Buen Data

buendata.com

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 242 68 92
ramiro@buendata.com
soluciones@buendata.com

Primer Diagnóstico de Plataformas LMS

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Primer Diagnóstico plataformas LMS ESAP Contrato No BOG-1464-2024

Fecha informe:

Concepto: Informe

Cliente: Escuela Superior de Administración Pública

Escuela Superior de Administración Pública

Fecha de entrega: 17 de diciembre 2024

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

TABLA DE CONTENIDO

TABLA DE CONTENIDO 3

Índice de Imágenes 4

PRIMER DIAGNÓSTICO ESAP 5

1. Diagnósticos de las plataformas LMS de la ESAP 5

1.1 Metodología Empleada 5

2. Recomendaciones primer Diagnóstico Realizado 5

3. Actividades realizadas Verificación de las Instancias ESAP LMS 12

3.1 Versión actual de las tres instancias 12

3.2 Revisión de seguridad por plataforma 14

3.2.1 Extensión 14

3.2.2. Posgrado 21

3.2.3 Posgrado 30

3.3. Revisión de Entorno de las tres instancias 38

4. Infraestructura y esquema topológico 41

5. Actualización de componentes generales para el funcionamiento de Moodle 43

6. Mantener suficiente espacio monitoreado para los esquemas de backup de la entidad 43

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Índice de Imágenes

Imagen 1. Actualización versión Extensión....13
Imagen 2. Actualización versión Posgrado....13
Imagen 3. Actualización versión Pregrado....14
Imagen 4. Seguridad Extensión 1....14
Imagen 5. Seguridad Extensión 2....15
Imagen 6. Análisis de Seguridad Extensión....16
Imagen 7. Análisis de Seguridad Extensión 2....20
Imagen 8. Seguridad Posgrado 1....21
Imagen 9. Seguridad Posgrado 2....22
Imagen 10. Análisis Seguridad Posgrado....24
Imagen 11. Análisis Seguridad Posgrado....29
Imagen 12. Seguridad Pregrado 1....30
Imagen 13. Seguridad Pregrado 2....30
Imagen 14. Seguridad Posgrado 2....33
Imagen 15. Seguridad Posgrado 2....37
Imagen 16. Entorno Extensión 1....38
Imagen 17. Entorno Extensión 2....39
Imagen 18. Entorno Posgrado 1....39
Imagen 19. Entorno Posgrado 2....40
Imagen 20. Entorno Pregrado 1....40
Imagen 21. Entorno Pregrado 2....41
Imagen 22. Esquema Topológico....42
Imagen 23. Versión del nodo....43
Imagen 24. Moodle logs Extensión....44
Imagen 25. Moodle logs Extensión....45
Imagen 26. Moodle logs Extensión....46

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

PRIMER DIAGNÓSTICO ESAP

Teniendo en cuenta el Plan de trabajo del Proyecto presentado por parte de Buen Data SAS, y según los ítems y actividades estipuladas bajo el marco del contrato No BOG-1464-2024. Se Presenta a continuación, el resultado del diagnóstico frente a la estructura de la Esap y especialmente orientadas a Moodle.

1. Diagnósticos de las plataformas LMS de la ESAP

Servicio de diagnóstico de las plataformas actuales de LMS de la ESAP, las cuales se encuentran actualmente migradas a la nube dispuesto por la Universidad, para identificar que cumplen con los requisitos y estándares mínimos que permitan garantizar el correcto funcionamiento para los usuarios proyectados en cada una de ellas, de acuerdo a la planeación de las ofertas académicas de la ESAP.

Buen Data realizó a inicios del proyecto en diciembre de 2024, el diagnóstico de las plataformas de la ESAP.

1.1 Metodología Empleada

Buen Data SAS realiza la revisión de las plataformas actualizadas, migradas a la nube de la entidad.

2. Recomendaciones primer Diagnóstico Realizado

El equipo de Buen Data ha encontrado las siguientes recomendaciones a nivel general de las instancias de Moodle:

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- **Actualizar Moodle de la versión 4.2 a la 4.4** es fundamental debido a que la versión 4.2 dejó de tener soporte de seguridad el 7 de octubre de 2024, lo que deja a la plataforma expuesta a vulnerabilidades y fallos que no serán corregidos. La versión 4.4, en cambio, cuenta con soporte activo que incluye tanto actualizaciones de seguridad como mejoras funcionales.

Entre los cambios más relevantes que justifican esta actualización se encuentran:

Correcciones de seguridad:

- Parcheo de vulnerabilidades críticas relacionadas con la protección de datos y autenticación.
- Mejoras en los mecanismos de control de acceso y cifrado.

Optimización del rendimiento:

- Reducción del tiempo de carga en áreas clave de la plataforma.
- Mejoras en la gestión de consultas a la base de datos y manejo de grandes volúmenes de usuarios.

Interfaz de usuario y accesibilidad:

- Cambios en la experiencia de usuario para facilitar la navegación.
- Ajustes en accesibilidad para cumplir con estándares más recientes.

Compatibilidad tecnológica:

- Integración más robusta con herramientas modernas.
- Mejor soporte para PHP 8.2 y 8.3, además de actualizaciones en bibliotecas internas.

Corrección de errores funcionales:

- Solución a problemas de rendimiento en actividades y cuestionarios.
- Ajustes en la configuración de roles y permisos para evitar comportamientos inesperados.
- Actualizar garantiza no solo la seguridad de la plataforma, sino también su estabilidad operativa y compatibilidad con tecnologías actuales, lo que permite una mejor experiencia para administradores y usuarios.

Buen Data
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

➢ Se Recomienda Actualización de Infraestructura Cloud

La infraestructura actual opera en un entorno de nube. Es fundamental realizar actualizaciones periódicas para garantizar la estabilidad, seguridad y compatibilidad del sistema con las últimas tecnologías.

Seguridad:
Las actualizaciones incluyen parches críticos que protegen contra vulnerabilidades conocidas. Mantener el sistema actualizado reduce los riesgos de ciberataques y accesos no autorizados.

Estabilidad:
Las versiones más recientes de los componentes de infraestructura mejoran la estabilidad general, minimizando interrupciones y fallos inesperados.

Compatibilidad:
La infraestructura actualizada es compatible con nuevas herramientas, servicios y frameworks, lo que facilita integraciones futuras y garantiza un funcionamiento óptimo de las aplicaciones.
Rendimiento:

Las mejoras en el rendimiento son comunes en las actualizaciones de sistemas y componentes, optimizando el uso de recursos y mejorando la experiencia de los usuarios finales.

Soporte:
Los proveedores de nube solo ofrecen soporte activo para versiones recientes, lo que asegura ayuda técnica en caso de problemas. Mantener componentes obsoletos puede limitar la capacidad de respuesta ante incidentes.

Recomendaciones:
Auditoría de Componentes:

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Identificar versiones actuales de sistemas operativos, plataformas y servicios en uso para planificar las actualizaciones necesarias.

Pruebas Previas:
Validar en un entorno de pruebas que las actualizaciones no afecten la operatividad del sistema.

Ejecución Escalonada:
Realizar las actualizaciones por etapas para minimizar riesgos y garantizar un proceso controlado.

Monitoreo Activo:
Implementar herramientas de monitoreo para identificar y resolver rápidamente cualquier problema tras las actualizaciones.

Beneficios esperados:

- Incremento en la seguridad y resiliencia del sistema.
- Reducción de fallos operativos.
- Compatibilidad con tecnologías actuales y futuras.
- Mejora en el rendimiento general y en la experiencia de usuario.

➢ Recomendación Actualización a Apache 2.4.62

Actualmente se está utilizando Apache con la versión de API 20120211, correspondiente a la serie 2.4 del servidor HTTP. Aunque esta serie sigue siendo soportada, es crucial mantener actualizado el software a la última versión estable para garantizar la seguridad y el óptimo funcionamiento de la infraestructura.

Seguridad:
La versión 2.4.62, lanzada en julio de 2024, incluye correcciones de vulnerabilidades críticas identificadas en versiones anteriores, reduciendo significativamente los riesgos de ataques.

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Estabilidad y Rendimiento:
Incorporación de mejoras en el rendimiento y optimización de procesos, garantizando una experiencia más fluida tanto para los usuarios como para los administradores del sistema.

Compatibilidad:
La actualización asegura el soporte para tecnologías más recientes y una mejor integración con módulos y servicios actuales.

Cumplimiento:
Mantener el software actualizado asegura el cumplimiento de buenas prácticas y normativas que demandan entornos seguros y protegidos.

Beneficios esperados:

- Mayor seguridad ante vulnerabilidades críticas.
- Estabilidad y rendimiento mejorados.
- Preparación para futuras actualizaciones y compatibilidad con servicios modernos.

➢ Recomendación de Evaluación de Actualización de PostgreSQL a la versión 15.10

Actualmente, se está utilizando PostgreSQL 15.8. La última versión menor disponible en la serie 15 es la 15.10, lanzada recientemente, y es altamente recomendable actualizar a esta versión para asegurar el correcto funcionamiento y la seguridad del sistema.

Seguridad y corrección de errores:
La versión 15.10 incluye parches críticos de seguridad y correcciones de errores importantes, lo cual es fundamental para proteger la base de datos contra vulnerabilidades conocidas y mejorar la estabilidad del sistema.

Compatibilidad y rendimiento:

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

La actualización a la versión 15.10 asegurará que se sigan las mejores prácticas y se mantenga la compatibilidad con las últimas mejoras en PostgreSQL, lo cual también podría mejorar el rendimiento general del sistema.

Moodle y PostgreSQL 17:
Moodle es compatible con PostgreSQL 17, la versión más reciente de PostgreSQL. Sin embargo, desde un enfoque conservador, la actualización a la versión 15.10 es una opción más segura en el corto plazo. Esto se debe a que la serie 15 aún recibe soporte activo y su actualización garantiza la estabilidad sin los riesgos asociados con la adopción inmediata de una versión mayor, como la 17, que podría implicar algunos ajustes adicionales en la infraestructura o en la aplicación.

Recomendación:
Evaluar la actualización a PostgreSQL 15.10:
Se recomienda realizar una actualización a la versión 15.10, ya que esta versión es la última de la serie 15 y ofrece un equilibrio entre seguridad, estabilidad y compatibilidad. La actualización a esta versión es especialmente adecuada para entornos que prefieren mantener una base estable antes de considerar una actualización a una nueva versión mayor.

- **Considerar PostgreSQL 17 a largo plazo:**

  Aunque Moodle soporta PostgreSQL 17, se sugiere evaluar la migración a esta versión en un futuro próximo una vez que se haya probado adecuadamente en un entorno de desarrollo. Esta versión introduce nuevas características y mejoras significativas, pero puede requerir ajustes adicionales.

