Deloitte.

Investigaciones de fraude: reflexiones sobre el rol del perito

25 Fórum del Auditor Profesional

Sitges, 9 de julio de 2015

1. El proceso de investigación: algo más que un dictamen pericial económico/contable

Principios generales de una investigación de fraude

Principios básicos a considerar

	Principios a considerar
#1	• Custodia de la información
#2	• Salvaguarda de los derechos de los trabajadores
#3	• Retroalimentación y consecuencias legales

Principios generales de una investigación de fraude

1- Custodia de la información

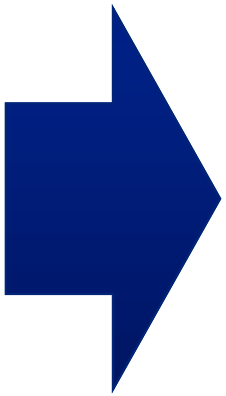
- Una correcta custodia de la información protege la integridad de las pruebas y facilita su admisión como evidencia en caso de un proceso judicial.
- Es importante documentar las cesiones temporales de las pruebas incluyendo la firma de los que las entregan y las reciben.

Información en formato electrónico:

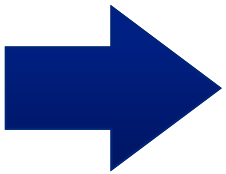
PC, teléfono móvil, servidor, dispositivo de almacenamiento externo, etc.

Información en formato documental

Información del equipo de investigación



- ¿Dónde se encuentra la información a custodiar?
- ¿Quién tiene acceso a ella?
- ¿Dónde va a quedar conservada?
- ¿Qué medidas se van a tomar para su preservación? (Almacenamiento bajo llave, precintado…)



- ¿Quién va a responsabilizarse de la información custodiada?
- ¿Cómo se garantiza la integridad y confidencialidad de la información?

Principios generales de una investigación de fraude

2- Salvaguarda de los derechos de los trabajadores

- Posibilidad de contar con asesores externos.
- Informar al comité de empresa y/o al responsable de los trabajadores.
- Tener en cuenta la política de privacidad (LOPD, procedimiento de acceso al contenido de los dispositivos electrónicos, cámaras de seguridad y registros de entrada/salida, etc.).

Principios generales de una investigación de fraude

3- Retroalimentación y consecuencias legales

- La evolución de la investigación y los hechos y circunstancias que se vayan poniendo de manifiesto pueden llevar a realizar nuevos procedimientos de investigación al objeto de alcanzar los objetivos establecidos.
- En función de las pruebas y de los resultados obtenidos en el curso de la investigación se determinará el alcance de las posibles consecuencias legales: sanción disciplinaria, despido, procedimiento judicial civil y/o penal.
- Necesaria participación del asesor legal.

¿Cómo actuar frente al fraude?

Fases de actuación

Fases típicas de un Plan de acción contra el fraude

1. Recepción de la sospecha y clasificación
2. Análisis y planificación
3. Investigación
4. Resultado y toma de decisiones
5. Puntos de mejora

¿Cómo actuar frente al fraude?

Análisis y planificación

Actividades críticas	Procedimientos
Preservar y asegurar la evidencia	• Custodiar la información antes de efectuar acciones de investigación o realizar comunicaciones a los afectados. • Mantener la integridad de los registros informáticos de los afectados. • Obtención previa de registros físicos e informáticos que puedan ser relevantes para sustentar la evidencia.
Confidencialidad	• Dentro de la organización (interna). • Hacia los clientes, proveedores, medios (externa).
Definir los Procedimientos de investigación	• Definición de procedimientos y de los recursos para su ejecución. • Existencia de una política que permita el acceso al disco duro de los ordenadores corporativos. • Sustitución de elementos críticos para asegurar la normal actividad de la sociedad. • En función de la evolución de los resultados, pueden detectarse necesidades que deberán ser cubiertas a través de nuevos procedimientos de investigación.

¿Cómo actuar frente al fraude?

