

28

Fecha de presentación: marzo, 2024

Fecha de aceptación: agosto, 2024

Fecha de publicación: octubre, 2024

PRAXIS DE LA CIBERSEGURIDAD

DE LAS PLATAFORMAS EDUCATIVAS MOODLE EN LA UNIVERSIDAD DE CIENFUEGOS

CYBERSECURITY PRAXIS OF MOODLE EDUCATIONAL PLATFORMS AT THE UNIVERSITY OF CIENFUEGOS

Maximino de Jesús Peña Matos ^{1*}

E-mail: mpena@ucf.edu.cu

ORCID: <https://orcid.org/0000-0003-0004-1788>

Vladimir Carrera Martínez ¹

E-mail: vcarrer@ucf.edu.cu

ORCID: <https://orcid.org/0000-0002-9883-7495>

¹ Universidad de Cienfuegos "Carlos Rafael Rodríguez", Cuba

Autor para correspondencia

Cita sugerida (APA, séptima edición)

Peña Matos, M. J. & Carrera Martínez, V. (2024). Praxis de la ciberseguridad de las plataformas educativas Moodle en la Universidad de Cienfuegos. *Universidad y sociedad*, 16 (S1), 230-237.

RESUMEN

La gestión de la Plataforma Educativa Moodle (PEM) aporta múltiples buenas experiencias, debido a su versatilidad, diversidad de prestaciones, recursos para la orientación y desarrollo de una Educación a Distancia personalizada, así como el elevado alcance de la misma por la facilidad de acceso a sus contenidos desde ubicaciones muy diversas. En el transcurso del manejo y explotación de las PEM en la Universidad de Cienfuegos (UCf) fueron detectados desagradables experiencias, asociadas al colapso de las mismas por insuficiente espacio de almacenamiento. En este trabajo se abordan las experiencias desde la ciberseguridad asociadas a esta problemática y se aportan recomendaciones para mitigarlas.

Palabras clave: Moodle, Gestión, Plataforma Educativa, Seguridad Informática.

ABSTRACT

The management of the Moodle Educational Platform (PEM) provides multiple good experiences, due to its versatility, diversity of features, resources for the orientation and development of a personalized Distance Education, as well as the high reach of the same due to the ease of access to its contents from very diverse locations. In the course of the management and exploitation of the PEM at the University of Cienfuegos (UCf), unpleasant experiences were detected, associated to their collapse due to insufficient storage space. This paper addresses the cybersecurity experiences associated with this problem and provides recommendations to mitigate them.

Keywords: Moodle, Management, Educational Platform, Computer Security.

INTRODUCCIÓN

La Plataforma Moodle se ha convertido en una de las herramientas educativas más difundidas entre la comunidad académica que utiliza las tecnologías de software libre para desarrollar el proceso docente a través de la internet construyendo, de esta manera, el aprendizaje de forma globalmente (Gamage et al., 2022; Espinosa et al., 2014; Fernández et al., 2022). Dentro de las características más sobresalientes de Moodle, se puede citar las siguientes (*Acerca de Moodle – MoodleDocs*, s. f.):

Mundialmente probado y de confianza: Impulsando a cientos de miles de ambientes de aprendizaje globalmente, Moodle se ha ganado la confianza de instituciones y organizaciones de diferentes tamaños. El número de usuarios de Moodle a nivel mundial, alcanzó más de 200 millones en agosto del 2020, entre usuarios académicos y empresariales, lo cual la convierten en la plataforma de aprendizaje más ampliamente utilizada del mundo.

Se puede añadir que:

- Soporta tanto la enseñanza como el aprendizaje.
- Fácil de usar.
- Gratuito, sin cargos por licenciamiento.
- Siempre actualizado.
- Amplia diversidad de idiomas.
- Plataforma de aprendizaje todo-en-uno.
- Altamente flexible y completamente personalizable.
- Escalable a cualquier tamaño.
- Accesible en cualquier momento, lugar y dispositivo.
- Extensos recursos disponibles en múltiples idiomas.
- Respaldado por una comunidad fuerte.
- Robusto y seguro.

