PERITAJE INFORMÁTICO, ANÁLISIS FORENSE DIGITAL Y RESPUESTA A INCIDENTES

INFORMATION TECHNOLOGIES EXPERTISE, DIGITAL FORENSIC AND INCIDENT RESPONSE

Autores:

Javier Rubio Alamillo. Colegio Profesional de Ingenieros Técnicos en Informática de la Comunidad de Madrid. info@peritoinformaticocolegiado.es ORCID 0000-0003-4693-6114

Carlos de Manuel Clemente. Colegio Oficial de Ingenieros Técnicos en Informática de Castilla-La Mancha. carlos.demanuel@coiticlm.es ORCID 0000-0002-6049-356X

Resumen:

En este artículo se reflexiona sobre la importancia de la actividad del peritaje informático realizada por titulados que, dada la complejidad de los asuntos objeto de estudio, requieren de profesionales cuyas competencias son adquiridas durante su etapa de formación universitaria y cuya actividad se necesita del apoyo de la organización profesional que le dota de formación posgrado, control y garantías.

Abstract:

This article reflects on the importance of the activity of information technologies expertise carried out by graduates who, given the complexity of the matters under study, require professionals whose skills are acquired during their university training and whose activity needs the support of the professional organization that provides them with postgraduate training, control and guarantees.

Palabras clave:

Peritaje informático; Análisis forense digital; Colegio Profesional

Keywords:

Computer Expertise; Digital Forensic; Professional Association

Indiscutiblemente, nuestra sociedad tiene como base industrial y cultural la información y su tratamiento automatizado a través de nuevas tecnologías basadas en programas informáticos y ordenadores. La Ingeniería Informática hoy en día nos permite, mediante el uso de principios científicos, las matemáticas y el ingenio humano, el desarrollo de soluciones que nos permiten realizar una explotación a gran escala de los datos y la información como elementos clave de nuestra sociedad. Igualmente nos proporciona una capacidad productiva asociada al control de máquinas y procesos mediante sistemas informáticos que nos permiten ser más eficientes y exactos en la mayor parte de los procesos productivos.

No cabe duda de la importancia de la Ingeniería Informática y de sus profesionales hoy en día. La llegada de la pandemia mundial de la COVID-19 lo puso en clara evidencia y vino a destacar las ventajas y desventajas competitivas de instituciones y organizaciones de todo tipo con respecto a su madurez tecnológica. Así, en los últimos tiempos, nuevas profesiones como la del perito informático se han convertido en una disciplina trasversal en todos los ámbitos de la sociedad. El delito informático, la prueba digital, el perito y su dictamen son cada vez más relevantes en nuestra sociedad informatizada. De aquí nace la necesidad de la actividad de peritaje informático y la del profesional perito informático que actúa como experto en la materia y que la Justicia usa como auxiliar confiable obligado a ejercer su función con el máximo rigor.

Los Colegios Profesionales han identificado la actividad y la salida profesional para sus miembros como esencial para esta sociedad, y así se mantienen y promocionan activades formativas que tratan de proporcionar la formación y la adquisición de competencias necesarias para la adecuada ejecución de estos trabajos profesionales. Los egresados universitarios de la Ingeniería Informática aparecen en el mundo laboral con las competencias estipuladas en la Resolución de 8 de junio de 2009, de la Secretaría

General de Universidades [1] donde se establecieron las recomendaciones para la propuesta por las universidades de memorias de solicitud de títulos oficiales en el ámbito de la Ingeniería Informática. Estas competencias adquiridas mediante su formación universitaria dotan al profesional del cimiento imprescindible para su desarrollo profesional y, por tanto, lo capacitan para ejercer como profesional experto en Ingeniería Informática. La formación en la actividad del peritaje informática ofertada por el Colegio Profesional viene a capacitar al egresado universitario para su desarrollo como experto, como perito informático.

