CIBERSECTO
SEGURIDAD DIGITAL

// CASO REAL · MÉXICO · MÉXICO 2026

ANÁLISIS DE CASO

La filtración del Poder Judicial de Guanajuato: qué pasó realmente.

Desde el 6 de mayo de 2026 el Sistema Integral de Gestión Operativa (SIGO) del Poder Judicial de Guanajuato presentó fallas atribuidas a un posible ciberataque. Semanas después, un especialista en ciberseguridad expuso una base de datos filtrada de empleados judiciales.

01 — LÍNEA DE TIEMPO CONFIRMADA

6 de mayo, 2026
El sistema SIGO deja de funcionar. Abogados litigantes reportan que no pueden subir documentos ni consultar expedientes de forma electrónica.

Semanas después
La magistrada presidenta Alma Delia Camacho Patlán declara públicamente que la falla no comprometió información sensible ni implicó robo de datos.

Mayo 2026 — versión distinta
El especialista en ciberseguridad Víctor Ruiz difunde la existencia de una base de datos de empleados del Poder Judicial con información altamente sensible ya expuesta.

02 — QUÉ DATOS SE FILTRARON (según el especialista)

DATO 01
Identidad
CURP, RFC, domicilios y teléfonos personales de empleados y funcionarios judiciales.

DATO 02
Laboral
Historial laboral completo dentro del Poder Judicial del estado.

DATO 03
Financiero
Ingresos, bienes, inversiones y adeudos declarados por el personal.

DATO 04
Patrimonial
Declaraciones patrimoniales y fiscales — el tipo de dato más buscado para fraude dirigido.

03 — POR QUÉ ES GRAVE (NO ES SOLO UNA "FALLA TÉCNICA")

⚠ **Guanajuato acumula al menos 7 ciberataques a instituciones de gobierno en menos de un año**, incluyendo la Fiscalía General del Estado (grupo Tekir APT, noviembre 2025).

⚠ **Datos patrimoniales de funcionarios judiciales son un blanco directo para extorsión** — quien conoce bienes, adeudos e ingresos de un juez o funcionario tiene material de presión.

⚠ **La respuesta institucional inicial minimizó el hecho** mientras la evidencia técnica apuntaba a exposición real de datos — un patrón que se repite en incidentes gubernamentales en México.

// REGLA DE ORO

Si trabajas en o con una institución de gobierno, asume que tus datos ya pudieron ser expuestos antes de que te lo confirmen.

Monitorea intentos de phishing dirigido, extorsión o suplantación que usen datos personales tuyos con precisión inusual.