En la UCf la plataforma Moodle se utiliza desde su versión 1.0, la cual fue liberada el 20 de agosto de 2002 (Historia de las versiones - MoodleDocs, s. f.). En sus inicios cuenta con muy pocos usuarios debido a la resistencia a la transición desde MicroCAMPUS. A partir de este momento la PEM se comienza a utilizar fundamentalmente en el pregrado, pero con el tiempo logra deslazar totalmente a la establecida por aquel entonces Plataforma MicroCAMPUS, debido a la cantidad de entusiastas que desde un inicio perciben las amplias prestaciones y posibilidades funcionales de Moodle. En la medida en que se fue ampliando la utilización de Moodle, surge la necesidad de incrementar el número de servidores con este Sistema de Gestión de Aprendizaje (LMS, Learning

Management System), orientando su uso no solamente al pregrado, sino a otros tipos de enseñanza.

Al momento de realizar el siguiente trabajo investigativo, en la UCf existen cinco servidores, donde se encontraba instalada la PEM, los cuales se citan a continuación.

- Clases Virtuales (Clases Virtuales de la Universidad de Cienfuegos)
- Cursos de Superación Postgraduada (Cursos de superación Postgraduada de la Universidad de Cienfuegos)
- Eventos (Eventos de la Universidad de Cienfuegos)
- Cursos (Cursos de la Universidad de Cienfuegos)
- Plataforma en Línea de Educación para el Desarrollo (Plataforma en Línea de Educación para el Desarrollo)

Seguidamente se describe cada uno de los servidores objeto de estudio en la UCf los cuales, en todos los casos, se encuentran virtualizados en servidores Proxmox versión 7.4-16 (Proxmox Virtual Environment 7.4 released, s, f.)

- Clases Virtuales. Es el servidor Moodle más robusto de la institución, con 3278 usuarios, está destinado a todos los estudiantes de pregrado y se encuentra integrado con el Directorio Activo de Windows. Virtualizado en un contenedor con el Sistema Operativo Ubuntu 20.04.6 LTS. Posee 16 GB de RAM, 32 GB de memoria SWAP y 8 núcleos. La versión de Moodle instalada en este servidor es la 4.1+ (Build: 20221216).
- Cursos de Superación Postgraduada. Destinado a todos los estudiantes de postgrado, cuenta con 1558 usuarios y se encuentra integrado con el Directorio Activo de Windows, aunque los usuarios externos a la universidad poseen la opción de autoregistrarse. Virtualizado en un contenedor con el Sistema Operativo Ubuntu 20.04.5 LTS. Posee 4 GB de RAM, 8 GB de memoria SWAP y 4 núcleos. La versión de Moodle instalada en este servidor es la 4.1+ (Build: 20221216).
- Eventos. Plataforma para la organización y desarrollo de eventos académicos, cuenta con 2051 usuarios y se encuentra integrada con el Directorio Activo de Windows, aunque se encuentra activa la opción de autoregistro para usuarios externos a la UCf. Virtualizada en un contenedor con el Sistema Operativo Ubuntu 20.04.5 LTS. Posee 4 GB de RAM, 8 GB de memoria SWAP y 4 núcleos. La versión de Moodle instalada en este servidor es la 4.1+ (Build: 20221216).
- Cursos. Orientado a la organización y desarrollo de cursos académicos de superación, cuenta con 705 usuarios y se encuentra integrado con el Directorio Activo de Windows, aunque con la opción de autoregistro para usuarios externos a la UCf activa. Virtualizado

en un contenedor con el Sistema Operativo Ubuntu 20.04.5 LTS. Posee 4 GB de RAM, 8 GB de memoria SWAP y 4 núcleos. La versión de Moodle instalada en este servidor es la 4.1+ (Build: 20221216).

- Plataforma en Línea de Educación para el Desarrollo. Es un servidor Moodle destinado a la organización y desarrollo de cursos académicos de superación, cuenta con 518 usuarios y se encuentra integrado con el Directorio Activo de Windows, con la opción de acceder a la plataforma como invitado, pero sin la posibilidad de que usuarios externos a la UCf puedan autogerarse. Virtualizado en un contenedor virtual con el Sistema Operativo Ubuntu 20.04.5 LTS. Posee 4 GB de RAM, 8 GB de memoria SWAP y 4 núcleos. La versión de Moodle instalada en este servidor es la 4.0.1+ (Build: 20220617).

