El hacker no destruyó su evidencia. Su propio personal lo hizo.

Probablemente actuando de buena fe.

21 septiembre de 2026 | Lectura: 4 min | 1032 palabras

▶ ESCUCHAR · 8 MIN

FORENSIA DIGITAL

El hacker no destruyó su evidencia. Su propio personal lo hizo.

Probablemente actuando de buena fe. Precisamente por eso, el caso podría ya no ser defendible ante un tribunal.

Cuando la buena fe debilita la evidencia

Viernes por la mañana. El gerente de Finanzas detecta tres transferencias bancarias que no corresponden. El VP de Finanzas llama al departamento de TI. TI hace exactamente lo que un equipo competente de tecnología está capacitado para hacer: contener el problema y comprenderlo rápidamente. Durante el almuerzo, un técnico de soporte ingresa a la computadora del empleado con una cuenta compartida de administrador, revisa los mensajes entrantes y salientes, copia las carpetas relevantes en una memoria USB ya utilizada y que contenía otros archivos y reinicia la computadora, que había estado comportándose de forma extraña.

Esa misma tarde, el empleado presenta su renuncia con efecto inmediato.

Para el lunes, la Administración tiene una idea clara de lo ocurrido. Llama a sus abogados externos, quienes formulan una pregunta: ¿quién accedió a esa computadora, cuándo lo hizo y se puede demostrar que nada fue alterado después?

Nadie puede responder. Cuatro técnicos de soporte utilizan la misma cuenta de administrador. La copia en la memoria USB tiene nuevas marcas de tiempo, no las originales. El reinicio de la computadora borró la memoria volátil y pudo haber provocado la rotación de registros que habrían ayudado a reconstruir la actividad del exempleado. La organización puede comprender el incidente, pero su capacidad para demostrar lo ocurrido se ha debilitado seriamente.

Nadie actuó de mala fe. Cada acción buscaba ayudar. Sin embargo, cada una alteró o eliminó evidencia digital potencial y debilitó la capacidad de la organización para defender el caso.

RISCCO

¿Qué es realmente la forensia digital?

Los equipos de tecnología están capacitados para restablecer las operaciones y resolver incidentes. Un perito informático tiene una responsabilidad diferente: preservar y reconstruir la evidencia digital para que pueda resistir el escrutinio ante un tribunal.

La forensia digital determina qué ocurrió de una manera que pueda sostenerse cuando alguien interesado en desacreditar la conclusión examine cada paso. Requiere adquirir los datos sin modificar la fuente, utilizar verificación criptográfica para demostrar la integridad de las copias forenses y documentar quién manejó la evidencia, cuándo, cómo y bajo qué autoridad.

Una investigación pregunta qué ocurrió. La forensia pregunta qué puede todavía demostrarse seis meses después, ante un juez o tribunal arbitral que no presenció los hechos.

Realidad, no ciencia ficción

Muchas organizaciones relacionan la forensia digital únicamente con ciberataques dramáticos. Las situaciones que suelen requerirla son, con frecuencia, menos cinematográficas:

- Un ejecutivo se va a un competidor llevándose archivos confidenciales que contienen la estrategia de expansión de la organización.
- Un empleado altera el archivo de pago de planilla antes de enviarlo al banco para su procesamiento.
- Un proveedor extranjero acuerda por correo electrónico saldar pagos vencidos adeudados a una empresa local. No se firma una adenda contractual y la correspondencia electrónica, único registro del acuerdo, posteriormente se elimina deliberadamente.

Estas situaciones comparten una misma condición: la evidencia digital puede ser sometida posteriormente a examen en un litigio, arbitraje, investigación interna o proceso regulatorio. El estándar se establece desde el momento en que la evidencia se identifica y recopila por primera vez. No puede aplicarse retroactivamente.

En la experiencia de RISCCO apoyando a abogados en casos con evidencia digital, algunas de las decisiones más perjudiciales ocurren antes de que los abogados o el perito informático reciban la primera llamada. Entre el incidente y la llegada del perito, personas bien intencionadas pueden alterar la evidencia mientras intentan comprender o contener el problema.

