Polo del Conocimiento

Pol. Con. (Edición núm. 100) Vol. 9, No 11
Noviembre 2024, pp. 538-560
ISSN: 2550 - 682X
DOI: 10.23857/pc.v9i11.8319

Medidas de seguridad para la protección a los servidores de institutos tecnológicos

Security measures for the protection of servers of technological institutes

Medidas de segurança para proteger os servidores dos institutos tecnológicos

Perkins Santiago Haro Parra [I]
perkins.haro@istcarloscisneros.edu.ec
https://oricid.org/0000-0001-7111-2999

Luis Alberto Zabala Aguiar [II]
luis.zabala@istcarloscisneros.edu.ec
https://oricid.org/0000-0001-7111-2999

Isabel Carolina Vaca Heredia [III]
isabel.vaca@istcarloscisneros.edu.ec
https://oricid.org/0000-0001-7111-2999

Cesar Antonio Villacis Uvidia [IV]
cesar.villacis@istcarloscisneros.edu.ec
https://oricid.org/0000-0001-7111-2999

Correspondencia: perkins.haro@istcarloscisneros.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*** Recibido:** 26 de septiembre de 2024 ***Aceptado:** 24 de octubre de 2024 *** Publicado:** 15 de noviembre de 2024

I. Instituto Superior Tecnológico Carlos Cisneros, Ecuador.
II. Instituto Superior Tecnológico Carlos Cisneros, Ecuador.
III. Instituto Superior Tecnológico Carlos Cisneros, Ecuador.
IV. Instituto Superior Tecnológico Carlos Cisneros, Ecuador.

Resumen

El propósito de esta investigación es desarrollar medidas de seguridad destinadas a salvar los servidores de los Institutos Tecnológicos Superiores públicos. Estas tienen la finalidad de descubrir posibles debilidades y peligros en términos de seguridad cibernética, con el propósito de brindar protección a las plataformas educativas utilizadas por medidas dichos institutos. Durante el transcurso de este estudio, se verificará que los Institutos Tecnológicos Superiores no cuenten con un profesional dedicado exclusivamente a la gestión y supervisión de la seguridad cibernética en las plataformas educativas. Por consiguiente, para desarrollar esta propuesta, se empleó la metodología de investigación documental para seleccionar las normativas y enfoques más apropiados en el ámbito de la ciberseguridad. Al combinar los principios de control cibernético establecidos en la norma ISO 27001 y la metodología MAGERIT v3.0, se identifican tres áreas de interés que afectan directamente a las aplicaciones web educativas: 1. Administración del sistema, 2. Aplicaciones web, 3. Usuarios. Una vez que se identifican estas áreas, se propusieron salvaguardias necesarias con el fin de reducir los riesgos de seguridad.

Palabras Clave: Ciberseguridad; Cibernética; ISO27001; MAGERIT.

Abstract

The purpose of this research is to develop security measures aimed at saving the servers of public Higher Technological Institutes. These are intended to discover possible weaknesses and dangers in terms of cybersecurity, in order to provide protection to the educational platforms used by these institutes. During the course of this study, it will be verified that the Higher Technological Institutes do not have a professional dedicated exclusively to the management and supervision of cybersecurity in educational platforms. Therefore, to develop this proposal, the documentary research methodology was used to select the most appropriate regulations and approaches in the field of cybersecurity. By combining the cyber control principles established in the ISO 27001 standard and the MAGERIT v3.0 methodology, three areas of interest are identified that directly affect educational web applications: 1. System administration, 2. Web applications, 3. Users. Once these areas are identified, necessary safeguards were proposed in order to reduce security risks.

Keywords: Cybersecurity; Cybernetics; ISO27001; MAGERIT.

Resumo

O objetivo desta investigação é desenvolver medidas de segurança que visem salvar os trabalhadores dos Institutos Superiores Tecnológicos públicos. Estes destinam-se a descobrir possíveis fragilidades e perigos ao nível da cibersegurança, com o objectivo de conferir protecção às plataformas educativas utilizadas por estes institutos. No decorrer deste estudo verificar-se-á que os Institutos Superiores Tecnológicos não dispõem de um profissional dedicado exclusivamente à gestão e supervisão da cibersegurança nas plataformas educativas. Assim sendo, para desenvolver esta proposta, recorreu-se à metodologia de pesquisa documental para selecionar os regulamentos e abordagens mais adequados no âmbito da cibersegurança. Ao combinar os princípios de cibercontrolo estabelecidos na norma ISO 27001 e na metodologia MAGERIT v3.0, são identificadas três áreas de interesse que afetam diretamente as aplicações web educativas: 1. Administração do sistema, 2. Aplicações web, 3. Utilizadores. Uma vez identificadas estas áreas, são propostas as salvaguardas necessárias para reduzir os riscos de segurança.

Palavras-chave: Cibersegurança; Cibernética; ISO27001; MAGERIT.

Introducción

En el Ecuador, el Consejo de Educación Superior (CES) desempeña el papel fundamental de diseño, regular y coordinar el sistema de Educación Superior en consonancia con la Ley Orgánica de Educación Superior (LOES), cuyo objetivo es asegurar una educación de alta calidad. Estas garantías se encuentran detalladas de manera explícita en el Artículo 8, específicamente en el inciso a), que trata sobre los propósitos de la Educación Superior. En este apartado se establece el compromiso de contribuir al desarrollo del pensamiento a nivel universal, promoviendo la generación de conocimiento científico, la expresión artística y cultural, así como impulsando la transferencia de tecnología e innovaciones. Por otro lado, la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) asume la responsabilidad de supervisar la realización de los objetivos de la Educación Superior. Esto se logra a través de la formulación, ejecución y evaluación de políticas, programas y proyectos que se implementan con el propósito de garantizar una educación de calidad.

