Análisis de riesgos y vulnerabilidades en la educación 4.0 del proceso de enseñanza – aprendizaje

Risk and Vulnerability Analysis in Education 4.0 of the Teaching - Learning Process

[1]Henry Gutiérrez-Oquendo, [2]Luz-O Giraldo

[1,2]Universidad Nacional Abierta y a Distancia —UNAD—

Recibido: 15/12/2021 Aprobado: 10/02/2022

Resumen

Este artículo expone el análisis de los riesgos y vulnerabilidades que presenta la educación 4.0 del proceso de enseñanza-aprendizaje, en la sociedad educativa digital, en la cual se vio sujeto el ciudadano a través de la contingencia mundial que vivimos en la actualidad. Para este fin, nos enfocamos en una investigación cualitativa que considera las condiciones y características propias de la educación 4.0; además de las probabilidades de que se produzcan incidentes de seguridad, materialización de amenazas en lo referente a los medios de comunicación que se dan en el proceso enseñanza – aprendizaje.

No obstante, llevamos a cabo el método de análisis, orientado en *Open Web Security Proyect (OWASP),* que se enfoca en identificar riesgos y proporcionar a la vez información sobre la probabilidad y el impacto técnico, utilizando esquema *OWASP-Top-10-2017;* por otra parte, se especifica en la Tabla 2, el control proactivo de riesgos y en la Tabla 3, los requisitos y descarga de software frente al marco de evaluación de riesgos *OWASP,* el cual, nos brindó sustento para establecer relación de riesgos y vulnerabilidades en la educación 4.0, y concluir, con recomendaciones de seguridad sobre la protección de información relevante de los actores involucrados en este proceso, y que no queden expuestas en manos inescrupulosas de ciberdelincuentes que aprovechan para realizar actos delictivos.

Palabras clave: educación 4.0, sociedad educativa digital, método de análisis, riesgos y vulnerabilidades.

Abstract

This article presents an analysis of the risks and vulnerabilities presented by Education 4.0 of the teaching-learning process, in the digital educational society, in which the citizen was subjected through the global contingency that we live in today. For this purpose, we focused on a qualitative research that considers the conditions

Citación: Gutiérrez Oquendo, H., & Giraldo , L. O. . (2022). Análisis de Riesgos y Vulnerabilidades en la Educación 4.0 del Proceso de Enseñanza – Aprendizaje. Publicaciones E Investigación, 16(1). https://doi.org/10.22490/25394088.5615

[1] Escuela de Ciencias Básicas Tecnología e Ingeniería –ECBTI–. Santiago de Chile / https://orcid. org/0000-0002-8300-2014 / Bafim1420@gmail.com
[2] https://orcid.org/0000-0003-3614-6469 / gitanarromani@gmail.com

https://doi.10.22490/25394088.5615

and characteristics of education 4.0; in addition to the probabilities of security incidents, materialization of threats regarding the media that occur in the teaching-learning process. However, we carried out the analysis method, oriented in Open Web Security Project (OWASP), which focuses on identifying risks and providing information on the probability and technical impact, using OWASP-Top-10-2017 scheme; on the other hand, it is specified in Table 2, the proactive risk control and in Table 3, the requirements and download software against the OWASP risk assessment framework, which gave us support to establish relationship of risks and vulnerabilities in Education 4. 0, and conclude with security recommendations on the protection of relevant information of the actors involved in this process, and that they are not exposed in unscrupulous hands of cybercriminals who take advantage to carry out criminal acts.

Key words: *Education 4.0, Digital education society, Method of analysis, Risks and vulnerabilities.*

1. Introducción

La educación es la clave para el desarrollo de cualquier nación o país, además que reside en personas versadas en un tema específico (Etecé, 2022). No obstante, a lo largo de la historia, algunos autores visualizan la educación desde su punto de vista, por ejemplo:

> Para Aristóteles, "La educación consiste en dirigir los sentimientos de placer y dolor hacia el orden ético". Para Coppermannc "La educación es una acción producida según las exigencias de la sociedad, inspiradora y modelo, con el propósito de formar a individuos de acuerdo con su ideal del hombre en sí". Y, Según Kant, "La educación tiene por fin el desarrollo en el hombre de toda la perfección que su naturaleza lleva consigo" (Rojas, 2018, párr. 3).

Conviene subrayar que la noción de ética en la educación se entrelaza con la exigencia social que conduce a su desarrollo. En la actualidad, por ejemplo, se habla de educación 4.0; la cual, ha realizado trasformaciones sociales, con el anhelo de inclusión de ciudadanos digitales, con competencias de herramientas que están a su disposición en la nube; mediando en procesos de comunicación sincrónica o asincrónica y culturales; en este punto nos referimos a centros educativos, universidades y administraciones públicas.

