El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad de Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito*

Claudio Paya Santos
Álvaro Cremades Guisado
Juan José Delgado Morán

Universidad Nebrija, España

cpaya@nebrija.es

Recibido: febrero 20 de 2017
Aceptado: marzo 24 de 2017

BIBLID [2225-5648 (2017). 7:1, 237-270]
http://dx.doi.org/10.5377/rpsp.v7i1.4312

Resumen

La comisión de prácticas delictivas en el ámbito del ciberespacio, representa una tendencia de creciente entidad e impacto en la sociedad española. Dicho fenómeno requiere, para su adecuado tratamiento del personal, de un conocimiento profundo de la ciberdelincuencia y de las competencias necesarias para trabajar en pos de su prevención e investigación, ya sea en el ámbito policial o en el empresarial. A este respecto, según la propia Estrategia de Ciberseguridad Nacional de España, las instituciones académicas se articulan como actores de una relevancia estratégica incuestionable, de cuyo buen hacer depende en gran medida la satisfacción de las altas necesidades formativas de quienes se dedican a luchar contra la ciberdelincuencia. El Máster en Ciberdelincuencia de la Universidad Nebrija representa una importante contribución en este ámbito.

Palabras clave

Ciberdelincuencia, ciberseguridad, formación universitaria, Universidad Nebrija.

- Estudio original elaborado para la revista "Policía y Seguridad Pública" en el marco de las gestiones de apoyo académicas internacionales realizadas por el Centro de Investigación Científica (CINC-ANSP).

The phenomenon of cybercrime in Spain: The proposal of the Nebrija University in staff training for the prevention and treatment of cybercrime

Claudio Paya Santos
Álvaro Cremades Guisado
Juan José Delgado Morán

Universidad Nebrija, España

cpaya@nebrija.es

Received: February 20, 2017
Accepted: March 24, 2017

BIBLID [2225-5648 (2017). 7:1, 237-270]
http://dx.doi.org/10.5377/rpsp.v7i1.4312

Abstract

The commission of crimes in the area of cyberspace, represents an increasing trend and impact in Spanish society. This requires a thorough knowledge of cybercrime and the skills necessary to work towards its prevention and research, whether in the police or in the business field, for the proper training of personnel. In this respect, according to the National Cybersecurity Strategy of Spain, academic institutions are articulated as actors of unquestionable strategic importance, whose good performance depends to a great extent on the satisfaction of the high training needs of those who are dedicated to fight against Cybercrime The Masters in Cybercrime of Nebrija University represents an important contribution in this area.

Keywords

Cybercrime, cybersecurity, university education, Nebrija University.

- Original study written for the "Policía y Seguridad Pública" Journal within the framework of the international academic support efforts conducted by the Centro de Investigación Científica (CINC-ANSP)

1. Introducción

Ciberseguridad es un término reciente que se utiliza para designar diversos campos de investigación, desarrollo e innovación; relacionados con el tratamiento del ciberespacio desde el punto de vista de su seguridad y fiabilidad para el usuario y el dominio público. La complejidad en la aplicación efectiva de las medidas de seguridad informática, está aumentando cada día más debido a la diversificación de frentes de actuación en seguridad informática, que responden al crecimiento del tipo de servicios informáticos profesionales utilizados y existentes en el mercado. Las empresas necesitan proteger el valor de sus negocios fortaleciendo la seguridad en todos los niveles de su infraestructura informática.

El ciberespacio proporciona infinidad de oportunidades y dota de gran valor añadido a procesos de muy diferente naturaleza: Comerciales, industriales, de comunicación, de interacción social, sanitarios, científicos, culturales. Pero, al mismo tiempo, el ciberespacio es fuente de multitud de amenazas a individuos, ciudadanos, empresas y al sector público. En consecuencia, puede decirse que los beneficios que brinda la información digital solo pueden conseguirse cuando se evitan o minimizan toda una serie de posibles riesgos y amenazas a su integridad y confidencialidad, que van desde el fraude y el robo, hasta los ataques a la privacidad. La comisión de delitos, haciendo uso malicioso de sistemas informáticos, lejos de ser una tendencia incipiente, representa ya en la actualidad un fenómeno muy presente en gran cantidad de países de todo el mundo, y, por supuesto, en España, donde su nocivo impacto se hace sentir de manera cada vez más clara afectando a cada vez más amplios sectores de la sociedad española.

