CIBERSEGURIDAD EN PLATAFORMAS EDUCATIVAS INSTITUCIONALES DE EDUCACIÓN SUPERIOR DE LA PROVINCIA DE TUNGURAHUA - ECUADOR

CYBERSECURITY FOR LEARNING PLATFORMS IN HIGHER EDUCATION INSTITUTIONS IN TUNGURAHUA PROVINCE OF ECUADOR

Pablo Israel Morales-Paredes
Coordinador de Carrera de Desarrollo de Software Instituto Superior Tecnológico Pelileo, (Ecuador).
E-mail: pimorales@institutos.gob.ec ORCID: https://orcid.org/0000-0003-2150-4585

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

Recepción: 02/05/2021 **Aceptación:** 31/05/2021 **Publicación:** 29/06/2021

Citación sugerida:
Morales-Paredes, P. I., y Medina-Chicaiza, P. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador. *3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10*(2), 49-75. https://doi.org/10.17993/3ctic.2021.102.49-75

RESUMEN

El objetivo de esta investigación es desarrollar un procedimiento de gestión de seguridad para las plataformas educativas de los Institutos Tecnológicos Superiores públicos de la provincia de Tungurahua, el cual ayude a identificar las vulnerabilidades y riesgos de ciberseguridad a fin de brindar protección a sus plataformas educativas. En el desarrollo de la presente investigación se determinó que los ITS no cuentan con una designación exclusiva de un docente a tiempo completo para el manejo y gestión de ciberseguridad de las plataformas educativas. Por lo tanto, para el desarrollo de esta propuesta se aplicó la metodología de investigación documental a fin de seleccionar las mejores normas y metodologías como soluciones en materia de ciberseguridad. Mediante la combinación del marco de control en ciberseguridad de la norma ISO27032:2012 y la metodología MAGERIT v3.0, se estableció tres áreas de afectación que implican directamente a las aplicaciones web educativas: 1. Administración del Sistema, 2. Aplicaciones Web, 3. Usuarios. Una vez identificadas estas áreas se plantean salvaguardas necesarias para mitigar los riesgos de seguridad.

PALABRAS CLAVE

Ciberseguridad, Plataforma Educativa, Entorno Virtual, Aplicaciones Web.

https://doi.org/10.17993/3ctic.2021.102.49-75

ABSTRACT

The main objective of this investigation is to develop a security management procedure for educational platforms of the public Higher Technological Institutes (HTI) of the Tungurahua province. This investigation can help to identify vulnerabilities and cybersecurity risks in order to provide protection to their educational platforms. During this study, the results determined that HTIs do not have full-time teachers, who are in charged for the management of the cybersecurity of their educational platforms. Therefore, this proposal applied desk-based research in order to select the best standards and methodologies as solutions for cybersecurity. Through the combination of the cybersecurity control framework of the ISO27032:2012 standard and the MAGERIT v3.0 methodology, this study established three areas of impact which directly involve educational web applications: 1. System Management, 2. Web Applications, 3. Users. After the identification of these areas, it is necessary to establish safeguards to mitigate security risks.

KEYWORDS

Cybersecurity, Educational Platform, Virtual Environment, Web Aplicattions.

https://doi.org/10.17993/3ctic.2021.102.49-75

1. INTRODUCCIÓN

En el Ecuador el Consejo de Educación Superior (CES) es el organismo encargado de planificar, regular y coordinar el sistema de Educación Superior mediante la Ley Orgánica de Educación Superior (LOES) la cual garantiza una Educación de calidad. Estas garantías se detallan claramente en su Art. 8, literal a) correspondiente a los fines de la Educación Superior, en donde se aportará al desarrollo del pensamiento universal, al despliegue de la producción científica, de las artes y de la cultura y a la promoción de las transferencias e innovaciones tecnológicas. Por su parte la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) es la responsable de velar que los fines de la Educación Superior se cumplan a través de la elaboración, ejecución y evaluación de políticas, programas y proyectos que deben verse plasmados para garantizar la educación de calidad.

Los Institutos Tecnológicos son parte del Sistema de Educación Superior conforme a lo establecido en el artículo 352 de la Constitución de la República del Ecuador, siendo regulados por el CES. En la Provincia de Tungurahua existen 13 Institutos Superiores Tecnológicos (IST), de los cuales 9 son de carácter público, de un total de 200 Institutos a nivel nacional, según datos recogidos en la página del CES. Estas instituciones han tenido un crecimiento significativo en los últimos años ya que según el Art. 118 literal b) de la LOES habilita a los Institutos Tecnológicos a otorgar títulos de tercer nivel. Esto implica que las Instituciones de Educación Superior deben promover la creación, desarrollo, transmisión y difusión de la ciencia, la técnica, la tecnología y la cultura claramente detallado en el Art 12. Literal b) de la LOES. Para su ejecución es determinante la transferencia e innovación tecnológica mediante la utilización de las Tecnologías de la Información y la Comunicación (TIC), fundamentales dentro la educación superior ecuatoriana.

La infraestructura digital actual permite la conectividad en línea mediante las aplicaciones móviles, en donde los estudiantes se integran hacia las nuevas experiencias del estudio remoto mediante plataformas educativas disponibles para gestión y conexión académica en cualquier parte del mundo, lo cual brinda una oportunidad para que los profesores implementen nuevas estrategias de enseñanza – aprendizaje

https://doi.org/10.17993/3ctic.2021.102.49-75

enmarcadas en las limitaciones del contexto virtual. Esta realidad es la puerta de la educación remota fortalecida a raíz de la pandemia del COVID-19; a pesar de que aún existen problemas conectividad a internet en las áreas rurales (Lockee, 2021). Sin embargo, Abrigo-Córdova, Granados-Gómez, Donald Sánchez-Sulú, y Celi-Vivanco (2019) mencionan que la mayoría de las instituciones educativas de nivel superior usan las plataformas de manera exclusiva para la preparación académica; de tal manera que incrementa la posibilidad de los ataques informáticos y violaciones de seguridad en las plataformas web educativas.