Sin embargo, ¿se ha pensado en los peligros que acarrea para el ciudadano (docente-estudiante), navegar sin conocimiento de seguridad informática en el mundo digital?, ¿está integrado al currículo, temas y saberes de la seguridad informática en lo referente a los datos protegidos para salvaguardar la integridad, confidencialidad y disponibilidad de la información? Como bien lo señalan Crisorio & Escudero "Sujeto y saber se articulan necesariamente en el currículum" (2017, p. 10).

Lo anterior, indica los problemas que aborda este artículo, ya que afectan aspectos de la vida en una construcción social, como se citó a Pernías (Domínguez Osuna *et al*., 2019) haciendo énfasis en que:

> La Industria 4.0, también se identifica como un término integrador de las tecnologías en la cadena de valor a los sistemas ciber físicos (CPS, Cyber Physical Systems), el Internet de las cosas (IoT, Internet of Things) y el Internet de los servicios, (201u, párr. 17)

Con esto queremos decir, que los centros educativos, Universidades y administraciones, deben adueñarse de los peligros ocultos en los medios y espacios que utilizan para llevar a cabo el proceso enseñanza-aprendizaje; es por esto, que mediante *Open Web Security Proyect (OWASP)*, nos enfocamos en el análisis de riesgos y probabilidad de impacto técnico, utilizando el esquema *([OWASP] OWASP-Top-10-2017-es.pdf, s. f.).*

2. Método

2.1. Educación 4.0

Como punto de partida, hacemos énfasis en la cuarta revolución industrial o Industria 4.0, para referirnos a la Educación 4.0, cuyo medio de aprendizaje y comunicación son las tecnologías digitales. Esta nueva formación usa el Internet como espacio común de educación, aprovechando el conocimiento a nivel mundial en el proceso enseñanza-aprendizaje, que va más allá de lo que se aprende en un aula, (Jiménez & Albo, 2021).

Es decir, la Educación 4.0 no tiene como punto central los contenidos, sino más bien, las competencias de aquellos ciudadanos digitales que saben hacer o aplicar, y que saben ser, como bien lo indica (Parrales, 2019) "los programas escolares deben cambiar radicalmente, la educación no debe estar centrada en el profesor sino en los estudiantes" (párr. 10).

En consecuencia, esta innovación educativa trajo consigo un rechazo en sectores educativos, que suponían una desaparición de profesionales en la carrera docente como actores primarios en los procesos de enseñanza-aprendizaje; pero su enfoque va más allá, y es obligar a los mismos, a capacitarse en herramientas que están a su disposición en la nube y seguridad informática para proteger datos, teniendo presente que educan u orientan jóvenes que su día a día es la tecnología inteligente. Así pues, el educador debe exigirse una mayor competencia pedagógica-motivacional, en su labor como formador.

De ahí que, la Educación 4.0, cobra sentido en la desigualdad social actual, dando respuesta a la falta de esperanza para construir mecanismos para la equidad, *(Innovacion-educativa-80-web.pdf, s. f., p. 12).* Así mismo, hace transformaciones sociales, culturales y económicas, mediando procesos de comunicación sincrónica o asincrónica, entre estudiantes, estudiantes-docentes y estudiantes-recursos; en efecto, aborda la problemática de la deserción académica, "incrementando la posibilidad de acceso a la educación a todos aquellos cuyos horarios del trabajo no le permitan asistir en un momento determinado" (Castro *et al.*, 2007, p. 217).

Sin embargo, esta interacción social en lo referente a la tecnología, en un ciberespacio de carácter global y creciente, enmarca individuos que en minoría poseen conocimientos, y en mayoría falencias individuales, sobre el uso y seguridad de las TIC; podemos incluso cuestionar sobre una ética Educativa 4.0, en la que sujeto y tecnología influyen de forma particular, o bidireccional, y que, a diferencia de una ética social o profesional, las reglas implementadas no son necesariamente efectivas en la solución de los problemas, que conlleva aceptar los medios de enseñanza-aprendizaje, y navegar por el espacio que requiere esta industria para impartir su servicio.

En pocas palabras, ya estamos frente a nuevos paradigmas de educación, por lo que cuestionar si es buena o mala la Educación 4.0 en nuestra sociedad actual, es irrelevante, pero si es necesaria una visión integral de políticas educativas, recursos y actores, que sumen acciones en el proyecto educativo; mediar en la ciberdelincuencia, salvaguardando activos; integrar las TIC y la seguridad informática al currículo; capacitar a los docentes en el tema referido e implementar controles en las aplicaciones que median el proceso de educación; entre otros.