Huelga decir que, en un terreno en constante transformación y que se presenta con una creciente complejidad como es el ciberespacio, la formación se presenta como una tarea a la que es necesario brindar una adecuada atención. En consecuencia, dada la relevancia estratégica de las iniciativas impulsadas desde el ámbito universitario para proveer de los conocimientos y habilidades necesarias a los responsables de velar por la seguridad de sus organizaciones en el ciberespacio, y especialmente a aquellos dedicados a prevenir y perseguir las actividades contrarias al ordenamiento jurídico español, deben de ser objeto de una profunda discusión en los foros especializados.

A tal efecto, y entre el abanico cada vez más amplio de universidades que comienzan a considerar la ciberseguridad como objeto de estudio, la Universidad Nebrija lanzó, en el curso académico 2016/2017, la primera edición del Máster en Ciberdelincuencia contando con la inestimable colaboración de la Fundación Policía Española, el Cuerpo Nacional de Policía y de Telefónica España, y con la aspiración de ofrecer los instrumentos necesarios en el análisis del fenómeno de la ciberdelincuencia desde una

perspectiva técnica, legal y de gestión, que permita a sus alumnos alcanzar un empleo solvente de las técnicas y procedimientos requeridos para desarrollar con éxito las funciones de investigación de estas modalidades delictivas. El presente trabajo expone de manera detallada la aportación de la Universidad Nebrija en este terreno, así como algunas de sus apuestas en clave de futuro.

2. El fenómeno de la ciberdelincuencia en España

2.1. Acotando los límites jurídicos del fenómeno de la ciberdelincuencia

La ciberdelincuencia es un fenómeno vinculado irremisiblemente a la problemática de la ciberseguridad. Al fin y al cabo, la proliferación del ciberdelito como forma emergente de criminalidad se encuentra directamente asociada a las principales características que definen al ciberespacio, ámbito en el que concurren un número insondable de actores de variable naturaleza e intencionalidad, que hacen un uso legítimo o ilegítimo de las redes informáticas para desarrollar sus actividades y satisfacer sus necesidades.

A medida que un número creciente de personas dependen en mayor o menor grado del cada vez más amplio abanico de posibilidades y servicios que el ciberespacio brinda, el fenómeno de la ciberdelincuencia adquiere mayores dimensiones, pues su aprovechamiento supone, en la mayoría de los casos, un cierto nivel de desprotección, lo cual es especialmente habitual cuando se trata de usuarios comunes no siempre provistos de los conocimientos y herramientas básicas para garantizar en el mayor grado posible su seguridad en el ciberespacio. De este modo, según la Estrategia de Ciberseguridad Nacional española:

> *"El ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información – incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas." (Departamento de Seguridad Nacional, 2013, p. 9).*

Dado el reducido riesgo y coste que puede suponer para el ciberdelincuente actuar, así como la naturaleza eminentemente transnacional y ubicua del ciberespacio y de los hechos delictivos que en él acontecen, la convergencia de los esfuerzos de los diferentes ejecutivos nacionales y de las organizaciones internacionales, representan una condición necesaria para la lucha efectiva contra el fenómeno del ciberdelito. A este respecto, es de obligada referencia el Convenio sobre la Ciberdelincuencia aprobado en Budapest el 23 de noviembre de 2001, ratificado por España el 1 de octu-

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

bre de 2010 y actualmente respaldado por un total de 52 países de todo el mundo. Este convenio, impulsado por el Consejo de Europa pero abierto a la adhesión de Estados no miembros, nacería con la doble finalidad de, por un lado, prevenir todo acto realizado contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, las redes que los vertebran y los datos que se encuentran en su seno, a través de la tipificación de este tipo de actos; y, por otro lado, la articulación de los medios necesarios para facilitar la detección, investigación y sanción de este tipo de hechos delictivos, tanto a escala nacional como internacional (Consejo de Europa, 2001b).

