. https://doi.org/10.1016/j.cose.2018.02.021

Amnuaysin, O., Nilsook, P., & Wannapiroon, P. (2022). Remote Laboratory Management Platform. Proceedings - 2022 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics, RI2C 2022, 185–190. https://doi.org/10.1109/RI2C56397.2022.9910334

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 3778 – 3796
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5039

Ang, K. L. M., Ge, F. L., & Seng, K. P. (2020). Big Educational Data Analytics: Survey, Architecture and Challenges. IEEE Access, 8(1), 116392–116414. https://doi.org/10.1109/ACCESS.2020.2994561

Armas, D. G. A., Toapanta, S. M., Díaz, E. Z. G., Trejo, J. A. O., Arellano, R. M., & Hifóng, M. M. B. (2024). An Approach to Information Security Based on the Legal Basis for an Organization in Ecuador. Journal of Computer Science, 20(10), 1330–1338. https://doi.org/10.3844/jcssp.2024.1330.1338

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946. https://doi.org/10.1016/j.comnet.2019.106946

Ben Amor, A., Abid, M., & Meddeb, A. (2020). Secure Fog-Based E-Learning Scheme. IEEE Access, 8, 31920–31933. https://doi.org/10.1109/ACCESS.2020.2973325

Bolu, C. A. (2022). Appropriate Online Laboratories for Engineering Students in Africa. 1–5.

Bundin, M., Martynov, A., & Shireeva, E. (2023). Citizen's Digital Profile. Legal Aspects and Current Practice in Russia. 2023 9th International Conference on eDemocracy and eGovernment, ICEDEG 2023, 1–4. https://doi.org/10.1109/ICEDEG58167.2023.10121979

Butler-Henderson, K., & Crawford, J. (2020). A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity. Computers and Education, 159(May), 104024. https://doi.org/10.1016/j.compedu.2020.104024

Callejas-Cuervo, M., Alarcón-Aldana, a. C., & López, a. B. (2016). Security evaluation model for virtual learning environments. Proceedings - 2016 11th Latin American Conference on Learning Objects and Technology, LACLO 2016. https://doi.org/10.1109/LACLO.2016.7751773

Centre, N. C. S. (2021). Alert: Further ransomware attacks on the UK education sector by cyber criminals. National Cyber Security Centre. https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector#section_1

Crichigno, J., Kfoury, E., Caudle, K., & Crump, P. (2021). A Distributed Academic Cloud and Virtual Laboratories for Information Technology Education and Research. 2021 44th International Conference on Telecommunications and Signal Processing, TSP 2021, 195–198. https://doi.org/10.1109/TSP52935.2021.9522672

Darren Turnbull, R. (2021). Transitioning to E-Learning during the COVID-19 pandemic: How have Higher Education Institutions responded to the challenge. In Springer-Education and Information Technologies (pp. 1–15).

El-Haleem, A. M. A., Anany, M. G., Elmesalawy, M. M., & Bakr, E. S. E.-D. (2023). A Matching Game-Based Laboratory Learning System for Resources Management in Remote Laboratories. IEEE Access, 11(January), 6246–6260. https://doi.org/10.1109/access.2023.3236578

Emilio Werner, Jhennifer Cristine Matias, M. D. B. & H. S.-H. (2023). Main Attacks and Ways to Keep Security Guidelines Updated in Remote Laboratories. In Lecture Notes in Networks and Systems (pp. 115–121).

Faculty, E. (2016). Security Evaluation Model for Virtual Learning Environments.