Técnicas de investigación

Técnicas de investigación	Descripción
Entrevistas	• Metodología PEACE (Preparación, Explicación, Adquisición de la información, Conclusión y Evaluación).
Financiera	• Análisis por áreas de riesgo.
Análisis de datos	• Obtención de evidencias de fraude a partir del análisis masivo de información electrónica de naturaleza contable, financiera o de gestión.
Business/Corporate Intelligence	• Búsquedas de información de personas físicas y jurídicas que permitan identificar vinculaciones personales y societarias.
Análisis de documentación	• Revisión de facturas, documentación bancaria y gastos personales.
Análisis de ordenadores	• Imagen y análisis forense de los dispositivos electrónicos. eDiscovery.

¿Cómo actuar frente al fraude?

Resultado y toma de decisiones

Resultados de la Investigación

- **Pruebas insuficientes**
- **Infracciones dentro de la relación laboral**
- **Infracciones que son constitutivas de delito**

Toma de decisiones

- **Archivo del caso**
- **Sanción disciplinaria / despido**
- **Proceso civil / penal**
- **Comunicación a las Autoridades Públicas y/o los medios**

→ **Dependiendo de la acción que se decida, los resultados serán plasmados en distintos documentos: Nota de Trabajo, Informe Interno y/o Informe Pericial**

2. La evidencia digital: ventajas, riesgos y requisitos

La evidencia digital
Contexto

- Hoy en día, todos los negocios necesitan de un acceso eficiente a información de calidad.
- Prácticamente toda la información que se crea es electrónica. (Casi el 90% nunca se imprime.)
- Las empresas, en un país como EEUU, generan anualmente 1 trillón de nuevos documentos electrónicos.
- Los correos electrónicos de un solo individuo pueden llegar a suponer unas 250.000 páginas impresas.
- El análisis de la información gestionada por 10 personas puede generar la necesidad de recopilar y revisar unos 2,5 millones de páginas.
- En casi todos los análisis, es tan necesaria la información electrónica como los documentos impresos “tradicionales”.
- En términos de seguridad, practicidad o coste/eficiencia, **no es aceptable la revisión manual** de toda esta información.

La evidencia digital

Evidencia digital y prueba electrónica

En el entorno descrito anteriormente, obtener evidencia digital se traduce en poner en marcha todo un entorno de control digital que permita el acceso eficaz y fiable a información útil en distintos contextos:

- Auditorías interna y externa. Obtener y proporcionar evidencia de auditoría, cada vez más se traduce en disponer en tiempo y forma a información en formato electrónico.
- Exigencias normativas. Atender a peticiones de información de la Administración o de algún regulador (CNMV, CNMC, Banco de España, etc.) exige cada vez en mayor medida disponer de los medios que expliquen y justifiquen la validez de la información aportada.
- Investigaciones internas. En aquellos casos en los que sea necesario investigar acciones potencialmente irregulares o que estén causando un perjuicio a la compañía, será vital actuar con eficacia y eficiencia.
- Disputas y acciones judiciales. Cuando cualquiera de las situaciones anteriores, o un conflicto con un tercero, puedan acabar requiriendo de la aportación de la información como prueba en un juicio hablaremos de prueba electrónica.

La evidencia digital. Retos en la obtención

¿Qué es necesario tener en cuenta?

- Cada vez existe un número mayor de fuentes de información: ERP, CRM, BI, terminales de usuario (PC, tablets, smartphones), correo electrónico, información en la nube, etc.
  - Las técnicas de extracción y análisis de información varían en función del tipo de sistema, y cada vez más exigen un conocimiento técnico del funcionamiento y características de dichos sistemas.
- La recopilación de la información, para que pueda considerarse evidencia, debe aportar garantías sobre tres aspectos: autenticidad, integridad y disponibilidad.
  - **Autenticidad**: cadena de custodia, documentación del procedimiento, fedatario público
  - **Integridad**: precintado digital, resumen digital o *hash*
  - **Disponibilidad**: posibilidad de acceso y a que se pueda replicar el análisis en las mismas condiciones

La evidencia digital. Expectativas razonables de privacidad

Best Practices: implantación de políticas de uso de los S.I.