El número total de usuarios de las plataformas educativas de la UCf es 8110, sin embargo, entre los primeros cuatro servidores se concentran 7592 usuarios, lo que representa el 94% del total de la comunidad académica que utiliza las plataformas educativas. Al margen de este análisis, estos cuatro servidores son los que poseen una mayor dinámica académica de utilización y por tanto una mayor carga académica. Por los argumentos anteriormente expuestos, el alcance del presente trabajo se limita a las cuatro siguientes plataformas educativas.

- Clases Virtuales.
- Cursos de Superación Postgraduada.
- Eventos.
- Cursos.

Seguidamente se describen los resultados de las investigaciones realizadas sobre los servidores objeto de estudio, haciendo énfasis en aspectos de seguridad que limitaban el buen desempeño de dichas Plataformas Educativas, específicamente en las causas que provocaban el colapso de las PE.

MATERIALES Y MÉTODOS

Los materiales que se utilizaron para el desarrollo de la presente investigación consistieron en el análisis del peso de las copias de seguridad de los contenedores Proxmox de los servidores Moodle en la UCf. Uno de los aspectos más preocupantes del resultado del análisis consistió en el alarmante y sistemático crecimiento del peso de las copias de seguridad, las cuales tenían un comportamiento anormal. Estos materiales utilizados para la investigación se obtuvieron de cada uno de los servidores virtuales Proxmox donde se encontraban alojados las PEM. Es necesario destacar que las PEM no permiten establecer una cuota de almacenamiento por usuario, lo cual representa

una seria deficiencia de seguridad, al existir usuarios poco éticos que utilizan estos huecos de seguridad y los explotan para emplear las PEM como hosting de almacenamiento. Este comportamiento inadecuado atenta contra el buen funcionamiento de las PEM e incluso, las pueden convertir en un hosting ilegal de almacenamiento de información repudiable desde el punto de vista académico, ético y social, lo cual hasta puede ser considerado como un delito informático en diferentes escenarios.

El método de investigación fundamental que se utilizó en el siguiente trabajo fue el hipotético-deductivo. Durante el desarrollo de la investigación se observó que los PEM que poseían auto registro de usuarios poseían más dificultades con las copias de seguridad robustas, por lo que se propuso una primera hipótesis que relacionaba el método de registro de los usuarios con el peso de las copias de seguridad de los contenedores. Por otro lado, al no existir la posibilidad de habilitar cuota de almacenamiento por usuario, se propuso la opción de encontrar un plugin que pudiera medir el tamaño de cada curso en la PEM. A partir de este punto se propuso una segunda hipótesis que relacionaba el tamaño de los cursos, con los cursos donde estaban matriculados los usuarios que poseían una elevada capacidad de almacenamiento. Como tercera hipótesis se asoció la desmedida capacidad de almacenamiento de algunos usuarios con un uso no pertinente desde el punto de vista académico e investigativo.

RESULTADOS Y DISCUSIÓN

Dentro de la administración de la PEM, ocupa un importante tiempo garantizar la seguridad y vitalidad de la misma, desde el punto de vista de velar por el uso inadecuado que le puedan dar algunos usuarios malintencionados e inescrupulosos. El método de auto registro de usuarios con ayuda de autenticación vía email, es una herramienta muy útil que posee la PEM para la creación de cuentas de forma automática, ya que esto facilita la matriculación en las diferentes variantes y hace más simple el trabajo al profesor de los cursos. El problema consiste en que, al permitir el registro de usuario nuevo, personas mal intencionadas usen la plataforma como repositorio de información como archivos, videos, música y programas. Lo anterior, combinado con la falta de control del espacio de almacenamiento que no es infinito, puede llegar a colapsar la plataforma, inhabilitando a la misma. Además, existe la posibilidad que los usuarios anteriormente descritos puedan almacenar información con contenidos no apropiados o indeseados, como pornografía en sus diferentes formas, información anti social, de carácter racial o con un enfoque de género inadecuado, entre otros. Si el problema anteriormente expuesto se combina con el hecho

