Crimen, cibercrimen y análisis forense informático

Francisco José de Haro Olmo

I.E.S. Celia Viñas
franciscoj.haro.edu@juntadeandalucia.es

Resumen Tras la publicación en el BOE[1] del Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información con una carga horaria de 720 horas, 43 créditos ECTS y que comienza a impartirse el mes de noviembre del curso 2020-2021, desarrollando los contenidos propuestos para el módulo profesional de Análisis Forense Informático, con un total de 120 horas. Estos contenidos abordan la metodología del análisis forense digital en distintos tipos de plataformas y dispositivos: sistemas informáticos, Cloud e IoT. Finalmente se presenta la estructura de un informe forense, así como las consideraciones legales y normas aplicables que se ha de tener en cuenta. Este documento pretende ofrecer una visión de los elementos que intervienen en cibercrimen y del papel que desempeña el análisis forense digital en la investigación de incidentes de ciberseguridad y cibercrimen, destacando la importancia y alcance del informe pericial.

Keywords: Ciberseguridad · Análisis Forense · Especialización · Formación Profesional · Máster

Fecha de publicación: 25/11/2020
https://iescelia.org/ciberseguridad/ceceti-afi-00

1. Introducción

Antes de nada deberíamos introducir algunos conceptos que nos acompañarán en el resto del tema y que fundamenta nuestro conocimiento en la materia.

Crimen: Delito grave o acto que es penalizado por la sociedad. La diferencia entre crimen y delito, es que el delito es determinado por las leyes de un determinado Estado, mientras que el crimen lo determina la sociedad. También se diferencian por su magnitud, de forma que un delito grave se considera crimen.

Delincuente: persona que comete un delito, especialmente el que lo hace habitualmente.

[1] Boletín Oficial del Estado

Ciberdelincuente: el que hace uso de los medios tecnológicos para cometer un delito. Podemos hablar de tipos de ciberdelincuentes.

Trabajador descontento que lleva a cabo un ataque desde dentro de la empresa.

Hacktivista, motivados por alguna ideología emplean sus conocimientos en llevar a cabo ataques a sistemas informáticos de objetivos previamente seleccionados. Hacker, conocido como pirata informático. Aquí podemos hablar de hacker de sombrero negro y hacker de sombrero blanco (ético).

Ciber-terroristas, son grupos organizados que emplean la tecnología para crear miedo entre una población. Rara vez se trata de un único individuo.

Cibercrimen: delito grave que se realiza a nivel informático. Es el uso de herramientas informáticas para realizar prácticas ilegales como pueden ser pornografía infantil, violación de privacidad, difamaciones.

Se dividen en dos categorías: - Actividad criminal, cuyo propósito son los propios sistemas informáticos. - Actividad delictiva en la que se utilizan dispositivos electrónicos o informáticos para cometer otros delitos. Tecnología como instrumento.

Algunos tipos de cibercrimen:

- Fraude por correo electrónico y en Internet.
- Fraude de datos personales (robo y uso indebido de información personal).
- Robo de datos financieros o de tarjetas bancarias.
- Robo y venta de datos corporativos.
- Chantaje cibernético (exigiendo dinero para evitar los ciberataques).
- Ataques de programas de extorsión (tipo de chantaje cibernético).
- Ciberespionaje.
- Acceso ilícito a sistemas informáticos.
- Interceptación de datos informáticos (MiTM).
- Falsificación documental.
- Descubrimiento y revelación de secretos.
- Amenazas y coacciones.
- Suplantación de identidad.
- Daños y sabotaje informático.
- Delitos contra la propiedad intelectual.
- Delitos contra la intimidad y acoso

Ciberseguridad: es la disciplina que aplica los mecanismos necesarios para proteger un sistema informático. En inglés, el término “cybersecurity” hace referencia a proteger la información que hay en un sistema informático así como las formas en que se comunica, de forma que se preserve la confidencialidad, integridad y disponibilidad. Sin embargo, el término “cybersafety” hace referencia a la protección de las personas en el uso de la tecnología, que no se pueda llegar a causar un daño personal, aquí se usa la tecnología como instrumento para dañar a las personas y hay que proteger ante esta posibilidad. La formación de los usuarios suele ser una buena opción para evitar, en la medida de lo posible los efectos de la ingeniería social en la seguridad de las personas (Ghafir et al, 2018).

Forense: relacionado con la justicia. De aquí la importancia de este término y la seriedad con la que se requiere que sea tratado. El origen del término forense, o sea la etimología de la palabra, procede de "forum", que era la plaza o espacio público de una ciudad donde se llevaban a cabo las intervenciones de los tribunales de justicia. Así un médico forense determina los aspectos legales de las lesiones que observa en una víctima, pudiendo establecer una conexión con el grado de responsabilidad demostrado por las evidencias que este encuentre, además de poder determinar las circunstancias en que se produjo un determinado delito.