Guillen, O. A. V., Anton, J. M., Maldonado, J. B., & Gamboa, J. Z. (2021). Termolabo project: Design and implementation of thermo-fluids systems online laboratory. IEEE Global Engineering Education Conference, EDUCON. https://doi.org/10.1109/EDUCON46332.2021.9454066

Guo, L., Abdul, N. M. M., Vengalil, M., Wang, K., & Santuzzi, A. (2022). Engaging Renewable Energy Education Using a Web-Based Interactive Microgrid Virtual Laboratory. IEEE Access, 10(1), 60972–60984. https://doi.org/10.1109/ACCESS.2022.3181200

Gursoy, M. E., Inan, A., Nergiz, M. E., & Saygin, Y. (2017). Privacy-Preserving Learning Analytics: Challenges and Techniques. IEEE Transactions on Learning Technologies, 10(1), 68–81. https://doi.org/10.1109/TLT.2016.2607747

IEEE Education Society. (2019). IEEE Std 1876-2019: IEEE Standard for Networked Smart Learning Objects for Online Laboratories. In IEEE Std 1876-2019 (Vol. 1). https://ieeexplore.ieee.org/document/8723446

Kiennert, C., De Vos, N., Knockaert, M., & Garcia-Alfaro, J. (2019). The Influence of Conception Paradigms on Data Protection in E-Learning Platforms: A Case Study. IEEE Access, 7, 64110–64119. https://doi.org/10.1109/ACCESS.2019.2915275

Leva, A., & Donida, F. (2008). Multifunctional remote laboratory for education in automatic control: The CrAutoLab experience. IEEE Transactions on Industrial Electronics, 55(6), 2376–2385. https://doi.org/10.1109/TIE.2008.922590

MacHado, G. S., Melo De Carvalho, M., De Souza Picanco, W., Antonio De Carvalho Ayres, F., Paiva De Medeiros, R. L., & Ferreira De Lucena, V. (2022). Implementation of the System of Remote Laboratories in the Area of Mechatronics for Learning without Human Supervision. Proceedings - Frontiers in Education Conference, FIE, 2022-Octob, 1–5. https://doi.org/10.1109/FIE56618.2022.9962608

Mariusz MACIEJEWSKI, Policy Department for Citizens' Rights and Constitutional Affairs, D. I. (2024). Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies (Issue April).

Microsoft. (2023). Global threat activity. Microsoft Security Intelligence. https://www.microsoft.com/en-us/wdsi/threats

Palka, L., & Schauer, F. (2015). Safety of communication and neural networks for security enhancement in data warehouse for remote laboratories and Laboratory Management System. 6Th ICCNT, 1–8.

Pereira, F., & Felgueiras, C. (2020). Learning Automation from Remote Labs in Higher Education. ACM International Conference Proceeding Series, 558–562. https://doi.org/10.1145/3434780.3436689

Prada, M. a., Fuertes, J. J., Alonso, S., García, S., & Domínguez, M. (2015). Challenges and solutions in remote laboratories. Application to a remote laboratory of an electro-pneumatic classification cell. Computers and Education, 85, 180–190. https://doi.org/10.1016/j.compedu.2015.03.004

Reid, D. P., Burridge, J., Lowe, D. B., & Drysdale, T. D. (2022). Open-source remote laboratory experiments for controls engineering education. International Journal of Mechanical Engineering Education, 50(4), 828–848. https://doi.org/10.1177/03064190221081451

Rivera, L. F. Z., & Larrondo-Petrie, M. M. (2016). Models of remote laboratories and collaborative roles for learning environments. Proceedings of 2016 13th International Conference on Remote Engineering and Virtual Instrumentation, REV 2016, February, 423–429. https://doi.org/10.1109/REV.2016.7444517

Rivera, L. F. Z., Larrondo-Petrie, M. M., & Da Silva, L. R. (2017). Implementation of cloud-based smart adaptive Remote Laboratories for education. Proceedings - Frontiers in Education Conference, FIE, 2017-Octob, 1–5. https://doi.org/10.1109/FIE.2017.8190473

Rivera, L. F. Z., & Petrie, M. M. L. (2016). Models of collaborative remote laboratories and integration with learning environments. International Journal of Online Engineering, 12(9), 14–21. https://doi.org/10.3991/ijoe.v12i09.6129

Ryan, Cooper, & Tauer. (2013). Open – source multi- purpose remote laboratory for IoT edcuation. Paper Knowledge . Toward a Media History of Documents, April, 12–26.