de que la PEM no posee una herramienta administrativa de limpieza, o de control de los archivos subidos, se complica enormemente la administración de la PEM ya que el primer problema está en encontrar los usuarios malintencionados, el segundo es detectar donde almacenaron la información y el tercero es eliminarlos, ya que la PEM no elimina los ficheros ni el usuario definitivamente de su base de datos ni del disco. En tales condiciones, al administrador de la plataforma no posee otra opción que acudir a sus conocimientos de bases de datos, entrar modo comando para determinar cuáles son los archivos, su localización, a quien le pertenecen, así como su nombre en el disco físico, pues la PEM los graba con un nombre codificado, para posteriormente decidir como eliminarlos de la base de datos y del disco. Este proceso se complejiza, pues la base de datos de la PEM posee múltiples tablas y registros relacionados entre sí, por lo que eliminar objetos de la base de datos sin usar los mecanismos del Moodle puede provocar problemas en el funcionamiento de la plataforma. Hasta el momento se han detectado dos localizaciones donde los usuarios malintencionados colocan esos archivos; uno es el Calendario y otro es en las Evidencias de Aprendizajes Previos, ya que en estas localizaciones no hay restricción en espacio, no siendo así en los archivos privados de los usuarios. Esta falta de restricción de la capacidad de almacenamiento de los usuarios en el Calendario y en las Evidencias de Aprendizajes Previos representa un serio problema de seguridad para el funcionamiento estable de la PEM.

Para poder determinar a los usuarios que con su accionar amenazaban la vitalidad de las PEM, fue necesario instalar el único plugin que se encuentra sobre el tema en cuestión y que se denomina "Tamaño del Curso". Este plugin hace un cálculo del tamaño de los cursos y los ordena por tamaño; desde los mayores a los más pequeños, cuestión que también representa una gran ayuda, pues aparte de los usuarios malintencionados que llenan las PEM, están los inconscientes y los que no se percatan de los daños que hace su comportamiento subiendo indiscriminadamente a la PEM archivos sin tratamiento de reducción del tamaño al óptimo, en función de lo que necesitan; o no hacen limpieza de los archivos innecesarios. Contra el uso inadecuado del espacio de almacenamiento en las PEM, también conspira la falta de conocimiento de los profesores sobre el uso de los Grupos de Estudiantes, ya que organizan una asignatura para cada curso académico, o tienen la misma asignatura en diferentes currículos de carreras, duplicando la información en la plataforma. Mientras más carreras y asignaturas duplicadas tengan las PEM, más complicado es su solución respecto al uso de la capacidad de almacenamiento, ya que el uso del disco aumenta exponencialmente.

El procedimiento utilizado para solucionar el problema de eliminación de los usuarios que hacen uso inadecuado del espacio de almacenamiento, así como sus archivos, fue el siguiente:

1. A través del plugin "Tamaño del Curso" y utilizando una de sus prestaciones, se determina a los usuarios que tienen la mayor cantidad de espacio usado.
2. Se revisa que el usuario no estaba matriculado en ningún curso.
3. Se procede a entrar en la base de datos y por consulta SQL determinar el ID del usuario en la tabla de usuarios.
4. En la tabla donde se registran los ficheros, a través de consulta SQL, encontrar los ficheros asociados a este ID de usuario, así como su localización.
5. Posteriormente se procede a eliminar los ficheros en el disco.
6. Luego se eliminan las entradas en la tabla de ficheros.
7. Finalmente, de la tabla de usuarios, se elimina el usuario implicado.

Para el acceso a la Base de Datos (BD), se accede a la misma vía comandos del Shell del Sistema Operativo para encontrar en qué recurso de las PEM tienen la información chatarra. El sistema de BD utilizada es MariaDB o MySQL, por lo que el primer paso consiste en listar las tablas. En la tabla files existe un campo que es el ID de usuario, por lo que haciendo una consulta con el comando JOIN sql se unen las dos tablas en una consulta, partiendo del nombre de usuario y obteniendo los datos de los ficheros almacenados. Al hacer la consulta, se identifica que, estos usuarios usan la plataforma como medio de almacenamiento, emplean los eventos del Calendario para subir ficheros. Es decir, tienen en cuenta el tamaño máximo permitido de subida de ficheros en la plataforma y compactaban los ficheros multimedia en archivos comprimidos de ese tamaño y los subían en los diferentes eventos de cada día del calendario, teniendo días con más de 60 eventos y en cada uno de ellos, al menos un fichero. La información en la base de datos para buscar o eliminar a los usuarios se encuentra en la tabla mdl_user, donde a partir del nombre de usuario se encuentra el valor del ID del mismo para luego en la tabla mdl_files, a partir de ese ID de usuario, encontrar en los campos component, filearea y source, los datos de los ficheros asociados a ese usuario. A la hora de eliminar el usuario es necesario revisar y eliminar en las demás tablas donde esté el ID correspondiente a ese usuario y eliminar los datos asociados al mismo.