  Beneficios esperados:
  - Mayor seguridad y estabilidad en la base de datos.
  - Menor riesgo de incompatibilidades y problemas operativos.
  - Preparación para futuras actualizaciones con una base sólida.

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- **Recomendación de Seguridad**

Es esencial abordar las vulnerabilidades de seguridad detectadas en la infraestructura y servicios, con el fin de reducir la superficie de ataque y mejorar la protección general del sistema. A continuación, se destacan algunas de las acciones clave que se deben implementar:

Revisión y Cierre de Puertos Innecesarios:
Es fundamental evaluar y gestionar adecuadamente los puertos abiertos en el servidor. Los puertos que no sean esenciales para el funcionamiento de los servicios deben ser cerrados o restringidos a direcciones IP específicas.

- **Implementación de Políticas de Seguridad (CORS y CST):**

Es necesario implementar las políticas adecuadas de CORS (Cross-Origin Resource Sharing) y CST (Content Security Policy) para evitar riesgos relacionados con la exposición de datos y garantizar la seguridad de las aplicaciones web.

Monitoreo Continuo:
Se recomienda implementar un sistema de monitoreo continuo para detectar cualquier cambio no autorizado en la configuración de seguridad, asegurando una respuesta rápida ante accesos no deseados o modificaciones en la infraestructura.

Revisión Periódica de Configuraciones de Seguridad:
Es importante realizar auditorías de seguridad periódicas para verificar la configuración de los servicios, puertos abiertos y políticas de acceso, adaptándolas según las mejores prácticas de seguridad y las necesidades del entorno.

Actualización de Servicios y Componentes:
Asegurarse de que todos los servicios y componentes estén actualizados con las últimas versiones estables, que incluyen correcciones de seguridad importantes.

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Capacitación Continua:
Fomentar la capacitación del equipo técnico en buenas prácticas de seguridad, gestión de puertos y políticas de seguridad, con el objetivo de prevenir posibles vulnerabilidades.

Esta recomendación abarca de forma general las acciones necesarias para subsanar las vulnerabilidades encontradas, sin entrar en detalles específicos de cada caso.

3. Actividades realizadas Verificación de las Instancias ESAP LMS

A continuación, se presenta la relación de la verificación por cada instancia de la Esap. Con los permisos y accesos concedidos por parte de la Escuela Superior de Administración Pública se presenta a continuación la validación del sitio, en cuanto a versión, seguridad y entorno:

- https://pregradoesap.esap.edu.co/my/
- https://posgradoesap.esap.edu.co/
- https://extensionesap.esap.edu.co/my/

3.1 Versión actual de las tres instancias

Seguidamente se evidencia la actual versión de las instancias de la ESAP 4.2.5 y 4.2.9

BuenData
DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Extensión

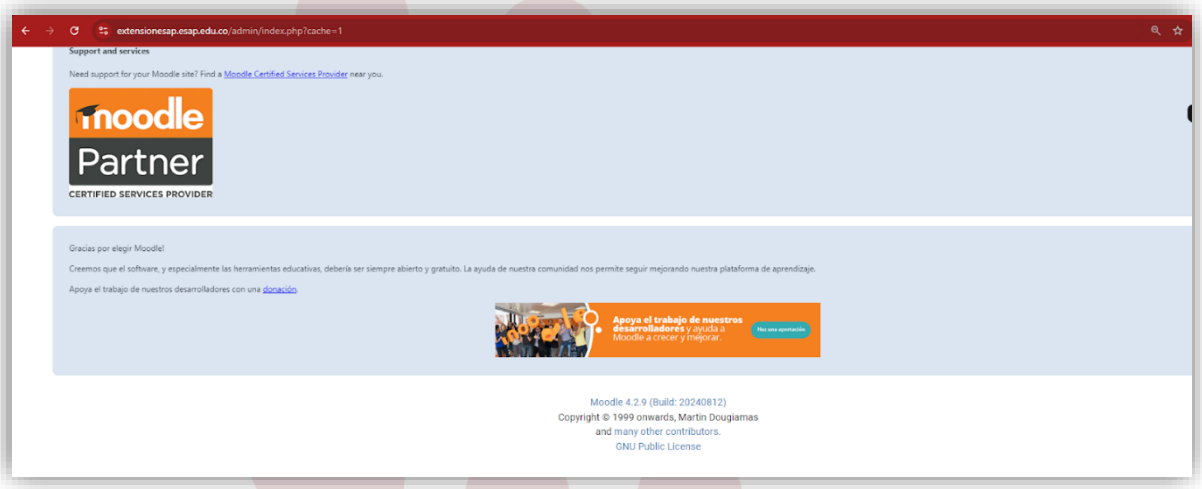


Imagen 1. Actualización versión Extensión

- Posgrado

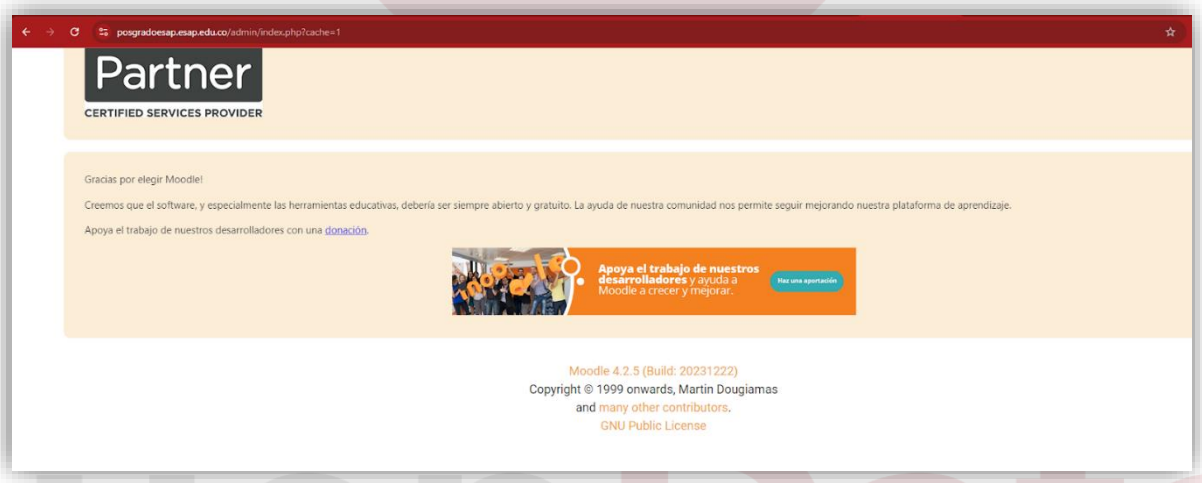


Imagen 2. Actualización versión Posgrado

DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Pregrado

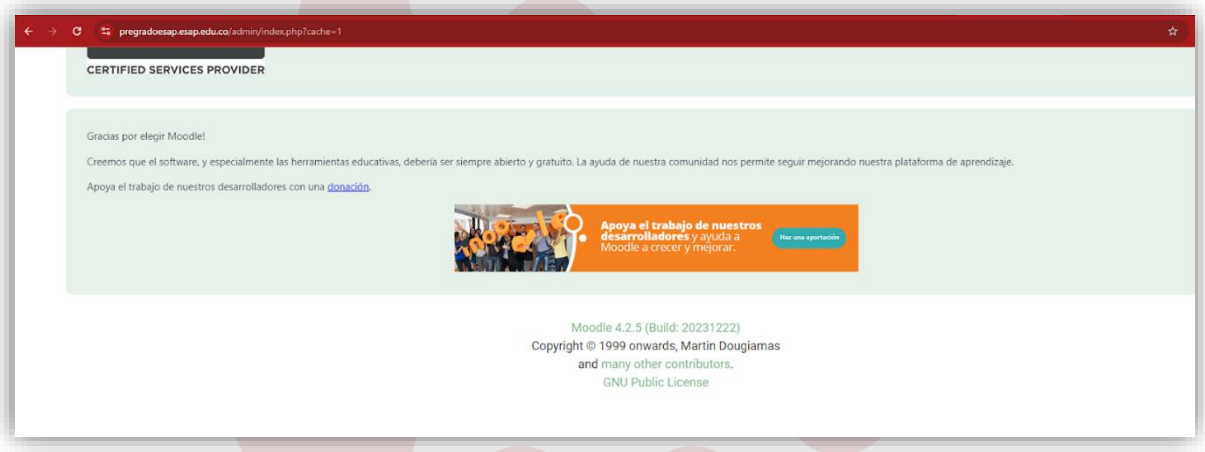


Imagen 3. Actualización versión Pregrado

3.2 Revisión de seguridad por plataforma

A continuación, se detalla la revisión de seguridad por cada instancia.