- Relacionado con el respeto del derecho a la intimidad, es necesario establecer claramente a los usuarios cuales son las expectativas razonables de privacidad o confidencialidad en los medios informáticos que la empresa pone a su disposición. Existe un rango de madurez en el grado de implantación de estas políticas:

(i) Nivel bajo de implantación.

Nos referimos a aquellas compañías cuya dirección tiene claras las conductas admisibles y las reprobables o constitutivas de actividad irregular, pero no disponen de los medios de notificación ni evaluación del grado de cumplimiento. En estos casos la justificación de una investigación tiene que ir muy vinculada a la proporcionalidad de la gravedad de los hechos objeto de sospecha.

(ii) Nivel medio de implantación.

En estos casos nos referimos a aquellas compañías que contemplan en sus manuales y políticas una referencia expresa al uso de los sistemas de información. En este escenario únicamente se confía en que la campaña de comunicación es suficiente para que los empleados la respeten, y en todo caso para que en caso de que se produzca un incidente se cuente con el respaldo suficiente para llevar a cabo una investigación.

(iii) Nivel alto de implantación.

En los casos en los que encontramos un mayor grado de concienciación sobre la necesidad de que exista una política relativa al uso de los sistemas de información, las compañías disponen de un medio de comunicación, y un seguimiento del grado de conocimiento por parte de los empleados. Idealmente, además existen los mecanismos para verificar periódicamente el grado de cumplimiento de las políticas y de las restricciones de uso que se establezcan sobre el uso de los sistemas.

La evidencia digital. Ventajas

Volumen de información: reto y oportunidad

A pesar de que su obtención y tratamiento requieren un conocimiento técnico especializado y el manejo de herramientas forenses específicas, existe un gran número de ventajas que hace atractivo el uso de evidencias digitales para mejorar el entorno de control de la compañía:

- Constituye una prueba objetiva y repetible de hechos que no pueden ser demostrados de otra manera.
- Aumenta la confiabilidad en la información aportada, mediante la comprobación de la consistencia entre distintos repositorios de datos.
- Permite combinar en el análisis fuentes de información interna y externa de la compañía.
- Tiene una faceta de prevención y disuasión contra el fraude si el análisis se realiza de manera periódica sobre los sistemas de información de la sociedad.
- Contribuye a mejorar el nivel de protección de los activos de la compañía, mediante la identificación de posibles insuficiencias de control que hayan sido aprovechadas por un usuario.

La evidencia digital. Requisitos

Localizar información clave mediante la palanca de la tecnología

La evidencia digital. Requisitos

Localizar información clave mediante la palanca de la tecnología

- El modelo anterior puede adaptarse internamente a cada compañía, o se puede contar con el soporte de un tercero que gestione desde el primer instante cada situación de crisis o incidente que requiera recopilar, preservar y analizar evidencias digitales.
- En cualquier caso, esta generación de evidencia exigirá:
  - Disponer de un cuerpo de técnicos que sean capaces de identificar el perímetro de actuación dentro de todo el mapa de sistemas de información de la compañía.
  - Disponer de una metodología y entrenamiento específicos sobre el seguimiento de la cadena de custodia de la información gestionada.
  - Disponer y manejar software forense específico que permita garantizar la integridad de la evidencia obtenida.
  - Disponer y manejar software forense específico que permita analizar y buscar toda aquella información de índole profesional relacionada con los hechos que se investiguen.
  - Documentar de manera rigurosa y exhaustiva el procedimiento de localización y selección de toda aquella información que se aporte.