Salimovna, F. D. (2019). Security issues in E-Learning system. Conference: 2019 International Conference on Information Science and Communications Technologies (ICISCT), 1–4.

Santana, I., Ferre, M., Izaguirre, E., Aracil, R., & Hernandez, L. (2013). Remote laboratories for education and research purposes in automatic control systems. IEEE Transactions on Industrial Informatics, 9(1), 547–556. https://doi.org/10.1109/TII.2011.2182518

Singh, A., & Sisodia, A. (2021). The Implementation of Blockchain Technology to Enhance Online Education. In Convergence of Blockchain Technology and E-Business (Issue 1). https://doi.org/10.1201/9781003048107-11

Stefanovic, M., Cvijetkovic, V., Matijevic, M., & Simic, V. (2011). A LabVIEW-based remote laboratory experiments for control engineering education. Computer Applications in Engineering Education, 19(3), 538–549. https://doi.org/10.1002/cae.20334

Tho, S. W., & Yeung, Y. Y. (2018). An implementation of remote laboratory for secondary science education. Journal of Computer Assisted Learning, 34(5), 629–640. https://doi.org/10.1111/jcal.12273

Transactions, I. (2016). Analysis for the Definition of an Information Security and Physical Safety Model for Learning Management in Online Laboratories. IEEE ACCESS, 4(1), 1–6.

Turnbull, D., Chugh, R., & Luck, J. (2022). An Overview of the Common Elements of Learning Management System Policies in Higher Education Institutions. TechTrends, 66(5), 855–867. https://doi.org/10.1007/s11528-022-00752-7

Uckelmann, D., Mezzogori, D., Esposito, G., Neroni, M., Reverberi, D., & Ustenko, M. (2021). Safety and Security in Federated Remote Labs – A Requirement Analysis. Advances in Intelligent Systems and Computing, 1231 AISC, 21–36. https://doi.org/10.1007/978-3-030-52575-0_2

Uckelmann, D., Mezzogori, D., Esposito, G., Neroni, M., Reverberi, D., Ustenko, M., & Baalsrud-Hauge, J. (2021). Guideline to Safety and Security in Federated Remote Labs. International Journal of Online and Biomedical Engineering, 17(4), 39–62. https://doi.org/10.3991/ijoe.v17i04.18937

Vanegas-Guillén, O., Parra-Rosero, P., Muñoz-Antón, J., Zumba-Gamboa, J., & Dillon, C. (2023). Remote Labs Meet Computational Notebooks: An Architecture for Simplifying the Workflow of Remote Educational Experiments. IEEE Access, 11(October), 132496–132515. https://doi.org/10.1109/ACCESS.2023.3336287

Vinodha, K., Deshmukh, V. M., & Rath, S. (2021). Secured Online Learning in COVID-19 Pandemic using Deep Learning Methods. 2021 IEEE International Conference on Mobile Networks and Wireless Communications, ICMNWC 2021, 1–5. https://doi.org/10.1109/ICMNWC52512.2021.9688338

Wang, Y., Sun, Q., & Bie, R. (2022). Blockchain-based secure sharing mechanism of online education data. Procedia Computer Science, 202, 283–288. https://doi.org/10.1016/j.procs.2022.04.037

Wei, P. (2022). Multidimensional Information Security Guarantee Strategy for Scientific Information of University Administrative Management System based on Data Matrix Algorithm. 5th International Conference on Inventive Computation Technologies, ICICT 2022 - Proceedings, Icict, 935–939. https://doi.org/10.1109/ICICT54344.2022.9850917

Werner, E., Matias, J. C., Daniel Berejuck, M., & Saliah-Hassane, H. (2021). Evaluation of blockchain techniques to ensure secure access on remote FPGA laboratories. 9th International Symposium on Digital Forensics and Security, ISDFS 2021, 1–5. https://doi.org/10.1109/ISDFS52919.2021.9486318.