El estudio realizado por Chhetri y Motti (2020) indica que entre los medios electrónicos más vulnerables en una red doméstica son las tablets, teléfonos inteligentes, computadoras de escritorio, portátiles y routers; debido a los siguientes factores: fuga de información, manipulación de datos, fallas en la interfaz de voz, detección del comportamiento del usuario, interrupción y las más relevante de todas, la autenticación de las cuentas de usuario, ya que no disponen con medidas de seguridad apropiadas y utilizan mecanismos simples tales como contraseñas débiles, credenciales predeterminadas como sus nombres o año de nacimiento; esto puede ser un error muy grave por parte del usuario, al momento de precautelar su información confidencial.

En el Ecuador no se ha desarrollado aún una estrategia nacional de ciberseguridad, que permita establecer los lineamientos, objetivos y plan de acción necesario para proteger los servicios, la información, las infraestructuras críticas y a los usuarios frente a ciber amenazas en el ciberespacio (Zambrano y Zambrano, 2019). Esta consideración también abarca a las Instituciones de Educación Superior a pesar de haber sido declarada en el Ecuador a la Ciberseguridad como política pública. Por lo tanto, existen aspectos que deben ser tomados en cuenta para proteger nuestros datos en la web. Con base al estudio de Redrován *et al.* (2018), el cual identifica a la accesibilidad, confiabilidad, seguridad y eficiencia como parte de las características de calidad que deben tener aplicaciones web, dado que en los últimos cinco años se ha experimentado un crecimiento en el uso de diferentes aplicaciones web y móviles en los Institutos Tecnológicos Superiores (ITS) dentro de la Provincia de Tungurahua.

https://doi.org/10.17993/3ctic.2021.102.49-75

La problemática se ha identificado mediante una entrevista realizada a los docentes encargados de TIC de los IST públicos de las ciudades de Ambato, Pelileo, Patate y Baños pertenecientes a la provincia del Tungurahua, en donde se evidencia que no cuentan con una designación exclusiva de un docente a tiempo completo para el manejo de las plataformas educativas, lo cual conlleva a tener riesgos de ciberseguridad en sus plataformas. Adicionalmente el personal no está capacitado y preparado para proponer un plan de respuesta a incidentes informáticos. Por tanto, los beneficiarios directos son los encargados de TIC de los ITS Públicos de la Provincia de Tungurahua, con estrategias para la administración segura de sus plataformas. En cambio, los beneficiarios indirectos son sus docentes y estudiantes, quienes accederán a las plataformas web educativas de manera segura y confiable por que se garantiza la integridad de su información.

El objetivo de esta investigación es desarrollar un procedimiento de gestión de seguridad para las plataformas educativas, la cual reduzca vulnerabilidades y riesgos de ciberseguridad en los Institutos Tecnológicos Superiores públicos de la provincia de Tungurahua.

2. METODOLOGÍA

La revisión empírica de los elementos teóricos se realizó mediante una búsqueda bibliográfica en Scielo, Scopus, Google Scholar y Microsoft Academic Search, en donde se pudo recopilar la información de la Ciberseguridad en aplicaciones educativas web, mediante la utilización del software Perish (Harzing, 2020). Para la búsqueda se consideró las siguientes palabras clave en los idiomas español e inglés como: ciberseguridad en aplicaciones web (cybersecurity in web applications), ciberseguridad en la educación Superior (cybersecurity in higher education), seguridad en plataformas educativas (security in educational platforms) dentro de los últimos diez años, tiempo en que la ciberseguridad ha tomado más fuerza y significancia. A continuación, se detalla en el cuadro resumen las métricas de la investigación que fueron encontradas:

https://doi.org/10.17993/3ctic.2021.102.49-75

Tabla 1. Métricas de la búsqueda realizada.

	Español	Inglés
Años de publicación	2010-2020	2010-2020
Años de las citas	10(2010-2020)	10(2010-2020)
Cantidad de documentos	999	1000
Citas	610	106153
Citas/Año	61.10	10615.30
Citas/Documentos	0.61	106.15
Autores/	1.51	2.81

Fuente: a partir de Perish (Harzing, 2020).

Cabe mencionar que del total de 1999 publicaciones encontradas sobre la temática de estudios se identifica que existe una mínima diferencia en el desarrollo de artículos y libros en español que en inglés. Pero se evidencia que existe un número mayor de publicaciones citadas en el idioma inglés, lo cual indica el nivel de desarrollo y madurez en términos de ciberseguridad en esa lengua.

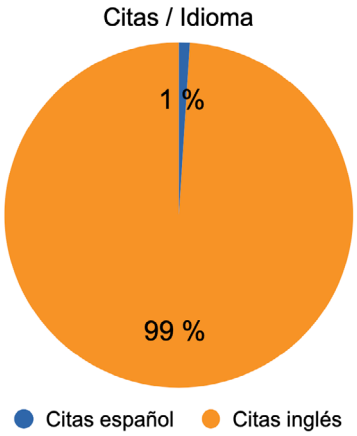


Figura 1. Citas en Español vs Citas en Inglés.
Fuente: a partir de Perish (Harzing, 2020).

El estudio de la Ciberseguridad y su aplicación en los ITS de la Provincia de Tungurahua tiene el propósito de determinar el nivel de Seguridad con el que cuenta el acceso a la información Institucional

https://doi.org/10.17993/3ctic.2021.102.49-75

además de conocer los riesgos, amenazas y vulnerabilidades de los sistemas de aprendizaje virtual. Mediante la utilización de la metodología MAGERIT V3.0 propuesta en el estudio de la Seguridad en entornos virtuales de Santiso, Koller, y Bisaro (2016), se pretende definir los incidentes más comunes en ciberseguridad en las aplicaciones web de los ITS. Esto permite plantear medidas de corrección en base a los controles sugeridos en la Norma ISO 27032 para proteger los sistemas en su integridad, disponibilidad y confiabilidad en el manejo de la información.