Haciendo un análisis del procedimiento utilizado para la detección de los usuarios que infringen las reglas de seguridad informática establecidas, se puede apreciar que el mismo es lo suficientemente complejo para ejecutarlo de forma sistemática. Esto conlleva a la búsqueda de métodos rápidos de detección de comportamientos anormales de los usuarios. Uno de esos métodos consiste en listar a los usuarios que no están matriculados en ningún curso, ya que carece de sentido común que usuarios se auto registren en una PEM y no estén matriculados en ningún curso. En consulta con los profesores y los gestores de la PEM se determina que la medida más razonable es eliminar a estos usuarios. Este proceso manifiesta la importancia que tiene para los administradores de una PEM el vínculo estrecho y sistemático con los profesores y gestores de cursos.

Otro comportamiento anormal en el funcionamiento de los usuarios de las PEM consiste en detectar a los que nunca han entrado a la plataforma en un tiempo razonable para iniciar algún tipo de intercambio docente. De la misma forma, previa consulta con profesores y gestores de cursos, se procede a la eliminación de estos usuarios.

Una tercera irregularidad detectada en el comportamiento de usuarios malintencionados consiste en la utilización de cuentas de correos en servidores que ofrecen este servicio de forma temporal, fundamentalmente para efectuar el registro en diferentes plataformas. En este sentido, se realiza una búsqueda de los principales servidores en la internet que brindan el servicio de cuentas de correos temporales (Mittal, 2022; Kurczyńska, 2023) y conociendo el dominio de los mismos, se procede a eliminar a todos los usuarios que se auto registran con cuentas de correo en esos dominios temporales.

Los recursos de almacenamiento de los servidores destinados a conservar y proteger la información de los usuarios en las Plataformas Educativas son limitados, por lo que su uso racional es de suma importancia. En tal sentido es necesario esclarecer que cada usuario posee un límite de almacenamiento para evitar la inoperatividad de las Plataformas Educativas, sin embargo, en varias oportunidades los servidores colapsaban por insuficiente espacio de almacenamiento, necesario para su correcto funcionamiento. Ante tal situación se desarrolla una investigación del comportamiento de la capacidad de almacenamiento de cada uno de los servidores, la cual demuestra que las causas de tal comportamiento se encuentran en las siguientes causas.

1. Uso de los servidores con auto registro para que diferentes personas sin ningún vínculo académico

con la UCf se conviertan en usuarios de las PEM institucionales.

2. Un elevado número de usuarios inactivos durante mucho tiempo en las PEM, que ocupan recursos de almacenamiento.
3. Uso inadecuado de la capacidad de almacenamiento por parte de algunos usuarios inescrupulosos, utilizando brechas de seguridad de las PEM.

Con relación al primer aspecto, vinculado con el control de los usuarios con posibilidades de auto registro en los servidores se toman dos medidas fundamentales.

- Primera: Donde sea posible, los administradores de las PEM comienzan el registro de usuarios de forma manual y el usuario recibe vía correo electrónico las instrucciones para concluir su registro exitoso en las PEM.
- Segunda: Donde sea pertinente, se habilita de forma temporal la opción de auto registro, en coordinación de las autoridades académicas que organizan las diferentes actividades.