El profesional que asume esta trayectoria realiza un ejercicio libre de la profesión de gran responsabilidad personal que, en algunas regiones como Castilla-La Mancha, requiere la colegiación obligatoria (Ley 5/2002, de 11 de abril, de las Cortes de Castilla-La Mancha, de creación del Colegio Oficial de Ingenieros Técnicos en Informática de Castilla-La Mancha[2] y la Ley 6/2002, 11 de abril, de las Cortes de Castilla-La Mancha, de creación del Colegio Oficial de Ingenieros en Informática de Castilla-La Mancha[3]), siendo el colegio un garante de la actividad realizada por el profesional para la sociedad a la que sirve, de acuerdo con el artículo 20.a de la Ley 10/1999, de 26 de mayo, de Creación de Colegios Profesionales de Castilla-La Mancha[4].

Una sociedad de la información cada vez más compleja es totalmente dependiente de la Ingeniería Informática y de sus profesionales. De esta forma el peritaje informático adquiere gran relevancia, en especial en lo que se refiere al uso por parte del sistema judicial, quien, como ocurre en otras especialidades, requiere el concurso profesional e imparcial de expertos en la materia que, por otra parte no menos importante, requieren de un conocimiento particular de los procedimientos y los entresijos del sistema judicial. Ello nos obliga a que el profesional adquiera una serie de conocimientos y competencias

[1] Resolución de 8 de junio de 2009, de la Secretaría General de Universidades, por la que se da publicidad al Acuerdo del Consejo de Universidades, por el que se establecen recomendaciones para la propuesta por las universidades de memorias de solicitud de títulos oficiales en los ámbitos de la Ingeniería Informática, Ingeniería Técnica Informática e Ingeniería Química. Disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2009-12977

[2] Disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2002-10341

[3] Disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2002-1034

[4] Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-1999-16379

específicos respecto al ejercicio del peritaje, en concreto cuando la autoridad judicial puede valorar especialmente la titulación oficial y la colegiación del profesional como garantías del Estado y de las entidades profesionales con respecto a sus competencias y garantía profesional.

El perito informático deberá usar una serie de procedimientos y técnicas que le permitan identificar, recopilar, preservar y analizar evidencias de tipo informático. Este proceso, en el que el perito usa sus conocimientos y diferentes herramientas forenses a su alcance dará como resultado la prueba informática aceptable en un procedimiento judicial. Como se puede observar, tan importante es el conocimiento específico del experto en la materia como su saber hacer como experto forense.

Unida a la informática forense, tenemos otra actividad conocida como respuesta ante incidentes que da lugar a la disciplina de análisis forense digital y respuesta a incidentes: *Digital Forensic & Incident Response* (DFIR). En el ámbito de DFIR, se pretende dar una respuesta rápida a un incidente de seguridad, mientras que el peritaje informático tiene como objetivo la conversión de evidencias en pruebas que puedan formar parte de un procedimiento judicial. Por supuesto, ambas actividades comparten el análisis forense cómo disciplina central, aunque con sustanciales diferencias en su forma de proceder respecto al fin que buscan.

DFIR pretende determinar el origen y alcance de un incidente de seguridad estableciendo mejoras que eviten la repetición del problema. Los incidentes de seguridad pueden afectar gravemente a la organización, por ejemplo, impactando gravemente a la protección de datos de carácter personal con posibles graves consecuencias económicas y, por supuesto, un gran perjuicio reputacional. Descubierto un incidente de seguridad, las organizaciones procederán, en base a su política de seguridad, con objeto de intentar atajarlo en primer lugar y procediendo de forma paralela o en segunda instancia para descubrir su origen y disponer de contramedidas que eviten su repetición. Este proceso de análisis y resolución se produce en vivo sobre los mismos sistemas afectados por el incidente, por lo que se presume una alta probabilidad de que las evidencias queden

contaminadas por la actuación de los analistas de seguridad, lo que posteriormente perjudica su conversión en prueba admisible en procedimiento judicial. Claramente el objetivo de DFIR es atajar el incidente de seguridad priorizando su resolución frente a una posible judicialización de este. La organización afectada debe ser consciente de que, una vez resuelto el problema y determinado su origen, es muy posible que las evidencias no puedan devenir a prueba que acompañe una posible denuncia ante los tribunales de justicia. La parte denunciada, si es que se pudiera llegar a determinar un posible responsable criminal del incidente (por ejemplo, pensemos en una empresa que ataca informáticamente a un competidor), mediante dictamen de un perito informático colegiado, siempre podrá alegar en su defensa la contaminación de las evidencias durante los procesos de resolución del incidente.

