Edición de lectura | 2026-11-20

Gestión del riesgo de PHP en entidades financieras

Adrian Dunkley | 2026-10-23

El documento de octubre de 2026 pide identificar los servicios que dependen de PHP, los responsables y las dependencias de terceros. El responsable conserva la versión observada, la fecha, el alcance del cambio y la evidencia del proveedor.

Traducción íntegra de la edición para responsables de supervisión y continuidad, 20 de noviembre de 2026. Adrian Dunkley, StarApple AI y Consejo Caribeño de Gestión del Riesgo de IA. Basada en la versión 1.8 del 23 de octubre de 2026.

Identifique los servicios que dependen de PHP

Designe un responsable de negocio y otro técnico para cada servicio afectado que usen los clientes. Incluya aplicaciones gestionadas por proveedores y entornos de recuperación. Registre la versión instalada, la fecha de observación, el entorno y quién responde del hallazgo. Un sistema puede depender de software que la entidad no gestiona directamente. Pida al proveedor pruebas sobre el servicio que se usa en la práctica.

Distinga entre exposición, interrupción y acceso no autorizado

Una debilidad requiere evaluación. Un aviso público no demuestra que una entidad financiera concreta haya perdido datos o sufrido un acceso no autorizado. También puede haber interrupciones si un operador suspende el servicio por precaución. Registre por separado los hechos observados, las preguntas pendientes y la siguiente comprobación.

Verifique la recuperación mediante una operación de cliente

Siga el proceso de cambios de la entidad para probar la reparación, confirmar que está activa y registrar el resultado. Incluya una operación habitual que el cliente pueda completar, pruebas del servicio en funcionamiento y una comprobación en el entorno de recuperación. La aprobación de una solicitud de cambio no demuestra por sí sola que el servicio reparado funciona correctamente.

Haga un seguimiento de la continuidad y del riesgo residual

Documente las interrupciones, la alternativa disponible para los clientes y la persona responsable de restablecer el servicio. Aplique la escala local de riesgo aprobada y pida al responsable que revise la exposición restante. Conserve las pruebas que respaldan las decisiones, las comunicaciones y el cierre.

Alcance de esta edición

Esta edición recoge la orientación para responsables de gestión. El documento original incluye anexos técnicos, hojas de trabajo y una actualización histórica de un aviso. Esta edición no evalúa ninguna institución concreta. Consulte la información actual del proveedor antes de adoptar una decisión técnica. El Consejo forma parte de la Asociación Caribeña de IA.

Referencias

NIST Cybersecurity Framework

Edición en inglés (PDF)