FORENSE CORPORATIVO · INVESTIGACIÓN INTERNA

BORRÓ EL ARCHIVO CLAVE ANTES DE ENTREGAR EL EQUIPO. EL SISTEMA GUARDÓ SU FANTASMA.

BORRAR UN ARCHIVO NO BORRA SU HISTORIA: LOS SISTEMAS GUARDAN LOS METADATOS DE LO QUE EXISTIÓ

> **LA PREGUNTA «¿QUIÉN TOCÓ LA BASE DE DATOS?» SOLO TIENE RESPUESTA SI LOS ACCESOS SE DISEÑARON PARA PODER RESPONDERLA.**

Copia forense íntegra y valores de integridad desde el primer acto, en las instalaciones corporativas.

EL PROBLEMA

Una empresa de soluciones tecnológicas enfrentaba una crisis con sus clientes: la migración de un sistema había salido mal, y toda la evidencia apuntaba a un empleado vinculado directamente al proceso. Las preguntas del encargo eran tres y muy concretas: ¿accedió ese empleado a la dirección de las bases de datos sensibles de la empresa y de sus clientes? ¿Con qué medios? ¿Existía en su equipo el archivo clave de la migración, y qué relevancia tenía?

El equipo del empleado quedó a la vista, con copia forense íntegra y valores de integridad desde el primer acto.

LA INTERVENCIÓN

Los registros respondieron la primera pregunta con contundencia: múltiples conexiones desde el equipo a la dirección señalada, realizadas por el canal de administración remota de servidores — no un acceso casual por el navegador: el canal del administrador, con evidencia de interacción directa con las bases de datos.

La segunda respuesta era más inquietante que la pregunta: accesos con privilegios de superusuario —el que todo lo puede — y, agravante técnico de primer orden, las credenciales almacenadas en el llavero del equipo, disponibles para quien usara esa máquina. Y entre los comandos recuperados, dos conductas que ningún manual de seguridad tolera: permisos abiertos a todo el mundo —la forma más burda de saltarse toda protección— y registros del comando de eliminación de archivos.

La tercera pregunta exhibe mejor que ninguna qué es la informática forense: el archivo clave no estaba en el equipo —había sido eliminado— pero el sistema de archivos conserva metadatos que permiten confirmar su existencia anterior. Bajo evidencia científica fue posible determinar que el archivo sí existió, que fue eliminado y que no era recuperable íntegramente: el documento que daba sentido a la migración había sido borrado, pero el sistema, como siempre, llevaba su diario. Junto a ello, un software de transferencia mantenido actualizado —lo que impidió verificar su historial— sugería el movimiento de archivos hacia fuera.

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

NO UNA SOSPECHA:
UN EXPEDIENTE TÉCNICO CON EL QUE ACTUAR.

CONEXIONES DOCUMENTADAS, PRIVILEGIOS MÁXIMOS, PERMISOS ABIERTOS Y EL FANTASMA DEL ARCHIVO, TODO ASENTADO

QUÉ SE LOGRÓ

Gracias al análisis forense, la empresa obtuvo lo que necesitaba para su responsabilidad interna y la confianza de sus clientes: registros irrefutables de las conexiones a las bases sensibles, accesos con privilegios máximos y credenciales guardadas, permisos contrarios a toda práctica y la existencia del archivo eliminado, confirmada científicamente.

> **La enseñanza de higiene corporativa: credenciales de superusuario en llaveros, permisos abiertos y accesos sin diferenciación son el caldo de cultivo de los incidentes que luego nadie puede atribuir.**

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 un archivo clave desapareció de un equipo, su fantasma sigue ahí: se documenta. Somos su aliado digital.

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