3.2.1 Extensión

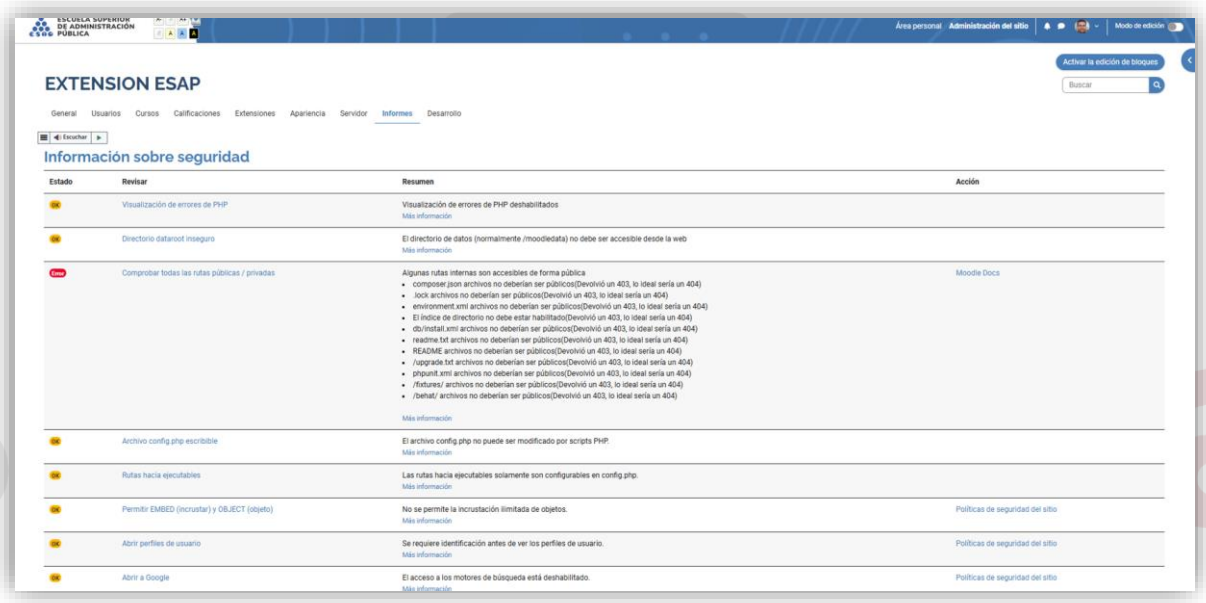


Imagen 4. Seguridad Extensión 1

DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

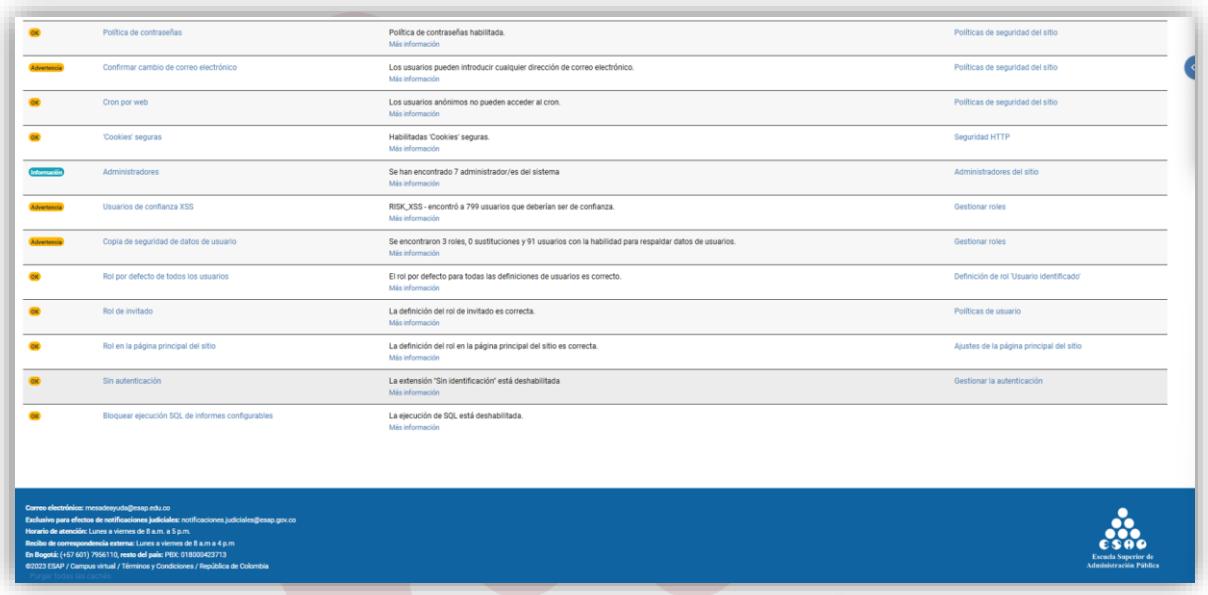


Imagen 5. Seguridad Extensión 2

Revisión de Plugins Extensión

Plugin	Versión Actual	Versión Moodle 4.4
Accesibilidad block_accessibility	1.39.03 (Build - 2021092201) 2021092202	No soportado oficialmente, sin reportes de mal funcionamiento.
Informes configurables block_configurable_reports	3.9.0 2020110300	4.5.0 (2024051300)
ReadSpeaker webReader block_readspeaker_embhl	2023121201	December release (Minor update) (2024121601)
Fusión de cuentas de usuario tool_mergeusers	2023061900	2024060300
Temas en pestañas format_onetopic	4.1.05(PiedrasTeherán) 2022081609	4.4.02(LasAcacias) (2024050902)
Moodle Benchmark report_benchmark	v1.5.1 2023012800	No soportado oficialmente, utilizar misma versión.
Páginas estáticas	v4.2-r1	v4.4-r1 (2024060100)

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

local_staticpage	2023090100	

Los plugins de la Suite LXP no serán actualizados. Además, el plugin del WS SINU tampoco recibirá actualización, pero se sugiere validar su compatibilidad antes de la actualización, ya que en la versión 4.4 de Moodle se han introducido cambios en los servicios web (WS)

Análisis de seguridad Extensión

		Confianza				
		Confirmado por usuario	Alta	Medios de comunicación	Baja	Total
Riesgo	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	1 (6,2 %)	1 (6,2 %)	1 (6,2 %)	3 (18,8 %)
	Bajo	0 (0,0 %)	1 (6,2 %)	4 (25,0 %)	1 (6,2 %)	6 (37,5 %)
	Informativo	0 (0,0 %)	1 (6,2 %)	3 (18,8 %)	3 (18,8 %)	7 (43,8 %)
	Total	0 (0,0 %)	3 (18,8 %)	8 (50,0 %)	5 (31,2 %)	16 (100%)

Imagen 6. Análisis de Seguridad Extensión

Cabecera Política de seguridad de contenidos (CSP) no configurada

Descripción de alerta:

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

Etiquetas de alerta:

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Falta de cabecera Anti-Clickjacking

Descripción de alerta:

La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra ataques de 'ClickJacking'.

Etiquetas de alerta:

- WSTG-v42-CLNT-09
- OWASP_2021_A05
- OWASP_2017_A06
- CWE-1021

Encabezado de seguridad de transporte estricto no establecido

Descripción de alerta:

HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL).

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.

Etiquetas de alerta:

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-319

Cookie Sin Bandera de Seguridad

Descripción de alerta:

Se ha establecido una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.

Etiquetas de alerta:

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-614
- WSTG-v42-SESS-02

Cookie sin el atributo SameSite

Descripción de alerta:

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida eficaz para contrarrestar la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y los ataques de sincronización.

Etiquetas de alerta:

- OWASP_2021_A01
- OWASP_2017_A05

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- WSTG-v42-SESS-02
- CWE-1275

Falta encabezado X-Content-Type-Options

Descripción de alerta:

La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.

Etiquetas de alerta:

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Librería JS Vulnerable

Descripción de alerta:

La librería identificada jquery, versión 3.6.4 es vulnerable.

Etiquetas de alerta:

- OWASP_2017_A09
- OWASP_2021_A06
- CWE-829

BuenData
DOCUMENTO CONFIDENCIAL

Puertos Expuestos Innecesariamente

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-17 10:04 -05
Nmap scan report for extensionesap.esap.edu.co (35.239.82.41)
Host is up (0.099s latency).
rDNS record for 35.239.82.41: 41.82.239.35.bc.googleusercontent.com
Not shown: 65527 filtered ports, 1 closed port
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
541/tcp  open  uucp-rlogin
4500/tcp open  sae-urn
8080/tcp open  http-proxy
8445/tcp open  copy