Analista Forense Informático: se trata de un experto en informática con una formación específica que lleva a cabo la investigación de los dispositivos electrónicos que han participado en la comisión de un delito, con el fin de obtener la información conducente a esclarecer las circunstancias en las que se cometió, identificar al autor y determinar el grado de responsabilidad. Esta investigación finaliza con la confección de un informe pericial que arroja las conclusiones tras el análisis de la información obtenida mediante un método científico que desemboca en unas conclusiones.

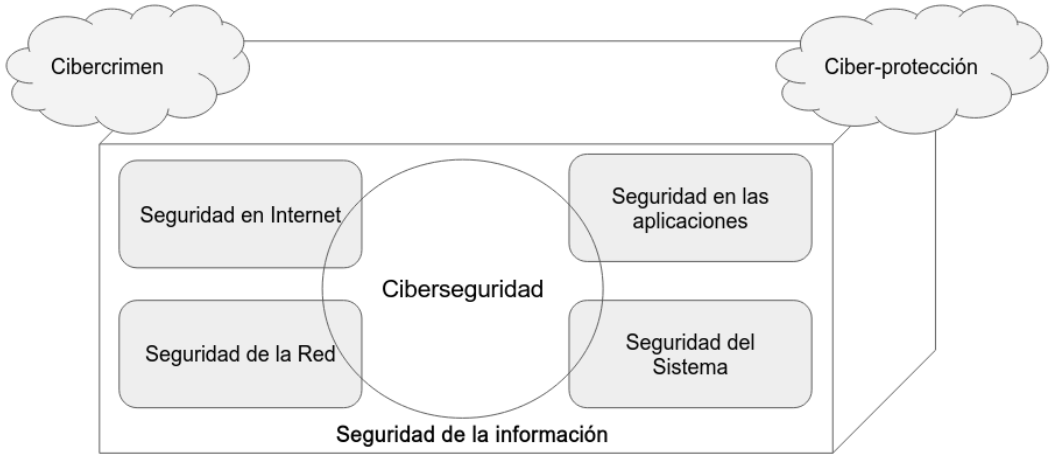

Figura 1. Fundamentos de ciberseguridad

1.1. La investigación del delito y el ciberdelito.

En la investigación de un delito intervienen los grupos especializados en investigación técnico policial para llevar a cabo lo que comúnmente se conoce como "inspección ocular", adquisición de evidencias o pruebas sobre el escenario del

crimen, para posteriormente en un laboratorio. En la investigación de un crimen tradicional se hace uso de disciplinas como la criminología (Paz Velasco, 2918; Soto Castro, 2017; Serrano Maillo, 2017)) y la criminalística (Bosquet Pastor, 2015), en un cibercrimen se ponen en juego otros conocimientos del ámbito tecnológico. En el escenario del crimen se etiquetan todas las pruebas y fotografían en la forma en que fueron encontradas a la vez que se recoge toda la información posible in situ y se etiqueta convenientemente para asegurar la cadena de custodia.. Aquellas evidencias que no se pueden analizar en profundidad en el escenario del crimen, se trasladan a un laboratorio, donde con el instrumental adecuado se puede realizar un análisis en profundidad. La investigación técnico policial termina con la realización del informe pericial, en el que se hace constar las pruebas obtenidas, la información que se ha conseguido averiguar a través de ellas, los métodos empleados y unas conclusiones que se derivan de la investigación desarrollada . Estas unidades de investigación, en España, la llevan a cabo por parte de la Policía Nacional, el grupo de Policía Científica, y por parte de la Guardia Civil, el grupo de Criminalística. Pero cuando se trata de delitos donde interviene la tecnología en alguna de sus formas, intervienen, además los grupos especializados en esta materia. En el caso de la Policía Nacional está la BCIT y en el caso de la Guardia Civil, es el GDT. En estos grupos es bien conocido el siguiente principio y sobre el que se basa gran parte del trabajo de investigación:

Principio de Intercambio de Locard:

El principio de Intercambio de Locard es un concepto que fue desarrollado por el Dr. Edmond Locard (1877-1966). Locard especuló que cada vez que se hace contacto con otra persona, lugar, o cosa, el resultado es un intercambio de materiales físicos. El creía que no importa a donde vayan los criminales o lo que hagan los criminales, estando en contacto con cosas, los criminales dejan todo tipo de evidencia, incluyendo ADN, huellas, cabellos, células de piel, sangre, fluidos corporales, piezas de vestimenta, fibras y más. A la misma vez, ellos toman también algo desde la escena.