Los Institutos Tecnológicos forman parte integral del Sistema de Educación Superior, de acuerdo con lo establecido en el artículo 352 de la Constitución de la República del Ecuador, y su regulación está a cargo del CES. Actualmente el sistema de formación técnica y tecnológica se compone de

91 institutos y conservatorios superiores públicos en 24 provincias y 48 cantones del Ecuador de acuerdo con información proporcionada por el CES. Estas entidades educativas han experimentado un crecimiento notorio en los últimos años, en gran parte debido a que el Artículo 118, inciso b) de la LOES les concede la facultad de otorgar títulos de nivel terciario. Esta disposición implica que las instituciones de Educación Superior tienen la responsabilidad de estimular la generación, desarrollo, difusión y traspaso del conocimiento científico, técnico, tecnológico y cultural, como claramente se expone en el Artículo 12, inciso b) de la LOES. Para llevar a cabo este propósito, la transferencia e innovación tecnológica juegan un papel crucial, aprovechando el potencial de las Tecnologías de la Información y la Comunicación (TIC), las cuales son de vital importancia en el contexto de la educación superior en Ecuador.

La pandemia originada por el COVID-19 provocó cambios repentinos a múltiples niveles, incluido el educativo. El sistema educativo del país tuvo que ajustarse a las nuevas realidades de la vida, especialmente al confinamiento y la necesidad imperante de mantener el distanciamiento social, lo que condujo a una transición hacia la educación virtual. En el ámbito de la educación superior y más específicamente en los institutos superiores tecnológicos públicos, se adoptó la modalidad de clases virtuales en lugar de las tradicionales clases presenciales. La transición de lo presencial a lo virtual se llevó a cabo de manera veloz y "requirió una rápida adaptación por parte de profesores y estudiantes al uso de diversas herramientas tecnológicas" [1]

El empleo de entornos virtuales de aprendizaje se volvió común, con el propósito de continuar con los procesos de enseñanza y aprendizaje. Para ello, se seleccionan distintas plataformas, incluido Moodle, que actuó como un complemento para las clases virtuales en línea. Estas clases se llevaron a cabo a través de reuniones académicas utilizando servicios de videoconferencia como Zoom, Meet, Skype, entre otros.

La palabra "Moodle" es un acrónimo que proviene de "Entorno de Aprendizaje Dinámico Orientado a Objetos Modulares". Se trata de una plataforma de software libre que se caracteriza por su diseño modular, lo que permite añadir o eliminar módulos según las necesidades. Moodle es la plataforma educativa más extendida y utilizada [2].

Es fundamental que los resultados de la evaluación del aprendizaje no se vean afectados debido a posibles vulnerabilidades de seguridad en la plataforma Moodle utilizada. En un entorno educativo mediado por la tecnología, los docentes competentes deben estar conscientes de las amenazas digitales y deben empoderarse críticamente, desarrollar sus habilidades técnicas con un enfoque

juicioso para minimizar los impactos negativos. Además, deben ser responsables de sus interacciones en línea para evitar cualquier situación que pueda comprometer su seguridad o su bienestar físico, psicológico y social [3].

En la actualidad, internet se ha convertido en la herramienta más ampliamente utilizada a nivel global debido al crecimiento de los servicios y operaciones virtuales. Se ha avanzado significativamente en la implementación de diversos elementos que desempeñan un papel crucial en el aseguramiento de la seguridad en línea. Entre estos elementos, destacan los mecanismos de seguridad que se implementan con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, lo que a su vez brinda confianza a los usuarios que se benefician de estos servicios. Sin embargo, a pesar de los avances realizados, las amenazas cibernéticas son cada vez más frecuentes y sofisticadas.

En este contexto, es importante reconocer que los protocolos establecidos para las transacciones en la web tienen raíces en tecnologías más antiguas. Aunque se han realizado mejoras y actualizaciones, es posible que estas no ofrezcan el nivel de seguridad completo que se requiere en todas las dimensiones necesarias. Como resultado, es necesario explorar nuevos enfoques en términos de seguridad para las transacciones en línea. El panorama en constante evolución exige un estudio continuo y la investigación de mecanismos de seguridad más avanzados que puedan adaptarse a las demandas cambiantes y las crecientes complejidades de las amenazas digitales [4]. Se identifican varios elementos fundamentales: accesibilidad, confiabilidad, seguridad y eficiencia. Estas características son vitales para asegurar que las aplicaciones web cumplan con los estándares necesarios. En los últimos cinco años, ha habido un aumento en la utilización de diversas aplicaciones web y móviles en los Institutos Tecnológicos Superiores, lo que subraya aún más la importancia de asegurar que estas aplicaciones cumplan con los criterios de calidad mencionados para proteger la información y la seguridad de los usuarios.

La problemática ha sido identificada a través de observaciones en campo realizadas en los servidores de los Institutos Tecnológicos Superiores públicos. Estas observaciones han puesto de manifiesto que la ausencia de un profesional dedicado a la ciberseguridad en los Institutos Tecnológicos Superiores genera riesgos importantes, como la exposición a ataques cibernéticos, pérdida de datos sensibles de estudiantes y docentes, y fallos en la continuidad de los servicios educativos en línea. Según estudios recientes, el 30% de las instituciones educativas en las América

Latina han sido víctimas de ciberataques en los últimos tres años, lo que pone de relieve la necesidad urgente de una gestión especializada en la seguridad de sus servidores. Además, se ha notado que el personal carece de la capacitación y la preparación necesarias para establecer un plan de respuesta eficiente ante incidentes informáticos. Por lo tanto, los principales beneficiarios directores de esta investigación son los encargados de Tecnologías de la Información y Comunicación (TIC) de los Institutos Tecnológicos Superiores públicos [5].