Nmap done: 1 IP address (1 host up) scanned in 340.41 seconds
```

Imagen 7. Análisis de Seguridad Extensión 2

Descripción de la alerta:

Se han detectado múltiples puertos abiertos en el servidor, además de los esenciales para servicios HTTP y HTTPS (puertos 80 y 443). Los puertos adicionales abiertos son:

- 22/tcp (SSH): Protocolo para acceso remoto seguro. Debe restringirse a direcciones IP específicas.
- 541/tcp (UUCP-RLOGIN): Utilizado por protocolos de acceso remoto antiguos y potencialmente inseguros. Si no es necesario, debe cerrarse.
- 4500/tcp (sae-urn): Asociado con protocolos de seguridad de red (como IPsec). Verificar su necesidad y restringirlo si no se usa.
- 8080/tcp (http-proxy): Generalmente usado para pruebas o entornos no productivos. Puede ser innecesario en producción.
- 8445/tcp (copy): Normalmente utilizado por aplicaciones específicas. Evaluar su propósito y restringirlo si no se utiliza.

Mantener puertos abiertos innecesarios incrementa la superficie de ataque, permitiendo posibles vectores de explotación.

Etiqueta alerta:

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- OWASP: A05:2021

3.2.2. Posgrado

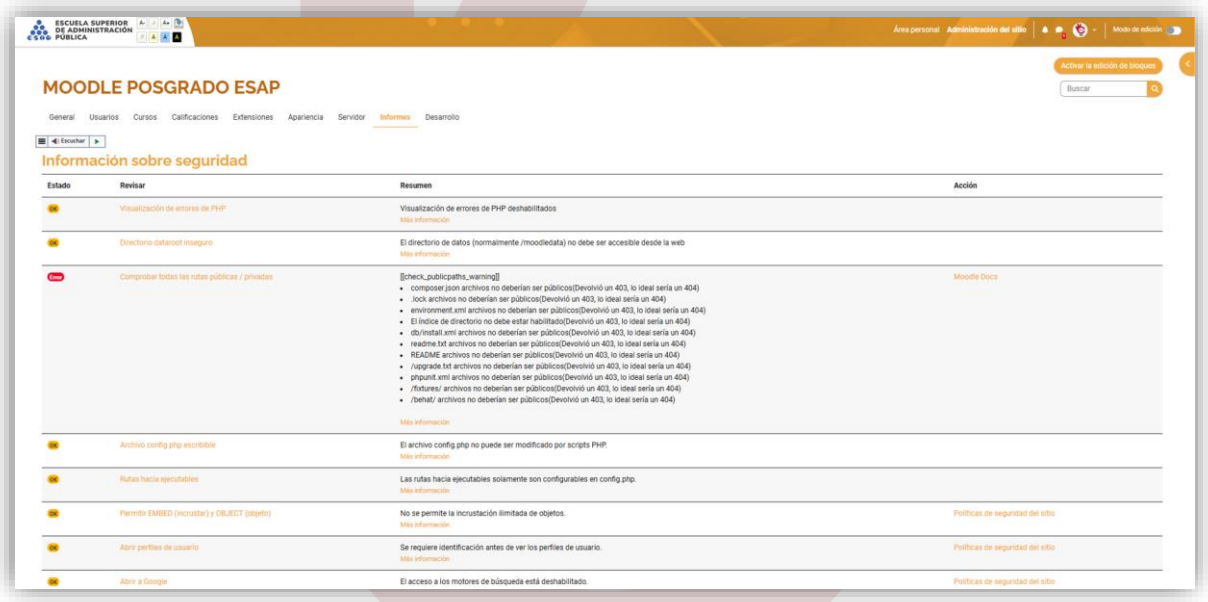


Imagen 8. Seguridad Posgrado 1

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

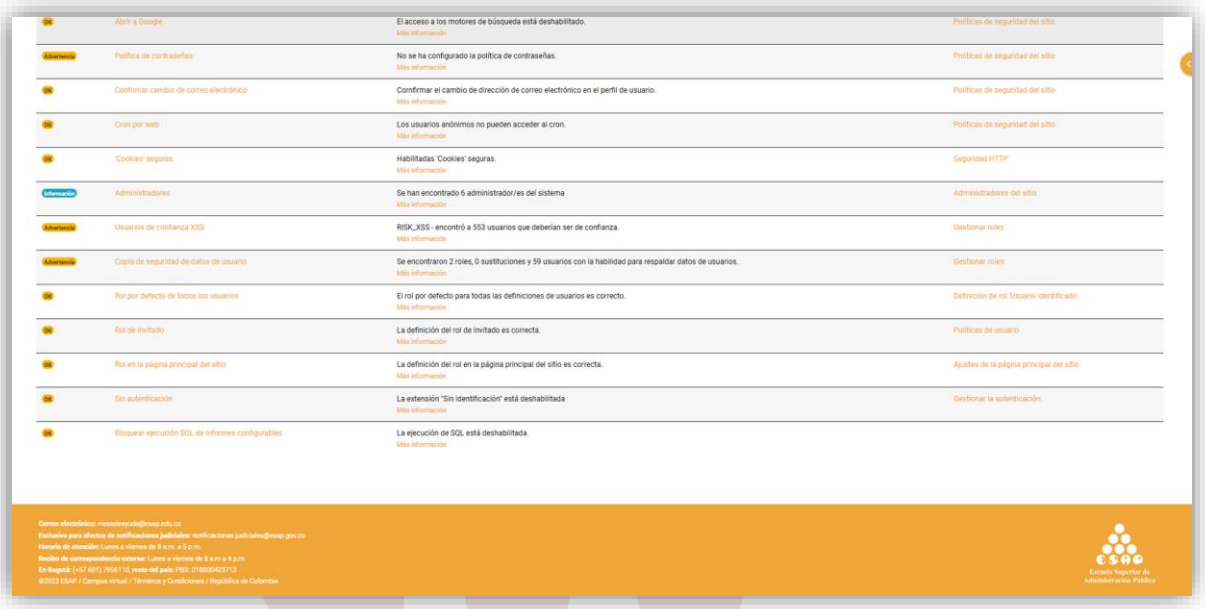


Imagen 9. Seguridad Posgrado 2

Revisión Plugins Posgrado

Plugin	Versión Actual	Versión Moodle 4.4
Asistencia mod_attendance	2023041800 2023041800	2024072400 (2024072400)
Lista de verificación mod_checklist	4.1.0.1 2024040201	4.1.0.3 (2024101900)
Programador mod_scheduler	4.0.0 2023052300	No soportado, mal funcionamientos reportados en las versiones 4.3, 4.4 y 4.5
Ejercicio 2 de Turnitin mod_turnitintooltwo	4.1+ 2024080102	4.1+ (2024091101)
Accesibilidad block_accessibility	1.39.03 (Build - 2021092201) 2021092202	No soportado oficialmente, sin reportes de mal funcionamiento.
Estado de Finalización block_completion_progress	Version for Moodle 4.1 onwards	Version for Moodle 4.4 onwards (2024042200)

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

	2023110100	
Informes configurables block_configurable_reports	4.1.0 2023121803	4.5.0 (2024051300)
Dedicación al curso block_dedication	2023112000 2023112000	2024072200 (2024072200)
ReadSpeaker webReader block_readspeaker_embhl	2024041801	December release (Minor update) (2024121601)
Reunión de Teams atto_teamsmeeting	v1.2.7 2020032707	v1.2.7 (2020032707)
Fusión de cuentas de usuario tool_mergeusers	2023061900	2024060300
Temas en pestañas format_onetopic	4.1.05(PiedrasTeherán) 2022081609	4.4.02(LasAcacias) (2024050902)
Moodle Benchmark report_benchmark	v1.5.1 2023012800	No soportado oficialmente, utilizar misma versión.
Turnitin Integrity plugin plagiarism_turnitinsim	v1.2 2023062901	v1.2 (2024112501)
Páginas estáticas local_staticpage	v4.2-r1 2023090100	v4.4-r1 (2024060100)

Los plugins de la Suite LXP no serán actualizados. Además, el plugin del WS SINU tampoco recibirá actualización, pero se sugiere validar su compatibilidad antes de la actualización, ya que en la versión 4.4 de Moodle se han introducido cambios en los servicios web (WS).

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Análisis de seguridad Posgrado

		Confianza				
		Confirmado por usuario	Alta	Medios de comunicación	Baja	Total
Riesgo	Alto	0 (0,0 %)	1 (5,6 %)	0 (0,0 %)	0 (0,0 %)	1 (5,6 %)
	Medio	0 (0,0 %)	1 (5,6 %)	1 (5,6 %)	1 (5,6 %)	3 (16,7 %)
	Bajo	0 (0,0 %)	1 (5,6 %)	5 (27,8 %)	1 (5,6 %)	7 (38,9 %)
	Informativo	0 (0,0 %)	1 (5,6 %)	3 (16,7 %)	3 (16,7 %)	7 (38,9 %)
	Total	0 (0,0 %)	4 (22,2 %)	9 (50,0 %)	5 (27,8 %)	18 (100%)

Imagen 10. Análisis Seguridad Posgrado

Revelación PII

Descripción de alerta:

La respuesta contiene Información de Identificación Personal, como el número de CC, SSN y datos sensibles similares.

Etiquetas de alerta:

- OWASP_2021_A04
- OWASP_2017_A03
- CWE-359

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Cabecera Política de seguridad de contenidos (CSP) no configurada

Descripción de alerta:

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

Etiquetas de alerta:

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Falta de cabecera Anti-Clickjacking

Descripción de alerta:

La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra ataques de 'ClickJacking'.

Etiquetas de alerta:

- WSTG-v42-CLNT-09
- OWASP_2021_A05
- OWASP_2017_A06
- CWE-1021

DOCUMENTO CONFIDENCIAL

Encabezado de seguridad de transporte estricto no establecido

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Descripción de alerta:

HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.

Etiquetas de alerta:

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-319

Bandera del pecado de las galletas HttpOnly

Descripción de alerta:

Se ha establecido una cookie sin el flag HttpOnly, lo que significa que JavaScript puede acceder a la cookie. Si un script malicioso puede ser ejecutado en esta página, entonces la cookie será accesible y puede ser transmitida a otro sitio. Si se trata de una cookie de sesión, el secuestro de sesión puede ser posible.

Etiquetas de alerta:

- CWE-1004
- OWASP_2021_A05
- OWASP_2017_A06
- WSTG-v42-SESS-02

Cookie Sin Bandera de Seguridad

Descripción de alerta:

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Se ha establecido una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.

Etiquetas de alerta:

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-614
- WSTG-v42-SESS-02

Cookie sin el atributo SameSite

Descripción de alerta:

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida eficaz para contrarrestar la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y los ataques de sincronización.

Etiquetas de alerta:

- OWASP_2021_A01
- OWASP_2017_A05
- WSTG-v42-SESS-02
- CWE-1275

Falta encabezado X-Content-Type-Options

Descripción de alerta:

La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.

Etiquetas de alerta:

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Librería JS Vulnerable

Descripción de alerta:

La librería identificada jquery, versión 3.6.4 es vulnerable.

Etiquetas de alerta:

- OWASP_2017_A09
- OWASP_2021_A06
- CWE-829

Puertos Expuestos Innecesariamente

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-17 10:04 -05
Nmap scan report for posgradoesap.esap.edu.co (35.239.82.41)
Host is up (0.100s latency).
rDNS record for 35.239.82.41: 41.82.239.35.bc.googleusercontent.com
Not shown: 65526 filtered ports, 1 closed port
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
541/tcp   open  uucp-rlogin
4500/tcp  open  sae-urn
8080/tcp  open  http-proxy
8445/tcp  open  copy
10443/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 232.75 seconds
```

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Imagen 11. Análisis Seguridad Posgrado

Descripción de la alerta: Se han detectado múltiples puertos abiertos en el servidor, además de los esenciales para servicios HTTP y HTTPS (puertos 80 y 443). Los puertos adicionales abiertos son:

- 22/tcp (SSH): Protocolo para acceso remoto seguro. Debe restringirse a direcciones IP específicas.
- 541/tcp (UUCP-RLOGIN): Utilizado por protocolos de acceso remoto antiguos y potencialmente inseguros. Si no es necesario, debe cerrarse.
- 4500/tcp (sae-urn): Asociado con protocolos de seguridad de red (como IPsec). Verificar su necesidad y restringirlo si no se usa.
- 8080/tcp (http-proxy): Generalmente usado para pruebas o entornos no productivos. Puede ser innecesario en producción.
- 8445/tcp (copy): Normalmente utilizado por aplicaciones específicas. Evaluar su propósito y restringirlo si no se utiliza.
- 10443/tcp (unknown): Puerto desconocido que puede representar un riesgo si no tiene un propósito claro.

Mantener puertos abiertos innecesarios incrementa la superficie de ataque, permitiendo posibles vectores de explotación.

Etiqueta alerta:

- OWASP: A05:2021

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

3.2.3 Posgrado

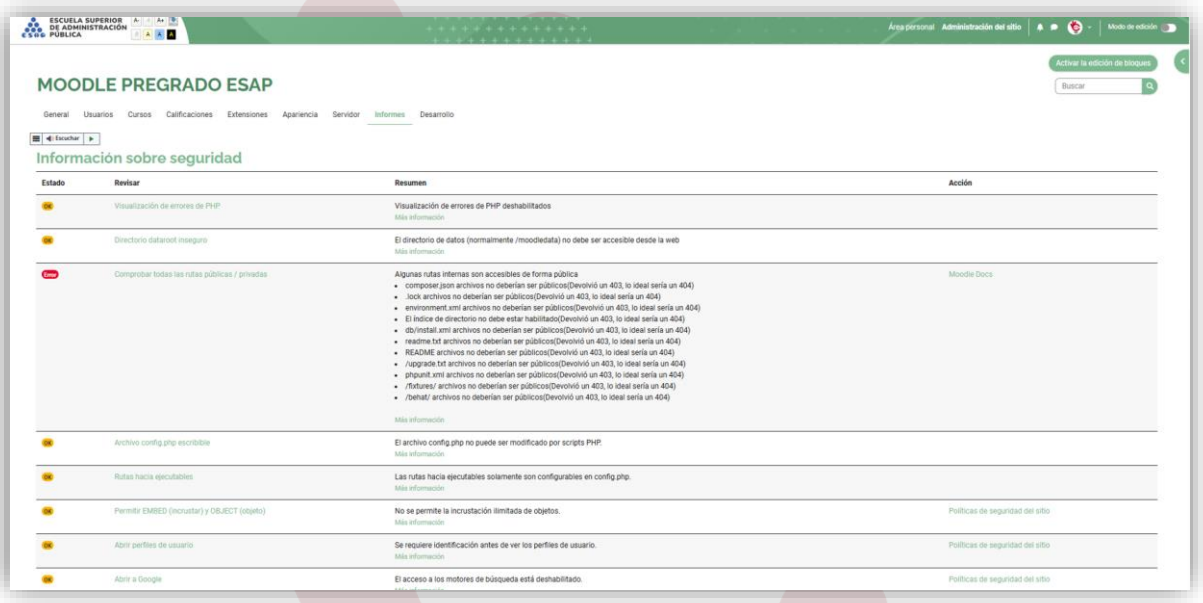


Imagen 12. Seguridad Pregrado 1

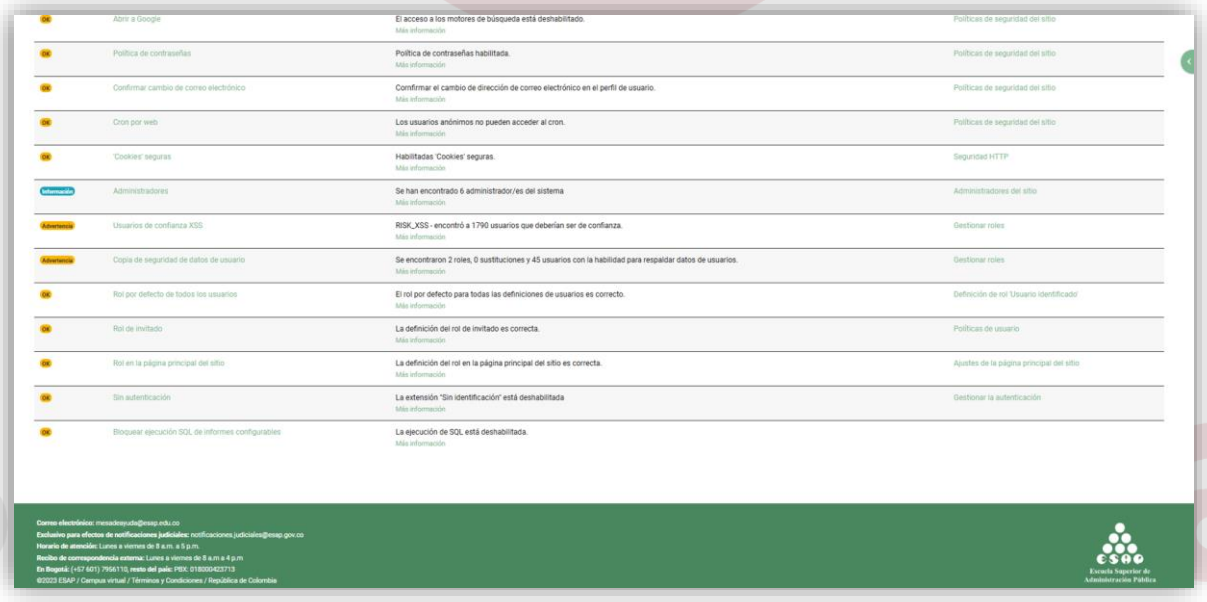


Imagen 13. Seguridad Pregrado 2

DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

moodle Partner
CERTIFIED SERVICES PROVIDER™

Revisión Plugins Posgrado

Plugin	Versión Actual	Versión Moodle 4.4
Asistencia mod_attendance	2023041801 2023041801	2024072400 (2024072400)
Lista de verificación mod_checklist	4.1.0.2 2024051800	4.1.0.3 (2024101900)
Juego mod_game	2024-07-26 2024072600	2024-12-05 (2024120500)
Programador mod_scheduler	4.0.0 2023052300	No soportado, mal funcionamientos reportados en las versiones 4.3, 4.4 y 4.5
Ejercicio 2 de Turnitin mod_turnitintooltwo	4.1+ 2024080102	4.1+ (2024091101)
Accesibilidad block_accessibility	1.39.03 (Build - 2021092201) 2021092202	No soportado oficialmente, sin reportes de mal funcionamiento.
Estado de Finalización block_completion_progress	Version for Moodle 4.1 onwards 2023110100	Version for Moodle 4.4 onwards (2024042200)
Informes configurables block_configurable_reports	4.1.0 2023121803	4.5.0 (2024051300)
Dedicación al curso block_dedication	2023112001 2023112001	2024072200 (2024072200)
ReadSpeaker webReader block_readspeaker_embhl	2024041801	December release (Minor update) (2024121601)
Examview qformat_examview	2021051700	Eliminado del core (https://tracker.moodle.org/browse/MDL-72517)
Reunión de Teams atto_teamsmeeting	v1.2.7 2020032707	v1.2.7 (2020032707)
Formato de botones format_buttons	4.x 2022020801	4.x (2024111100)

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Formato de Secciones Flexibles format_flexsections	4.1.0 2024052200	4.1.3 (2024120800)
Formato rejilla format_grid	401.2.3 2022112609	404.1.3 (2024032905)
Formato de temas de menú format_menutopic	michelle-4.0.2 2023050703	No soportado oficialmente, usar la versión michelle-4.2.1 (2024052001)
Temas en pestañas format_onetopic	4.1.12(PiedrasTeherán) 2022081612	4.4.02(LasAcacias) (2024050902)
Formato de cursos Edwiser format_remuiformat	4.1.7 2024042500	4.1.10 (2024102300)
Formato Ruta format_trail	4.2.0.0 2023060501	4.4.0.0 (2024091721)
Moodle Benchmark report_benchmark	v1.5.1 2023012800	No soportado oficialmente, utilizar misma versión.
Plugin de control antiplagio Turnitin plagiarism_turnitin	3.5+ 2024072401	4.1+ (2024120501)
Páginas estáticas local_staticpage	v4.1-r2 2023010501	v4.4-r1 (2024060100)

Los plugins de la Suite LXP no serán actualizados. Además, el plugin del WS SINU tampoco recibirá actualización, pero se sugiere validar su compatibilidad antes de la actualización, ya que en la versión 4.4 de Moodle se han introducido cambios en los servicios web (WS).

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Análisis de seguridad.

		Confianza				
		Confirmado por usuario	Alta	Medios de comunicación	Baja	Total
Riesgo	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	1 (6,2 %)	1 (6,2 %)	1 (6,2 %)	3 (18,8 %)
	Bajo	0 (0,0 %)	1 (6,2 %)	4 (25,0 %)	1 (6,2 %)	6 (37,5 %)
	Informativo	0 (0,0 %)	1 (6,2 %)	3 (18,8 %)	3 (18,8 %)	7 (43,8 %)
	Total	0 (0,0 %)	3 (18,8 %)	8 (50,0 %)	5 (31,2 %)	16 (100%)

Imagen 14. Seguridad Posgrado 2

Cabecera Política de seguridad de contenidos (CSP) no configurada

Descripción de alerta:

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Etiquetas de alerta:

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Falta de cabecera Anti-Clickjacking

Descripción de alerta:

La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra ataques de 'ClickJacking'.

Etiquetas de alerta:

- WSTG-v42-CLNT-09
- OWASP_2021_A05
- OWASP_2017_A06
- CWE-1021

Encabezado de seguridad de transporte estricto no establecido

Descripción de alerta:

HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.

Etiquetas de alerta:

- OWASP_2021_A05
- OWASP_2017_A06

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- CWE-319

Cookie Sin Bandera de Seguridad

Descripción de alerta:

Se ha establecido una cookie sin el indicador de seguridad, lo que significa que se puede acceder a la cookie a través de conexiones no cifradas.

Etiquetas de alerta:

- OWASP_2021_A05
- OWASP_2017_A06
- CWE-614
- WSTG-v42-SESS-02

Cookie sin el atributo SameSite

Descripción de alerta:

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida eficaz para contrarrestar la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y los ataques de sincronización.

Etiquetas de alerta:

- OWASP_2021_A01
- OWASP_2017_A05
- WSTG-v42-SESS-02
- CWE-1275

Falta encabezado X-Content-Type-Options

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Descripción de alerta:

La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.

Etiquetas de alerta:

- CWE-693
- OWASP_2021_A05
- OWASP_2017_A06

Librería JS Vulnerable

Descripción de alerta:

La librería identificada jquery, versión 3.6.4 es vulnerable.

Etiquetas de alerta:

- OWASP_2017_A09
- OWASP_2021_A06
- CWE-829

Puertos Expuestos Innecesariamente

BuenData
DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-16 23:35 -05
Nmap scan report for pregradoesap.esap.edu.co (35.239.82.41)
Host is up (0.099s latency).
rDNS record for 35.239.82.41: 41.82.239.35.bc.googleusercontent.com
Not shown: 65527 filtered ports, 1 closed port
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
4500/tcp  open  sae-urn
8080/tcp  open  http-proxy
8445/tcp  open  copy
10443/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 445.92 seconds
```

Imagen 15. Seguridad Posgrado 2

Descripción de la alerta: Se han detectado múltiples puertos abiertos en el servidor, además de los esenciales para servicios HTTP y HTTPS (puertos 80 y 443). Los puertos adicionales abiertos son:

- 22/tcp (SSH): Protocolo para acceso remoto seguro. Debe restringirse a direcciones IP específicas.
- 4500/tcp (sae-urn): Asociado con protocolos de seguridad de red (como IPsec). Verificar su necesidad.
- 8080/tcp (http-proxy): Generalmente usado para pruebas o entornos no productivos. Puede ser innecesario en producción.
- 8445/tcp (copy): Normalmente utilizado por aplicaciones específicas. Evaluar su propósito y restringirlo.
- 10443/tcp (unknown): Puerto desconocido que puede representar un riesgo si no tiene un propósito claro.

Mantener puertos abiertos innecesarios incrementa la superficie de ataque, permitiendo posibles vectores de explotación.

Etiqueta alerta:

- OWASP: A05:2021

DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

3.3. Revisión de Entorno de las tres instancias

- Extensión

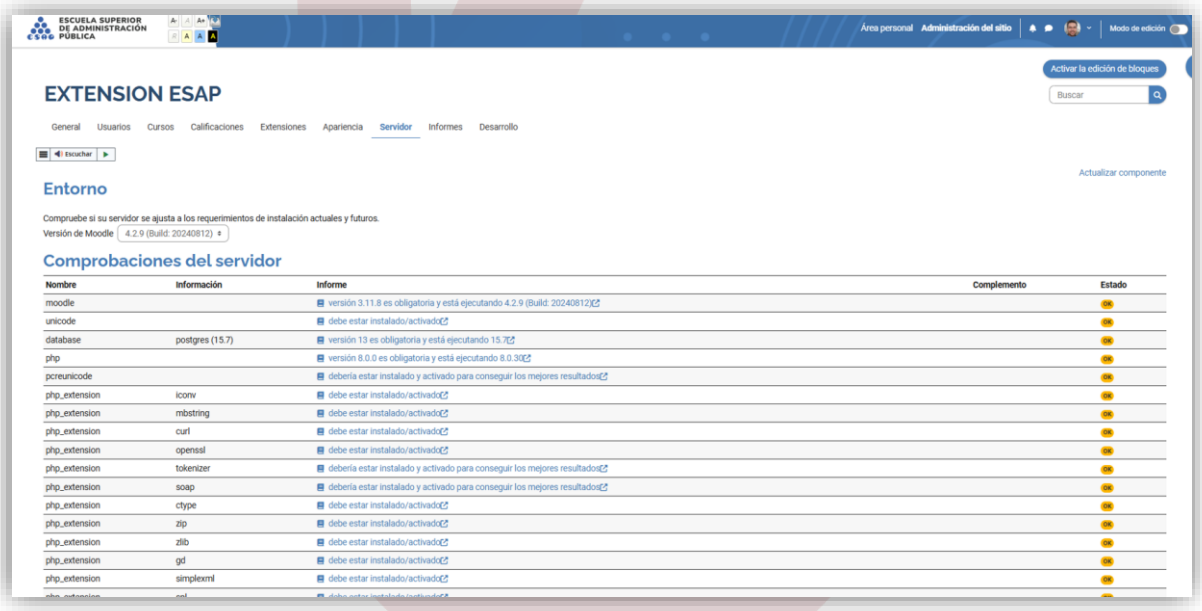
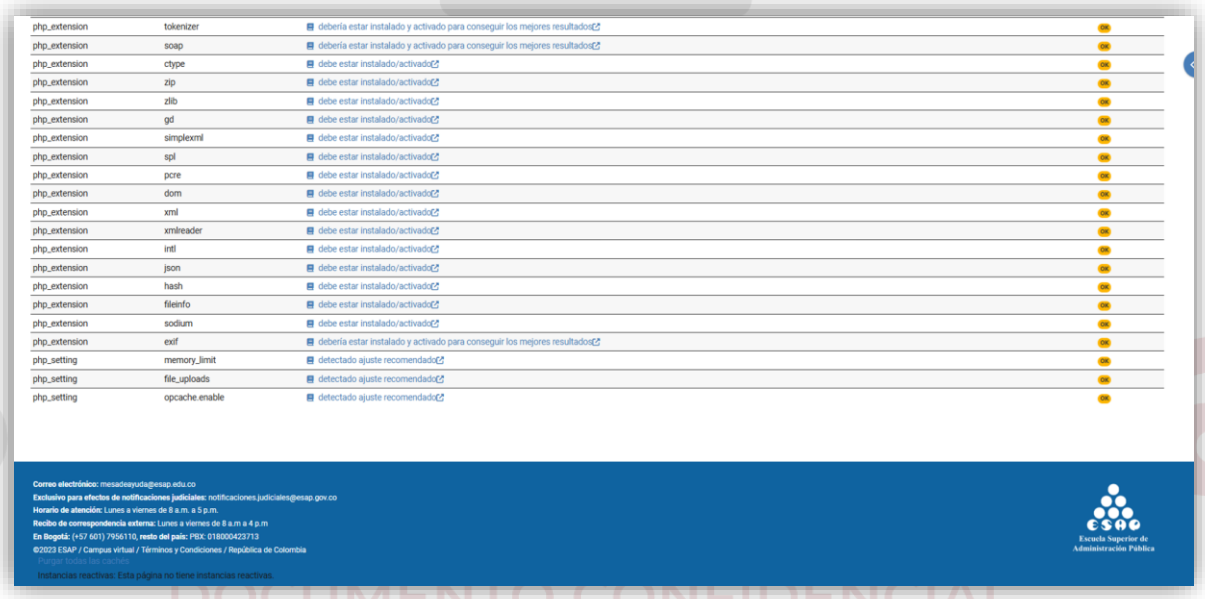


Imagen 16. Entorno Extensión 1



DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Imagen 17. Entorno Extensión 2

- Posgrado

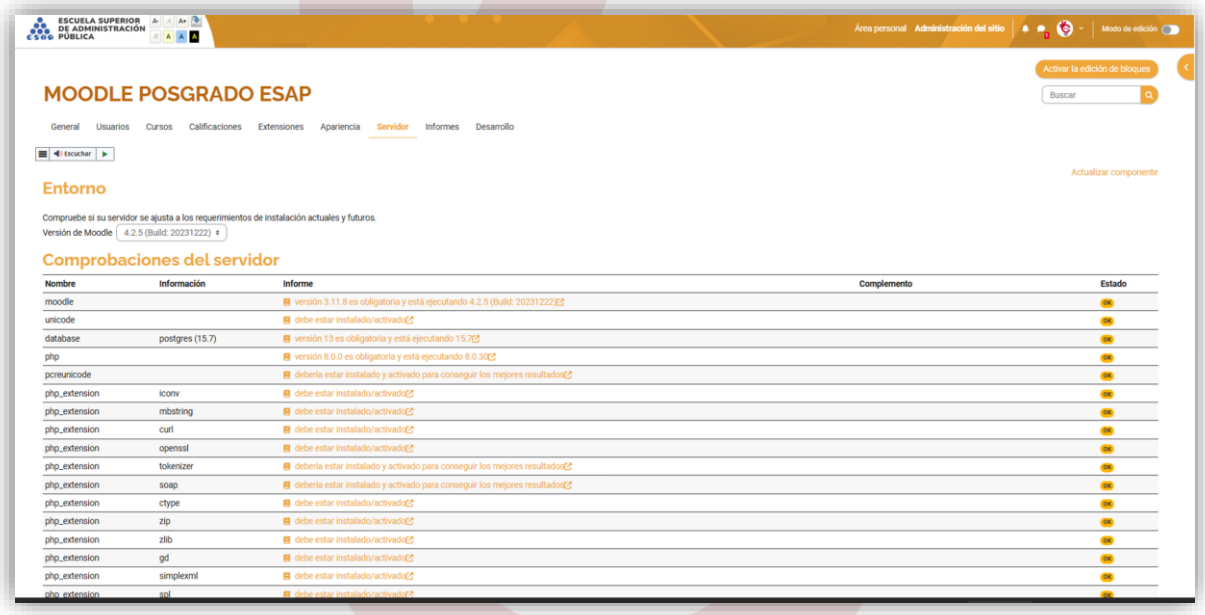
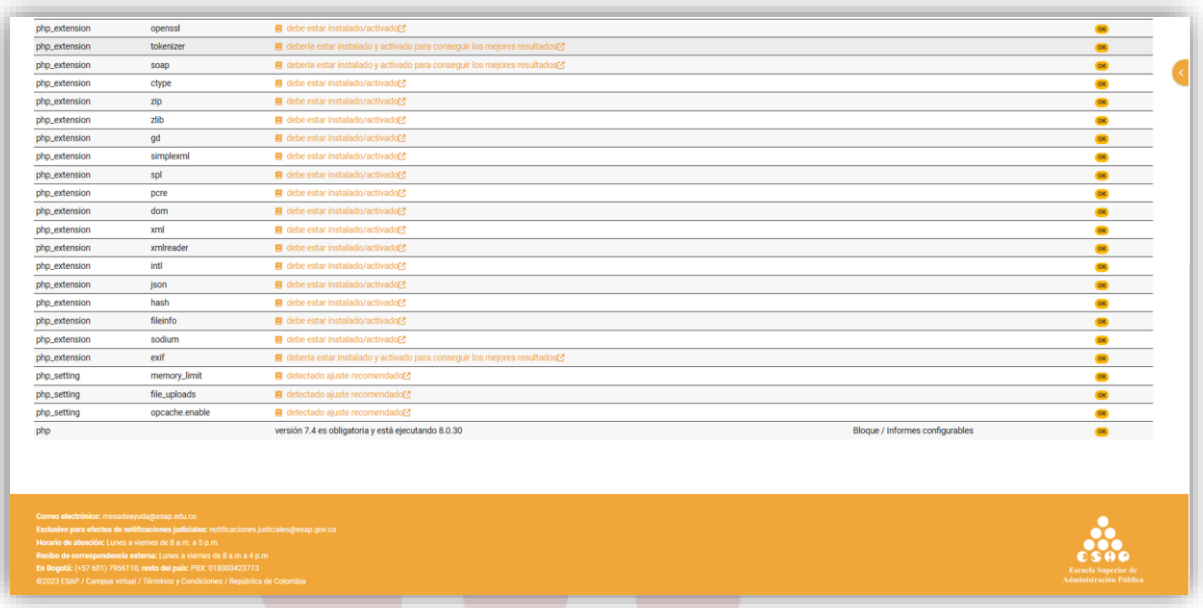


Imagen 18. Entorno Posgrado 1

BuenData
DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

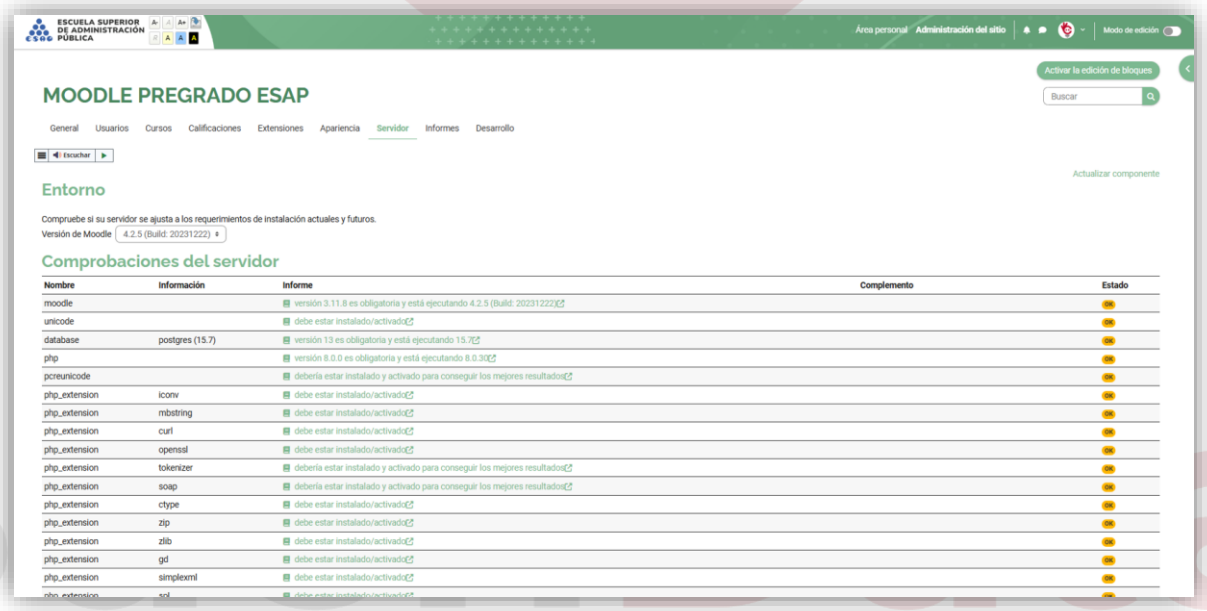


php_extension	openssl	debe estar instalado/activado	
php_extension	tokenizer	debería estar instalado y activado para conseguir los mejores resultados	
php_extension	soap	debería estar instalado y activado para conseguir los mejores resultados	
php_extension	ctype	debe estar instalado/activado	
php_extension	zip	debe estar instalado/activado	
php_extension	zlib	debe estar instalado/activado	
php_extension	gd	debe estar instalado/activado	
php_extension	simplexml	debe estar instalado/activado	
php_extension	spl	debe estar instalado/activado	
php_extension	pcre	debe estar instalado/activado	
php_extension	dom	debe estar instalado/activado	