3. RESULTADOS

3.1. ESTADO DEL ARTE

Es importante analizar los principales aportes teóricos sobre la ciberseguridad y su campo de desarrollo a lo largo de su historia. A continuación, se detallan cuatro apartados relevantes como son: 1.- Estudio de la Ciberseguridad; 2.- Aplicaciones web educativas; 3.- Ciberseguridad educativa en el Ecuador; 4.- Normas y Metodologías para la prevención y respuesta a incidentes de ciberseguridad en plataformas web educativas. Este estudio abre un camino importante para definir un procedimiento metodológico basado en una norma de calidad, en donde se define controles de ciberseguridad para salvaguardar los sistemas y aplicaciones web dentro de los IST de la provincia de Tungurahua.

3.2. ESTUDIO DE LA CIBERSEGURIDAD

La Ciberseguridad a lo largo de su evolución ha tenido diferentes áreas de estudio, de las cuales se ha identificado tres con más relevancia en investigaciones a nivel mundial con una relación respecto al estudio específico de las ciber amenazas y soluciones de ciberseguridad.

Tabla 2. Áreas de Estudios en Ciberseguridad.

Áreas de Estudio en Ciberseguridad	Estudio de amenazas (autores)	t	Soluciones de Ciberseguridad (autores)	t

https://doi.org/10.17993/3ctic.2021.102.49-75

Aplicaciones Web	(Hernández Moreno, 2017) ; (Jang-Jaccard y Nepal, 2014) ; (Mulligan y Schneider, 2011) ; (Juarez, 2019) ; (ENISA, 2020)	4	(Crescenzi-Lanna, Valente, y Suárez-Gómez, 2019) ; (Romero Moreno, 2010) (Barea *et al.,* s.f.) ; (Santiso *et al.,* 2016) ; (Zambrano y Zambrano, 2019) ; (MAGERIT, 2012) ; (Li *et al.*, 2019)	7
			Aplicaciones Educativas	
			(Zambrano y Zambrano, 2019) ; (Santiso *et al.,* 2016) ; (Haz *et al.,* 2019); (Congacha y García, 2017)	4
Infraestructura Redes	(Lewis, 2006) ; (Roldán-Molina, Almache-Cueva, Silva-Rabadão, Yevseyeva y Basto-Fernandes, 2017)	2	(Vega Villacís y Ramos Morocho, 2017) ; (Zambrano y Zambrano, 2019) ; (Carlini, 2016) ; (Vargas, Recalde, y Reyes, 2017) ; (Mirkovic y Benzel, 2012) ; (Grossman *et al.*, 2015) ; (Arango, 2020) ; (Ramirez y Venkataramanan, 2019)	8
			Aplicaciones Educativas	
			(Mirkovic y Benzel, 2012)	1
Seguridad en la nube	(Carlini, 2016) ; (Aguilar, 2011) (Seefeldt y Tadoro, 2019) ; (Antonio *et al.,* 2016)	4	(Juarez, 2019)	1

Fuente: elaboración propia.

Se ha identificado que la mayor parte de estudios en ciberseguridad están enmarcados en brindar soluciones a las aplicaciones web e infraestructura de redes, las cuales son las más afectadas por los ciber ataques. Estos estudios abren una puerta para continuar con el desarrollo de procedimientos que permitan estar preparados a los continuos y futuros ataques de los cuales los sistemas e infraestructuras sufren todos los días. Además, existen muy pocos estudios con procedimientos que ofrezcan mitigar los riesgos de ciberseguridad en aplicaciones web o entornos educativos.

3.2.1. APLICACIONES WEB EDUCATIVAS

BENEFICIOS

https://doi.org/10.17993/3ctic.2021.102.49-75

Las aplicaciones web educativas o e-learning, se pueden definir como una forma de enseñanza-aprendizaje que hace uso de las nuevas tecnologías disponibles para vincular la planificación académica con un entorno educativo que generalmente está fuera del aula física. Estas aplicaciones educativas según Sánchez (2009) han permitido dar apoyo a las asignaturas presenciales, lo cual ha dado paso al concepto educativo blended learning que consiste en mezclar la formación presencial con la formación a través de las TIC. Gracias a las aplicaciones web educativas podemos tener los siguientes beneficios:

- Acceder a la plataforma educativa desde cualquier parte del mundo gracias al acceso y disponibilidad de internet.
- Brindan igualdad de oportunidades a todas las personas de cualquier edad sin restricciones.
- Registro de actividad, acceso y entrega de tareas, lo cual permite una evidencia de participación de los estudiantes.

CIBER AMENAZAS

Las ciber amenazas a las plataformas educativas a raíz de la pandemia del COVID-19 se han incrementado considerablemente en este año según el Reporte de Ciberseguridad (BID-OEA, 2020, p. 16). Los organismos European Union Agency for Cybersecurity (ENISA), ESET Security y EcuCert del Ecuador realizaron estudio actualizado sobre los riesgos latentes que pueden afectar a las infraestructuras tecnológicas y aplicaciones web a nivel mundial.

Tabla 3. Top 5 de ciber amenazas 2020.

N°	ENISA (2020)	ESET Security Report (2020)	ECUCERT (2020)
1	Malware	Malware	Click Fraud
2	Ataques vía Web	Ransomware	DDoS
3	Phishing	Criptominería	Keylogging
4	Ataques a aplicaciones Web	Phishing	Warez
5	Spam	Exploits	Spam

Fuente: elaboración propia.

https://doi.org/10.17993/3ctic.2021.102.49-75

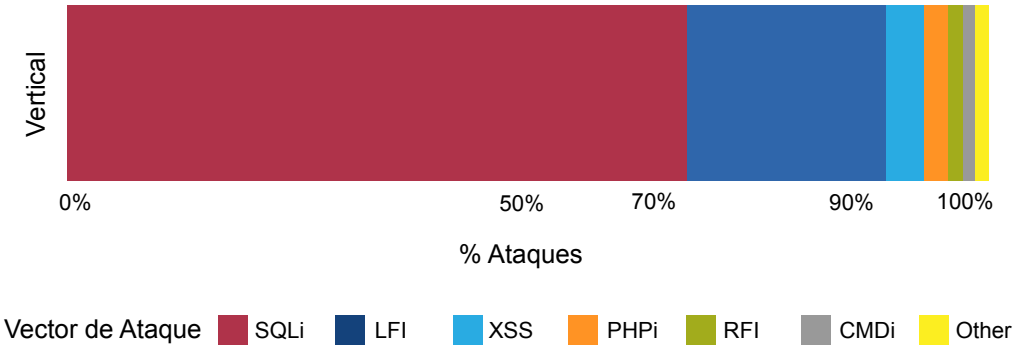
En base a la referencia anterior las aplicaciones web educativas pueden ser un blanco fácil para los ciberataques. Por lo tanto, es importante identificar cómo estas amenazas afectan a las aplicaciones dentro de las siguientes etapas de seguridad:

Tabla 4. Clasificación de las ciber amenazas de las aplicaciones web.