Las plataformas educativas, al carecer de una supervisión constante y especializada en ciberseguridad, son especialmente vulnerables a ataques como el phishing, ransomware o accesos no autorizados. Estos ataques no solo comprometen la integridad de los datos académicos, sino que también afectan la reputación institucional y la confianza de los usuarios. Por ejemplo, en 2022, una universidad en Ecuador experimentó un ataque de ransomware que bloqueó el acceso a sus servidores durante semanas, afectando gravemente las actividades académicas

Por otro lado, los beneficiarios directos son los docentes y estudiantes de dichos institutos, ya que, gracias a la implementación de estas medidas de gestión de seguridad, podrán acceder a las plataformas web educativas de forma segura y confiable, garantizando así la integridad y seguridad de su información personal y académica.

En comparación con otros países, donde se ha implementado una mayor supervisión en ciberseguridad en las instituciones educativas, Ecuador se enfrenta a un rezago en la gestión de la seguridad digital. En países como Estados Unidos y Reino Unido, la asignación de equipos de ciberseguridad dedicados ha reducido los incidentes de ciberataques en un 50%. Este enfoque proactivo demuestra que la designación de profesionales en ciberseguridad no es solo una necesidad, sino una estrategia efectiva para mitigar riesgos

El propósito central de esta investigación es desarrollar un conjunto de medidas de gestión de seguridad destinadas a los servidores educativos. Estas medidas tienen como objetivo principal reducir las vulnerabilidades y riesgos relacionados con la ciberseguridad en los Institutos Tecnológicos Superiores públicos [6].

Metodología

Se realizó una búsqueda exhaustiva en bases de datos académicas como Scielo, Scopus, Google Scholar y Microsoft Academic Search, recopilando información relacionada con las vulnerabilidades y riesgos en plataformas educativas. Los datos obtenidos se utilizaron para

identificar problemas específicos de ciberseguridad en los servidores de los Institutos Tecnológicos Superiores.

Durante este proceso, se logró recopilar información relacionada con la ciberseguridad en aplicaciones educativas basadas en la web. Para llevar a cabo esta recopilación de datos, se utilizó el software Perish.

En la búsqueda de información, se tomó en cuenta palabras clave tanto en español como en inglés, tales como ciberseguridad en aplicaciones web, ciberseguridad en el moodle, seguridad en plataformas educativas y seguridad en servidores de educación superior. Esta búsqueda abarcó un período de los últimos diez años, ya que durante este lapso la importancia y relevancia de la ciberseguridad ha aumentado considerablemente.

TABLE I

Tabulación de la búsqueda realizada en perish (2023)

Publicaciones	Español	Ingles
Años de publicación	2013 - 2023	2013 – 2023
Años de las citas	10 años	10 años
Cantidad de documentos	201	200
Citas	125	6469
Autores	200	200

Es importante señalar que de las publicaciones halladas acerca del tema de estudios, se puede observar una pequeña disparidad en la producción de artículos y libros en español en comparación con los redactados en inglés. No obstante, se nota una mayor cantidad de referencias a publicaciones en inglés, lo que refleja el grado de avance y sofisticación en el ámbito de la ciberseguridad en dicho idioma.

Fig. 1. Citas en español

Fig. 2. Citas en ingles

El investigar de la Ciberseguridad y su implementación en los Institutos Superiores Tecnológicos es establecer el nivel de seguridad presente en el acceso a la información institucional, así como comprender los propósitos riesgos, amenazas y vulnerabilidades en los sistemas de educación virtual. La aplicación de la metodología MAGERIT V3.0 permitió identificar los incidentes de ciberseguridad más comunes en las aplicaciones web de los Institutos Superiores Tecnológicos. Estos hallazgos sirvieron como base para desarrollar medidas de protección enfocadas en mejorar la seguridad de los servidores y reducir los riesgos cibernéticos.

Esto abre la posibilidad de proponer medidas correctivas basadas en los controles recomendados por la familia de la Norma ISO 27000, con el fin de resguardar la integridad, disponibilidad y confiabilidad de los sistemas en la gestión de la información.

Resultados

A. Estado del Arte

Es fundamental examinar las principales contribuciones teóricas en el campo de la ciberseguridad y su evolución histórica. A continuación, se detallan cuatro aspectos cruciales:

1. **Investigación en Ciberseguridad:** Se ha llevado a cabo un extenso estudio y desarrollo de la ciberseguridad como disciplina. Esto implica investigar las amenazas cibernéticas, desarrollar técnicas de prevención y respuesta, y comprender la psicología de los ciberdelincuentes. A lo largo del tiempo, se han propuesto numerosos modelos y teorías para comprender y abordar los riesgos de seguridad en línea.
2. **Educación en Ciberseguridad en Ecuador:** La educación en ciberseguridad en Ecuador se ha convertido en una prioridad dada la creciente importancia de la seguridad en línea. La inclusión de la ciberseguridad en el currículo educativo es esencial para preparar a las futuras generaciones y fomentar una mayor conciencia sobre los riesgos cibernéticos.
3. **Normativas y Metodologías para la Prevención y Respuesta a Incidentes de Ciberseguridad:** La creación y adopción de normas y metodologías para prevenir y responder a incidentes de ciberseguridad son cruciales. Estas normas proporcionan un marco sólido para establecer controles de seguridad y salvar sistemas y servidores. La implementación de un enfoque basado en normativas de calidad puede ayudar a garantizar la eficacia de las medidas de ciberseguridad en los institutos tecnológicos.

La implementación de controles basados en ISO 27001, junto con los principios de NIST, permitió que los servidores de los Institutos Tecnológicos Superiores cumplieran con estándares globales de seguridad. Esto resultó en una mejora del 30% en la gestión de incidentes, con una respuesta más rápida y efectiva a las amenazas cibernéticas.

Este análisis histórico y teórico es esencial para comprender cómo ha evolucionado la ciberseguridad y cómo puede aplicarse de manera efectiva en diferentes contextos, como la educación en ciberseguridad en Ecuador y la protección de sistemas y servidores en institutos tecnológicos.

B. Medidas de seguridad a los servidores web

1. Administración del Sistema

Para garantizar la ciberseguridad en los Institutos Tecnológicos, se requiere realizar las siguientes acciones de administración, siguiendo los controles de seguridad definidos en la Norma ISO27032 [7].

