FORENSE CORPORATIVO · INTEGRIDAD DE REGISTROS

UN PROVEEDOR AVISÓ POR ESCRITO DE LA TRAMPA. ESE CORREO ES ORO PROBATORIO.

QUIEN PIDIÓ LA MODIFICACIÓN VA A NEGARLA DESPUÉS: SU ÚNICA VOZ ES EL MENSAJE, SELLADO Y FECHADO

> **TU SISTEMA DE REGISTRO ES TU ACTIVO MÁS ATACABLE: EL CLIENTE QUE QUIERE PAGAR MENOS O FINGIR MÁS TIENE INCENTIVO DIRECTO PARA TOCARLO.**

Doble encargo: autenticar los registros de operación y preservar la advertencia del tercero.

EL PROBLEMA

Una empresa de seguridad privada opera un sistema que registra en tiempo real el número de patrullas activas, su ubicación y los valores de operación — el corazón de su servicio, porque quien paga monitoreo paga por saber dónde están las patrullas.

La empresa detectó que sus registros presumiblemente habían sido alterados, y entonces ocurrió lo que ninguna auditoría habría logrado: un proveedor le escribió advirtiendo que una empresa cliente quería modificar el sistema que ella provee.

LA INTERVENCIÓN

La escena es de manual de ética empresarial: un proveedor tecnológico que recibe del cliente la petición de alterar un sistema de registro y, en lugar de ejecutarla, avisa por escrito a la empresa afectada. Ese correo fue copiado de la bandeja y sellado con su valor de integridad, con las normas de conservación de mensajes de datos y cadena de custodia — porque un correo así debe poder exhibirse con la certeza de que no fue fabricado después.

Sobre los registros de patrullas, el dictamen determinó su autenticidad y disponibilidad para ulterior consulta, con la empresa poseyendo los archivos originales y un procedimiento replicable: cualquier experto puede repetir el análisis y llegar a la misma conclusión.

Con ello, la empresa obtenía las dos piezas para actuar contra quien quiso manipular su servicio: los registros auténticos que mostraban la realidad, y la evidencia documentada de la intención de alterarlos.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.

LA INTEGRIDAD DE LOS DATOS SE AUDITA ANTES DEL INCIDENTE, NO DESPUÉS.

LOS SISTEMAS HONESTOS NO SOLO REGISTRAN BIEN: SE DEFIENDEN CON EVIDENCIA

QUÉ SE LOGRÓ

Gracias al doble peritaje, la empresa quedó en posición de defender su servicio con evidencia: registros de operación autenticados y replicables, y la advertencia del tercero preservada con huella digital desde el día en que llegó.

> **La enseñanza para toda empresa cuya reputación vive en sus registros —monitoreo, rastreo, tiempo, asistencia—: cuando un tercero te avisa por escrito de una trampa, presérvalo con huella el día que llega.**

POR QUÉ DURIVA ES LA MEJOR OPCIÓN

≡

EFICIENCIA

Metodología propia probada en miles de dictámenes, con equipos que trabajan en paralelo sobre la evidencia.

TIEMPO

Respuesta ágil en escenarios de urgencia procesal, con la misma calidad técnica y documentación completa.

18

TRAYECTORIA

Más de 18 años de cómputo forense en México y América Latina. Creador del primer sistema operativo forense latinoamericano, presidente del Consejo Americano de Ciberseguridad y Cómputo Forense, autor de seis libros especializados.

Si su negocio vive de sus registros, su integridad se audita antes del incidente. Somos su aliado digital.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.