Locard & Curiel (2010)

Ante el cibercrimen se introducen elementos que hasta ahora no existían y hace que los procedimientos sean algo diferentes en algunos aspectos, si bien han de respetar la normativa legal muy escrupulosamente para que no se invalide ni la investigación ni los resultados derivados de esta. Los factores que intervienen en la aparición del hecho delictivo son parecidos:

Siguiendo la explicación de la figura anterior, que está basada en una de las teorías de la criminología, la Teoría de las Actividades Rutinarias, formulada por Marcus Felson y Lawrence E. Cohen en 1979 (Serrano, 2017), existen unos factores mínimos para que se produzca el delito o acto criminal o cibercrimen, en el caso tecnológico. Por una parte es necesaria la existencia de un AUTOR, que en el caso concreto del cibercrimen necesita una formación muy concreta y específica para poder llevar a cabo la acción delictiva. Esta es una de las características especiales que diferencian a los cibercriminales de un cri-

minal tradicional, ya que sin estos conocimientos de la tecnología no se puede llevar a cabo el ataque a un sistema informático, y mucho menos hacerlo sin dejar rastro de ello. Otro factor necesario es el objetivo, en criminología se viene denominando una VÍCTIMA elegible y que en el caso de ciberdelitos, puede ser un sistema informático perteneciente a una empresa, banco o de cualquier organización, incluso organismos públicos. Hay varios tipos de delitos que pueden realizarse contra personas empleando la tecnología (Reep-van den Bergh, C. M. M., & Junger, M., 2018) ¿Por qué se elige una víctima y no otra? Esta es una cuestión de la que se ocupa la ciencia conocida como victimología y que estudia estos aspectos. Recientemente hemos visto cómo varias empresas internacionales han sufrido ataques de ransomware alcanzando a cifrar todos los datos de sus servidores y haciendo imposible su acceso hasta que paguen el rescate que solicitan los atacantes. Este hecho está poniendo en sobreaviso a todas las empresas, sean del tamaño que sean, sobre la necesidad de implementar la ciberseguridad de una forma seria y ser capaces de revertir las consecuencias de cualquier tipo de ataque, devolviendo el sistema informático a su estado de normal funcionamiento. El tercer factor es el conocido como AUSENCIA DE CONTROLES o de guardianes. En el caso de la ciberseguridad refleja todo el entorno del sistema, las directivas y controles de seguridad que se despliegan en la organización para minimizar la posibilidad de sufrir un ataque y estar en la mejor disposición en el caso de ser objetivo de uno.

En la investigación del delito se tienen en cuenta los siguientes aspectos y que a su vez pueden ser considerados en el estudio del ciberdelito:

- Autor. Uno de los objetivos es determinar la identidad del autor.

- Motivación: es el móvil que tiene el autor para cometer el delito.

- Victimología: selección del objetivo, cómo se aborda, se explota y abandona.

- Modus Operandi: es la forma en la que se desarrolla la comisión del delito. A través de esto se puede llegar a identificar al autor.

- Firma: hecho característico en la comisión del ciberdelito que lleva a cabo el autor para diferenciar "su obra" de otras.

- Escenario: uno/varios. ¿Por qué este? Relación con la víctima, con el autor. En el caso del cibercrimen se podría hablar de varios escenarios posibles, pueden verse implicados varios sistemas informáticos, de forma que a través de unos se consigue actuar sobre otros.

- Registro de tiempos: franjas horarias, intervalos. Las marcas de tiempo son un dato muy relevante en el análisis forense. Seguir la línea de tiempo es fundamental para determinar el origen y su desarrollo. (TimeLine).

- Retirada o huida: también es importante investigar sobre la forma en la que el ciberdelincuente abandona el sistema, si intenta borrar su rastro, si lo consigue o no. Este hecho aporta información sobre su destreza y experiencia en la comisión del delito (conciencia forense, antecedentes).

En el cibercrimen hay algo muy característico: que se necesita cierta formación para cometer un delito mediante el uso de dispositivos informáticos, ya sea directa o indirectamente.

Por otro lado, también la investigación del cibercrimen también requiere de una formación y unos procedimientos muy elaborados ya que no sólo se trata de un trabajo técnico, sino que además se han de cumplir con todas las garantías judiciales y estándares de calidad establecidos para asegurar el correcto tratamiento de las evidencias y su cadena de custodia.

Artículo 13 de la Ley de Enjuiciamiento Criminal. Se consideran como primeras diligencias la de consignar las pruebas del delito que puedan desaparecer, la de recoger y poner en custodia cuanto conduzca a su comprobación y a la identificación del delincuente, la de detener, en su caso, a los presuntos responsables del delito, y la de proteger a los ofendidos o perjudicados por el mismo, a sus familiares o a otras personas, pudiendo acordarse a tal efecto las medidas cautelares a las que se refiere el artículo 544 bis o la orden de protección prevista en el artículo 544 ter de esta ley.

Pero la aplicación del Análisis Forense Informático no es únicamente en el ámbito policial, en las empresas y organizaciones también se utiliza como medio de investigación de una intrusión en el sistema, de un robo de información o de cualquier acción cibernética que le ponga en riesgo un activo (información o recurso en el sistema de valor) de la empresa. En este caso, el informe arrojado del proceso de investigación tecnológica y la aplicación de métodos de análisis forense digital, sirve para tomar medidas de protección para reducir riesgos o minimizar el impacto de un ataque. Para la realización de este tipo de investigaciones existen varias recomendaciones de estándares que indican cómo se han de desarrollar los procedimientos así como otros aspectos a tener en cuenta para que todo el proceso cuente con las mayores garantías a la hora de acreditar de forma fehaciente el resultado de la investigación.