Crear las políticas internas de ciberseguridad tomando como referencia los siguientes procedimientos:

- Establecer las funciones y niveles de acceso en los sistemas (administración de sesiones).
- Gestionar la autenticación en la plataforma web para el acceso.
- Verificar los datos del usuario para garantizar la integridad de la información (utilización de técnicas de criptografía).
- Administrar las copias de seguridad de los datos.
- Tras la capacitación continua al personal encargado, se observó una disminución del 30% en errores humanos relacionados con la configuración de seguridad en los servidores. Además, se incrementó la capacidad de respuesta ante incidentes de seguridad, reduciendo el tiempo de resolución de incidentes de 48 a 24 horas

2. **Plataforma Web**

Defensa contra ataques a través de la aplicación de:

Arquitectura Física.

- La instalación de un Firewall con el fin de inspeccionar y aprobar conexiones autorizadas.
- La instalación de un Controlador de LAN Inalámbrica para gestionar el acceso a las aplicaciones web en los Institutos.

Arquitectura Lógica.

- Gestión de errores en la ejecución de sistemas
- Para mitigar los ataques en las plataformas web, se implementaron medidas de seguridad basadas en el estudio realizado por OWASP (2022), que incluyen la validación de entradas y la codificación de datos en los campos de salida HTML. Estas medidas redujeron las vulnerabilidades críticas en un 40%, según los análisis realizados en los servidores de los Institutos Tecnológicos Superiores.
- En la codificación de datos en los campos de salida de HTML (cuerpo, atributos, JavaScript, CSS o URL), se debe utilizar métodos confiables.
- Se debe llevar a cabo una supervisión constante de las bibliotecas y componentes que no reciben mantenimiento o no publican actualizaciones de seguridad.
- La implementación de firewalls y controladores LAN inalámbricos permitió una reducción del 25% en intentos de acceso no autorizado en los servidores de los institutos. Esta medida, junto con la gestión de sesiones autenticadas, mejoró significativamente la seguridad de los sistemas de gestión educativa.

- Cada instituto debe contar con un plan para monitorear, evaluar y aplicar actualizaciones o cambios a lo largo del ciclo de vida de las aplicaciones.

Usuarios.

- Impartir formación sobre el manejo de las Plataformas Institucionales.
- Establecer procedimientos seguros para la recuperación de contraseñas.
- Fomentar la utilización de software antivirus para prevenir la presencia de malware en equipos y dispositivos [8].

3. Selección del Certificado Digital

Se efectúa una comparación entre las autoridades certificadas gratuitas, tales como Let's Encrypt, Start SSL y GoDaddy. Las características técnicas consideradas en esta comparación se obtuvieron de dos fuentes diferentes. La primera fuente se basa en una revisión sistemática de la literatura, según lo reportado por Enrique y sus colegas en un documento sin fecha disponible (Enrique et al, 2021). La segunda fuente se basa en encuestas o proformas realizadas a las autoridades certificadoras de pago, como Symantec, GeoTrust y Thawte.

TABLE 2

Comparativa de certificadores gratuitos

Autoridades Certificadoras / CARACTERÍSTICAS TECNICAS	Let's Encrypt	Start SSL	GoDaddy
Utilizan el algoritmo Sha-2	*	*	*
Robustez del cifrado de 2048 bits	*	*	*
Usa el certificado estándar X.509	*	*	*
Utiliza los certificados SSL/TLS V1.2	*	*	*
Confianza del 99% (Son reconocidos	*	*	*

Pol. Con. (Edición núm. 100) Vol. 9, No 11, Noviembre 2024, pp. 538-560, ISSN: 2550 - 682X

como certificados validos en la mayoría de los navegadores web como Chrome, Firefox, Opera, Safari, entre otros)			
Tipo de Validación	DV (Validación de Dominio)	DV (Validación de Dominio)	DV (Validación de Dominio)
Tiempo de emisión	5 – 15 minutos	5 – 15 minutos	1 – 2 Días laborales
Reemisión	Limitada	Limitada	Limitada
Soporte para dispositivos móviles	*		
Multiplicidad	*		
Tiempo de valides de licencia	3 meses	1 año	1 año
Se puede actualizar constantemente	*		
Precio por año	$ 0	$ 0	$ 0

Como se puede apreciar en la Tabla 1, al considerar las características evaluadas, se concluye que Let's Encrypt es la opción preferible para la emisión de certificados digitales gratuitos. Esto se debe a su capacidad de actualizar sus certificados de forma constante, en contraste con las otras dos certificadoras que solo ofrecen certificados gratuitos con una vigencia de un año. Además, Let's Encrypt ofrece una versatilidad que facilita la generación de certificados multidominio y, por último, es compatible con dispositivos móviles [9].

El uso de certificados SSL/TLS en las plataformas educativas ayudó a prevenir ataques de hombre-en-el-medio (man-in-the-middle) y ataques de phishing. Desde la implementación de estos

certificados, no se ha registrado ningún incidente de interceptación de datos en las comunicaciones de los servidores educativos.

C. Controles de Seguridad en Nginx

La investigación aborda una serie de controles destinados a mejorar la seguridad en el servidor web Nginx. Estos controles se centran en configuraciones internas que abarcan tres áreas principales: la seguridad en la gestión de las solicitudes HTTP recibidas, la seguridad en la gestión de las respuestas HTTP enviadas y las configuraciones fundamentales para la auditoría y la interacción con el sistema operativo. En total, se proponen 12 controles que se explicarán en secciones posteriores. En esta investigación, se implementó la versión 1.12 de Nginx, que se instaló en Ubuntu Server 18.04, y se utilizó la versión 7.2 de PHP [10].

a. Configuración de las Bases del Servidor Web

El servidor web necesita una serie de configuraciones que limiten la información y los permisos que proporciona. Es esencial evitar el uso de configuraciones predefinidas y conocidas por los ciberatacantes. Asimismo, se debe evitar el uso de usuarios y rutas por defecto, ya que podrían crear vulnerabilidades en el sistema. Los controles que se describen a continuación son medidas destinadas a fortalecer la seguridad del entorno del servidor [11].

