



Alerta mundial pone en riesgo a las Universidades

PHP, un lenguaje liviano, compromete la seguridad informática en las Universidades de todo el Perú.



RESUMEN

El Observatorio de Educación Superior por encargo de la Asociación Nacional de Universidades Públicas del Perú (ANUPP) ha realizado un **Informe Técnico sobre la “Alerta Mundial ante el fallo crítico de PHP”**.

En los últimos días se han conocido dos fallas críticas en PHP, **uno de los lenguajes más utilizados para construir páginas y aplicaciones web. Las vulnerabilidades identificadas pueden permitir que un atacante remoto ejecute códigos en un servidor sin necesidad de contar previamente con usuario o contraseña.** También pueden exponer información sensible almacenada temporalmente en la memoria del sistema (Betz & Popa, 2026).

El problema es relevante porque **PHP** está detrás de una parte importante de Internet y **es utilizado directa o indirectamente por plataformas como WordPress, Drupal, Joomla, Laravel y otros sistemas de gestión de contenidos.** El riesgo depende de la versión instalada, de la configuración del servidor y de las medidas de protección existentes (NHS England Digital, 2026).

El problema se agrava al reportarse intentos de uso de información sensible identificados incluso antes de hacerse público. Esto muestra que, en la actualidad, el tiempo entre la publicación de una vulnerabilidad y los primeros intentos de aprovecharla puede ser muy corto (Amazon Web Services, 2026).



Para las universidades, la principal conclusión es: **no basta con tener una página web funcionando; es indispensable saber qué versión de PHP utiliza, mantenerla actualizada, revisar periódicamente plugins y componentes, contar con copias de seguridad y monitorear de manera permanente los servidores.**

En ciberseguridad, un sistema que aparentemente funciona con normalidad, pero que no recibe actualizaciones, puede convertirse rápidamente en un riesgo para la continuidad institucional y para la protección de la información.

II La falla mundial en PHP y los problemas que esta ocasionando

TABLA 1 Principales consecuencias de la falla en PHP

Problema	Qué significa en términos prácticos para una universidad
Ejecución remota de código	Una extraña puede ejecutar instrucciones en un servidor vulnerable sin autenticarse.
Exposición de información de memoria	Las vulnerabilidades pueden permitir acceder a sesiones, tokens, datos temporales u otra información sensible.
Interrupción de servicios	pueden provocar caída o inestabilidad de servidores, afectando admisión, matrícula, pagos, consultas académicas o trámites digitales.
Intentos de explotación reales	Intentos de uso de datos sensibles desde el 17 de octubre de 2026, cuatro días antes de la divulgación pública.
Escaneo automatizado masivo	Cloudflare confirmó tráfico de ataque contra sus clientes y variaciones deliberadas de los payloads para intentar evadir las protecciones.
Riesgo para sistemas antiguos	PHP 8.1 y versiones anteriores no recibirán parches oficiales. Las organizaciones que siguen allí tienen que migrar.
Mayor carga operativa para TI	Es necesario inventariar servidores, versiones, contenedores, proveedores de hosting, aplicaciones heredadas y dispositivos que incorporan PHP, aplicar parches y reiniciar efectivamente los procesos.
Movimiento hacia otros sistemas	Si el servidor web comparte credenciales, redes o infraestructura con aplicaciones internas, una intrusión inicial puede utilizarse para avanzar hacia otros recursos.
Riesgo reputacional y regulatorio	Una filtración, caída de sistemas o modificación del sitio obliga a gestionar comunicación de crisis, posibles incidentes de datos personales y afectación de confianza institucional.

II.1 La falla mundial en PHP y los problemas que puede ocasionar en las Universidades del Perú

Para el presente informe se ha hecho una revisión sobre 95 universidades, entre públicas y privadas, incluyendo universidades que se encuentran en proceso de institucionalización; se usaron los datos y la arquitectura que son públicas, se evaluaron los 95 portales de estas universidades, sus campus virtuales, intranets, sistemas académicos, gestión documental, trámites y otros servicios. Se hizo una bitácora de observación estructura con los estigmas visibles como cabeceras del servidor, código de la página y las cookies.

Las limitaciones del informe son: el acceso solo a la “fachada” de los ecosistemas, en 28 sitios no se pudo identificar plenamente su tecnología y eso es una limitación para el informe, pero también que estas instituciones ocultan bien sus datos. Lo que se presentará a continuación es un diagnóstico general y no un examen particular a una universidad, tampoco exhibiremos los datos de ninguna universidad.