2.1.1. Medios de enseñanza-aprendizaje en la educación 4.0

En cuanto a los medios utilizados por la Educación 4.0, donde convergen la tecnología digital; se muestra un fallo o debilidad, ya que impactan de manera positiva o negativa nuestro proceso de aprendizaje; a la vez, se abre pasos agigantados en la inteligencia artificial; la robótica; Internet de las cosas; la bío o nanotecnología; la impresión 3D; los vehículos autónomos; la ciencia de materiales; la computación cuántica; y el almacenamiento de energía (Márquez, 2020).

Este fallo hace referencia en la reestructuración de escenarios de enseñanza-aprendizaje; si bien son vistos como una oportunidad para la construcción colectiva de saberes. Para Guzmán et al. (2019), es necesario que las instituciones educativas tomen en consideración

características de la Educación 4.0, como es la cooperación estudiante y docente; fomentar la resolución de problemas; creación de entornos reales; comunicación activa e implementación de las TIC como herramientas de acceso, organización, creación y difusión de contenidos, a fin de incorporarlas en su proceso de enseñanza aprendizaje (2019, p. 2).

En consecuencia y en estudios de Harrison & Killion (2007) como se citó en Villasol (2019) "es necesario para afrontar los continuos cambios normativos y sociales. Poner un foco en un docente digital especialista curricular, proveedor de recursos, instructor, facilitador de apoyo en el aula y del aprendizaje" (p. 3). En lo referente, Márquez (2020) señala que,

> Es menester incorporar el dinamismo tecnológico a las instituciones de educación superior, empero, de la mano de docentes conocedores de las TIC apropiadas a los contenidos curriculares que permitan una formación profesional centrada en las competencias, no necesariamente explícitas en la malla curricular, sino en aquellas que les serán de utilidad como profesionistas de una sociedad enmarcada en una Industria 4.0 y capaces de enfrentar la 5.0 por venir (p. 9).

En definitiva, los rechazos en algunos sectores educativos están sustentados en la ausencia de saberes digitales en el currículo para la carrera docente, y en contrapunto, las instituciones educativas, demandan al profesional docente en contratación, estar capacitado en herramientas tecnológicas para formar en competencias más que en contenidos, e ir más allá de lo que se aprende en un aula.

2.1.2. Espacio común de la educación 4.0

Pongamos por caso, que la Educación 4.0, hace énfasis en herramientas de distribución de contenidos, con formatos como: HTML, PDF, TXT, ODT, PNG; herramientas de comunicación y colaboración sincrónica y asincrónica; herramientas de seguimiento y evaluación; herramientas de administración de y asignación de permisos; herramientas complementarias; plataformas comerciales de software; etc.

Un claro ejemplo, es la Web 2.0, que comprende aquellos sitios, para facilitar la comunicación a través de redes sociales y académicas, "Se trata de aplicaciones que generen colaboración y de servicios que reemplacen las aplicaciones de escritorio", *(Queeslaweb2.0-with-cover-page-v2.pdf, s. f., p. 2).* En su estudio, Garza (2011) como se citó en (Castro *et al*., 2007) "la plataforma de Internet y los espacios electrónicos en los que armonizan los alumnos y el profesor se convierte en el ambiente, que emula la interacción" (p. 222).

Y es que tecnología, aplicación y educación, son conceptos estrechamente ligados, que requieren de un proceso de selección, planeación, desarrollo, evaluación de actividades y estrategias, como lo señala Parra Bernal *et al*. (2021) "para que la innovación educativa aporte de manera significativa, es necesario establecer con claridad el uso de la tecnología, ya que vincularla a la práctica no garantiza procesos innovadores".

En consecuencia, en la educación online se debe tener controles de seguridad, puesto que las aplicaciones que sustentan la web y que potencian los componentes tecnológicos centrales del lado del servidor, y el lado clientes, como: AJAX y Rich Internet Application (RIA), permiten una mejor interface al lado del cliente en su propio navegador; no obstante, como hace énfasis, («Top 10 Web 2.0 Attack Vectors», 2006) en la preocupación de la seguridad de la Web 2.0; enfatizando en la seguridad, contra vectores de ataque, como son los gusanos de tipo Yamanner, Samy y Spaceflash, que explotan los marcos AJAX del lado del cliente, comprometiendo la confidencialidad; por otra parte, está el lado del servidor, cuyos servicios web en XML, que remplazan algunas funcionalidades claves, a través de interfaces del servidor para invocar métodos GET, POST o SOAP desde el propio navegador.

En sus propias palabras, Top 10 Web 2.0 Attack Vectors, indica: "marcos RIA que se ejecutan en XML, XUL, Flash, Applets y JavaScripts están agregando nuevos conjuntos posibles de vectores. RIA, AJAX y los servicios web están agregando nuevas dimensiones a la seguridad de las aplicaciones web" (2006, párr. 4).