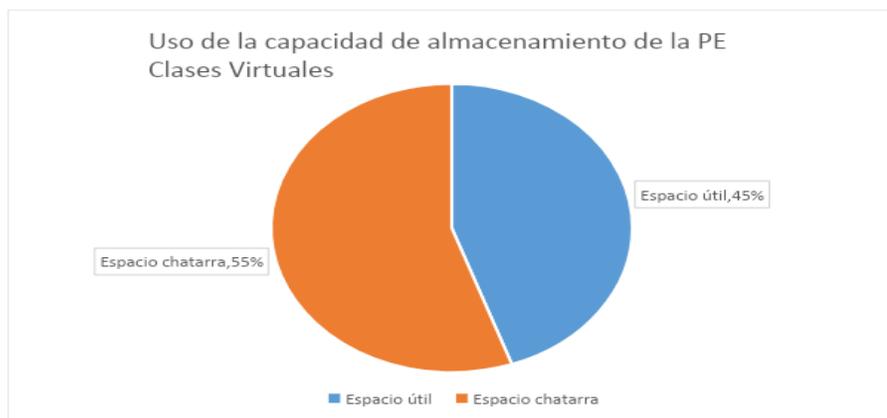
Respecto al segundo aspecto, asociado a la inactividad prolongada de los usuarios, se determina, donde fuera pertinente, eliminar a todos los usuarios con un período de inactividad mayor a 365 días.

Con relación al tercer tema, asociado al uso inadecuado de la capacidad de almacenamiento por parte de algunos usuarios, el tratamiento dado es muy diferente en cada caso, ya que el mismo exige un estudio más profundo, asociado a la seguridad informática y el análisis del comportamiento de las bases de datos de las PEM.

Como resultado de este análisis se determina que la brecha de seguridad que utilizaban los usuarios inescrupulosos consistía en almacenar información a través de sus calendarios en la PEM. Al realizar una búsqueda bibliográfica sobre el tema se encuentra que un problema similar fue descrito en Moodle in English (2019), donde el autor del trabajo buscaba solución para eliminar del Calendario los íconos en pantalla que ocupaban demasiado espacio. Sin embargo, la evolución del problema de almacenar información no pertinente a las prestaciones del Calendario aprovechándose de esta brecha de seguridad, se ha convertido en un grave problema de seguridad para las PEM, no descrito en las fuentes de información consultadas (Anuncios de seguridad, 2023).

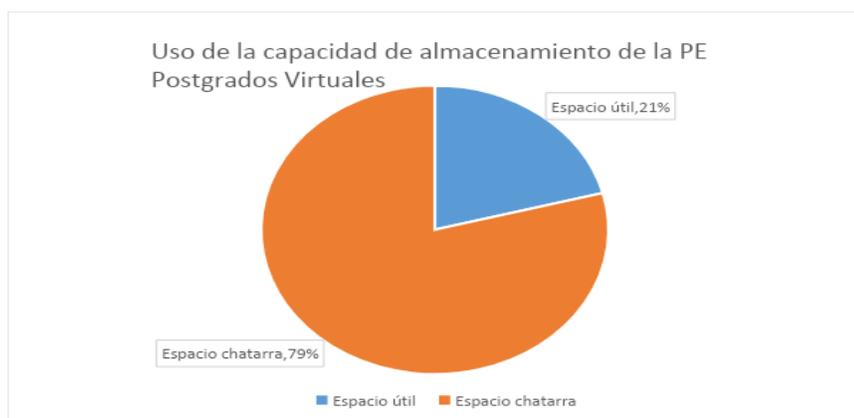
Como resultado de las medidas adoptadas vinculadas a la investigación realizada, se puede reducir considerablemente el uso del espacio de almacenamiento chatarra en cada uno de los servidores, lo cual se muestra en las figuras 1, 2, 3 y 4 a continuación.

Fig. 1. Utilización de la capacidad de almacenamiento de la PE Clases Virtuales.



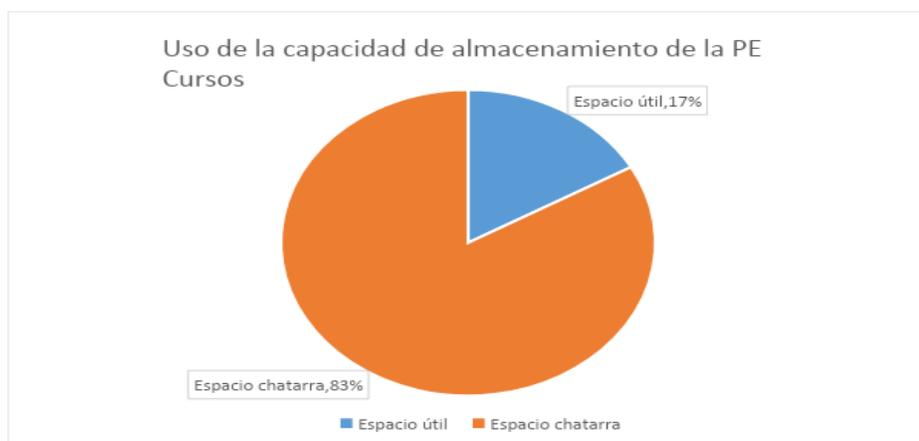
Fuente: Elaboración propia.

