AUDITORÍA DE CORREO · IMPARCIALIDAD PERICIAL

EL CLIENTE ESPERABA UN CULPABLE. EL DICTAMEN ENTREGÓ LA VERDAD: NO LO HABÍA.

UN PERITAJE QUE SOLO SIRVE CUANDO CONFIRMA LA SOSPECHA NO ES UN PERITAJE: ES UNA COTIZACIÓN DE COMPLACENCIA

> **QUE EXISTA EL OTORGAMIENTO DE UN PERMISO NO DEMUESTRA, POR SÍ SOLO, QUE EL PERMISO SE HAYA USADO.**

Decenas de miles de registros de auditoría analizados, con las limitaciones documentadas.

EL PROBLEMA

Una firma financiera llegó con una sospecha que le quitaba el sueño: el administrador de su correo corporativo —la persona con las llaves de todos los buzones— podía estar leyendo los mensajes de las cuentas más sensibles: crédito, inversión, recursos humanos.

El encargo era un reporte detallado de la actividad administrativa: ¿accedía a cuentas del dominio? ¿A cuáles? ¿Podía eliminar mensajes? El cliente esperaba un culpable. El dictamen entregó otra cosa, y ahí está su valor.

LA INTERVENCIÓN

El vector de investigación era claro: los registros de auditoría de la plataforma. Primer episodio revelador: para la cuenta asignada, los accesos a los registros fueron deshabilitados — y en lugar de escalar el conflicto, que habría alertado al personal bajo sospecha, se optó por exportar la totalidad de los eventos de todas las cuentas del dominio: decenas de miles de registros de actividad, meses de operación.

Sobre ese océano se aplicó el filtro que responde a la pregunta del millón: la instrucción con la que un administrador se otorga acceso al buzón de otro. Los eventos aparecieron, y aquí la precisión de honestidad técnica: otorgar un permiso no demuestra que se haya usado. Al interpretar el detalle, el panorama quedó claro — el administrador podía acceder a varios buzones sensibles del dominio, corroborado por un segundo método independiente.

Después, los alias —ese foco clásico de abuso que desvía correo sin que el titular lo note—: revisados uno por uno, resultaron legítimos y coherentes con la operación. Y la conclusión que define el caso: tras el análisis meticuloso de todos los registros, no se identificaron irregularidades ni acciones malintencionadas del administrador ni de ningún otro empleado. Los permisos existían; el abuso, no.

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

LA PREGUNTA CORRECTA NO ES «¿CONFIAMOS EN ÉL?» SINO «¿CADA CUÁNTO REVISAMOS A QUÉ BUZONES PUEDE ENTRAR?».

LA DIFERENCIA ENTRE LA PARANOIA Y LA CERTEZA ES, SIMPLEMENTE, LEER LOS REGISTROS

QUÉ SE LOGRÓ

Gracias a la auditoría completa, la firma obtuvo certeza en su investigación interna: el mapa exacto de permisos del administrador, la legitimidad de los alias y la conclusión documentada de que no hubo acceso indebido — con recomendaciones de verificación periódica.

> **La enseñanza corporativa: el poder de un administrador de correo es absoluto en la práctica si nadie audita los permisos. Los registros estaban ahí desde el primer día.**

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 duda de su administrador de correo, audite los registros: la respuesta puede ser inocente. Somos su aliado digital.