Etapas de Seguridad en aplicaciones web	Ciber amenaza
Autenticación	Phishing Comunicación insegura
Disponibilidad	DDoS (denegación de servicios)
Confidencialidad	Manejo incorrecto de errores Fuga de Información
Integridad	SQLi (Inyección SQL) XSS (secuencia de comandos en sitios cruzados) PHPi (Inyección PHP) RFI (Remote File Inclusion) CMDi (Inyección de Comandos)

Fuente: elaboración propia.

Existe una percepción generalizada de que los ataques a las aplicaciones web son bastante diversos, sin embargo, los datos de la investigación de seguridad sugieren que la mayoría de los ataques a aplicaciones se limitan a: Inyecciones SQL, Directory Transversal o Inclusión local de archivos (Local File Inclusion), secuencia de comandos en sitios cruzados o (XSS), pérdida de autenticación y gestión de sesiones, (ENISA, 2020).



https://doi.org/10.17993/3ctic.2021.102.49-75

Figura 2. Ataques más comunes a aplicaciones web.
Fuente: (ENISA, 2020).

3.2.2. CIBERSEGURIDAD EDUCATIVA EN EL ECUADOR

En lo que se refiere a la educación, en el año 2020, el uso de las aplicaciones de educación virtual y aplicaciones para video llamadas o conferencias se han incrementado sustancialmente debido a la pandemia del COVID-19. Esta realidad aceleró la migración de la educación presencial a la virtual, por lo tanto, la SENESCYT puso en funcionamiento las plataformas tecnológicas (IES) y el acceso de equipos tecnológicos para los estudiantes, en base al informe de evaluación de los efectos e impactos de la pandemia en la educación superior.

Esta nueva realidad lleva consigo riesgos al momento de acceder a recursos virtuales en línea, por tal motivo la Asociación Ecuatoriana de Ciberseguridad (AECI), realizó un estudio en el primer semestre del año 2020, en donde se identificó que en el Ecuador uno de los principales riesgos es la falta de gestión y dedicación exclusiva de ciberseguridad en las empresas o instituciones educativas; a pesar de aquello, el Ecuador ha logrado obtener a una cierta madurez en materia de seguridad informática, ya que se ha entendido que unos de los recursos más valiosos que pueden tener las empresas es el personal capacitado en materia de ciberseguridad. Cabe indicar, además, que el gobierno ecuatoriano también contribuye a la seguridad de las redes de telecomunicaciones y el uso de Internet a nivel nacional, mediante el Centro de Respuesta a Incidentes Informáticos (EcuCERT) perteneciente a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). De esta manera el Ecuador pretende correlacionar a los usuarios con el acceso a los servicios, información y participación por medios electrónicos con calidad y seguridad, lo cual está contemplado dentro del Plan Nacional de Gobierno Electrónico 2018-2021 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018).

https://doi.org/10.17993/3ctic.2021.102.49-75

3.2.3. NORMAS Y METODOLOGÍAS PARA LA PREVENCIÓN Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD EN PLATAFORMAS WEB

Se considera necesario realizar una revisión de las normativas y metodologías para la gestión de seguridad y riesgo informático más utilizados en el ámbito de la ciberseguridad:

Tabla 5. Normas y metodologías más utilizadas en Ciberseguridad.

Soluciones de Ciberseguridad	Estudios/artículos (autores)	Utilización			Total
Metodologías	(Santiso *et al.*, 2016) ; (Guzman, 2019) ; (Santos *et al.*, 2016) ; (Zambrano y Zambrano, 2019) ; (Morales *et al.*, 2020)	MAGERITv3.0	AMFE		
		4	1		5
Normas	(Toapanta *et al.*, 2020) ; (Juarez, 2019) ; (Danilo *et al.*, 2015) ; (Santos *et al.*, 2016) ; (Morales *et al.*, 2020)	ISO27001	ISO27032	ISO15408	
		1	2	1	4

Fuente: elaboración propia.

Se concluye que una de las metodologías más utilizadas para el análisis y gestión de riesgos en seguridad de la Información es la MAGERITv3.0, desarrollada por el Consejo de Administración Electrónica de España, enfocada principalmente a entidades de Administración Pública. Esta metodología ofrece un método sistemático para analizar los riesgos derivados del uso de las TIC, para luego definir las medidas de mitigación más apropiadas. Dentro de las normas más utilizadas para la protección de la ciberseguridad es la ISO27032:2012 la cual ofrece un marco de gestión con controles específicos para los sistemas, infraestructura y usuarios finales, adaptados a las necesidades internas de los IST para el manejo y prevención de ataques. Este marco de seguridad, se complementa con el plan de contingencia planteado en el estudio de Padilla y Freire (2019) donde propone tres fases de respuesta a los ciberataques como son: Alerta, Transición y Recuperación de las infraestructura física o virtual que tiene cada institución.

https://doi.org/10.17993/3ctic.2021.102.49-75

3.2.4. PROCEDIMIENTOS Y ESTRATEGIAS DE CIBERSEGURIDAD

Existen varios procedimientos y estrategias que se han desarrollado en materia de ciberseguridad. A continuación, se ha identificado cuales son las normas y metodologías más utilizadas en el desarrollo de soluciones de ciberseguridad en las aplicaciones web.

Tabla 6. Procedimientos y estrategias de Ciberseguridad.

