DIARIO DIGITAL DEV / RECURSO DE LECTURA

Registros de una IA: cómo comprobar que no fueron alterados

Acuerda qué registros se protegen, desde cuándo y con qué mecanismo se detectan cambios o faltantes. Exige una verificación ejecutada, con alcance y resultado revisables, y un ensayo controlado que detecte alteraciones. La integridad del archivo conservado no demuestra que se registraron todas las acciones ni que la información original era correcta.

Antes de aceptar la integridad de los registros

[ ] El mapa separa acciones de la aplicación y actividad de infraestructura.

[ ] El alcance define ambiente, origen, período y momento inicial de protección.

[ ] Los permisos efectivos identifican escritura, lectura y administración.

[ ] La verificación tiene una ejecución y un resultado revisables.

[ ] El ensayo distingue archivos intactos, alterados, ausentes y no accesibles.

[ ] Los pendientes tienen responsable y un procedimiento de preservación.

Próximas acciones

1. Identifica qué evidencia de una acción del asistente necesitarías investigar.

2. Pide al proveedor una demostración del mecanismo y de sus límites de cobertura.

3. Acuerda el ensayo, el informe de aceptación y los responsables de preservar y revisar hallazgos.

Notas para tu equipo

_____

_____

_____

_____

Artículo y fuentes

https://www.digital-dev.cl/blog/registros-acciones-ia-integridad-almacenamiento/

OWASP: Logging Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

Amazon Web Services: Validating CloudTrail log file integrity
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html

Amazon Web Services: Validating CloudTrail log file integrity with the AWS CLI
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-cli.html