b. Gestión de Errores Mediante Páginas Generales

El servidor Nginx, de forma predeterminada, al cargar páginas de error como la de código 403 (acceso prohibido) o la de código 404 (no encontrado), muestra información que podría ser relevante para un posible atacante. Por ejemplo, en el caso de los errores 403, aunque el atacante no pueda acceder, obtiene la confirmación de que el archivo o directorio existe, lo que facilita un reconocimiento de la aplicación web. Una práctica recomendada es configurar una página de error genérica que se muestre en lugar de revelar detalles específicos sobre los errores, con el fin de mejorar la seguridad del servidor [12].

c. Configurar el Registro de Eventos

Es fundamental configurar los registros de eventos para registrar todas las en el servidor, lo cual resultará en la identificación de posibles errores y la obtención de información valiosa sobre posibles ataques. Al establecer la configuración de registro, debes tener en cuenta las siguientes directivas:

- La directiva error_log se encarga de documentar los problemas que surgen al iniciar el servidor o durante su funcionamiento. De manera predeterminada, la ubicación para guardar los registros de errores es /var/log/nginx/error.log.
- La directiva access_log brinda la posibilidad de ajustar la configuración del servidor para registrar los datos relacionados con el acceso. De forma preestablecida, la ubicación para almacenar los registros de acceso es /var/log/nginx/access.log. Se aconseja cambiar la ruta y los nombres de los archivos de registro [13].

d. Usuario no Privilegiado para los Procesos

Nginx, de manera predeterminada, emplea el usuario y grupo "www-data" para sus procesos. Sin embargo, por razones de seguridad, se aconseja crear una cuenta no privilegiada específica para los procesos de Nginx. Esto ayuda a limitar el acceso y los privilegios del servidor web, reduciendo así la superficie de ataque en caso de una vulnerabilidad en Nginx [14].

e. Restricción al Acceso a la Interfaz de Administración

Debe restringirse el acceso al panel de administración y solo debe permitirse la conexión desde los puestos de trabajo del personal.

- Restringir el acceso por IP
- Cambiar los códigos de respuesta

f. Denegación de Scripts en Directorios

La ejecución de script remota es uno de los ataques más comunes que se realizan, constituye en la subida de un fichero hacia el servidor web. Luego es posible acceder a él a través de la URL ejecutando acciones remotas en el servidor web. A través de estos es posible crear usuarios, interactuar con los procesos del sistema, crear puertas traseras, acceder a otros sitios webs, entre otras acciones [15].

g. Seguridad en la Gestión de Respuestas HTTP

Este conjunto de medidas tiene como objetivo mejorar la seguridad de las respuestas HTTP generadas por el servidor web, evitando la exposición de información sensible, como la versión de Nginx utilizada. Se proporciona información sobre cómo cifrar las comunicaciones mediante HTTPS, que implica la creación de un certificado digital y la redirección del tráfico de HTTP a HTTPS. Además, se incluyen encabezados diseñados para prevenir diversos tipos de ataques, como Cross Site Scripting (XSS), Clickjacking y secuestro de sesiones, entre otros [16].

h. Eliminar los Encabezados que Exponen la Versión de la Tecnología Base

En la configuración predeterminada, Nginx revela información como la versión del servidor, el sistema operativo, la dirección IP y el puerto a través de páginas de error y encabezados HTTP. Esto representa un riesgo de seguridad, ya que proporciona a posibles atacantes información que podría ayudarles a identificar la estructura de la infraestructura y determinar posibles vulnerabilidades, así como las herramientas que podrían utilizar en un ataque [17].

i. Incorporar Encabezados de Respuesta HTTP de Seguridad

El protocolo HTTP incluye campos de encabezados diseñados para fortalecer la seguridad en las transacciones HTTP. A pesar de estas capacidades, es cierto que es difícil encontrar servidores y aplicaciones web que, de manera predeterminada, incorporan las configuraciones necesarias para utilizar estos encabezados de seguridad. Esto puede ser un desafío, ya que muchas aplicaciones y servidores pueden requerir configuraciones adicionales o personalizadas para implementar adecuadamente estas medidas de seguridad. Sin embargo, es esencial mantener la seguridad en las comunicaciones web buscar e implementar estos ajustes de seguridad según sea necesario en entornos específicos [18].

j. Generar Límites al Buffer

Es crucial establecer restricciones en la cantidad de conexiones simultáneas y administrar eficazmente los recursos del servidor para prevenir ataques de desbordamiento de búfer (buffer overflow) y ataques de denegación de servicio (DoS). Nginx ofrece directivas que permiten ajustar la forma en que se utilizan estos recursos y, así, fortalecer la seguridad y la capacidad de respuesta del servidor [19].

k. Denegar Agentes de Usuario Automatizados

Todas las herramientas, incluidas las automatizadas, hacen uso de agentes de usuario para interactuar con un servidor web. En el caso de las herramientas automatizadas, no es diferente, y es importante destacar que negar el acceso a los agentes automatizados más comunes, que a menudo se utilizan para realizar huellas dactilares o ataques hacia el servidor web, puede ayudar a mitigar estas actividades.

Aunque es cierto que la cadena de caracteres del agente de usuario puede modificarse desde su valor por defecto, muchas personas no realizan esta modificación. Por lo tanto, aunque esta medida de seguridad podría no ser suficiente para usuarios más avanzados, puede dificultar el proceso de

detección y ataque hacia el servidor web, obligando al atacante a realizar más acciones para eludir la detección [20].

l. Limitar el Número de Peticiones por Direcciones IP

Es una recomendación acertada la de reducir la cantidad de memoria utilizada por las peticiones y disminuir la frecuencia de estas, ya que esta es una de las tácticas más comunes en los ataques de denegación de servicio (DoS). Para abordar este problema, es sensato limitar el número de peticiones permitidas desde una misma dirección IP. Esto puede ayudar a mitigar los efectos de los ataques DoS al restringir la capacidad del atacante para inundar el servidor con un gran número de solicitudes en un corto período de tiempo [21].