Otro efecto preocupante y que supone una conducta delictiva aprovechando las tecnologías para llevarlo a cabo es el ciberbullying. En este caso el estudio de los dispositivos móviles, tanto de la víctima como de la persona acosadora, revela información de interés.

1.2. Aportación de Inteligencia.

Existe un punto donde los datos se transforman en información, con una aportación de valor en su conjunto. La gestión de la información cumple con el ciclo de vida de la inteligencia, que consta de los siguientes pasos: planificación, obtención, análisis y difusión. Estas fases que componen el ciclo de la inteligencia no son ajenos al ciclo que aparece en el análisis forense informático, proceso en el que a partir de datos obtenidos de los medios de prueba (evidencias), se somete a un estricto procedimiento de actuación y medidas preventivas con el fin de obtener información útil para responder a las cuestiones inicialmente

planteadas, como puede ser la autoría de un delito, las circunstancias en las que se llevó a cabo y que servirá de ayuda al juzgado o a la organización para tomar las medidas consecuentes.

Podríamos hablar de Inteligencia Criminal que es el tipo de inteligencia que realizan los servicios de información policiales y cuyo fin es analizar e investigar tanto la criminalidad organizada, como aquellas otras formas delictivas cuya complejidad o gravedad impide su eficaz prevención mediante una investigación policial, fiscal o judicial del caso concreto. También se ocupa del análisis estratégico de tendencias y amenazas en materia delictiva (Izquierdo, 2018).

Existen otros tipos de inteligencia empleados en diferentes sectores. Desde la inteligencia militar, donde Sun Tzu en su obra "El arte de la guerra" supone una referencia en el ámbito militar y que además ha sido extrapolado a otros sectores, como puede ser el de los negocios, aportando estrategias de inteligencia aplicables en diferentes escenarios y situaciones. Por nombrar algunos sectores más en los cuales se aplica este enfoque para generar inteligencia y así tener la mejor información posible a la hora de tomar decisiones:inteligencia económica, competitiva, estratégica, política o industrial, sin olvidar la inteligencia artificial.

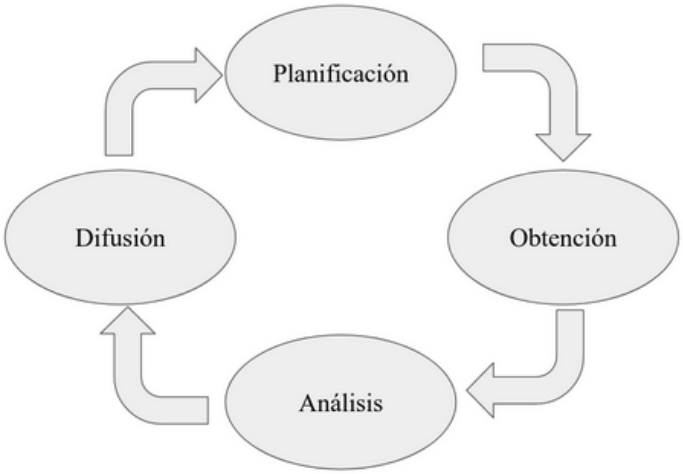

Figura 2. Ciclo de Inteligencia

Las distintas fases del ciclo de inteligencia están caracterizadas por procesos diferenciados y con un objetivo concreto. Durante la fase de planificación se define el alcance de la investigación y se realizan las preguntas a las que se quiere encontrar una respuesta, se delimitan los recursos que se emplearán y las directrices para llevar la investigación a cabo. En la fase de obtención se trata de recopilar todos los datos posibles, sin detenernos a examinar su contenido ni interrelación con otros datos, únicamente recolectar la mayor cantidad de datos de

la forma más precisa posible, sin interferencias, sin distorsiones que puedan contaminar la información obtenida. Durante la fase de análisis es cuando se genera información de valor, se genera inteligencia susceptible de ser utilizada por la organización para responder a las cuestiones planteadas inicialmente. Finalmente se dispone a comunicar o difundir la información de valor con la organización a nivel estratégico de forma que sirva para la toma de decisiones tras la realización del feedback que aporta la difusión de la información obtenida (Seisdedos, 2020). Este modelo es cíclico ya que se vuelve a repetir para conseguir una evolución en la consecución del objetivo e ir redirigiendo la investigación a medida que se tiene más información sobre el asunto investigado.

2. Ciberseguridad.

Recientemente observamos que los incidentes de ciberseguridad avanzan y se hacen cada vez más populares, llegando a causar pérdidas millonarias que hacen tambalearse a empresas más que consolidadas.

Los problemas en la seguridad de los sistemas informáticos hace que los cibercriminales consigan acceder a la información, bien para comerciar con ella, bien para causar un daño a la empresa o cualquier otro tipo de fin ilícito y tipificado como delito. Los daños para la empresa u organización pueden ser tanto económicos como reputacionales ya que pone en evidencia la gestión que estas hacen de los datos de sus usuarios y clientes.