Es posible que muchos docentes en contratación, comprendan que las tecnologías base y la arquitectura de las aplicaciones de la Educación 4.0, son diseñadas (en el mayor de los casos), por microservicios escritos en node.js y Sprint Boot; que estas, han remplazado las aplicaciones monolíticas con contenedores y gestión de secretos detrás de un API, o servidor RESTful, esperando a ser consumidas por aplicaciones de una sola página (SPAs), las cuales están escritas en *frameworks JavaScript* (lenguaje principal de la web, ejecutando del lado del servidor), y los *frameworks* web modernos como Bootstrap, Electrón, Angular y React, ejecutándose del lado cliente, (s. f., p. 5). Pero, desconocen en gran medida los desafíos de seguridad que traen estas arquitecturas.

Surgen entonces algunas preguntas, ¿Cuál es el perfil del docente a contratar en la Educación 4.0?, será que el enfoque de las instituciones educativas, donde su visión está sujeta a que la formación online es solo para ingenieros y técnicos que emulan la interacción académica en espacios virtuales?, ¿Qué va a pasar con los docentes que por azares del destino no fueron integrados en sus procesos de formación con las TIC?, etc.

Son un sinfín de etc. que podemos agregar a esta lectura, pero en lo referente a este artículo y que no podemos dejar al lado, es la pregunta que abre el problema fundamental de la investigación, y es: ¿Cómo aborda la Educación 4.0 la seguridad de los activos en el proceso enseñanza-aprendizaje?; si bien, los docentes pueden ser especialistas en entornos virtuales; salvaguardar los activos, es una especialidad y saber, que debe involucrar no solo a los ingenieros y técnicos en sistemas, sino además del personal administrativo-educativo (inclúyase docentes) y a los mismos estudiantes como activos más preciados de esta industria 4.0.

2.2. Vulnerabilidad en la Educación 4.0

Por lo que se refiere a la inclusión de la Educación 4.0 en la sociedad; sabemos que las TIC se unifican en un espacio llamado web, que permiten una interacción sin barreras geográficas; diversidad de información; aprendizaje autónomo; desarrollo de habilidades; fortalecimiento de la iniciativa; corrección inmediata, etc. Sin dejar a un lado los fallos o debilidades, en el diseño del mismo medio que se vale la Educación 4.0 para llevar a cabo el proceso de enseñanza-aprendizaje, para este tema en particular («Top 10 Web 2.0 Attack Vectors», 2006) y ([OWASP], s. f.), nos brindan un top de 10 vulnerabilidades, que permiten la explotación para violar la seguridad del espacio y el medio que sustenta la Educación 4.0, y que se muestra en la Figura 1.

Fig. 1. Vulnerabilidades OWASP Top ten en relación con el análisis de riesgos en la Educación 4.0

Nota: actualizaciones OWASP Top 10, del 2013 al 2017, estos riesgos están respaldados en datos de la comunidad, reordenando los riesgos y reescribiéndolos desde cero. Datos extraídos de OWASP (s. f.)

En relación con estos riegos y vulnerabilidades ya estudiados por este Proyecto Abierto de Seguridad en Aplicaciones Web, en sus siglas en inglés OWASP, se enfoca el análisis de esta investigación y que en resumen, son las entidades educativas que imparten Educación 4.0, las que deben propiciar la seguridad en los medios que sustentan la base de su actividad comercial; evitando ataques activos y pasivos que tienen como objetivo la alteración de los recursos del sistema, o simplemente analizar el tráfico de la red, como se especifica en la Tabla 1.

Tabla 1.
Ataques activos y pasivos

Activos	Pasivos
Suplantación de identidad	Obtención de contenido de mensaje
Modificación de mensajes	
Repetición	Análisis de tráfico
Denegación de servicios	

Nota: en lo referente a los ataques pasivos y ataques activos, es muy difícil detectarlos, ya que los pasivos no producen alteración alguna; por otra parte, para mitigar los activos, se establecen medidas preventivas en unión con herramientas que permiten la detección o recuperación.

2.3. Análisis de riesgos en la educación 4.0.

Antes de pasar al análisis, queremos añadir otras tecnologías como lo son: XHTML; separación de contenido del diseño de uso de hojas de estilo; JavaScript asincrónico y XML; uso de Flas, Flex o Lazlo; uso de Ruby o Rails para programar páginas dinámicas; proveedor APIs o XML para que las aplicaciones puedan ser manipuladas *(Queeslaweb2.0-with-cover-page-v2.pdf, s. f., p. 3);* que al igual que las anteriores, tienden a incidentes de seguridad que permiten la materialización de amenazas.

En concreto, Open Web Security Proyect ([OWASP], s. f., p. 7) y *(Marco de evaluación de riesgos de OWASP | Fundación OWASP, s. f.);* brinda sustento teórico a esta investigación, con lo cual, se llevó a cabo un análisis de riesgos, en orden descendente; mayor a menor, que puede ser explotado por un atacante en las aplicaciones web, que sustentan la Educación 4.0.