En el caso del peritaje informático, éste no pretende generalmente atajar un incidente de seguridad. Su objetivo es básicamente la conversión de evidencias en pruebas. La actuación del profesional perito informático, que deberá trabajar con procedimientos estandarizados de identificación, adquisición y análisis de las evidencias, se convierte en fundamental, pudiendo certificar que la prueba no ha sido alterada y que se ha producido una correcta cadena de custodia. La preservación de la evidencia frente a su contaminación obliga al perito a que la adquisición de la evidencia se realice ante un fedatario público, como puede ser un notario o secretario judicial, quienes deberán, en cada caso, levantar actas o diligencias de las acciones realizadas por el perito con anotación de las huellas digitales obtenidas de las evidencias originales. Finalmente, el perito realizará un análisis forense de las evidencias digitales volcadas, buscando la constitución de la prueba. Dicho análisis podrá determinar orígenes y causas de un incidente de seguridad, lo que deberá ser manifestado en un dictamen pericial que podrá ser ratificado ante una autoridad judicial.

Pese a compartir una fase de análisis forense, se exhiben notables diferencias entre el trabajo realizado ante la respuesta a un incidente y el realizado en un peritaje informático. En la respuesta a un incidente de seguridad, se trabajará sobre sistemas en vivo y, por tanto, en pleno funcionamiento, priorizando la rapidez en encontrar el origen del problema

y su posible solución. Así, la actuación sobre dichos sistemas, aun usando las mejores herramientas, no puede garantizar el mantenimiento de la cadena de custodia porque no se podrá tener la certeza absoluta de que, al trabajar sobre pruebas en vivo (sistemas informáticos en funcionamiento), éstos no queden contaminados por el trabajo del analista forense en busca del origen y de la solución al incidente.

Las técnicas DFIR son preceptivas cuando pretendemos dar una respuesta rápida a un incidente aplicando una resolución lo antes posible, no deteniendo los sistemas y el negocio de la organización en la medida de lo posible. En dichos casos, la judicialización del problema debe tener en cuenta que las técnicas usadas pueden ser invasivas, provocando la posible anulación de las evidencias.

El peritaje informático es una actividad que se desarrollará sobre sistemas apagados, es decir, que las evidencias se han adquirido o clonado ante fedatario público quien también dejará constancia de las huellas digitales que matemáticamente podrán corroborar el estado de no alteración de las pruebas. El trabajo sobre las evidencias originales rompería la cadena de custodia en el proceso del peritaje y, además, no debemos olvidar que dicha cadena de custodia sólo se garantiza desde el instante en que se calcula la huella digital de la evidencia, siendo obligatoria la certificación de tiempo correspondiente (de lo que se encarga el fedatario, al anotar en la diligencia la fecha en la que se produce el volcado y el cálculo de la huella digital del mismo).

Los sistemas informáticos pueden ser de gran complejidad, la capacidad para clonar evidencias y trabajar con copias idénticas dota al perito de varios elementos clave para realizar un análisis más exhaustivo del problema y realizar el dictamen con la mayor precisión técnica posible. El tiempo y la capacidad de usar clonaciones proporcionan una mayor capacidad del análisis del incidente y de sus consecuencias sobre el sistema.

En conclusión, podemos decir que el peritaje informático, el análisis forense digital y la respuesta a incidentes tienen en común ser actividades excepcionalmente relevantes en un mundo informatizado. Sin embargo, ambas se distinguen por su finalidad y por la forma en cómo los procesos de adquisición deben realizarse para dar cumplimiento a su

finalidad. Respecto a los profesionales, mucho podríamos debatir de la conveniencia o legalidad de la titulación o la colegiación, en cualquier caso, moviéndonos por la razón y el interés de obtener el mejor servicio, siempre deberíamos valorar en mayor medida la adquisición de competencias que nuestros titulados obtienen del sistema educativo universitario, así como de la formación y garantías que los Colegios Profesionales aportan a la sociedad, todo ello muy a pesar de las normativas sobre competencia que, actualmente, más que conseguir para la sociedad un claro beneficio por el control de ésta, vienen a producir un efecto negativo penalizando funciones básicas del colegio oficial en sus facetas de control de la actividad y del profesional.