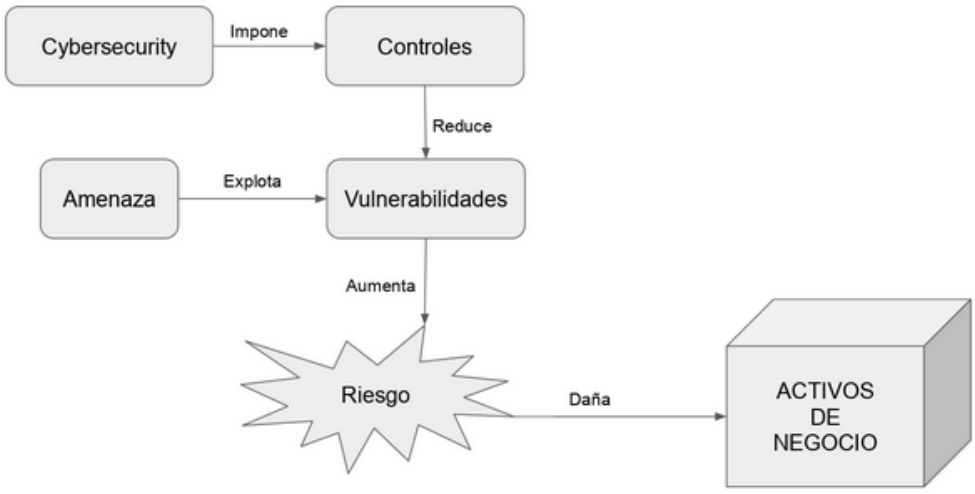

Figura 3. Interrelación de conceptos de ciberseguridad

De aquí que la ciberseguridad deba ser tenida en cuenta de una forma más que seria. En 2020, con la situación especial que se ha desarrollado al incrementarse la actividad online, el teletrabajo, la enseñanza online y casi todos los servicios que se puedan ofrecer a través de internet son susceptibles de ser atacados. La transformación digital se ha acelerado, tanto en nuestro país como a nivel internacional, el incremento de la actividad online ha inundado nuestras redes, comercios, servicios públicos y todo tipo de empresas y organizaciones se han sumado a esta transformación. Los ciberdelincuentes están continuamente aprendiendo nuevas formas, buscando vulnerabilidades, debilidades en los sistemas que puedan transformar en un punto de ataque y así comprometer el sistema.

La existencia de información supone un activo para la organización, que debe proteger a toda costa. Cuanto mayor es el valor de la información mayor serán los riesgos que asume el sistema informático. La existencia de vulnerabilidades se ve incrementada sin aviso, nuevas amenazas aparecen cada día y aprovechan esos fallos de seguridad para hacerse un espacio, un hueco por el que penetrar en el sistema y llegar hasta la información. Detectar esto nos ayuda a crear un sistema seguro, nos lleva a diseñar e implementar unos controles de seguridad enfocados a prevenir y evitar, al menos minimizar, posibles riesgos en los sistemas de información.

2.1. Funciones de la ciberseguridad.

Identificar. Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales.

Proteger. Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

Detectar. Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad., permitiendo el descubrimiento oportuno de los mismos.

Responder. Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente.

Recuperar. Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

2.2. Objetivos de la ciberseguridad.

La conservación de la INTEGRIDAD de los datos de forma que no puedan ser alterados por usuarios sin autorización. La CONFIDENCIALIDAD de forma que únicamente aquellas personas para las que está destinada la información sean las que accedan a ella y nadie más. Y la DISPONIBILIDAD para que la información esté siempre que se requiera de una forma lícita. Estas tres cualidades debe tener en cuenta cualquier sistema informático para garantizar la seguridad de la información. Si además queremos incorporar la seguridad en las comunicaciones habría que añadir la característica de NO REPUDIO, que asegura el hecho de que ninguna de las partes participantes en la comunicación pueda negar su participación: ni el emisor puede negar que lo ha enviado, ni el receptor que lo ha recibido, de forma que exista un mecanismo fehaciente que lo permita (CDIN). Para cumplir con esta finalidad se diseñan una serie de controles que tienen como misión comprobar que se cumplen con unos estándares según los niveles de seguridad requeridos y relacionados con la naturaleza de la información almacenada.

2.3. Controles estándares de ciberseguridad.

Existen distintos estándares de controles a implementar, entre ellos encontramos: NIST CSF [2], CIS, COBIT (presentados más adelante). A nivel nacional encontramos las guías de la serie STIC [3], concretamente las relacionadas con el ENS [4], Serie CCN-STIC-800, que establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS (RD 3/2010).

NIST CSF. En 2014, el Instituto Nacional de Normas y Tecnología (NIST) creó un Marco de Ciberseguridad (CSF) que guía a las organizaciones en su camino hacia el desarrollo de sistemas informáticos seguros. Establece una base flexible que todas las empresas pueden seguir y esculpir según sus necesidades. Por esta razón, tiene un gran éxito y es empleado por un gran número de organizaciones.

Este Marco está dividido en cinco partes que incluyen la identificación de capacidades y vulnerabilidades, la protección y la seguridad de la infraestructura vital, la detección de las amenazas a la seguridad lo antes posible, la respuesta adecuada a las infracciones y la recuperación rápida y eficiente con el menor tiempo de inactividad posible.