Respuestas a incidentes de Ciberseguridad	Estudios/artículos (autores)	Normas		Metodologías		Total
		ISO27001	ISO27032	MAGERIT V3.0	AMFE	
Procedimientos	(Santiso *et al.,* 2016) ; (Guzman, 2019) (López, 2019) ; (Arango, 2020) ; (Morales *et al.,* 2020)	1	2	2	1	6
Estrategias	(Vargas *et al.,* 2017) ; (Meriño *et al.,* 2019)		2			2

Fuente: elaboración propia.

Los procedimientos y estrategias estudiadas, en su mayoría utilizan la Norma ISO27032; la cual se encarga específicamente de la gestión y buenas prácticas de seguridad considerando todo el Ciberespacio (Equipamiento de red, Software, Interconexión de redes, personas, servicios de internet). Esta norma abarca los siguientes controles: Aplicaciones (Validación, Autenticación), Servidores (guías de instalación, monitoreo), usuario final (Antivirus, seguridad web, firewall) y Personas (educación continua, campañas de security awareness). De igual manera MAGERIT v3.0 es una de las metodologías más implementadas ya que gestiona de manera prudente las medidas de seguridad y confianza de los usuarios con sus servicios e infraestructura. Esta metodología se divide en tres partes: 1. Gestión de riesgos, 2. Tipifica criterios mediante la valoración de activos, 3. Brinda un conjunto de técnicas para el análisis de riesgos.

3.3. PROCEDIMIENTO METODOLÓGICO DE GESTIÓN DE CIBERSEGURIDAD PARA LAS PLATAFORMAS WEB EDUCATIVAS EN LOS ITS DE LA PROVINCIA DE TUNGURAHUA

https://doi.org/10.17993/3ctic.2021.102.49-75

Para alcanzar el objetivo planteado, se propone el siguiente procedimiento para la Gestión de riesgos de ciberseguridad dentro de los ITS de la Provincia de Tungurahua.

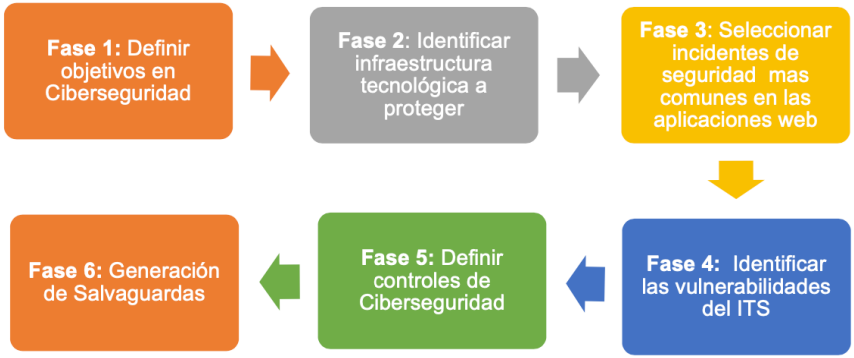


Figura 3. Fases del Procedimiento de Gestión.
Fuente: elaboración propia.

3.3.1. FASE 1: DEFINIR OBJETIVOS DE CIBERSEGURIDAD

Para establecer objetivos de Ciberseguridad en los ITS es necesario crear una conciencia en términos de precautelar la ciberseguridad por parte de las autoridades. Hoy en día los datos más sensibles son gestionados por las TIC, por lo tanto, definir los procesos internos de seguridad se hace indispensable. Por tal motivo, se ha visto necesario establecer objetivos institucionales en términos de ciberseguridad para brindar protección a toda la comunidad educativa.

- Implementar la Unidad de Gestión de Ciberseguridad dentro del Departamento de TIC Institucional.
- Crear una Normativa de Ciberseguridad Institucional.
- Alinear los procesos de gestión de seguridad dentro del Plan Operativo Anual.
- Permitir procesos de autogestión para solventar problemas de seguridad en las infraestructuras tecnológicas.

https://doi.org/10.17993/3ctic.2021.102.49-75

Con estos objetivos se pretende mitigar los riesgos y vulnerabilidades de las aplicaciones educativas.

3.3.2. FASE 2: IDENTIFICAR INFRAESTRUCTURA TECNOLÓGICA A PROTEGER

Para identificar las infraestructuras de hardware y software que se pretende proteger es necesario tomar como referencia las áreas definidas en el estado del arte como las más vulnerables para los ciberataques.

- Plataformas Web: Plataformas educativas e-learning, Sistemas de gestión educativa, Repositorios Digitales, página web institucional.
- Infraestructura: Servidor Web, Servidor de aplicaciones.
- Redes: Red interna Institucional.
- La Nube: Aplicaciones Web alojadas en servidores externos.

3.3.3. FASE 3: SELECCIONAR INCIDENTES DE SEGURIDAD MÁS COMUNES EN LAS APLICACIONES WEB

En esta fase se ha tomado una referencia al "Catálogo de Amenazas" definido en la metodología MAGERIT V3.0 para seleccionar las amenazas o riesgos que pueden afectar a la infraestructura y las aplicaciones web educativas. Los riesgos de ciberseguridad se las ha dividido en tres áreas de afectación: Administración del Sistema, Plataforma y Usuarios. A partir de esta referencia cada ITS debe seleccionar cuales son los incidentes más comunes que afecten a sus aplicaciones.

Tabla 7. Cuadro de selección de Amenazas comunes en aplicaciones web.

✓	**Administración del Sistema**	✓	**Plataforma Web**	✓	**Usuarios**
	Error de operación y mantenimiento del sistema		DDoS (denegación de servicios)		Errores en la utilización de la plataforma
	Error de supervisión y monitoreo		SQLi (Inyección SQL)		Ingeniería social
	Publicación accidental de información		XSS (secuencia de comandos en sitios cruzados)		Fuga de información

https://doi.org/10.17993/3ctic.2021.102.49-75

	Manipulación y destrucción accidental de la información		PHPi (Inyección PHP)		Suplantación de acceso
	Falta de procesos de seguridad de la información		RFI (Remote File Inclusion)		
	Fuga de información		CMDi (Inyección de Comandos)		
	Acceso de usuarios no autorizados		Phishing		
	Mal uso de privilegios del sistema				
	Poca preparación del personal				
	Manejo incorrecto de errores				

Fuente: a partir de (MAGERIT, 2012).