Fig. 2. Utilización de la capacidad de almacenamiento de la PE Postgrados Virtuales.



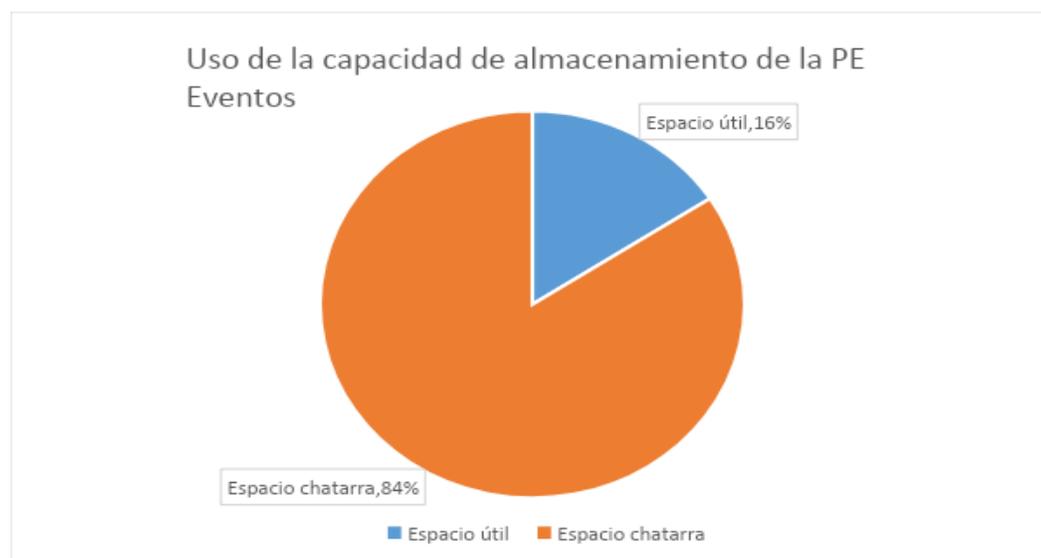
Fuente: Elaboración propia.

Fig 3. Utilización de la capacidad de almacenamiento de la PE Cursos.



Fuente: Elaboración propia.

Fig 4. Utilización de la capacidad de almacenamiento de la PE Eventos.



Fuente: Elaboración propia.

Como se puede apreciar de las figuras, el espacio chatarra de almacenamiento en los servidores con PEM ocupa, en el mejor de los casos el 55% y en el caso más crítico, esa cifra asciende a un 84%, lo cual representa un serio problema de seguridad para la estabilidad de los servidores ya que, esa tendencia desatendida puede provocar el colapso del servicio de las PE por insuficiente espacio de almacenamiento. Una vez determinado y localizado al detalle el problema anterior, se procede a la eliminación del espacio chatarra de almacenamiento.

En la tabla 1 se presenta una comparativa asociada al tamaño de las salvas de los contenedores virtuales de las PEM de la UCf que se muestra seguidamente, se puede apreciar el comportamiento del tamaño de las salvas de seguridad de los contenedores Proxmox donde se encuentran las PEM antes y después de la eliminación del espacio chatarra de almacenamiento en los mismos.

Tabla 1. Comparativa sobre el comportamiento del tamaño de las salvas de seguridad de los contenedores virtuales de las PEM de la UCf.

PEM	Tamaño original de la salva (GB)	Tamaño final de la salva (GB)	Reducción (%)	Método de acceso
Clases Virtuales	342,87	152,93	55,4	Integrado con AD
Postgrados Virtuales	58,72	12,27	79,1	Integrado con AD, Auto registro
Cursos	73,4	12,32	83,22	Integrado con AD, Auto registro
Eventos	36,57	5,78	84,19	Integrado con AD, Auto registro

Fuente: Elaboración propia.