Los 5 grandes dominios del framework NIST CSF: identificar, proteger, detectar, responder y recuperar. NIST CSF es el estándar de ciberseguridad que en los últimos años ha tomado un protagonismo creciente al haber sido elegido por grandes compañías a nivel internacional como su marco de trabajo de ciberseguridad

[2] National Institute of Standards and Technology Cybersecurity Framework
[3] Seguridad de las Tecnologías de la Información y las Comunicaciones
[4] Esquema Nacional de Seguridad

Niveles de seguridad. Son 4 los niveles de implementación que presenta el marco NIST. Estos niveles representan las prácticas llevadas a cabo por la organización que son de alcance creciente y que van desde la mera respuesta informal y reactiva hasta enfoques más evolucionados y formales que incluyen información sobre el riesgo.

Controles Criticos de Seguridad (CIS). *"Mientras que los Controles CIS se centran en la acción técnica, los desarrolladores de los Controles reconocieron que muchas de estas recomendaciones obligarían a los equipos técnicos operacionales a cambiar las prácticas para mejorar tanto los controles operacionales como la seguridad, reevaluar sus estrategias básicas de defensa y ser más estructurados y disciplinado en sus actividades. No hay una solución de çaja mágica"para la ciberseguridad. Por lo tanto, el éxito con los Controles de CIS (o cualquier programa defensivo) depende de que las organizaciones desarrollen y operen a partir de una nueva hoja de ruta integral para mejorar la ciberdefensa."*

Guía práctica para implementar los controles críticos de seguridad. (2020).

COBIT. Control Objetives for Information and Related Technology (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas) , es un marco de trabajo creado por ISACA [5] para el gobierno de las tecnologías de la información. Fue diseñado para ser una herramienta de soporte para los gestores, ya que trata de cubrir los huecos entre los temas técnicos, riesgos de negocio y los requerimientos de control. COBIT es una guía reconocida para ser aplicada en cualquier industria, sobre todo, asegura calidad, control y fiabilidad de los sistemas de información en una organización.

Trata con unos requerimientos de negocio: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

3. Análisis Forense Informático.

El Análisis Forense Informático es la agrupación de técnicas científicas y técnicas de análisis especializadas en las infraestructuras tecnológicas. Esas técnicas nos posibilitan realizar una identificación, preservación, análisis y presentación de datos y documentación, que pueden ser válidamente aceptados en un proceso legal. El Análisis Forense Informático es, por tanto, un análisis que se realiza una vez se ha detectado la amenaza y ésta se ha materializado. Nos permite analizar las consecuencias que han producido en los sistemas informáticos de la empresa, averiguar quién ha sido el autor, las causas, la metodología empleada y detectar las debilidades de nuestros sistemas informáticos que han ocasionado el ataque.

Para llevar a cabo una labor efectiva, el analista forense debe disponer de unas herramientas adecuadas, tanto hardware como software. Es habitual trabajar con

[5] Information System Audit and Control Association

Figura 4. Fases del método forense digital

algunas versiones de Sistemas Operativos y software específico para este tipo de trabajos, entre los cuales podemos encontrar los siguientes:

Herramientas de captura de datos y discos.
Visores de archivos.
Herramientas de análisis de archivos.
Herramientas de análisis de registro.
Herramientas de análisis de Internet.
Herramientas de análisis de correo electrónico.
Herramientas de análisis de dispositivos móviles.
Herramientas de análisis de red.
Herramientas de análisis de bases de datos.
...

El origen del Análisis Forense Informático se remonta al año 1984, cuando el FBI implantó el programa "Magnet Media" para analizar los archivos digitales. En el sector privado, en las empresas, el objetivo de esta disciplina era algo diferente, se centraba en rastrear e identificar los ataques de los hackers en los sistemas informáticos. En 1986, Clliff Stoll, un administrador de sistemas Unix del Lawrence Berkeley National Laboratory, intentó descubrir por qué había una discrepancia de 0,75 dólares en un registro de contabilidad y terminó identificando a un hacker alemán que había entrado en sus sistemas confidenciales para vender datos a la KGB. Fue el inicio de lo que sería un sistema trampa. El gran especialización y profesionalización del análisis forense digital se produce en los años 90 a 2000 con la investigación de ciertos delitos, como la pornografía infantil en Internet, la guerra de Afganistán, donde se recogían los ordenadores de insurgentes enemigos para extraer de ellos los datos que hubiera para convertirlos en información útil. En 2006, se produce otro hito en EEUU al revisar las reglas del procedimiento civil de Estados Unidos para implementar un régimen obligatorio para el descubrimiento de pruebas electrónicas. El Análisis Forense Digital también lo podemos encontrar con las siglas DFIR [6]. Hoy en día en España hay multitud de empresas que prestan este tipo de servicio. La mayoría tratan con