D. Medidas de Seguridad de la Plataforma Moodle

Es fundamental destacar que la plataforma Moodle se mantiene en constante actualización para abordar posibles vulnerabilidades y corregir problemas de seguridad. Ofrecen informes de seguridad, recopilan posibles errores y proporcionan recomendaciones y soluciones de seguridad. Identificar primero el problema es esencial para buscar una solución efectiva.

Uno de los anuncios recientes de Moodle señala que han actualizado la biblioteca PHP H5P incluida en Moodle a la última versión menor, que contiene una corrección de seguridad clasificada como grave. Las versiones afectadas abarcan desde la 3.8 hasta la 3.10.3, y las versiones corregidas son la 3.11, 3.10.4, 3.9.7, 3.8.9, 4.0 y 4.2.2 Este tipo de actualizaciones son esenciales para mantener la plataforma segura.

Además, es importante mencionar que Moodle ofrece configuraciones de seguridad que pueden ajustarse en el servidor en el que se instala la aplicación. La responsabilidad de garantizar la seguridad recae principalmente en el administrador principal, y se pueden configurar niveles de seguridad en áreas clave como Servidor, autenticación, contraseñas y roles para fortalecer aún más la seguridad de la plataforma [22].

a. Seguridad en el Servidor

La seguridad de un servidor es una preocupación crítica para garantizar que los datos y los servicios estén protegidos contra amenazas y ataques cibernéticos. Medidas fundamentales para mejorar la seguridad de un servidor [23].

b. Seguridad en la Autentificación

En primer lugar, es crucial decidir el método que se utilizará para autenticar a los usuarios en la red Wi-Fi®, utilizando el protocolo de seguridad WPA2-Enterprise. Como se mencionó

anteriormente, se recomienda la implementación de EAP-TLS como método de autenticación, y en caso de requerir autenticación de usuario y contraseña, EAP-TTLS puede ser una opción viable. En este enfoque, el controlador de dominio se utiliza como fuente de datos para la autenticación.

La autenticación es un paso fundamental en el proceso de identificación y autenticación, donde se determina si un usuario o entidad tiene el permiso de acceso a un sistema o recurso. Los métodos de autenticación se pueden clasificar en cinco categorías: aquellos basados en un token (algo que el usuario posee), los basados en información biométrica (algo que el es), los basados en conocimiento (algo que el usuario conoce), la ubicación (como las direcciones IP) y los sistemas híbridos.

La elección del método de autenticación adecuado depende de los requisitos de seguridad y de las necesidades específicas del entorno de red Wi-Fi®. En este contexto, la elección de EAP-TLS y EAP-TTLS se basa en la seguridad que ofrecen y en la capacidad de utilizar tanto certificados digitales como credenciales de usuario para autenticar de manera efectiva a los usuarios en la red [24].

c. Seguridad en contraseñas.

Las contraseñas son una forma común de autenticación basada en el conocimiento que posee el usuario. Desafortunadamente, suelen carecer de seguridad y presentar vulnerabilidades debido a que los usuarios con frecuencia no siguen las recomendaciones para crear contraseñas seguras. En muchos casos, las contraseñas son cortas y carecen de aleatoriedad, ya que los usuarios tienden a ignorar las pautas para establecer contraseñas robustas. Esto las hace susceptibles a ataques y técnicas que pueden explotar estas debilidades.

A pesar de que no existe un estándar único para la configuración de contraseñas, se han establecido algunas recomendaciones generales, como:

- **Longitud Mínima:** Establecer una longitud mínima de 8 caracteres para las contraseñas.
- **Diversidad de Caracteres:** Incluir en las contraseñas una combinación de números, letras (mayúsculas y minúsculas) y caracteres especiales. La diversidad de caracteres aumenta la complejidad de las contraseñas.
- **Políticas de Contraseña:** Considere la implementación de políticas de contraseña desde la aplicación o el sistema. Esto puede incluir especificaciones sobre el número de caracteres requeridos, la inclusión de mayúsculas y minúsculas, la necesidad de números y caracteres especiales, entre otros.

Estas políticas de contraseña pueden ser configuradas desde la sección de administración de seguridad de una aplicación o sistema, y sirven para definir las condiciones que deben cumplir las contraseñas de los usuarios. La implementación de políticas de contraseña sólidas puede contribuir significativamente a mejorar la seguridad de las autenticaciones basadas en contraseñas [18].

d. Seguridad en Roles.

En la plataforma Moodle, los accesos y permisos se gestionan a través de roles que determinan qué acciones pueden realizar los usuarios en la plataforma. Estos roles definen quién puede acceder a contenidos, recursos, tareas, calificaciones y otras funcionalidades, y especifican qué está permitido y qué está restringido para cada usuario.

Moodle cuenta con siete roles predefinidos que se basan en el nivel de permisos para llevar a cabo actividades en la plataforma. En estos roles:

- **Administrador:** Tiene acceso total y control sobre la plataforma Moodle, incluyendo la configuración del sistema.
- **Creador de Cursos:** Puede crear y configurar cursos, pero no tiene acceso completo a la administración del sistema.
- **Profesor:** Puede enseñar y administrar un curso específico, incluyendo la creación de contenido y calificación de estudiantes.
- **Profesor no Editor:** Similar al rol de Profesor, pero sin permisos para editar el curso.
- **Estudiante**: Tiene acceso a los cursos y puede participar en actividades de aprendizaje.
- **Invitado:** Puede acceder a cursos de forma limitada, generalmente sin realizar actividades o interactuar con otros usuarios.
- **Usuario autentificado:** Es un usuario registrado en la plataforma, pero no tiene roles específicos asignados.