2.3.1. A1: 2017 – Inyección:

Hemos visto que la Educación 4.0, reside en servicio web interno y externo, por lo que las vulnerabilidades de inyección se facilitan en consultas SQL, NoSQL, LDAP, XPath, comandos del SO, analizadores XML, encabezados SMTP, lenguajes de expresión, parámetros y consultas, ([OWASP], s. f., p. 8).

En consecuencia, las debilidades de seguridad que impactan en la Educación 4.0, se reflejan en pérdida o corrupción de información, que para cualquier institución educativa no es conveniente, ya que la integridad de los datos es un factor que prima en su servicio. Como lo es la denegación de servicios (DoS), no recomendada para este sector empresarial, puesto que los recursos del sistema y la información deben estar disponibles para los usuarios autorizados.

2.3.2. A2:2017 – Perdida de autenticación:

Debido a la fuga de información y cuentas administrativas por defecto, se puede atacar mediante fuerza bruta o diccionario para romper los hashes de las contraseñas y así comprometer el sistema de información, impactando en robo de identidad; lavado de dinero, y divulgación de información sensible protegida legalmente ([OWASP], s. f., p. 9).

Esta debilidad de seguridad afecta la Educación 4.0, ya que la suplantación de identidad perturba la autenticación, la cual, se encarga de confirmar la identidad de conexión y de igual forma, corrobora, que la información recibida proveniente de otra entidad sea verdadera; hablamos entonces de origen-destino y origen de los datos.

2.3.3. A3:2017 – Exposición de datos sensibles:

A causa de utilizar GPU, se pueden obtener contraseñas originales, ejecutando un vector de ataque de mayor impacto, como es *Man in the Middel,* o robar datos en texto plano del servidor; esto es posible, ya que las entidades educativas, por lo general no cifran datos sensibles (empleo de criptografía), y el empleo de algoritmos débiles de *hashinhg*, para el almacenamiento de contraseñas son fáciles de detectar ([OWASP], s. f., p. 10).

Este fallo impacta en la Educación 4.0, ya que se compromete la autenticación de las entidades origen/destino; autenticación de los datos; la confidencialidad; confidencialidad de flujo de tráfico e integridad de los datos.

2.3.4. A4:2017 – Entidad externa de XML (XXE):

Como resultado de explorar el código vulnerable en uno de los estándares que sustenta la Educación 4.0,

como son los procesadores XML (si es antiguo), se pueden extraer datos; ejecutar solicitudes remotas desde el servidor; escanear sistemas internos e incluso realizar ataque de denegación de servicio.

Por consiguiente, es necesario utilizar formatos como JSON; evitar la serialización; actualizar los procesadores y bibliotecas XML; deshabilitar las entidades externas de XML y procesamiento DTD, en todos los analizadores sintácticos; verificar funcionalidades de carga de archivos XML o XSL validar XML entrante usando validación XSD o similar, ([OWASP], s. f., p. 11).

2.3.5. A5:2017 – Pérdida y control de acceso:

En particular, un equipo sin conexión a red debe ser accedido físicamente para efectuar un ataque, al contrario de uno que, si está conectado a una red, como es el caso de estudio, que se expone a numerosos ataques.

Por esto, es importante realizar auditorías en las instituciones que se dedican a impartir Educación 4.0, esto, ya que, en algunos casos, en el área de sistemas, solo utilizan las herramientas SAST y DAST, que, si bien permiten detectar ausencia de controles, no es un desconocimiento que para la pérdida de control de acceso, es necesario utilizar medios manuales o de forma automática en algunos *frameworks*, que carecen de controles de acceso, ([OWASP], s. f., p. 12).

2.3.6. A6:2017 – Configuración de seguridad incorrecta:

También, las configuraciones incorrectas, impactan en la Educación 4.0, por sus servicios de red y que por lo general los fallos dan a los atacantes acceso no autorizado a datos o funciones del sistema.

Es recomendable parchear el sistema constantemente; no acceder a cuentas por defecto; proteger archivos y directorios; todo esto con el fin de "proteger" la plataforma que emplea para llevar a cabo las actividades de enseñanza-aprendizaje, el servidor de aplicaciones y la base de datos, ([OWASP], s. f., p. 13).

2.3.7. A7: 2017 – Secuencia de comandos en sitios cruzados (XSS):

Si bien, el impacto de este riesgo no es tan significativo en la Educación 4.0, y estamos hablando de XSS reflejado, XSS en DOM y severa para XSS; es importante mantener los datos no confiables separados del contenido activo del navegador, ([OWASP], s. f., p. 14).