Nuestras limitaciones son el no poder reconocer la versión exacta de PHP de todos los sistemas; por lo tanto, la tabla siguiente es una evaluación de lo que es de acceso público y sobre ello las consecuencias que consideramos potenciales.

TABLA 2 Principales problemas de las universidades

Prioridad	Problema estructural	Consecuencia
1	Sistemas y versiones antiguas	Imposibilidad de parchear rápidamente
2	Fragmentación de servidores y subdominios	TI puede desconocer parte de su propia superficie
3	Interconexión entre web y sistemas críticos	Una intrusión puede propagarse
4	Concentración de identidad y datos	Una cuenta comprometida puede abrir múltiples servicios
5	Ausencia de inventario tecnológico actualizado	La universidad no sabe exactamente qué debe proteger

III Estado situacional de las Universidades en el Perú

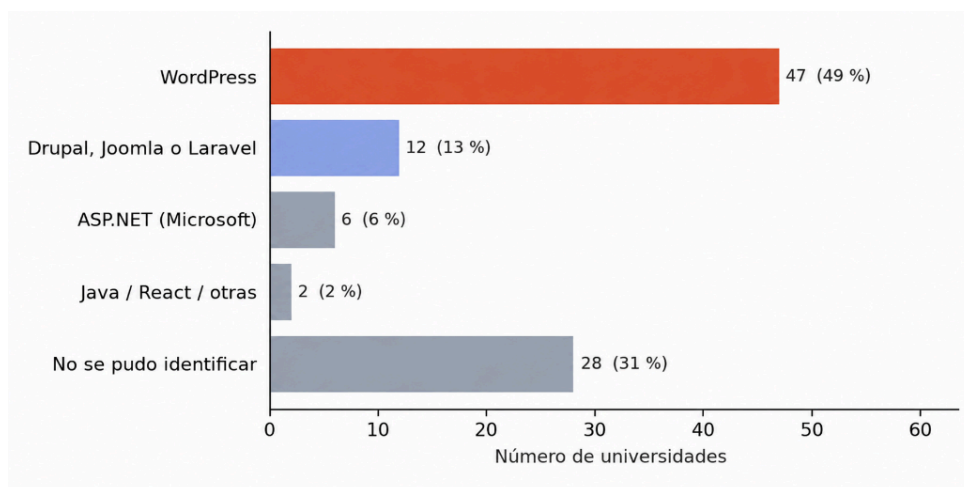
Revisamos las páginas webs de 95 universidades peruanas, entre públicas y privadas, no probamos contraseñas, ni hemos penetrado la seguridad, solo recogimos información a la que se puede acceder con una auditoría de los datos abiertos.

III.1 WordPress domina el mercado

50 %

Aproximadamente el 50% usa WordPress. lo cual no es malo por sí mismo, pero depende de plugins, los cuales muchas veces están desactualizados y con permisos de todo tipo, y los plugins son de donde suelen aparecer los problemas.

GRÁFICO 1 Tecnología principal de los portales universitarios del Perú



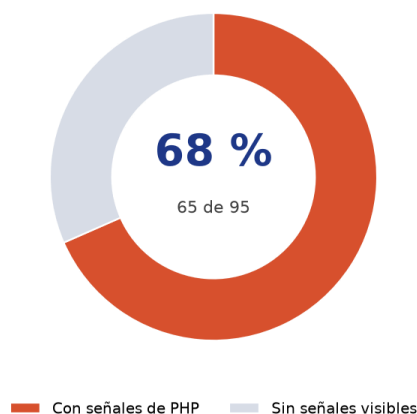
WordPress aparece en 47 sitios. La razón, porque es barato, hay mucha gente que lo maneja y se instala en una tarde. El costo llega después, cuando nadie lleva el control de qué plugins hay instalados ni de cuándo se actualizaron por última vez.

III.2 PHP está debajo de casi todo

2 de 3

Dos de cada tres corren sobre PHP. muestran códigos de PHP, directas o a través de WordPress, Joomla, Drupal o Laravel.

