Carlos Andrés Molina Molina <carlos.molina@insor.gov.co>

Seguimiento Incidente de Seguridad — Limpieza de Malware Residual en Portal Educativo INSOR (13 de Marzo de 2026)

Carlos Andrés Molina Molina <carlos.molina@insor.gov.co> 13 de marzo de 2026 a las 11:46
Para: Hector Alejandro Márquez Ramírez <hector.marquez@insor.gov.co>, Boris Julián Pérez Pérez <boris.perez@insor.gov.co>, Carlos Fredy Rey Camacho <carlos.rey@insor.gov.co>, Rosa Angelina Moncada Castillo <Rosa.Moncada@insor.gov.co>, Juan Pablo Arango Hernandez <juan.arango@insor.gov.co>

Cordial saludo,

Por medio del presente, informo sobre las acciones de seguimiento realizadas el día de hoy, 13 de marzo de 2026, en relación con el incidente de seguridad del portal educativo.insor.gov.co reportado y atendido inicialmente el pasado 27-28 de febrero de 2026.

Situación detectada
Durante una revisión de control posterior a la limpieza original, se identificó la persistencia de contenido malicioso residual en el directorio /publicaciones del sitio WordPress, el cual no fue erradicado completamente durante la intervención inicial. Adicionalmente, se detectó que el archivo de plantilla del tema activo (publicaciones.php) había sido completamente sustituido por el atacante con contenido de spam de casino, lo que permitía seguir sirviendo páginas fraudulentas bajo el dominio institucional.

Acciones ejecutadas
Cuarentena de 3 archivos maliciosos del directorio /publicaciones (spam SEO tipo TERNATETOTO — casinos/apuestas).
Restauración del template legítimo publicaciones.phpdel tema WordPress desde una copia limpia verificada.
Bloqueo preventivo de ejecución PHP en el directorio /publicaciones mediante directiva .htaccess.
Escaneo completo del sistema de archivos, confirmando la ausencia de indicadores de compromiso activos tanto en WordPress como en Moodle.

Acciones pendientes recomendadas:

Solicitar desindexación en Google Search Console de la ruta /publicaciones/ para eliminar los resultados de búsqueda contaminados.
Depurar backups antiguos (anteriores a febrero 2026) almacenados en el servidor, los cuales podrían contener copias del malware y reinfectar el sistema en caso de restauración.
Recomendaciones dadas en el pasado informe

Se adjunta el informe técnico detallado con el registro completo de hallazgos, acciones y verificaciones realizadas.

Quedo atento a cualquier inquietud o requerimiento adicional.

Cordialmente,

Carlos Andrés Molina

Contratista
Ingeniero de Software
Subdirección de Promoción y Desarrollo
Instituto Nacional para Sordos – INSOR

carlos.molina@insor.gov.co
Carrera 89ª #64C-30, Bogotá, Colombia
www.insor.gov.co

Informe_Limpieza_Residual_2026-03-13.md
9K