No obstante, en la Tabla 2 y Tabla 3, se especifican enlaces que permiten la instalación de herramientas que detectan problemas de XSS en forma automática, en especial tecnologías maduras PHP, J2EE / JSP, ASP.NET

2.3.8. A8:2017 – Deserialización insegura:

Debido a las comunicaciones remotas e inter-procesos (RPC/IPC), protocolos de comunicación, Web Service y Brokers de mensaje, permiten la vulnerabilidad del sistema frente a ataque al caching y persistencia, bases de datos, servidores de cache y sistemas de archivos.

La Educación 4.0, no se ve muy afectada frente a este riesgo al igual que A6, ya que la explotación de deserialización no es fácil, "los *exploit* distribuidos raramente funcionan sin cambio o ajuste en su código fuente"; si bien, para tener una arquitectura segura frente a este fallo es no aceptar objetos serializados de fuentes no confiables, es importante implementar verificadores de integridad, ([OWASP], s. f., p. 15).

2.3.9. A9:2017 – Componentes con vulnerabilidades conocidas:

A diferencia del A8, que los *exploits* distribuidos raramente funcionan sin cambios o ajustes en el código fuente, para esta explotación, es sencillo obtener *exploits* para atacar los componentes tanto del lado cliente como del lado servidor (des configurados), software sin soporte o desactualizado (servicios web, aplicaciones, DBMS, APIs), entre otras.

Por lo que, la Educación 4.0 debe tener una constante monitorización a fuentes CVE y NVD, obtener componentes de fuentes conocidas, utilizar herramientas para mantener un inventario de versiones de componentes, ([OWASP], s. f., p. 16).

2.3.10. A10:2017 – Registro y monitoreo insuficientes:

Este riesgo muestra la mayor parte de brechas de seguridad, esto ya que el atacante depende de la ausencia de monitoreo; es importante examinar los registros después de las pruebas de penetración; asegurarse de que todos los errores de inicio de sección; control de acceso y validación de entradas al lado del servidor, ([OWASP], s. f., p. 17).

Para tener una mayor claridad y guía de mitigación de riesgos, (*Proyecto de seguridad de aplicaciones web abiertas, 2017*) proporciona una estrategia para determinar si una entidad posee suficiente monitoreo.

3. Resultados

En relación con el análisis de riesgos que se llevó a cabo en este artículo, referenciado con el proyecto OWASP, que detalla, no solo las técnicas de seguridad por orden de importancia como se evidencia en la Tabla 2, sino, además, recursos software, para colocar como instalador de ventana; macOS y código fuente, y así poder evaluar los riesgos a los que se enfrenta el proceso enseñanza-aprendizaje, de la Educación 4.0, ver Tabla 3.

Ahora bien, pensar en seguridad en la utilización de las TIC no está lejos de las necesidades que abarcan los centros educativos, universidades y administraciones públicas, que por compromiso, profesional, ético y competitivo deben salvaguardar la confidencialidad, integridad y disponibilidad de la información de sus activos.

De ahí la importancia de este artículo que brinda un análisis detallado de las amenazas o mejor, posibles riesgos de que una vulnerabilidad sea explotada, como se indicó paso a paso, mediante el marco de evaluación de riesgos en lo referente a OWASP.

Es probable además, que muchas instituciones que imparten Educación 4.0 refuten este escrito porque no han registrado fallo o debilidad en el diseño de sus aplicaciones, pero no indica, que no estén exentos de tener un asalto a la seguridad, mediante amenazas inteligentes que en su efecto ya han sido explotadas más no detectadas; por lo que, es recomendable este análisis, ya que está sustentado en una comunidad que se dedica a la investigación de riesgos y amenazas, con el objetivo de que las aplicaciones y API se confiables.

3.1 Establecer controles en entornos que sustentan la educación 4.0

Puesto que en la web se integran un sin número de atacantes que pueden utilizar diferentes vectores de ataque, en relación con las aplicaciones que sustentan la Educación 4.0 en el proceso enseñanza-aprendizaje, dejamos a disposición la Tabla 2.

Tabla 2.
Control proactivo de riesgos

Riesgo	Control	Referencia
A1	Definir requisitos de seguridad	*(OWASP Top Ten Controles Proactivos 2018 | C1, 2018)2018*
A2	Aprovechar los marcos de trabajo y las bibliotecas de seguridad	*(OWASP Top Ten Proactive Controls 2018 | C2, 2018)*
A3	Acceso seguro a la base de datos	*(OWASP Top Ten Proactive Controls 2018 | C3, 2018)*
A4	Codificar y escapar datos	*(OWASP Top Ten Proactive Controls 2018 | C4, 2018)*
A5	Validar todas las entradas	*(OWASP Top Ten Proactive Controls 2018 | C5, 2018)*
A6	Implementar identidad digital	*(OWASP Top Ten Proactive Controls 2018 | C6, 2018)*
A7	Hacer cumplir los controles de acceso	*(OWASP Top Ten Proactive Controls 2018 | C7, 2018)*
A8	Proteja los datos en todas partes	*(OWASP Top Ten Proactive Controls 2018 | C8, 2018)*
A9	Implementar registro y monitoreo de seguridad	(OWASP Top Ten Proactive Controls 2018 | C9, 2018)
A10	Manejar todos los errores y excepciones	(OWASP Top Ten Proactive Controls 2018 | C10, 2018)