Sobre el análisis de los datos de la tabla anterior se puede apreciar, que el comportamiento de la reducción de las salvas de seguridad se corresponde con la magnitud del espacio chatarra de almacenamiento. Sin embargo, es evidente, que los mayores espacios chatarra de almacenamiento se encuentran en los servidores, donde los usuarios poseen la posibilidad de auto registrarse, por lo que se recomienda tomar medidas para limitar esta opción, en la medida de las posibilidades.

CONCLUSIONES

Como resultado de la investigación realizada sobre la el funcionamiento de las PEM en la UCf asociado a utilización de espacio de almacenamiento indebido por parte de usuarios inescrupulosos, se determinan las causas que conllevan al colapso de las PEM, las cuales están vinculadas a tres razones fundamentales. En primer lugar, se detecta una brecha de seguridad en las PEM, que le permite a los usuarios almacenar información de forma ilimitada en sus Calendarios y Evidencias de Aprendizajes Previos. En segundo lugar, el uso indebido de la posibilidad que ofrecen las PEM de auto registro a sus usuarios. Y, por último, el uso inadecuado de correos electrónicos temporales en el proceso de auto registro de los usuarios. En todos los casos se confirmaron las hipótesis valoradas para el presente trabajo investigativo.

La investigación realizada además, demuestra claramente que la PEM posee, entre otras, tres vulnerabilidades que afectan su desempeño; la primera consiste en no poder restringir el tamaño de uso del disco duro en el servidor por usuarios; la segunda es permitir el registro de usuarios sin restricción de aprobación, otorgándole derechos indebidos, permitiéndoles estar en ese status indefinidamente sin que esté matriculado en ningún curso; y la tercera vulnerabilidad radica en no verificar el espacio de almacenamiento antes de que los usuarios realicen alguna acción de escritura en el disco ni emitir notificaciones al respecto, por lo que si el disco duro se satura, la PEM deja de funcionar con un error que no tiene aparentemente nada que ver con lo que está sucediendo.

Todas estas vulnerabilidades, cuyo objetivo es violentar las reglas de seguridad informática establecidas en la UCf respecto a las PEM fueron mitigadas adecuadamente en cada uno de los casos con los recursos disponibles por las PEM.

REFERENCIAS BIBLIOGRÁFICAS

- Acerca de Moodle—MoodleDocs. (s. f.). https://docs.moodle.org/all/es/Acerca_de_Moodle
- Anuncios de seguridad. (2023). <https://moodle.org/security/index.php>
- Historia de las versiones—MoodleDocs. (s. f.). https://docs.moodle.org/all/es/dev/Historia_de_las_versiones
- Espinosa, H. R., Betancur, L. F. R., & Aranzazu, D. (2014). Alfabetización informática y uso de sistemas de gestión del aprendizaje (LMS) en la docencia universitaria. *Revista de la Educación Superior*, 43(171), 139-159. <https://doi.org/10.1016/j.resu.2015.03.004>

- Fernández, A. M., Reyes, M. J., & López, M. I. V. (2022). Tecnologías de la información y comunicación (TIC) en formación y docencia. *FMC - Formación Médica Continuada en Atención Primaria*, 29(3, Supplement 1), 28-38. <https://doi.org/10.1016/j.fmc.2022.03.004>
- Gamage, S. H. P. W., Ayres, J. R., & Behrend, M. B. (2022). A systematic review on trends in using Moodle for teaching and learning. *International Journal of STEM Education*, 9(1), 9. <https://doi.org/10.1186/s40594-021-00323-x>
- Kurczyńska, S. (2023). Protect your privacy and avoid spam with these top-rated disposable email providers! Selzy Blog. <https://selzy.com/en/blog/best-temporary-email/>
- Mittal, N. (2022). Nine Best Disposable Email Services for Temporary Email in 2023. Mailmodo. <https://www.mailmodo.com/guides/temporary-email-address/>
- Moodle in English: Calendar - Get rid of icons in display, taking too much space. (2019). <https://moodle.org/mod/forum/discuss.php?d=386928>
- Proxmox Virtual Environment 7.4 released. (s. f.). <https://www.proxmox.com/en/about/press-releases/proxmox-virtual-environment-7-4>