A09:2021/2025

ERRORES DE REGISTRO Y ALERTAS DE SEGURIDAD

EL PELIGRO DE LA INVISIBILIAD ANTE LOS ATAQUES

Véro Grué

QUE ES EL A09?

No se trata de un error de sintaxis, sino de una falta de visibilidad.

Ocurre cuando una aplicación no genera registros suficientes o no monitoriza eventos críticos, impidiendo detectar intrusiones en tiempo real.

"No puedes detener lo que no puedes ver"

IMPACTO EN EL NEGOCIO

Análisis Forense Imposible: "Algo pasó, pero no sabemos qué, quién ni cómo".

Incumplimiento Legal: Multas por normativas como el RGPD (que exige detectar y reportar brechas en 72h).

Efecto "Puerta Abierta": Los atacantes regresan porque no se parcheó el origen.

¿CÓMO PREVENIRLO?

Integridad: Los logs no deben ser escribibles por el usuario del servidor web (para que un atacante que entre no pueda borrar sus huellas).

Centralización: Usar herramientas como el visor de eventos o sistemas externos (SIEM).

Retención: Guardar registros durante al menos 30-90 días.

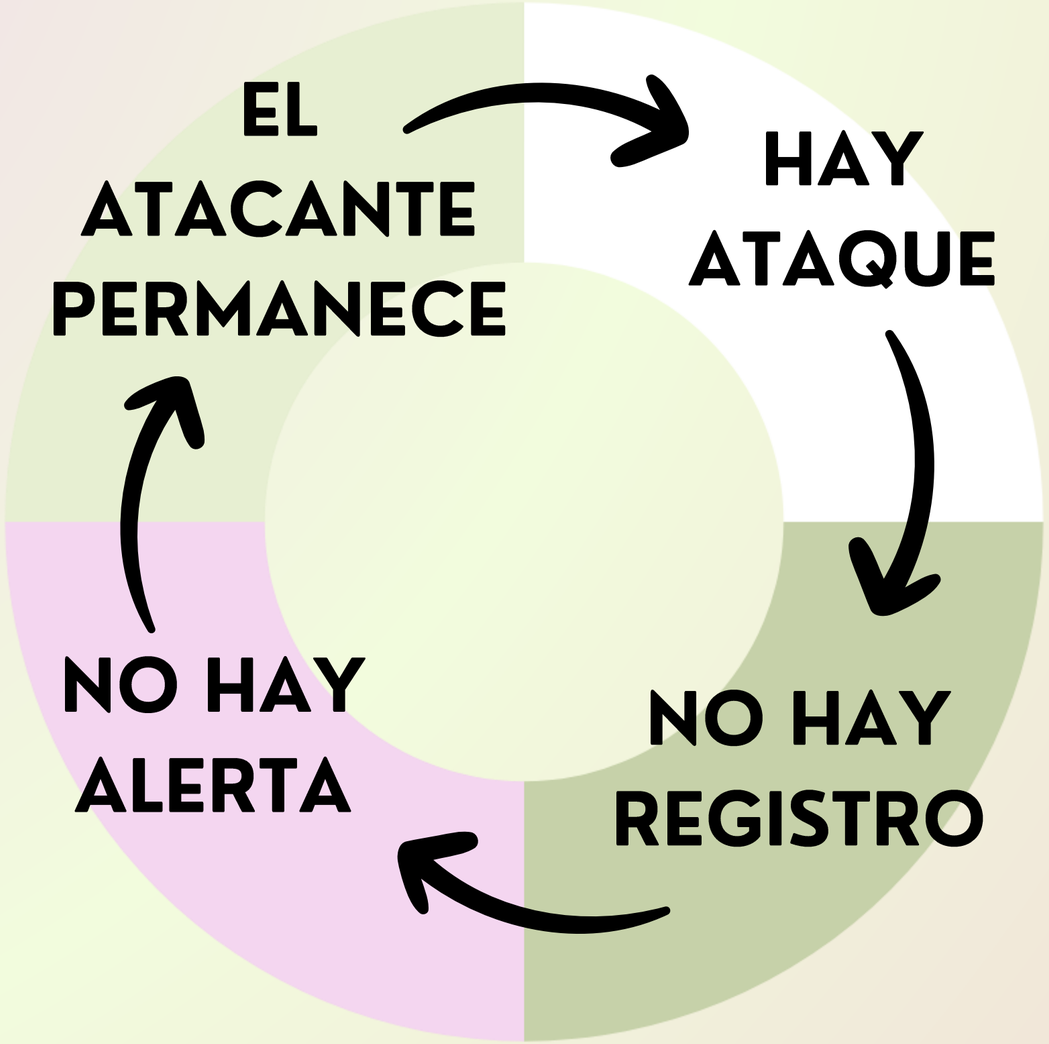
VULNERABILIDAD EN LA AP. FIJNAL

Login Silencioso: Si validarUsuario falla y simplemente redirige al login con un error, no queda constancia de quién intentó entrar.

Excepciones en el catch: Muchos bloques try-catch están vacíos o solo imprimen el error en pantalla, pero no lo guardan en un archivo persistente.

Manipulación de Datos: Si un usuario cambia el nombre de un departamento o lo borra, no sabemos quién hizo el cambio si no hay un log de "auditoría".

CIRCULO DE LA CEGUERA



CONCLUSIÓN

Un sistema seguro no es el que no recibe ataques, sino el que es capaz de detectarlos, registrarlos y responder antes de que sea tarde.

Gracias por asistir