3.3.4. FASE 4: IDENTIFICAR LAS VULNERABILIDADES DEL ITS

Para identificar las vulnerabilidades en las aplicaciones web es necesario realizar pruebas de penetración basados en el hacking ético, las cuales se resumen a continuación en 4 etapas basadas en el estudio de Páez (2014):

a) Reconocimiento: Establecer el objetivo estudiar (aplicaciones web, sistemas de gestión educativa, página web), para buscar las posibles vulnerabilidades que pueda tener.

b) Exploración: Usar la información obtenida en la etapa de reconocimiento con el fin de detectar vulnerabilidades definidas en la Fase 3.

c) Enumeración: Recopilar la información vital, como puertos abiertos, servicios, usuarios de la red activos que puedan afectar al sistema.

d) Informes: Registrar las vulnerabilidades encontradas en el test de penetración y sobre estas generar recomendaciones o salvaguardas para evitar posibles ataques externos que afecten a la autenticación, disponibilidad, Integridad y confidencialidad.

https://doi.org/10.17993/3ctic.2021.102.49-75

Es necesario relacionar las vulnerabilidades encontradas con los incidentes más comunes en las aplicaciones web para definir una referencia al momento de encontrar las soluciones definidas en la siguiente fase.

3.3.5. FASE 5: DEFINIR CONTROLES DE CIBERSEGURIDAD

Una vez definidos los riesgos, es necesario realizar un cruce con los controles de la norma ISO 27032, con el objetivo de determinar las mejores soluciones de seguridad para las aplicaciones web enmarcadas en los incidentes y riesgos más comunes.

Riesgos de Ciberseguridad en las Plataformas Web	Controles de Ciberseguridad ISO27032:2012	1. Control de Aplicaciones	- Gestión de Sesiones	- Validación de Datos	- Protección de ataques	- Procesos de autenticación	2. Control de Servidores	- Configuraciones seguras	- Gestión de parches	- Monitorización	- Respaldos	3. Usuarios Finales	- Actualizaciones de Sistema Operativo	- Uso de aplicaciones	- Herramientas y configuraciones de seguridad	4. Ingeniería Social (Personas)	- Programas de concientización	- Pruebas regulares	- Controles de seguridad	- Capacitación Constante
Administración del Sistema																				
Error de operación y mantenimiento del sistema			x										x	x					x	
Error de supervisión y monitoreo			x		x	x		x	x	x			x	x	x			x	x	
Publicación accidental de información			x	x		x		x		x									x	
Manipulación y destrucción accidental de la información						x		x	x	x	x				x				x	
Falta de procesos de seguridad de la información					x	x		x	x	x	x		x		x			x	x	
Fuga de información			x	x	x	x		x		x	x			x	x		x	x	x	x
Acceso de usuarios no autorizados			x	x	x	x		x		x					x			x	x	
Mal uso de privilegios del sistema			x	x		x		x		x					x			x	x	
Poca preparación del personal						x		x	x	x	x		x	x	x		x	x		x
Manejo incorrecto de errores			x	x	x	x		x	x	x								x	x	
Plataforma Web																				
DDoS (denegación de servicios)			x	x	x	x		x		x	x				x		x	x	x	x
SQLi (Inyección SQL)			x	x	x	x		x		x	x				x		x	x	x	x
XSS (secuencia de comandos en sitios cruzados)			x	x	x	x		x		x	x				x		x	x	x	x
PHPi (Inyección PHP)			x	x	x	x		x		x	x				x		x	x	x	x
RFI (Remote File Inclusion)			x	x	x	x		x		x	x				x		x	x	x	x
CMDi (Inyección de Comandos)			x	x	x	x		x		x	x				x		x	x	x	x
Phishing			x	x	x	x		x		x	x				x		x	x	x	x
Usuarios																				
Errores en la utilización de la plataforma								x	x	x	x		x	x	x		x	x	x	x
Ingeniería social													x	x	x		x	x	x	x
Fuga de información				x	x	x		x	x	x					x			x	x	x

Figura 4. Matriz de Correlación de Riesgos y Controles de Ciberseguridad ISO 27032:2012.
Fuente: elaboración propia.

https://doi.org/10.17993/3ctic.2021.102.49-75

La matriz de riesgos se ha definido conforme al estudio realizado por Santiso *et al.* (2016) en donde se realiza un análisis de correlación de las amenazas y controles con respecto a la norma ISO 27001. En cambio, esta propuesta se basa en la norma ISO 27032:2012, la cual establece controles de ciberseguridad para precautelar la información que está enlazada a la web. Este estudio varía conforme la realidad de cada instituto con respecto al tipo de infraestructura que disponen, procesos de gestión implementados, perfiles de usuario, amenazas, entre otras. Por tanto, es necesario que cada Instituto realice su propio análisis de riesgos para identificar sus amenazas y encontrar las mejores soluciones de seguridad que se deben implementar.

3.3.6. FASE 6: GENERACIÓN DE SALVAGUARDAS

Para solventar los problemas de ciberseguridad que afectan a cada institución es necesario implementar salvaguardias que brinden seguridad al entorno de las aplicaciones web. Por tanto, a continuación, se plantean salvaguardias de seguridad en base a los resultados en la matriz de correlación de la Fase 5 con respecto a las áreas de afectación.

SALVAGUARDA 1: ADMINISTRACIÓN DEL SISTEMA

Para la gestión de la ciberseguridad en los ITS es necesario llevar a cabo las siguientes actividades de administración en base a los controles de seguridad de la Norma ISO27032.