La excelencia técnica no equivale a experiencia forense

Un buen auditor de sistemas, especialista en ciberseguridad, administrador de bases de datos o gerente de TI puede tener una gran capacidad técnica, pero eso no lo convierte automáticamente en perito informático ni en testigo experto.

La diferencia no radica únicamente en la profundidad técnica. También exige disciplina para preservar la evidencia, demostrar su integridad, distinguir los hechos de la interpretación, documentar cada acción relevante y explicar las conclusiones a personas sin formación técnica.

El informe pericial escrito es donde un trabajo técnicamente sólido puede fracasar. Debe ser lo suficientemente preciso para resistir el escrutinio y suficientemente claro para que un abogado, fiscal, juez o árbitro comprenda qué ocurrió, cuándo y cómo.

Tenga presente lo que ninguna certificación puede proporcionar por sí sola: defender el informe mientras los abogados de la contraparte cuestionan la metodología, las herramientas, los tiempos, la cadena de custodia e incluso si el perito pudo haber manipulado la evidencia. Las preguntas están diseñadas para generar presión. La serenidad, claridad y criterio profesional necesarios se adquieren bajo esa presión con la experiencia.

¿Por qué RISCCO?

RISCCO hace más que determinar qué ocurrió. Preservamos lo que todavía puede demostrarse.

Desde hace más de ocho años, firmas de abogados y organizaciones recurren a RISCCO cuando una controversia, investigación o arbitraje depende de comprender, preservar y defender evidencia digital. Trabajamos junto con los abogados desde las primeras horas críticas hasta el análisis forense, la elaboración del informe pericial y su sustentación.

Nuestra capacidad en forensia digital se sustenta en la misma experiencia que RISCCO aplica al riesgo de TI, ciberseguridad, privacidad de datos, auditoría de sistemas y analítica de datos. Por ello, nuestros peritos comprenden no solo el dispositivo o la imagen forense, sino también el entorno de control, los sistemas y procesos de negocio relacionados con la evidencia.

- Decenas de investigaciones de forensia digital e informes periciales relacionados con delitos informáticos, fraude e incidentes de seguridad, incluidos casos presentados ante autoridades judiciales y tribunales arbitrales internacionales.

- Colaboración habitual con abogados externos, respaldada por una firma con 17 años de experiencia atendiendo a más de 200 organizaciones en Centroamérica y el Caribe.

En Panamá, RISCCO realiza investigaciones de forensia digital y aporta peritos informáticos idóneos. En otras jurisdicciones, podemos asesorar a los abogados y apoyar a peritos con idoneidad local mediante análisis forense, metodología, revisión técnica y preparación de hallazgos, sujeto a los requisitos de cada país.

Si un incidente digital puede convertirse en una controversia, investigación o reclamación, preserve primero e investigue después. La evidencia digital defendible determina lo que usted puede demostrar.

Ahí es donde RISCCO marca la diferencia.

CONTACTE A RISCCO

Panamá, Centroamérica y el Caribe

Antonio Ayala I.
CEO
aayala@riscco.com

Marinelda Morales
Gerente de Ventas
mmorales@riscco.com

República Dominicana y Puerto Rico

Eury Valdez
Asesor Comercial
efvaldez@riscco.com

El Salvador, Guatemala, Honduras, Costa Rica y Nicaragua

Jeniffer Escoto
Asesor Comercial
jescoto@riscco.com

Acerca de RISCCO

RISCCO es una firma internacional independiente de consultoría comprometida con transformar la forma en que las organizaciones gestionan el riesgo y adoptan la Inteligencia Artificial. Combinamos un enfoque riguroso de GRC (Gobierno, Riesgo y Cumplimiento) con analítica avanzada de datos e Inteligencia Artificial para ayudar a nuestros clientes a anticipar riesgos, fortalecer su gobierno y resolver desafíos complejos. Con sede en Panamá y presencia en seis países, en 2026 cumplimos 17 años atendiendo a más de 200 organizaciones líderes en Centroamérica y el Caribe.

Rigor internacional. Ejecución ágil. Impacto medible.
Pensamos como estrategas. Ejecutamos como especialistas.

riscco.com