Nota: mostramos en la Tabla 2, los controles proactivos de riesgo, con base en las técnicas de seguridad que deben tenerse en cuenta en un proyecto de desarrollo de software *(OWASP Top Ten Proactive Controls 2018 | Introduction | OWASP Foundation, 2018).*

En esta tabla, se alertan sobre los diez riesgos más críticos en aplicaciones Web, con el ánimo de incentivar en la utilización de estándares de verificación de seguridad en aplicaciones de OWASP, (2018). En la actualidad, la seguridad es de todos los actores involucrados en el proceso de enseñanza-aprendizaje, no es solo de las entidades educativas.

Por último, la Tabla 3, establece un marco de evolución de riesgos y requisitos del sistema para llevar a cabo su protección.

Tabla 3.
Requisitos y descargas de software

Requisitos	Descargas
NodeJS	*(Node.js,* s. f.*)*
Angular	*(Angular,* s. f.*)*
SonarQube	*(Download | SonarQube,* s. f.*)*
Escáner de sondas	*(Escáner de sonda | Documentos de SonarQube,* s. f.*)*
Mongobd	*(MongoDB Community Download,* s. f.*)*

Nota: en esta tabla, se facilita por medio de una guía, la cual se puede descargar (Marco de evaluación de riesgos de OWASP | Fundación OWASP, s. f.), un marco de evaluación de riesgos, explicando el proceso y requisitos previos (software), paso a paso, para realizar satisfactoriamente la instalación en diferentes sistemas operativos.

4. Discusión

Es innegable que la Educación 4.0 aprovecha el conocimiento a nivel mundial de los ciudadanos que se desenvuelven en este mundo digital, pero es importante resaltar la seguridad en las aplicaciones demandadas para ejecutar el proceso de enseñanza-aprendizaje, y que son utilizadas por la mayoría de los actores que están involucrados en el proceso educativo.

En primer lugar, se recomienda a las entidades que brindan servicio de Educación 4.0, establecer un fortalecimiento en seguridad para salvaguardar activos en su proceso de enseñanza-aprendizaje, y que, por desconocimiento (en su mayoría), muchos involucrados en el proceso educativo dejan a la deriva a ciberdelincuentes, sus datos protegidos, los cuales aprovechan para establecer actos delictivos.

En segundo lugar; este artículo, brinda sustentación teórica basándose en referencias calificadas para salvaguardar activos, además, de ampliar conocimientos en la participación social digital, que abren posibilidades para tener acceso a la ciencia y especialmente a la tecnología entre las capas poblacionales privadas de la misma.

Para concluir, educar y educarse en la actualidad conlleva a la necesidad de capacitarse en el uso apropiado de las TIC en la Educación, ya que es un problema que clama y reclama en una necesidad inmediata, en la cual nos vimos inmersos a través de la contingencia mundial y el acercamiento social digital, es por ello, que el conocimiento de la seguridad informática en cada especialidad o área del saber ya no reside solo en los especialistas sino en todo aquel ciudadano digital que emerge en el mundo digital, como lo es la Educación 4.0.

Referencias

Angular. (s. f.). *The modern web developer's platform.https://angular.io/*

Autores Varios (s. f.). Casos y retos de la educación 4.0. *Innovación Educativa,* 19(80).https://www.ipn.mx/assets/files/innovacion/docs/Innovacion-Educativa-80/Innovacion-educativa-80-web.pdf

Castro, S., Guzmán, B. & Casado, D. (2007). Las TIC en los procesos de enseñanza y aprendizaje. *Laurus*, 13(23), 213-234. https://www.redalyc.org/articulo.oa?id=76102311

Crisorio, R. L. & Escudero, C. (2017). *Educación del cuerpo: Curriculum, sujeto y saber.* Universidad Nacional de La Plata. http://www.memoria.fahce.unlp.edu.ar/libros/pm.504/pm.504.pdf

Domínguez Osuna, P. M., Oliveros Ruiz, M. A., Coronado Ortega, M. A., Valdez Salas, B., Domínguez Osuna, P. M., Oliveros Ruiz, M. A., Coronado Ortega, M. A. & Valdez Salas, B. (2019). Retos de ingeniería: enfoque educativo STEM+A en la revolución industrial 4.0. *Innovación Educativa,* 19(80), 15-32. http://www.scielo.org.mx/scielo.php?script=sci_abstract&pid=S1665-26732019000200015&lng=es&nrm=iso&tlng=es