[6] Digital Forensics & Incident Response

temas de ciberseguridad en general y presentan, además una alta especialización en análisis forense digital. Comparten este espacio con los profesionales de las Fuerzas y Cuerpos de Seguridad del Estado que son los que tienen la autoridad en la investigación de cualquier delito y en la custodia de las pruebas. El hecho de que existan profesionales de este tipo en organizaciones empresariales tiene sentido en cuanto a la investigación de incidentes de seguridad para determinar su origen, circunstancias y como evitar futuros ataques. También cuando se presenta una segunda peritación para oponerse a las conclusiones presentadas en un informe presentado en juicio por la parte contraria o en procedimientos extrajudiciales, donde únicamente hay interés en conocer qué ha pasado con un dispositivo o con la información que este contenía o manejaba, sin que llegue a mediar denuncia por delito alguno. La innovación tecnológica avanza a una velocidad de vértigo y cada día aparecen nuevos dispositivos con nuevas funcionalidades, incluso nuevas formas de interconexión entre ellos. No es extraño encontrar dispositivos "wearables" susceptibles de ser analizados para determinar la información que pudiera aportar al verse involucrado de una u otra forma en la comisión de un delito. Véase el ejemplo de un reloj deportivo con funciones GPS y de salud, el cual es capaz de almacenar información muy valiosa, que analizada convenientemente aporta inteligencia al proceso forense, convirtiendo los datos en información. Es el IoT [7] que se impone en la sociedad actual y nos inunda con su tecnología. Un campo muy concreto y que ha conseguido un alto grado de especialización es el de los teléfonos móviles. Esto es así por el hecho de que estos dispositivos se emplean como instrumento para cometer delitos o simplemente determinar las circunstancias en las que ocurrió un crimen y ayudar a esclarecer los hechos, como el caso de Laura Luelmo (Dolz, 2020).

Un nuevo campo de acción para el Análisis Forense Informático es la tecnología "Cloud", la cual está en auge por las ventajas que ofrece, a la vez que hacerse más interesante para los posibles atacantes y sus acciones maliciosas sobre esta tecnología. Para terminar, el proceso concluye con la elaboración de un informe con doble vertiente, un informe técnico forense y un informe ejecutivo forense. Es el resultado de un cuidadoso proceso donde, haciendo uso de métodos científicos y sistemáticos se plasma la información obtenida junto con unas conclusiones finales derivadas de los datos extraídos y los resultados analizados. La redacción de este informe está sujeto a normas y estándares que se han de tener en consideración para su posterior utilización en un juzgado con valor probatorio. La utilidad del Análisis Forense Digital está acreditada ya que ayuda a determinar las circunstancias en la que se ha cometido un delito si para ello ha intervenido la tecnología, y a su vez puede llegar a identificar al autor. Es importante que este trabajo de investigación se lleve a cabo con la máxima diligencia y prudencia, ya que una mala praxis, o simplemente actuar con prisas, puede hacer que se destruyan algunas o todas las pruebas que pudieran existir.

[7] Internet of Things

3.1. El perito informático.

En primer lugar saber que un perito informático es un profesional con una dilatada trayectoria en el ámbito informático o TIC (Tecnologías de la Información y Comunicación) y sobre todo con un profundo conocimiento técnico - además de una titulación oficial en informática - ya que debe afrontar retos que, en muchas ocasiones, serán innovadores y deberán investigar sobre el funcionamiento de dispositivos, sistema operativo incluso software específico. El perito debe de presentar unas características para dedicarse a esta función, resaltar que un perito informático ha de estar preparado para presentarse en un juicio oral para informar sobre el informe pericial que ha elaborado ante un caso concreto y responder a las preguntas que las partes le formulen. Se trata de un trabajo serio y profesional, con una alta componente de responsabilidad y compromiso. Un perito responde de lo que haya escrito en su informe, que debe haberse realizado mediante métodos científicos y bajo unas condiciones determinadas, así como el seguimiento de una normativa concreta.

Legislación de aplicación a peritos judiciales:

ÁMBITO CIVIL: Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Ley de Enjuiciamiento Civil (LEC): artículos 335-352.

ÁMBITO PENAL: Real Decreto del 14 de septiembre de 1882. Ley de Enjuiciamiento Criminal (LECrim): artículos 456-485. Un perito judicial no es policía, ni abogado, ni juez ni notario, por lo que no tiene presunción de veracidad sobre el asunto tratado, debe demostrar mediante argumentación razonada y evidencias técnicas sus afirmaciones. Es un profesional en un campo determinado sobre el que realiza un informe a petición de una de las partes (o de las dos) para conocer y presentar unos resultados sobre la investigación realizada de la forma más objetiva posible (método científico).

Obligaciones del perito:

Actuar con la mayor objetividad posible. Considerar tanto lo que pueda favorecer como perjudicar al cliente. Conocer las sanciones penales en las que puede incurrir.

Responsabilidad de un perito:

Secreto profesional (Art. 199 CP): de 1 a 4 años de prisión.
Falsedad (Art. 390 y 404 CP): de 3 a 6 años de prisión.
Ocultación de datos (Art. 413 CP): de 1 a 4 años de prisión.
Divulgación de datos (Art. 417 CP): de 2 a 4 años de prisión.
Aprovechamiento del cargo (Art. 439 CP): de 1 a 4 años de prisión.
Aprovechamiento de la información (Art. 442 CP): de 1 a 6 años de prisión.