De este modo, constatando ya entonces la cada vez mayor importancia de las tecnologías de la información en el seno de las sociedades, así como las consiguientes dificultades que entrañaba desde un punto de vista jurídico abordar los problemas que el uso de estas tecnologías comenzaba a presentar, se tornaba imprescindible armonizar en mayor medida los ordenamientos jurídicos nacionales en materia de delitos informáticos, establecer los medios necesarios para el procesamiento de las prácticas delictivas que hacen uso de sistemas informáticos, y configurar los instrumentos adecuados para la cooperación entre Estados en este ámbito (Consejo de Europa, 2001a). En ese mismo sentido, según María Concepción Rayón Ballesteros y José Antonio Gómez Hernández:

> *"La tipificación de las conductas resulta complicada, pues muchas veces los hechos son tan novedosos que no están contemplados en las normas penales. El Derecho Penal se enfrenta a una criminalidad progresivamente más poderosa y peligrosa que demanda una mayor complejidad técnica y jurídica. Se hace imprescindible una política legislativa flexible, dinámica y moderna que afronte este tipo de delincuencia tan cambiante. Sería deseable que las nuevas legislaciones modernas puedan hacer frente a las múltiples manifestaciones de la ciberdelincuencia mediante la configuración de tipos penales abiertos, dejando al margen casuísticas descriptivas, complejas y farragosas". (Rayón y Gómez, 2014, p. 230).*

Ante la necesidad palmaria de definir jurídicamente las modalidades delictivas emergentes vinculadas al ciberespacio, dicho convenio, que cuenta además con un protocolo adicional referido a la utilización de los sistemas informáticos para la difusión de propaganda racista y xenófoba (Consejo de Europa, 2003), recoge la definición de toda una serie de hechos delictivos:

- Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, que incluyen hechos como el acceso ilícito a sistemas informáticos, la interceptación ilícita de transmisiones no públicas dirigidas o emitidas a un sistema informático, los ataques a la integridad de los datos y sistemas informáticos y, por

último, la posesión y puesta a disposición de dispositivos o datos para la comisión de delitos.

- Los delitos informáticos, que abarcan la falsificación y el fraude informático.

- Los delitos relacionados con el contenido, limitados exclusivamente a la producción, difusión o tenencia de pornografía infantil.

- Los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, relacionado con la protección de las obras literarias y artísticas.

Partiendo de esta tipología, y con la finalidad de introducirla en el ordenamiento jurídico español, es promulgada la Ley Orgánica 1/2015, por medio de la cual se modificó el articulado del Código Penal español con la aspiración de "superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea" (Boletín Oficial del Estado, 2015, p. 27071). De esta manera, quedaban introducidos y modificados toda una serie de diversos delitos relacionados con el uso de sistemas informáticos, entre los que se encuentran el delito de acoso electrónico, el descubrimiento y revelación de secretos, los delitos de daños y delitos de interferencia ilegal en sistemas de información o datos, los delitos contra la propiedad intelectual, y los abusos con fines sexuales a menores cometidos a través de Internet u otros medios de telecomunicación.

Sin embargo, dada la necesidad de dar una respuesta amplia a todas las prácticas delictivas en el ámbito del ciberespacio, el Ministerio del Interior considera también ciberdelitos aquellos delitos contra el honor y las amenazas y coacciones, siempre que para cuya comisión sean empleados sistemas informáticos. De este modo, la tipología final de ciberdelitos que en la actualidad es contemplada por el Sistema Estadístico de Criminalidad (SEC) del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, que puede consultarse en el Anexo I del presente trabajo, se adapta de mejor manera a la realidad de la ciberdelincuencia en España.

2.2. La magnitud del fenómeno de la ciberdelincuencia en España

Delimitados ya algunos de los entornos jurídicos del fenómeno del ciberdelito en España, es pertinente preguntarse acerca de sus dimensiones reales. Cabe advertir que, como es obvio, las estadísticas publicadas por los organismos competentes en la persecución de estas prácticas delictivas, únicamente contemplan los hechos conocidos por estas mediante la interposición de una denuncia por parte de un particular o por investigación de oficio, y que, en consecuencia, solo representan parcialmente el

fenómeno de la ciberdelincuencia al existir un gran número de casos que no son oportunamente puestos en conocimiento de los cuerpos y fuerzas de seguridad del Estado, cosa habitual ante determinadas modalidades delictivas. Sin embargo, los informes y anuarios estadísticos publicados por el Ministerio del Interior representan una fuente de información de extraordinario valor y utilidad para cualquiera que pretenda hacerse una idea aproximada de la magnitud del fenómeno del ciberdelito en España.