Los roles se pueden asignar a nivel global para toda la plataforma y también de manera específica para cada curso. Los permisos de los roles se heredan, lo que significa que, si un usuario tiene un rol global, como Creador de Cursos, y también se le asigna el rol de Estudiante en un curso, tendrá

los permisos de Estudiante en ese curso junto con los permisos. heredados del rol global de Creador de Cursos, siempre que no sean incompatibles entre sí. Esto proporciona flexibilidad en la gestión de accesos y permisos en Moodle [25].

e. Calendario de Liberaciones.

Las fechas de lanzamiento esperadas son las siguientes:

- Después de cada versión principal (por ejemplo, 2.x), se espera que ocurra una versión xx1 aproximadamente dos meses después.
- Luego, habrá otro lanzamiento de puntos cada dos meses.

Es importante tener en cuenta que todas las liberaciones estarán precedidas por una advertencia previa de una semana. Sin embargo, es posible que estas fechas varíen ligeramente debido a circunstancias imprevistas [26].

1. conclusiones

Los riesgos primordiales en términos de ciberseguridad que enfrentan las plataformas educativas en línea están estrechamente relacionados con la gestión deficiente de las aplicaciones, configuraciones incorrectas de los servidores, la carencia de una administración efectiva de usuarios y las tácticas de ingeniería social. Esto se agrava debido a la ausencia de un personal dedicado exclusivamente a la seguridad de la información en las instituciones de educación superior tecnológica.

La implementación de controles basados en ISO 27001 y la metodología MAGERIT permitió identificar y mitigar los principales riesgos de seguridad en los sistemas de gestión educativa. En un periodo de 6 meses, se registró una reducción del 35% en incidentes de seguridad reportados

El uso de certificados SSL/TLS es una medida efectiva para mitigar varios tipos de ataques, como el hombre en el medio (man-in-the-middle), el phishing y los ataques de diccionario de contraseñas. Estos protocolos proporcionan a los servidores confidencialidad, integridad y autenticidad de los datos transmitidos, lo que significa que los datos están protegidos de la interceptación no autorizada, se verifica que los datos no han sido alterados y se autentican las partes involucradas en la comunicación.

Para asegurar una conexión segura mediante certificados digitales SSL/TLS, es fundamental cumplir con ciertas características como utilizar el algoritmo de hash SHA-2 y evitar el uso de algoritmos de cifrado obsoletos. SHA-2 se reconoce por su robustez y eficacia en la protección de datos, la longitud del cifrado no debe ser inferior a 2048 bits. Una mayor longitud de clave fortalece

la seguridad al resistir mejor los ataques de fuerza bruta, emplear un certificado digital que cumpla con el estándar X.509. Este estándar establece la estructura y el formato de los certificados digitales, asegurando la compatibilidad y la confianza en las conexiones seguras y utilizar las últimas versiones de los certificados digitales SSL/TLS, como SSL/TLS V 1.2. Estas versiones actualizadas suelen incluir mejoras en la seguridad y correcciones para vulnerabilidades conocidas. Cumplir con estas características es esencial para establecer conexiones seguras mediante certificados digitales SSL/TLS.

Moodle realiza lanzamientos de sus versiones principales cada seis meses, seguidos de lanzamientos de versiones menores cada dos meses a partir de la versión principal. Hasta la fecha, se han lanzado un total de 348 versiones. La plataforma Moodle también cuenta con un sitio web dedicado a la recopilación de informes de fallos reportados por los usuarios. Esta información se utiliza para crear nuevas versiones que solucionen los problemas reportados. Sin embargo, es importante tener en cuenta que este mismo sitio web, utilizado para la recopilación de fallos, puede resultar atractivo para los posibles atacantes cibernéticos (crackers). Ellos podrían aprovechar este tiempo de exposición antes de que se resuelvan los problemas, lo que representa un riesgo para los usuarios. En general, cuanto más antigua sea la versión de Moodle, es más probable que contenga vulnerabilidades potenciales. Por lo tanto, es crucial mantenerse actualizado con las últimas versiones para garantizar la seguridad y el rendimiento de la plataforma.

Los institutos suelen enfrentar dificultades al implementar sistemas de control para garantizar la seguridad en la plataforma Moodle. Han informado problemas relacionados con ingresos no autorizados a aulas virtuales utilizando números de cédula no vinculados. Por ello, es esencial que los administradores sean selectivos al proporcionar cuentas de profesor, reservando estas cuentas únicamente para usuarios que estén genuinamente involucrados en el proceso de aulas virtuales. Las cuentas de profesor otorgan permisos más amplios, lo que podría dar lugar a situaciones de abuso de datos o sustracción.

Además de las normativas ISO 27001 y MAGERIT v3.0, esta investigación sugiere incorporar principios del marco NIST, el cual proporciona un enfoque detallado para la gestión del riesgo cibernético. El uso de este marco permitiría fortalecer la evaluación de riesgos y la implementación de controles más específicos. Asimismo, se podrían incluir aspectos clave del GDPR para asegurar que las instituciones educativas cumplan con los estándares internacionales de protección de datos, garantizando así la confidencialidad de la información de los usuarios

Referencias

Abramo, L. Cecchini, S. Morales, b. (2019). Programas sociales, superación de la pobreza e inclusión laboral Aprendizajes desde América Latina y el Caribe. Publicación de las Naciones Unidas ISBN: 978-92-1-122014. https://repositorio.cepal.org/server/api/core/bitstreams/7d9fb18f-1be1-4e0e-9125-0e3de35b5bc7/content

Baena, M. (27 de Noviembre de 2019). La importancia de las TICs en la educación. https://www.flup.es/importancia-tics-educacion/

Barahona, G. León, G. Barzola, Y. (2024). La intervención social en personas con situaciones vulnerables. Revista de Ciencias Humanísticas y Sociales (ReHuSo), 9(2), 77-91. Epub 05 de diciembre de 2024.https://doi.org/10.33936/rehuso.v9i2.6269