SonarQube. (s. f.). *Download SonarQube.* https://www.sonarqube.org/downloads/index_usd.html

Etecé. (2022, enero 31). Educación. *Concepto*. https://concepto.de/educacion-4/

SonarQube. (s. f.). *SonarScanner.* https://docs.sonarqube.org/latest/analysis/scan/sonarscanner/

Guzmán, M. T. V., Morales, P. G. & Torres, M. G. M. (2019). *Propuesta de un modelo educativo para su integración a la educación 4.0. ANFEI Digital, 11,* https://www.anfei.mx/revista/index.php/revista/article/view/600

Iglesia Villasol, M. C. (2019). Caja de herramientas 4.0 para el docente en la era de la evaluación por competencias. *Innovación educativa (*México, DF), 19(80), 93-112. https://www.redalyc.org/journal/1794/179462794006/

Jiménez, C. S. H. & Albo, M. V. (2021). Educación 4.0 como respuesta a la Industria 4.0: Un estudio analítico-descriptivo. *Ciencia Latina Revista Científica Multidisciplinar,* 5(1), 1042-1054. https://doi.org/10.37811/cl_rcm.v5i1.310

Fundación OWASP. (s. f.). *Marco de evaluación de riesgos de OWASP* https://owasp.org/www-project-risk-assessment-framework/

Márquez, A. M. B. (2020). Educación 4.0. En las instituciones universitarias. *Educación*, 4, 10. https://www.adayapress.com/wp-content/uploads/2020/09/contec8.pdf

MongoDB (s. f.). *Community Download. MongoDB.* https://www.mongodb.comtry

Node.js. (s. f.). Download. Node.js. https://nodejs.org/en/download/

OWASP *(2018). OWASP Application Security Verification Standardhttps://owasp.org/www-project-application-security-verification-standard/*

OWASP. *(2018). OWASP Top Ten Controles Proactivos 2018 | C1: Definir requisitos de seguridad | https://owasp.org/www-project-proactive-controls/v3/en/c1-security-requirements.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C2: Leverage Security Frameworks and Libraries | https://owasp.org/www-project-proactive-controls/v3/en/c2-leverage-security-frameworks-libraries.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C3: Secure Database Access |https://owasp.org/www-project-proactive-controls/v3/en/c3-secure-database.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C4: Encode and Escape Data | https://owasp.org/www-project-proactive-controls/v3/en/c4-encode-escape-data.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C5: Validate All Inputs | https://owasp.org/www-project-proactive-controls/v3/en/c5-validate-inputs.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C6: Implement Digital Identity | https://owasp.org/www-project-proactive-controls/v3/en/c6-digital-identity.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C7: Enforce Access Controls |https://owasp.org/www-project-proactive-controls/v3/en/c7-enforce-access-controls.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C8: Protect Data Everywhere | https://owasp.org/www-project-proactive-controls/v3/en/c8-protect-data-everywhere.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C9: Implement Security Logging and Monitoring | https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | C10: Handle all Errors and Exceptions | https://owasp.org/www-project-proactive-controls/v3/en/c10-errors-exceptions.html*

OWASP *Foundation. (2018). OWASP Top Ten Proactive Controls 2018 | Introduction | https://owasp.org/www-project-proactive-controls/v3/en/0x04-introduction.html*

OWASP *(2017). Los diez riesgos más críticos en Aplicaciones Web.https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf*

OWASP *(2017). Proyecto de seguridad de aplicaciones web abiertas: Actualización del proyecto OWASP Top 10 2017. https://owasp.blogspot.com/2017/08/owasp-top-10-2017-project-update.html*

Parra Bernal, L., Rengifo Rodríguez, K., Parra Bernal, L. & Rengifo Rodríguez, K. (2021). Prácticas pedagógicas innovadoras mediadas por las TIC. Educación, 30(59), 237-254. https://doi.org/10.18800/educacion.202102.012

Parrales, M. (2019, octubre 8). *¿Qué es la Educación 4.0 y por qué es tan relevante?* Inspire Education Latin America. https://inspire-edu.tech/educacion-4/

Ceupe (s. f.). Que es la web 2.0. Queeslaweb2.0-with-cover-page-v2.pdf.

Rojas, J. M. R. (2018). *La educación como modelo de desarrollo humano, social y medio de liberación del ser humano en su aspecto material y espiritual.* https://revistaartefacto.usta.edu.co/index.php/univer-citario/139-la-educacion-como-modelo-de-desarrollo-humano-social-y-medio-de-liberacion-del-ser-humano-en-su-aspecto-material-y-espiritual

Shah, S. (9 de octubre de 2006). Top 10 Web 2.0 Attack Vectors. Help Net Security. https://www.helpnetsecurity.com/2006/10/09/top-10-web-20-attack-vectors/