Según el ya citado SEC, en el año 2015 se registraron un total de 60 154 ciberdelitos, de los cuales el 67.9% (40 864), correspondieron a fraudes informáticos, cerca de un 16.8% (10 112), a la de amenazas y coacciones, y en torno al 4% (2 386) a la de acceso e interceptación ilícita, representando el resto de modalidades delictivas un 11.2% aproximadamente. En cuanto a su distribución geográfica, destacan Andalucía con un 18.5% del montante total, además la Comunidad de Madrid con un 16.8%, la Comunidad Valenciana con un 12.6%, siendo además un 7.7% de los delitos denunciados en el extranjero. Dadas las dificultades inherentes a la hora de determinar los responsables de estas prácticas delictivas, únicamente se ha esclarecido el 32.2% (19 372) de los casos conocidos, saldándose con 5 445 imputaciones y detenciones, y con 46 860 victimizaciones[1] (Ministerio del Interior, 2015a).

En cuanto al perfil del ciberdelincuente, el 76% de los detenidos e imputados por este tipo de hechos son hombres (4 137), siendo especialmente partícipes en delitos sexuales (97%) y en interferencia en los datos y en el sistema (96%), mientras que en los delitos de falsificación informática y de fraude informático se registra una menor participación de estos (66% y 69%, respectivamente). Por otro lado, la nacionalidad de los detenidos e imputados es de forma mayoritaria española (85.7%), y entre los ciudadanos extranjeros partícipes de ciberdelitos, destacan los ciudadanos de Estados miembros de la Unión Europea (5.6%). Por su parte, las estadísticas de victimizaciones reflejan que el delito de fraude informático es la modalidad delictiva de mayor impacto en la sociedad, seguido del delito de amenazas y coacciones, con un 60.5% y un 22.8% del montante total respectivamente, siendo los hombres y mujeres de entre 26 a 40 años los grupos en los que se registra mayor victimización (37.7%).

Desde una perspectiva diacrónica, lo cierto es que, al igual que en el resto de países del entorno, la ciberdelincuencia en España se articula como una tendencia que ha mostrado un fuerte crecimiento durante los últimos años. De este modo, como puede verse en los datos recogidos en la Tabla 1, en el periodo 2011-2015 la magnitud de la cibercriminalidad no ha he-

1 Según el Sistema Estadístico de Criminalidad del Ministerio del Interior, por "victimización" debe de entenderse el número de hechos denunciados por personas que manifiestan ser víctimas o perjudicados por alguna infracción penal, mientras que el concepto de "víctima" se refiere a personas individuales.

cho sino aumentar, tanto en términos absolutos, con un incremento significativo del número total de ciberdelitos conocidos al año, como relativos, representando los ciberdelitos una pequeña pero cada vez mayor porción del total de infracciones penales cometidas.

Por otro lado, si bien el número de ciberdelitos en los que ha sido identificada su autoría ha aumentado año tras año, no lo ha hecho al mismo ritmo que el número de ciberdelitos conocidos, registrando un descenso de la tasa de esclarecimiento de ciberdelitos de forma consecutiva durante los últimos 3 años sobre los que existen cifras oficiales. Además, los datos recogidos por el SEC muestran que, dadas las ya mencionadas dificultades existentes para identificar a los responsables, en estas modalidades delictivas los autores gozan de mayor impunidad que la existente en la totalidad de infracciones penales conocidas, teniendo los ciberdelitos una tasa de esclarecimiento ligeramente menor. Además, aunque en cuanto al número total de victimizaciones solo existen estadísticas de los años 2014 y 2015, el crecimiento anual de este indicador sugiere que el impacto de la ciberdelincuencia en España, si bien aún pequeño, reviste una magnitud creciente. En definitiva, tal y como concluye el Anuario Estadístico del Ministerio del Interior:

> *"La variedad de los delitos informáticos, de la delincuencia informática, encuadrados dentro del término cibercriminalidad, y la diversidad de comportamientos constitutivos de esta clase de ilícitos es cada vez ma¬yor.(...) Estas formas delictivas han ido adquiriendo la suficiente entidad y gravedad como para constituir ataques serios a intereses jurídica¬mente protegidos de carácter tradicional, como a otros intereses novedosos y que en la actualidad no po¬seen una protección específica". (Ministerio del Interior, 2016, p. 423).*

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

Tabla 1 La evolución de la cibercriminalidad en España (2011-2015)

	2011	2012	2013	2014	2015
Infracciones penales	2 285 525	2 268 867	2 172 133	2 092 040	2 036 815
Ciberdelitos conocidos	37 458	42 812	42 403	49 935	60 154
Tasa de ciberdelincuencia	1.64%	1.89%	1.95%	2.39%	2.95%
Ciberdelitos esclarecidos	-	15 025	16 378	17 918	19 372
Tasa de esclarecimiento de ciberdelitos	-	35.1%	38.62%	35.88%	32.2%
Tasa de esclarecimiento general	39.9%	39.1%	41.9%	42.4%	35.1%
Victimizaciones	-	-	-	40 790	46 860

Fuente: Elaboración propia con base a los anuarios estadísticos del Ministerio del Interior de los años 2015, 2014, 2013, 2012 y 2011.