La evidencia digital. Prueba electrónica

Cautelas adicionales para garantizar la admisibilidad de la prueba

- **Jurisprudencia**. Han existido en distintos órdenes jurisdiccionales diferentes interpretaciones sobre las posibilidades de obtención y análisis de la prueba electrónica. Sin embargo, la sentencia del Tribunal Constitucional de 7 de octubre de 2013 señala los dos puntos clave para admitir el análisis de los ordenadores, y de manera aún más específica el análisis del correo electrónico:
  - Respeto del **derecho a la intimidad**. Para lo cual es necesario analizar las expectativas razonables de privacidad o confidencialidad del usuario. Asimismo, es necesario justificar la proporcionalidad de los procedimientos llevados a cabo en el análisis, y en la obtención de los resultados.
  - Respeto del **secreto de las comunicaciones**. El cual tutela únicamente el proceso de comunicación, pero no el mensaje en sí mismo.

La evidencia digital. Prueba electrónica

Cautelas adicionales para garantizar la admisibilidad de la prueba

- **Sentencia del Tribunal Superior de Justicia de Madrid de 30 de octubre de 2009. Derecho a la intimidad en relación con los medios informáticos aportados por el empresario.**

La cuestión que se plantea en esta sentencia es la calificación del despido de una trabajadora que trabaja como secretaria y que accede sin tener autorización a correos personales del Director General de la Compañía.

Tras pedirle dos veces la copia del disco duro de su ordenador y negarse, se realiza en presencia notarial una imagen forense del disco duro del ordenador de la trabajadora por parte de una entidad especializada. El resultado es que se confirma que está accediendo a los mensajes del Director General y, en consecuencia, se la despide.

El TSJ de Madrid concluye que el registro del ordenador es lícito porque el ordenador es un instrumento de producción del que es titular el empresario y éste tiene facultades de control de la utilización que incluyen lógicamente su examen. Dicho esto, el TSJ entiende que el despido es procedente porque se ha producido una trasgresión de la buena fe contractual y un abuso de confianza, ya que el comportamiento de la trabajadora constituye un grave quebrantamiento de los deberes de lealtad y fidelidad que impregnan la relación de trabajo.

empresarial que la ley vincula a la defensa de su patrimonio o del patrimonio de otros trabajadores de la empresa. Por el contrario, cuando se trata de medidas de control sobre los **medios informáticos** puestos a disposición de los trabajadores forman parte del poder de dirección ordinario: el ordenador es un instrumento de producción del que es titular el empresario y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del art. 18 ET, pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del art. 20 ET para entrar dentro de la esfera personal del trabajador.

La evidencia digital. Prueba electrónica

Cautelas adicionales para garantizar la admisibilidad de la prueba

Un juez ava
directivos s

• Exculpado del 'caso Pi
ordenadores de altos

Un juez de Barcelona ha concluido que es legal rastrear el correo electrónico de un directivo si hay sospechas de que es desleal con la empresa. El magistrado ha exculpado al informático Matías Bevilacqua, un excolaborador del CNI que estaba imputado por revelación de secretos en el *caso Pitiusa*, una red de espionaje masivo en la que están implicados detectives, funcionarios y empresarios de toda España y que sigue en fase de investigación.

Los responsables de grandes empresas como Unilever, Dupont Ibérica y Mutua Universal contrataron los servicios de la detective Sara Dionisio para averiguar si algunos de sus directivos desviaron información o dieron trato de favor a proveedores. La investigadora privada contó para esa tarea con Bevilacqua, experto en encriptación de datos al que Iñaki Urdangarin contrató para hurgar en los correos de los discos duros del instituto Nóos.

El juez da la razón al despacho de Fermín Morales, que defiende a Bevilacqua, y concluye que el informático no vulneró el derecho a la intimidad de los directivos. Cree que el acceso a sus ordenadores corporativos fue "lícito". El ingeniero realizó una "búsqueda ciega" sobre la actividad empresarial, pero no rastreó "datos de la vida íntima" de los directivos. La empresa les investigó ante unas sospechas que resultaron ser ciertas: en dos casos, los directivos fueron despedidos y sus despidos fueron considerados procedentes.

Si desea información adicional, por favor, visite www.deloitte.es