GRÁFICO 2 Sitios con señales de PHP, directas o por el gestor que usan



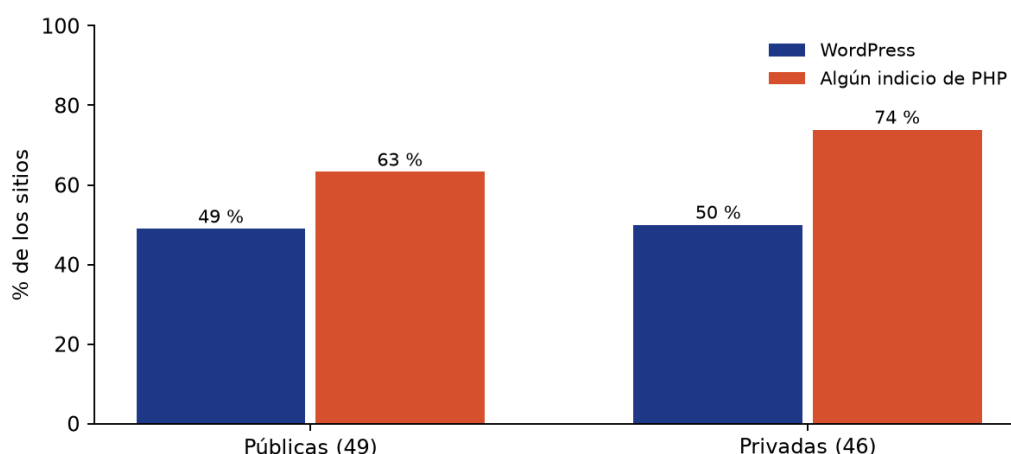
Contando WordPress, Joomla, Drupal, Laravel y las páginas que simplemente se sirven con extensión .php, 65 de 95 sitios descansan sobre PHP. Es un lenguaje sólido cuando se mantiene al día, lo que falla casi siempre es el mantenimiento.

III.3 Públicas y privadas, parecidas



Esta semana PHP tuvo un problema serio, el 21 de octubre se publicaron dos fallas críticas (CVE-2026-109618 y CVE-2026-109619) que permiten ejecutar código sin usuario ni contraseña. Ya hay código de ataque público masivo, se han corregido las versiones corregidas son 8.2.35, 8.3.36, 8.4.27 y 8.5.12; sin embargo, la versión 8.1 y las anteriores no han recibido parche oficial.

GRÁFICO 3 Porcentaje de sitios con WordPress y con indicios de PHP, según el tipo de universidad

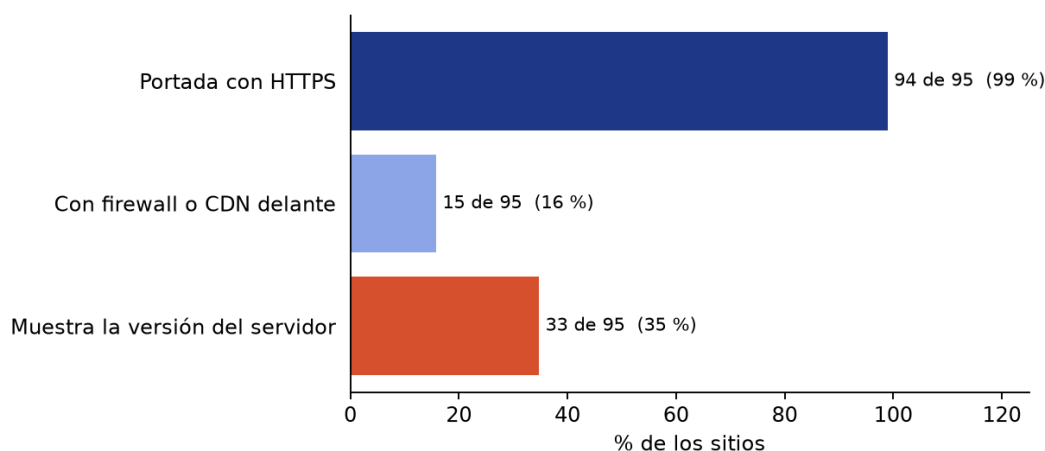


No encontramos una brecha grande entre públicas y privadas. Los dos grupos dependen de las mismas herramientas, y los dos tienen la misma tarea pendiente.

III.4 Protecciones básicas: bien en lo primero, flojo en lo demás

Casi todas (94 de 95) cargan por HTTPS, que es lo mínimo y solo 15 tienen un firewall o CDN adelante, que filtra tráfico malicioso antes de que llegue al sitio; 33 muestran la versión de su servidor, un dato que no hace falta hacerlo público (regalar al intruso).