Con independencia del papel troncal que asumen los cuerpos y fuerzas de seguridad del Estado y otros organismos oficiales en la investigación de la ciberdelincuencia, es pertinente preguntarse si este es un fenómeno que atañe únicamente a las administraciones públicas o si, por el contrario, existen otros actores directamente interesados. A este respecto destacan no solo el amplio espectro de los usuarios comunes, sino también las organizaciones empresariales, objetos habituales de diferentes modalidades delictivas como el fraude informático o el ciberespionaje.

El informe "Encuesta sobre fraude y delito económico 2016. Resultados en España" publicado por la firma de consultoría PwC, y que se nutre de las opiniones de más de 6 000 altos ejecutivos de diferentes sectores económicos de 115 países, pone de manifiesto cual es la percepción existente en el ámbito empresarial en relación al fenómeno de la ciberdelincuencia: el 65% de los encuestados españoles consideran que la vulnerabilidad de sus empresas ante los ciberdelitos ha aumentado en los últimos 24 meses, cuando en 2014 solo emitieron una respuesta afirmativa el 16%. Pese a esta creciente percepción de la ciberdelincuencia en el mundo empresarial, el 42% de los encuestados españoles refleja que los consejos de administración de sus empresas no solicitan información periódica alguna sobre el estado de preparación de la organización para hacer frente a

ciberdelitos, y solo un 33% afirma que cuentan con un plan de respuesta ante un eventual ciberataque y un 40% ha articulado un equipo de respuesta inmediata que pueda movilizarse ante tales eventualidades (PwC, 2016). Así, entre diferentes conclusiones, el informe destaca que:

> *"Los resultados obtenidos por nuestros encuestados alarman sobre la inquietante falta de planes de emergencia o respuesta ante la detección de un ciberdelito y en aquellos casos, en los que se cuenta con dicho plan, llama la atención la falta de participación de la Alta Dirección y otro personal clave en las primeras actuaciones a llevar a cabo ante la detección del delito (...) para prevenir este tipo de delitos, es necesario que toda la organización considere la ciberseguridad como una responsabilidad propia, por lo que es imprescindible alertar y concienciar a la misma." (PwC, 2016, p. 18).*

No es de extrañar, en coherencia con todo lo anterior, que este tipo de prácticas delincuenciales represente para las autoridades españolas un fenómeno que requiere una atención cada vez mayor. Así, según el Centro Criptológico Nacional adscrito al Centro Nacional de Inteligencia, "la sofisticación de las técnicas usadas, la disponibilidad de nuevas o renovadas herramientas (incluyendo la prestación de servicios delincuenciales bajo demanda –on demand·) y la pulcritud en la perpetración de tales acciones constituyen una preocupación en franco crecimiento" (Centro Criptológico Nacional, 2016, p. 7).

En esta misma línea, tal y como pone de relieve el informe de 2016 The Internet Organised Crime Threat Assessment (Evaluación de la amenaza del crimen organizado en internet, en español), publicado por el Centro Europeo contra el Cibercrimen (EC3) de Europol, que analiza año tras año las tendencias clave a nivel europeo en este ámbito, España juega un papel especialmente relevante en determinadas modalidades ciberdelictivas, siendo junto a Italia en la Unión Europea, uno de los principales emisores de correo basura, y además, una de las 10 grandes fuentes mundiales de ataques de denegación de servicio, con aproximadamente el 7% del montante total (Europol, 2016).

2.3. Ciberdelincuencia y ciberterrorismo: Amenazas de creciente sofisticación

En lo que se refiere a la persecución de la ciberdelincuencia, no cabe duda de que uno de los principales obstáculos que encuentran las fuerzas y cuerpos de seguridad del Estado es el acceso por parte de los ciberdelincuentes a herramientas informáticas que permiten de manera sencilla asegurar en gran medida su anonimato. A este respecto, "lo cierto es que sigue siendo en la actualidad más compleja, pese a los rastros digitales del delito, la identificación de los autores de estas conductas que la de otros sujetos que cometen similares infracciones en el mundo real" (Miró,

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

2011, p. 12), lo que ofrece a los ciberdelincuentes grandes posibilidades de actuar de forma impune.