php_extension	xml	debe estar instalado/activado	
php_extension	xmlreader	debe estar instalado/activado	
php_extension	intl	debe estar instalado/activado	
php_extension	json	debe estar instalado/activado	
php_extension	hash	debe estar instalado/activado	
php_extension	fileinfo	debe estar instalado/activado	
php_extension	sodium	debe estar instalado/activado	
php_extension	exif	debería estar instalado y activado para conseguir los mejores resultados	
php_setting	memory_limit	detectado ajuste recomendado	
php_setting	file_uploads	detectado ajuste recomendado	
php_setting	opcache.enable	detectado ajuste recomendado	
php		versión 7.4 es obligatoria y está ejecutando 8.0.30	Bloque / Informes configurables

Correo electrónico: mesadeayuda@esap.edu.co
Exclusivo para efectos de notificaciones judiciales: notificaciones.judiciales@esap.gov.co
Horario de atención: Lunes a viernes de 8 a.m. a 5 p.m.
Recibo de correspondencia externa: Lunes a viernes de 8 a.m a 4 p.m
En Bogotá: (+57 601) 7956110, resto del país: PBX: 018000423713
©2023 ESAP / Campus virtual / Términos y Condiciones / República de Colombia

Imagen 19. Entorno Posgrado 2

- Pregrado



ESCUELA SUPERIOR DE ADMINISTRACIÓN PÚBLICA

Área personal Administración del sitio Modo de edición

MOODLE PREGRADO ESAP

Activar la edición de bloques

Buscar

General Usuarios Cursos Calificaciones Extensiones Apariencia Servidor Informes Desarrollo

Ocultar

Actualizar componente

Entorno

Compruebe si su servidor se ajusta a los requerimientos de instalación actuales y futuros.

Versión de Moodle 4.2.5 (Build: 20231222)

Comprobaciones del servidor

Nombre	Información	Informe	Complemento	Estado
moodle		versión 3.11.8 es obligatoria y está ejecutando 4.2.5 (Build: 20231222)		
unicode		debe estar instalado/activado		
database	postgres (15.7)	versión 13 es obligatoria y está ejecutando 15.7		
php		versión 8.0.0 es obligatoria y está ejecutando 8.0.30		
pcreunicode		debería estar instalado y activado para conseguir los mejores resultados		
php_extension	iconv	debe estar instalado/activado		
php_extension	mbstring	debe estar instalado/activado		
php_extension	curl	debe estar instalado/activado		
php_extension	openssl	debe estar instalado/activado		
php_extension	tokenizer	debería estar instalado y activado para conseguir los mejores resultados		
php_extension	soap	debería estar instalado y activado para conseguir los mejores resultados		
php_extension	ctype	debe estar instalado/activado		
php_extension	zip	debe estar instalado/activado		
php_extension	zlib	debe estar instalado/activado		
php_extension	gd	debe estar instalado/activado		
php_extension	simplexml	debe estar instalado/activado		

Imagen 20. Entorno Pregrado 1

DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

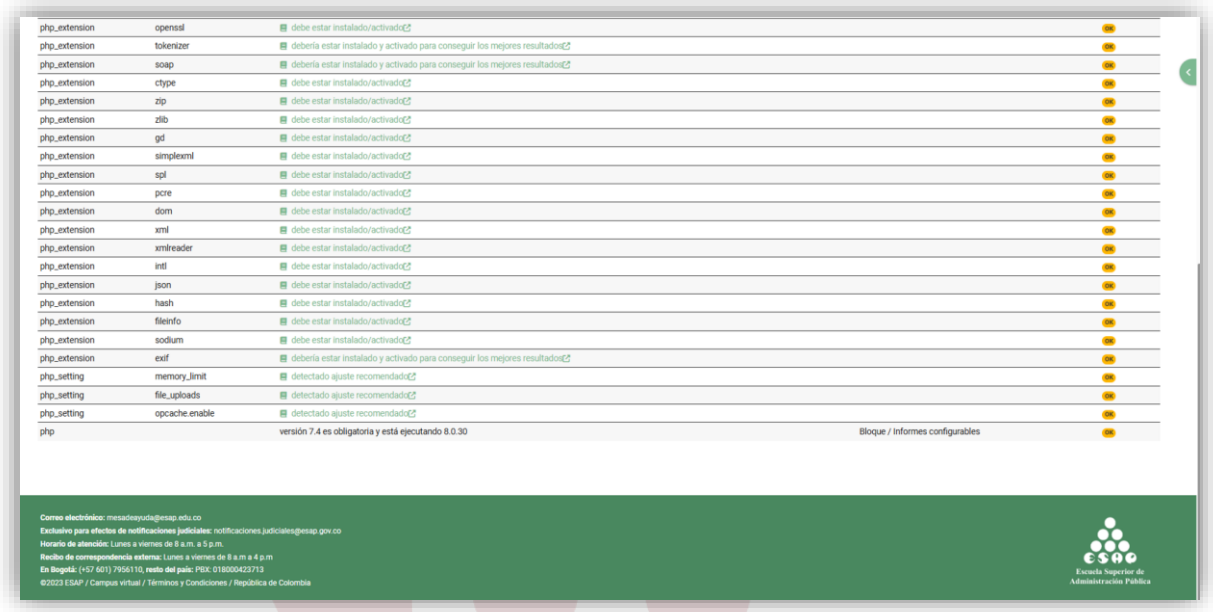


Imagen 21. Entorno Pregrado 2

4. Infraestructura y esquema topológico

Luego de la migración realizada de las instancias a la nube, se presenta la infraestructura y el esquema topológico y la versión del nodo del clúster de la ESAP.

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

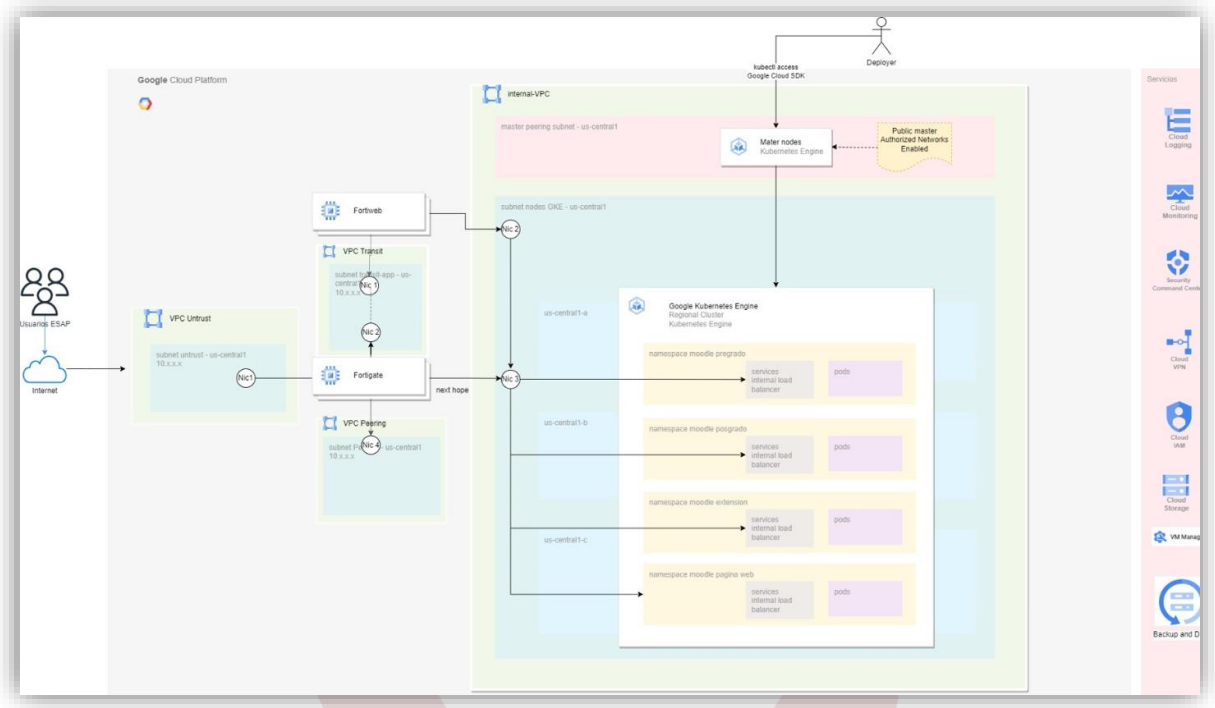


Imagen 22. Esquema Topológico

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

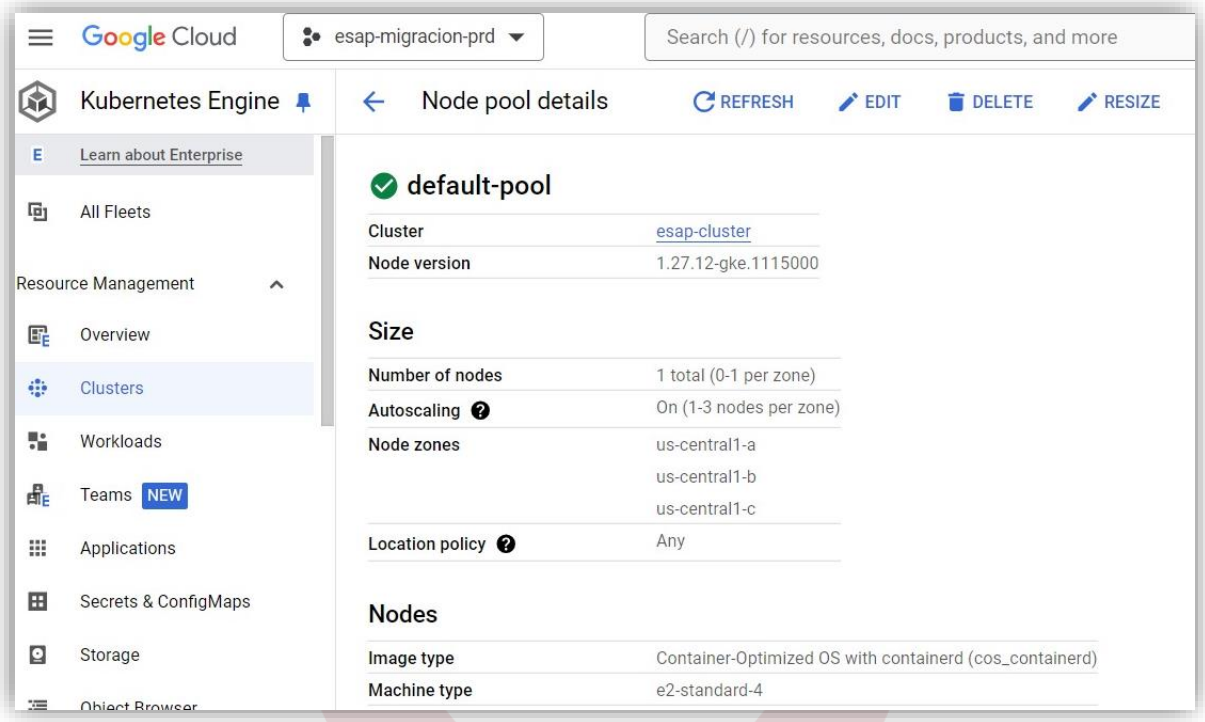


Imagen 23. Versión del nodo

5. Actualización de componentes generales para el funcionamiento de Moodle

Durante el proceso de ejecución del proyecto, se recomienda realizar ajustes, asesorías y proporcionar soporte continuo para mantener el correcto funcionamiento de Moodle.

6. Mantener suficiente espacio monitoreado para los esquemas de backup de la entidad

Se recomienda implementar y/o mantener una política de backups diarios para las instancias de Moodle. A continuación, se detallan los parámetros sugeridos para la gestión de backups:

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Tipo de Backup: Diario.
- Retención de Backups Diarios: 30 días.
- Retención Mensual: Mantener un backup mensual del último mes.
- Retención Anual: Conservar 12 backups anuales, uno por cada mes.

Además, se recomienda establecer una política interna dentro de Moodle para la limpieza periódica de logs, a fin de optimizar el rendimiento y evitar la acumulación innecesaria de datos.

A continuación, se presenta la evidencia:

- Extensión

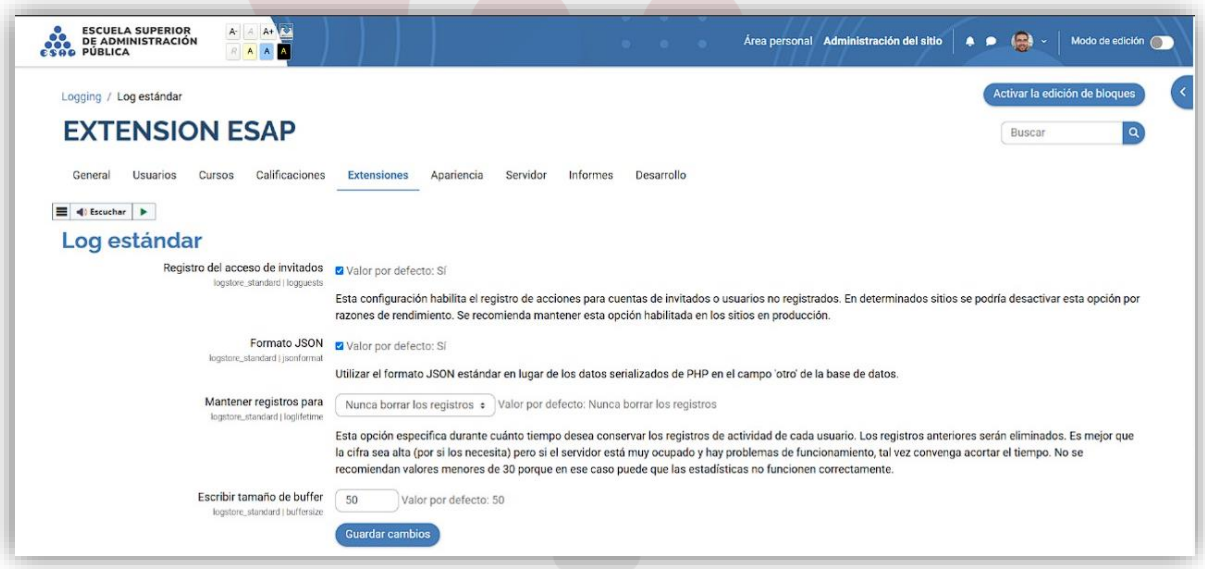


Imagen 24. Moodle logs Extensión

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Posgrado

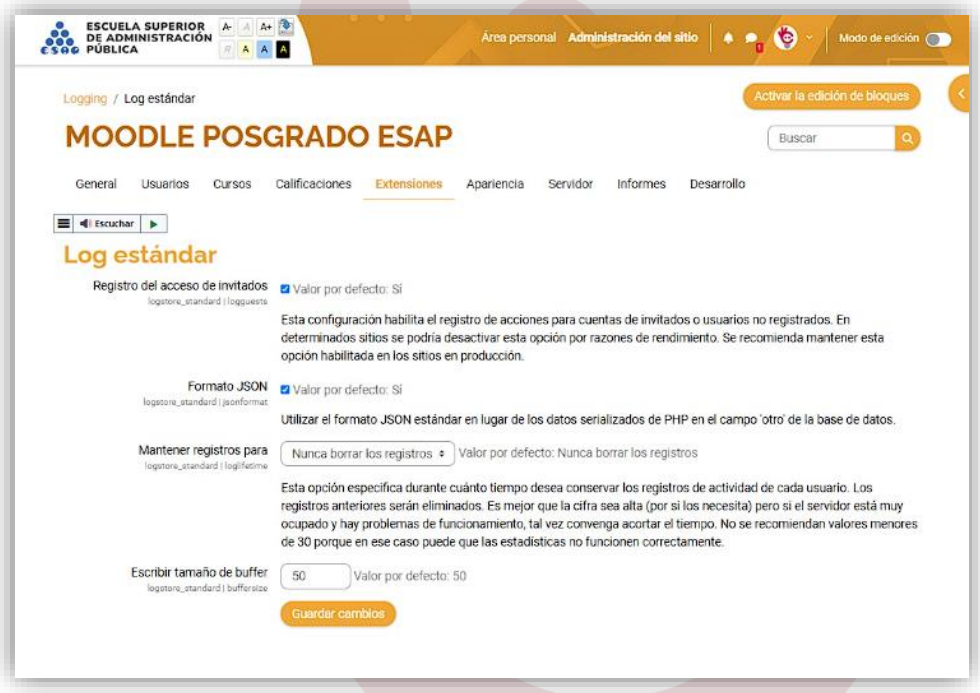


Imagen 25. Moodle logs Extensión

BuenData
DOCUMENTO CONFIDENCIAL

moodle Partner
CERTIFIED SERVICES PROVIDER™
cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

- Pregrado

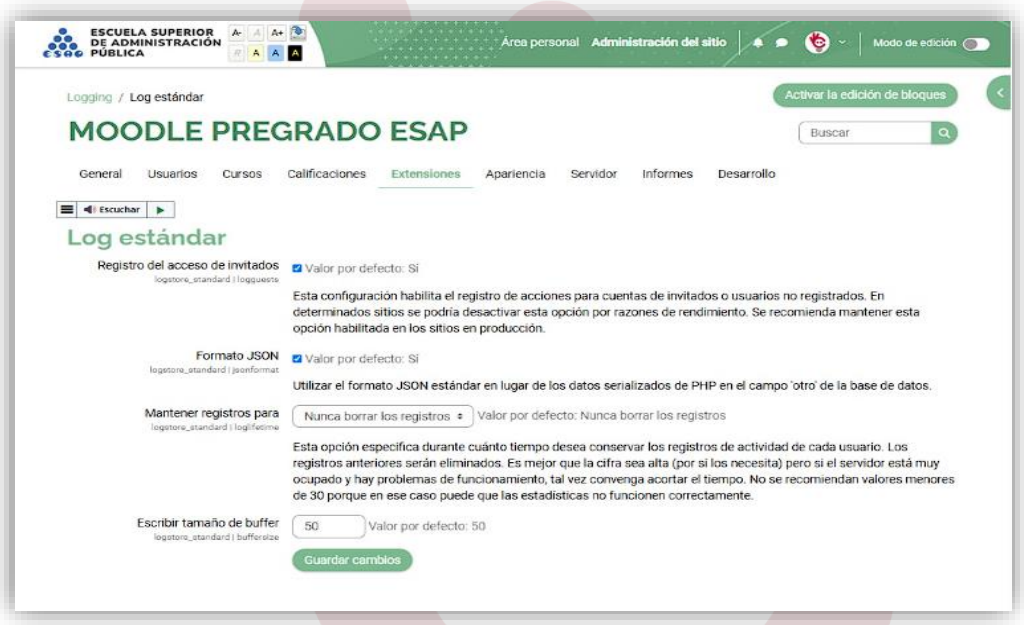
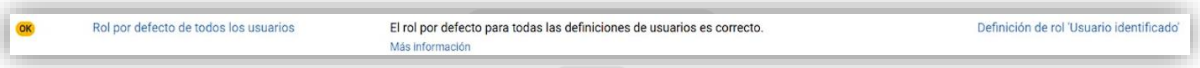


Imagen 26. Moodle logs Extensión

- Se han aplicado las recomendaciones de revisar y ajustar el rol "identificado en sitio" en Moodle. Las cuales quedaron por defecto



BuenData
DOCUMENTO CONFIDENCIAL

cel: 314 628 22 15
hemerson@buendata.com
soporte@buendata.com

Elaborado por:

Jean Ortega – Ingeniero Moodle
Leslie Martínez – Gestora de Proyecto

Revisado por:

Hemerson Carreño – Gerente de proyecto

(+57) 314 628 22 15 - 314 242 68 92 - 319 498 86

Comuníquese a través de los siguientes medios:

www.Buendata.com
Calle 65ª # 16 – 30 Bogotá -

leslie@buendata.com - soluciones@buendata.com – ramiro@buendata.com – hemerson@buendata.com

BuenData
DOCUMENTO CONFIDENCIAL