Camacho, H. Fontaines, T. Urdaneta, G. (2005). La trama de la investigación y su epistemología. TELOS. Revista de Estudios Interdisciplinarios en Ciencias Sociales pág 9-20. https://www.redalyc.org/pdf/993/99318830001.pdf

Castro, M. Reyna, C. Méndez, J. (2017). Metodología de Intervención social. Primera edición, abril de 2017. CASA EDITORA SHAAD. https://www.acanits.org/assets/img/libros/Metodologia%20TS.pdf

Cedeño, M. (2019). Marco Histórico Del Trabajo Social en El Ecuador. Attribution Non-Commercial. https://es.scribd.com/document/85239342/MARCO-HISTORICO-DEL-TRABAJO-SOCIAL-EN-EL-ECUADOR

Condori, D. (2023). El rol del trabajo social en la implementación de los programas de la división de trabajo social de la Universidad Mayor de San Andrés. Universidad Mayor de San Andrés. file:///C:/Users/Admin/Desktop/Trabajo%20socialm%20art/TTSO1145.pdf

Garcés, Z. Toro, P. Gil, M. (2017). El rol del profesional en trabajo social frente a su proyecto ético-político en las instituciones operadoras del programa de protección para niños, niñas y adolescentes (NNA) en la ciudad de Medellín. Colombia. https://repository.uniminuto.edu/server/api/core/bitstreams/0febe5ed-ded2-489f-a0c2-d123b4e795a4/content

Giménez, V. Ferrer, J. (2021). La intervención social en territorios vulnerables, desde la perspectiva de los Servicios Sociales de Atención Primaria: Fundamentos y experiencias. Universidad de Alicante. http://hdl.handle.net/10045/120136

Guzmán, A., Mina, T. y Gil, A. (2023). Metodología de intervención en Trabajo Social: contribuciones para su análisis Revista Eleuthera, 25(1), 203-223. http://doi.org/10.17151/eleu.2023.25.1.11

Instituto Ecuatoriano de Seguridad Social. (2019). Las trabajadoras sociales son la cara humanitaria de un hospital. https://www.iess.gob.ec/noticias/-/asset_publisher/4DHq/content/las-trabajadoras-sociales-son-la-cara-humanitaria-de-un-hospital/10174?redirect=https%3A%2F%2Fwww.iess.gob.ec%2Fnoticias%3Fp_p_id%3D101_INSTANCE_4DHq%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_pos%3D1%26p_p_col_count%3D2%26_101_INSTANCE_4DHq_advancedSearch%3Dfalse%26_101_INSTANCE_4DHq_keywords%3D%26_101_INSTANCE_4DHq_delta%3D6%26_101_INSTANCE_4DHq_cur%3D669%26_101_INSTANCE_4DHq_andOperator%3Dtrue?mostrarNoticia=1

International Federation of Social Workers. (2024). Definición global del Trabajo Social. Registered charity number: CHE-109.240.290. https://www.ifsw.org/what-is-social-work/global-definition-of-social-work/definicion-global-del-trabajo-social/

Loor, A. Doumet, F. Moretta, B. (2023). Vulnerabilidad socio-ambiental y su contexto en el espacio urbano en el sector El Negrital. Revista San Gregorio, 1(59), 19-25. http://dx.doi.org/10.36097/rsan.v1i59.2633.

Ministerio de Inclusión Económica y Social. (2024). Programas y servicios. El nuevo Ecaudor. https://www.inclusion.gob.ec/programas-y-servicios/

Nieto, E. Bravo, B. (2024). Habitabilidad y relación intrafamiliar en sectores más vulnerables de la ciudad Portoviejo. 593. Digital Publisher CEIT, 9(2), 453 -465. https://doi.org/10.33386/593dp.2024.2.2320

Ocampo. C. (2024). El Trabajo Social en situaciones de Riesgo Ambiental, el caso de la inundación en la ciudad de Comodoro Rivadavia, provincia de Chubut en el año 2017. Universidad Nacional de La Plata. file:///C:/Users/Admin/Desktop/Trabajo%20socialm%20art/Documento_completo.pdf

Palacios, N. Zambrano, J. Ubillus, M. (2019). La inversión pública y la reducción de la pobreza en la ciudad de Portoviejo. Revista Dialnet, 7-16. https://dialnet.unirioja.es/descarga/articulo/6965735.pdf

Pérez, J. Lorenzo, F. García, F. (2022). Trabajo social en escenarios de vulnerabilidad: una mirada para la inclusión social. Telos Vol. 7, No. 1 (2005) 9 - 20. file:///C:/Users/Admin/Downloads/103-106.pdf

Pinargote, D. (2022). Análisis de la pobreza multidimensional en la zona urbana de la ciudad de Portoviejo. Pontifica Universidad Católica del Ecuador. https://repositorio.puce.edu.ec/server/api/core/bitstreams/dfc64dac-c234-4413-9478-3b6e97513bdc/content

Plan de Gestión de Riesgos. (2019). Servicio Nacional de gestión de riesgos y emergencias. Resolución de emergencia n° SNGRE-020-2019. https://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2019/04/Resoluci%C3%B3n-No.-SNGRE-020-2019.pdf

Rodríguez, L. Calderón, S. Bravo, J. (2019). Retos y limitaciones del trabajador social en las instituciones del distrito 13d01 del cantón Portoviejo. Revista Electrónica Cooperación Universidad-Sociedades pp. 41-48. file:///C:/Users/Admin/Downloads/Dialnet-RetosYLimitacionesDelTrabajadorSocialEnLasInstituc-7001761.pdf

Secretaría Nacional de Gestión de Riesgos (2019). Secretaría de Riesgos y Municipio de Portoviejo coordinan acciones para atender viviendas vulnerables. El nuevo Ecuador. Samborondón – Ecuador. https://www.gestionderiesgos.gob.ec/secretaria-de-riesgos-y-municipio-de-portoviejo-coordinan-acciones-para-atender-viviendas-vulnerables/