Especial atención al artículo 264 del Código Penal:

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado

producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

- Se hubiese cometido en el marco de una organización criminal.

- Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

- El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

- Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

- El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

- Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Dada la responsabilidad que acarrea el desempeño de la figura de perito judicial, existen unas características recomendables que debería presentar cualquier persona que desee dedicarse a esto:

- Tener una titulación relacionada con el objeto de la pericia.
- Dominar y/o tener experiencia en el objeto de la pericia.
- Ser serio, responsable y fiable.
- Saber redactar, escribir bien.
- Hablar bien en público. Ser convincente.
- Soportar bien la presión.
- No implicarse emocionalmente.
- Tener flexibilidad de horario.
- Disponer de seguro de responsabilidad civil.

Encontramos una clasificación de los peritajes que se pueden llevar a cabo. Por un lado tenemos los peritajes judiciales, entre los que están los designados por el tribunal y los designados por una de las partes. Por contraposición, tenemos también los peritajes extrajudiciales, que son aquellos en los que se realizan

a petición de una empresa, compañía de seguros o de una persona física interesada en un asunto en concreto (p.e. sospecha de que exista algo "raro" en un teléfono móvil y se quiera conocer sobre el tema).

Algunas recomendaciones generales:

1. Documentarlo todo. TODO.
2. No responder en caliente. Reflexionar y consultar antes de informar.
3. Aprender a decir NO.
4. No se puede mentir ni ocultar información.
5. No se puede aceptar que nos dicten la pericial (no favores).
6. No se es notario, ni abogado, ni policía, ni juez: eres perito.
7. No decir suposiciones. Sólo lo contrastado y demostrado.
8. Tu dictamen es tu opinión. Justificada, pero tu opinión.
9. Deber de ser objetivo. No favorecer al cliente intencionadamente.
10. Se es responsable de lo que se diga - consecuencias.
11. PRIVACIDAD y CONFIDENCIALIDAD.

4. Conclusiones.

En una primera parte se han mostrado los elementos que se relacionan con el crimen y el cibercrimen, estableciendo una pauta de relación y estudio. Posteriormente se ha presentado también una visión general del análisis forense digital y su relación con los elementos que componen la ciberseguridad y los controles que se definen sobre unos estándares de calidad reconocidos internacionalmente, de forma que aporte conocimiento sobre esta disciplina así como el método de trabajo en un estudio de carácter forense digital. En próximos trabajos se desarrollará el método forense al detalle siguiendo los estándares de calidad y normativos requeridos conducentes a realizar un trabajo objetivo basado en el método científico, sistemático e informado.

Este trabajo ha sido realizado como parte del material didáctico correspondiente al módulo profesional de ANALISIS INFORMÁTICO FORENSE, incluido en el Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información (Real Decreto 479/2020) que se imparte en el I.E.S. Celia Viñas de Almería (España)

A su vez forma parte del material aportado al Grupo de Trabajo ITSEC: Técnicas Avanzadas de Ingeniería en Ciberseguridad [21401GT011] de la Dirección General de Formación del Profesorado e Innovación - Consejería de Educación y Deporte de la Junta de Andalucía (España)

Referencias

1. Izquierdo, H. (2018). Manual de inteligencia económica y competitiva. Tirant lo Blanch.
2. Guía práctica para implementar los controles críticos de seguridad. (2020). Retrieved 1 October 2020, from https://ciberseguridad.blog/guia-practica-para-implementar-los-controles-criticos-de-seguridad/
3. NIST Cybersecurity Framework (2018). Retrieved 1 October 2020 from https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf
4. Locard, E. & Curiel López de Azcárate, A.M. (2010). Manual de técnica policial. Maxtor.
5. OEA & AWS (2019). Ciberseguridad - Marco NIST. White Paper Series. https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf
6. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74(10), 4986-5002. https://doi.org/10.1007/s11227-018-2337-2
7. Dolz, P. (2020). Laura Luelmo, cronología de un crimen. Retrieved 2 October 2020, from https://elpais.com/sociedad/2018/12/26/actualidad/1545820102_840732.html
8. Velasco de la Fuente, P. (2018). Criminalmente: todo lo que hay que saber sobre criminología. Ariel.
9. Seisdedos, C. (2020). Ciberinteligencia frente al Cibercrimen COVID19 - Derecho de la Red. Retrieved 2 October from https://derechodelared.com/covid-ciberinteligencia/
10. Soto Castro, J. E. (2017). Manual de investigación psicológica del delito: el método VERA. Pirámide.
11. Serrano Maíllo, A. (2017). Teoría criminológica: la explicación del delito en la sociedad contemporanea. Dykinson.
12. Bosquet Pastor, S. (2015). Criminalística Forense. Tirant Lo Blanch.
13. Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime Science, 7(1), 5. https://doi.org/10.1186/s40163-018-0079-3
14. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.