GRÁFICO 4 Señales de protección visibles en la portada.



IV ¿Por qué las Universidades se encuentran vulnerables?

La tecnología avanza imparable y las nuevas generaciones han ingresado a una escalada de acceso a la información desde temprana edad, no es una situación de genialidad encontrar a un adolescente programando, creando aplicativos o incluso vulnerando sistemas de seguridad avanzados. Hasta hace algunos años vulnerar sistemas de seguridad significaba revisar miles de líneas de códigos en búsqueda de la falla y atacar, la imagen del experto especialista, casi genio ya no existe más; las herramientas de la inteligencia artificial han reducido las barreras, se pueden leer códigos en minutos y explotarlos en cuestión de minutos también.

El caso de PHP de esta semana lo muestra bien. Las fallas se hicieron públicas el 21 de octubre y el código de ataque, bautizado PHP2Shell, ya circula en la Darknet / DeepWeb. Algunas fuentes hablan de primeros intentos de explotación; otras dicen que todavía no se sabe qué tan extendidos están. Las dos fallas están en PHP mismo, no en un sitio concreto. Cualquier página hecha con WordPress, Drupal, Laravel o con un sistema propio en PHP queda expuesta hasta que se actualice.

V

Medidas que han sido adoptadas a nivel internacional

El 21 de octubre de 2026 se difundieron actualizaciones destinadas a corregir estas vulnerabilidades, las medidas adoptadas internacionalmente frente a **PHP2Shell** pueden agruparse en tres niveles: corrección definitiva, mitigación temporal y contención/monitoreo. La conclusión común de PHP, AWS, Google Cloud, NSA y NHS es inequívoca: **la única corrección completa para CVE-2026-109618 y CVE-2026-109619 es actualizar PHP a una versión corregida** (PHP Group, 2026).

TABLA 3 Medidas aplicadas para corregir y eliminar el problema

Medida	Qué se hizo	Alcance
Actualización inmediata de PHP	Se liberaron PHP 8.2.35, 8.3.36, 8.4.27 y 8.5.12	Es la solución completa para CVE-2026-109618 y CVE-2026-109619
Migración de versiones antiguas	PHP 5.4–8.1 ya no recibe corrección oficial upstream	Deben migrarse a una rama soportada
Reglas WAF específicas	AWS creó PHP2Shell_BODY y PHP2Shell_BODY_Extended; otros proveedores desplegaron reglas equivalentes	Reduce exposición mientras se actualiza, pero no sustituye el parche
Inventario urgente	NSA recomendó identificar todos los equipos, servicios y aplicaciones que dependen de PHP	Permite localizar sistemas olvidados o no gestionados
Deshabilitación de funciones peligrosas	Se recomendó desactivar session.upload_progress.enabled y ciertos mecanismos asociados a los disparadores	Mitigación temporal y defensa adicional
Reinicio de procesos PHP	Tras actualizar/configurar, se debe reiniciar PHP-FPM, Apache u otros workers	Evita que continúe ejecutándose código vulnerable ya cargado en memoria
Restricción de cargas de archivos	En sistemas no parchables inmediatamente, se recomendó limitar o bloquear temporalmente cargas multipart/form-data	Reduce la superficie de ataque
Monitoreo reforzado	Revisión de logs, errores fatales, timeouts, peticiones anómalas y actividad de explotación	Busca detectar ataques ocurridos antes o durante el parcheo

Medida	Qué se hizo	Alcance
Aislamiento de sistemas	Cuando un servidor antiguo no puede actualizarse rápidamente, debe limitarse su exposición a Internet	Contención temporal
Migración de sistemas legados	Aplicaciones incompatibles con PHP moderno requieren actualización del framework/código o reemplazo	Solución estructural

V.1 Medidas que deberían adoptar las universidades peruanas

Ya fueron puestas en alerta por el **Centro Nacional de Seguridad Digital (CNSD) de la Presidencia del Consejo de Ministros**, quien emitió el **21 de octubre de 2026** una alerta específica sobre PHP2Shell, identificando las vulnerabilidades **CVE-2026-109618 y CVE-2026-109619** y advirtiendo que podían permitir ejecución remota de código, acceso no autorizado y compromiso de servidores vulnerables. También informó que ya existían intentos de explotación y que la publicación de pruebas técnicas incrementaba el riesgo de ataques masivos (CNSD, 2026).