- Desarrollar la Normativa interna de Ciberseguridad en base a los siguientes controles:
  - Definición de Roles y Privilegios en los Sistemas (gestión de sesiones).
  - Gestión de Acceso mediante métodos autenticación en la plataforma web.
  - Validación de datos de usuario para definir la integridad de la información (criptografía).
  - Gestión de respaldos de la Información.
  - Capacitación Constante del Personal a Cargo.

https://doi.org/10.17993/3ctic.2021.102.49-75

SALVAGUARDA 2: PLATAFORMA WEB

Protección de ataques mediante la implementación de:

Arquitectura física:

- Implementación de un Firewall, para auditar y autorizar conexiones permitidas.
- Implementación de un Wireless LAN Controller para los accesos a las aplicaciones web dentro de los Institutos.

Arquitectura lógica:

- Manejo de errores de ejecución de los sistemas.
- Para la protección de ataques en las plataformas web se ha visto necesario tomar ciertas referencias de seguridad en base al estudio realizado por (OWASP, 2019).
- Codificar los datos de requerimientos HTTP con confiables en los campos de salida de HTML (cuerpo atributos, JavaScript, CSS o URL).
- Supervisar bibliotecas y componentes que no poseen mantenimiento o no liberan parches de seguridad.
- Cada instituto debe asegurar la existencia de un plan para monitorizar, evaluar y aplicar actualizaciones o cambios durante el ciclo de vida de las aplicaciones.

SALVAGUARDA 3: USUARIOS

- Capacitación en el uso de las Plataformas Institucionales.
- Definir procesos seguros para el restablecimiento de contraseñas.
- Promover el uso de antivirus para evitar malware en los quipos y dispositivos.

https://doi.org/10.17993/3ctic.2021.102.49-75

4. CONCLUSIONES

El procedimiento metodológico planteado logra establecer un marco de gestión de ciberseguridad aplicable a la infraestructura física y virtual de las plataformas web educativas de los IST de la provincia de Tungurahua, basado en un estándar y metodología de calidad internacional.

La educación virtual durante el último año se ha incrementado notablemente por el COVID-19, por tanto, el estudio planteado ofrece medios para precautelar la confidencialidad, integridad y disponibilidad de las plataformas web educativas institucionales.

Los principales riesgos de ciberseguridad que sufren las plataformas web educativas tienen que ver directamente con el control inadecuado de las aplicaciones, mala configuración de servidores, falta administración de usuarios e ingeniería social, esto ligado a la falta de designación de un personal exclusivo para el área de seguridad de la información en los IST.

El uso del procedimiento de gestión propuesto brinda una guía para el control y seguimiento de cada una de las áreas que implican riesgos de seguridad como son las aplicaciones, infraestructura y usuarios finales mediante el uso de controles basados en la Norma ISO27032:2012 y la metodología MAGERIT V3.0.

Las salvaguardias planteadas no pretenden ser soluciones absolutas sino más bien son el punto de partida para futuras investigaciones dentro de las Instituciones de educación superior enmarcados en planes de gestión que impliquen nuevos controles a amenazas que se puedan presentar en el futuro dentro de la educación online.

REFERENCIAS BIBLIOGRÁFICAS

https://doi.org/10.17993/3ctic.2021.102.49-75

Abrigo-Córdova, I., Granados-Gómez, Donald Sánchez-Sulú, N., y Celi-Vivanco, Y. (2019). El aula virtual: una experiencia educativa desde diversos ámbitos universitarios latinoamericanos. *Revista Ciencia Matria, Vl*(27).

Aguilar, L. J. (2011). *Introducción. Estado Del Arte De La Ciberseguridad.* (1697–6924), 35. http://www.pensamientopenal.com.ar/system/files/2015/01/doctrina38717.pdf

Antonio, J., López, A., Rosalba, C., y Rodríguez, R. (2016). Paakat: Revista de Tecnología y Sociedad Seguridad en internet. *Revista de Tecnología y Sociedad, 6*(11), 2007–3607.

Arango, L. (2020). *Diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa cibersecurity de colombia ltda.* 117. http://repositorio.unan.edu.ni/2986/1/5624.pdf

Barea, F., Romero, I., Rojo, I., y Villagr, A. (s.f.). *Plataforma de gestión De Escenarios De Ciberseguridad Para Aprendizaje Y Entrenamiento.* http://oa.upm.es/55294/

Carlini, A. (2016). *Documento de Opinión. Ciberseguridad Un Nuevo Desafío Para La Comunidad Internacional,* 950–966.

Chhetri, C., y Motti, V. (2021) Identifying Vulnerabilities in Security and Privacy of Smart Home Devices. En Choo, K.K.R., Morris, T., Peterson, G.L., y Imsand, E. (eds) *National Cyber Summit (NCS)* Research Track 2020. NCS 2020. Advances in Intelligent Systems and Computing, vol 1271. Springer, Cham. https://doi.org/10.1007/978-3-030-58703-1_13

Congacha, A., y García, V. J. (2017). Modelación, simulación y automatización de procesos en la gestión de servicios académicos universitarios. *3C Tecnologia. Glosas de innovación aplicadas a la pyme, 6*(2), 32–51. https://www.3ciencias.com/wp-content/uploads/2017/06/ART-3.pdf

https://doi.org/10.17993/3ctic.2021.102.49-75

Crescenzi-Lanna, L., Valente, R., y Suárez-Gómez, R. (2019). Safe and inclusive educational apps: Digital protection from an ethical and critical perspective. *Comunicar, 27*(61), 88–97. https://doi.org/10.3916/C61-2019-08

Danilo, H., Cabrera, S. A., Abad, E. M., Torres, V. A., y Verdum, J. C. (2015). Definition of cybersecurity businness framework based on ADM-TOGAF. 1–7. https://doi.org/10.1109/cisti.2015.7170391

ENISA. (2020). Trust Services Security Incidents 2019. https://doi.org/10.2824/047833

Grossman, I. R. L., Forest, R., Heath, J. E., Key, S. L., Us, F. L., Richardson, R. D., … y Alexander, K. B. (2015). (12) *United States Patent. 1*(12).

Guzman, S. (2019). *Guía para la Implementación de la Norma ISO 27032*. Universidad Católica de Colombia, 69.