La alerta peruana siguió básicamente el mismo enfoque de los organismos internacionales: **parchar primero; si no es posible, reducir o eliminar temporalmente la exposición pública.**

Y hoy con este Informe del Observatorio de Educación Superior tienen una hoja de ruta suficiente para actuar rápidamente ante cualquier inconveniente y sobre todo, sensibilizar y prevenir sobre la vulnerabilidad de nuestros sistemas de gestión.

Las universidades peruanas deberían tratar PHP2Shell como un incidente de riesgo institucional, no solo como un problema del área de informática. La prioridad inmediata es identificar qué sistemas usan PHP y corregirlos antes de que una vulnerabilidad técnica termine afectando matrícula, notas, pagos, datos personales o continuidad académica.

Las medidas que recomendaría son estas:

- 1 Inventariar todos los sistemas que usan PHP.
- 2 Actualizar inmediatamente a una versión corregida.
- 3 Migrar las versiones fuera de soporte.
- 4 Desconectar temporalmente los sistemas que no puedan corregirse.
- 5 Reiniciar efectivamente PHP después del parcheo.
- 6 Desactivar session.upload_progress.enabled mientras corresponda.
- 7 Aplicar WAF/CDN como segunda barrera, no como sustituto del parche.
- 8 Reducir temporalmente la superficie de ataque.
- 9 Revisar retrospectivamente los registros.
- 10 Segmentar los sistemas críticos.
- 11 Proteger las cuentas privilegiadas con MFA.
- 12 Verificar backups y recuperación.
- 13 Crear un equipo de respuesta a incidentes.
- 14 Preparar un protocolo de comunicación.
- 15 Incorporar ciberseguridad a la gobernanza universitaria.

VI ¿Qué está en juego?

Un sitio de portada comprometido es una molestia. El problema real es lo que hay al lado: correos institucionales, datos de matrícula, notas, trámites y pagos de miles de estudiantes. Cuando el sitio público y los sistemas internos comparten servidor o credenciales, una falla en el primero abre la puerta al resto. Si ocurre, las consecuencias no son abstractas: se cae la matrícula o el examen de admisión en plena fecha, se filtran datos personales de estudiantes y docentes, y la universidad queda obligada a explicarlo ante la comunidad, ante SUNEDU y ante la autoridad de protección de datos personales. Reponerse cuesta mucho más que actualizar a tiempo.

Hay además un daño que se ve menos y dura más: la reputación. Una página institucional que redirige a sitios de apuestas o a estafas aparece en buscadores, y los estudiantes y postulantes la ven antes que cualquier comunicado.

VII ¿Qué hacer?

Es una pregunta muy amplia, para nosotros como Observatorio de Educación Superior, velamos por el bienestar de las instituciones educativas superiores público y privada, por ello estamos alineados en la colaboración con toda la institución peruana.

VIII Referencias

Amazon Web Services. (2026). Amazon Threat Intelligence identifies PHP2Shell exploitation prior to public disclosure in MadPot. AWS Security Blog. <https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/>

Betz, C., & Popa, R. A. (2026, 21 de octubre). Responding to core PHP vulnerabilities CVE-2026-109618 and CVE-2026-109619. Google Cloud Blog. <https://cloud.google.com/blog/products/identity-security/responding-to-core-php-vulnerabilities-cve-2026-109618-cve-2026-109619>

NHS England Digital. (2026, 21 de octubre). Critical vulnerabilities in PHP (PHP2Shell) (Threat ID CC-4875). <https://digital.nhs.uk/cyber-alerts/2026/cc-4875>

PHP Group. (2026). PHP: Hypertext Preprocessor. <https://www.php.net/>

Centro Nacional de Seguridad Digital. (2026, 21 de octubre). Alerta integrada de seguridad digital N.º 206-2026-CNSD. Presidencia del Consejo de Ministros. <https://www.gob.pe/institucion/pcm/informes-publicaciones/8748439-alerta-integrada-de-seguridad-digital-n-206-2026-cnsd>



Contacto



CORREO

info@observatorio.com.pe



TELÉFONO / WHATSAPP

963 050 354



WEB

observatorio.com.pe

REDES SOCIALES



[oesobservatorio](https://www.facebook.com/oesobservatorio)



[@oes_observatorio](https://www.instagram.com/oes_observatorio)



[@oesobservatorio](https://twitter.com/oesobservatorio)



[observatorioeducacion](https://www.linkedin.com/company/observatorioeducacion)