Harzing, A. W. (2020) *Publish or Perish*. https://harzing.com/resources/publish-or-perish

Haz, L., Flores, M., Ximena, A., Guzman, C., y Espín, L. (2019). Implementation of IT Security and Risk Management Process for an Academic Platform. En *Advances in Intelligent Systems and Computing*, 379–386. https://doi.org/10.1007/978-3-030-02351-51-5_43

Hernández, A. (2017). Ciberseguridad y confianza en el ámbito digital. *Información Comercial Española, ICE: Revista de Economía*, (897), 55–66.

Jang-Jaccard, J., y Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Juarez, F. A. B. (2019). Ciberseguridad en un entorno de Internet de las Cosas Industrial (IIoT). En *8th International Conference on Software Process Improvement, CIMPS 2019 - Applications in Software Engineering*, 1–6. https://ieeexplore.ieee.org/document/9082437/

Lewis, J. (2006). Cybersecurity and Critical Infrastructure Protection. *Center for Strategic & International Studies, 1*(9), 12. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf

Li, L., He, W., Xu, L., Ash, I., Anwar, M., y Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*(February 2018), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Lockee, B. B. (2021). Online education in the post-COVID era. *Nature Electronics, 4*(1), 5–6. https://doi.org/10.1038/s41928-020-00534-0

López, C. J. (2019). *Desarrollo de una guía de controles ciberseguridad para la protección integral de la pyme.* 79. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/95026/6/cjlopezTFM0619memoria.pdf

MAGERIT. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Libro I - Método. Ministerio de Hacienda y Administraciones Públicas, 2006(630-12-171–8), 127. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Meriño, I., Nieto, W., Moreno, S., y Hernández, Y. (2019). Diseño de un Framework de Arquitectura Empresarial para Instituciones Públicas de Educación Superior. *Revista Ibérica de Sistemas e Tecnologias de Informação, E17*, 742–755. http://www.risti.xyz/issues/ristie17.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2018). *Plan Nacional de Gobierno Electrónico.* https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/09/PNGE_2018_2021sv2.pdf

Mirkovic, J., y Benzel, T. (2012). Teaching cybersecurity with DeterLab. *IEEE Security and Privacy, 10*(1), 73–76. https://doi.org/10.1109/MSP.2012.23

 https://doi.org/10.17993/3ctic.2021.102.49-75

Morales, J., Zambrano, N., Lectong, T., y Zambrano, M. (2020). Proceso de Ciberseguridad : Guía Metodológica para su implementación. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação,* (26), 11.

Mulligan, D. K., y Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus, 140*(4), 70–92. https://doi.org/10.1162/DAED_a_00116

OWASP. (2019). *Copyright y Licencia Tabla de Contenidos Sobre OWASP.* https://github.com/OWASP/Top10/issues

Padilla, V. S., y Freire, F. F. (2019). A Contingency Plan Framework for Cyber-Attacks. *Journal of Information Systems Engineering & Management, 4*(2), 2–7. https://doi.org/10.29333/jisem/5898

Páez, M. (2014). *Propuesta de Procedimiento para la ejecución de Pentest dentro del esquema de pruebas de las fábricas de software para aplicaciones web, 7,* 69. http://polux.unipiloto.edu.co:8080/00002027.pdf

Ramirez, D., Ramirez, V., y Venkataramanan, G. (2019). Ciberseguridad En Infraestructuras. Aplicación a Los Elementos De Un Smart Grid. *Dyna Ingenieria E Industria, 94*(1), 518–522. https://doi.org/10.6036/9041

Redrován, F., Loja, N., Correa, K., y Piña, J. (2018). Comparación de métricas de calidad para el desarrollo de aplicaciones web. *3C Tecnología. Glosas de innovación aplicadas a la pyme, 7*(3), 94–113. https://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/620

Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., y Basto-Fernandes, V. (2017). A Comparison of Cybersecurity Risk Analysis Tools. *Procedia Computer Science, 121*, 568–575. https://doi.org/10.1016/j.procs.2017.11.075

Romero, L. (2010). La seguridad informática en el trabajo con la plataforma "Moodle." *Revista de Humanidades,* (17), 169–190.

https://doi.org/10.17993/3ctic.2021.102.49-75

Sánchez, J. (2009). Plataformas de enseñanza virtual para entornos educativos. *Pixel-Bit: Revista de Medios y Educación, 34*, 217–233. http://www.sav.us.es/pixelbit/actual/15.pdf

Santiso, H., Koller, J., y Bisaro, M. (2016). Seguridad en Entornos de Educación Virtual. *Security in Virtual Education Environments., 14*(14), 67–88. http://search.ebscohost.com/login.aspx?direct=-true&db=fua&AN=120577699&lang=es&site=ehost-live

Santos, A., Sanchez, L. E., Alvarez, E., Huerta, M., y Fernandez, E. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions, 14*(6), 2897–2911. https://doi.org/10.1109/TLA.2016.7555273

Seefeldt, J., y Tadoro, S. (2019). *El efecto orwell en la sociedad en red: ciberseguridad, régimen global de vigilancia social y derecho a la privacidad en el siglo xxi*, 85. https://buleria.unileon.es/handle/10612/12563?locale-attribute=pt_BR

Toapanta, S. M. T., Gustavo, E., y Gallegos, L. E. M. (2020). Analysis of appropriate standards to solve cybersecurity problems in public organizations. En *ACM International Conference Proceeding Series*, (May), 14–19. https://doi.org/10.1145/3404663.3404678

Vargas, R., Recalde, L., y Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad*, (20).

Vega, G., y Ramos, R. (2017). Vulnerabilidades Y Amenazas a Web. *3C Tecnología. Glosas de innovación aplicadas a la pyme, 6*(1), 53–66. https://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/53

Zambrano, N., y Zambrano, M. (2019). Ciberseguridad Y Su Aplicación En Las Instituciones De Educación Superior Públicas De Manabí. *Espam, 199*. http://repositorio.espam.edu.ec/bitstream/42000/1032/1/TTMTI3.pdf

https://doi.org/10.17993/3ctic.2021.102.49-75

https://doi.org/10.17993/3ctic.2021.102.49-75