Durante los últimos años, entre los diferentes sistemas de navegación anónima existentes, el que ha ganado una mayor popularidad es la conocida como red Tor, que desde 2002 ofrece la posibilidad de proteger la identidad de los usuarios a través de una vasta red de servidores operados por voluntarios de todo el mundo, dificultando la localización física del usuario y su tráfico gracias a los múltiples nodos que componen la red Tor. En todo caso, si bien este tipo de sistemas ofrece soluciones de una eficacia considerable para el usuario medio, lo cierto es que distan de ser infalibles en términos absolutos, tal y como muestran los diferentes ataques que han sufrido por parte de organizaciones estatales y no estatales (Jané, 2017), pudiendo ser ataques de denegación de servicio, poblar sus redes con nodos controlados por un tercero, o reidentificar al usuario de la red a través de los datos del nodo de salida, que habitualmente se encuentran sin cifrar, entre otros (Salvador, 2012).

Cabe destacar que las prestaciones de la red Tor no se circunscriben únicamente al ocultamiento por parte de los ciberdelincuentes de su identidad digital para operar en la "Internet superficial" (Surface web), sino que, además, ofrece la posibilidad a estos de acceder a determinados contenidos en Internet que no se encuentran indexados por los motores de búsqueda convencionales, la denominada "Internet profunda" (Deep web). Entre todos estos contenidos no indexados, cuya magnitud supera a la de la web superficial, se encuentra la "Internet oscura" (Dark web), para acceder a ella es necesario contar con software específico como Tor, u otras aplicaciones como I2P o Freenet, cada uno de los cuales cuenta con diferentes redes de usuarios y direcciones, conocidas como Darknets.

Si bien las estimaciones más recientes apuntan a que cerca de la mitad de los dominios y de las URL de la Internet oscura albergan contenidos legales (Gollnick y Wilson, 2016), esta se articula como un espacio en el que concurren un amplio abanico de actividades ilícitas de diferente naturaleza:

> *"Una muestra de los productos y servicios ilegales que están disponibles dentro de las Darknets abarca los siguientes: Contenidos pirateados, drogas, dinero falsificado, productos de lujo robados, tarjetas de crédito y cuentas bancarias; robo de identidad, pasaportes y otros documentos oficiales, armas, munición y explosivos; servicios de mercenarios y asesinos a sueldo; contenidos de abuso sexual a menores; tráfico de seres humanos (adultos y menores); y tráfico de órganos". (Martín, 2017, p. 78).*

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

No cabe duda de que un entorno tan opaco como la Internet oscura es una plataforma idónea para las actividades de los ciberdelincuentes, y más en particular, para las organizaciones terroristas, que durante los últimos años han venido recurriendo a las posibilidades que ofrece el ciberespacio de manera cada vez más intensa con diversas finalidades, que van "desde el reclutamiento, la propaganda, la financiación, el adiestramiento, la incitación o provocación a realizar acciones terroristas; hasta el acopio y difusión de información con finalidad terroristas" (Lodeiro, 2017, p. 51). Sin embargo, la labor de los organismos nacionales e internacionales dedicados a la lucha contra las organizaciones terroristas, ha hecho que la Internet superficial sea un terreno poco seguro para estas últimas, dado que la actividad de sus miembros en ella puede ser monitorizada con facilidad, del mismo modo que pueden ser proscritos sus medios propagandísticos. En coherencia con lo anterior, no debe de extrañar que el uso de la Internet oscura por parte de organizaciones terroristas se haya convertido en una de las mayores preocupaciones de los servicios de seguridad, que requieren de nuevos métodos para analizar la actividad de organizaciones de corte yihadista como el Daesh en este ámbito de actuación (Weimann, 2016).

En todo caso, las posibilidades que ofrecen las Tecnologías de la Información y la Comunicación a las organizaciones terroristas, no se limitan a los aspectos logísticos y propagandísticos de su actividad, sino que también tienen un alcance eminentemente operativo. A este respecto, es destacable la importancia de los ataques a las infraestructuras consideradas críticas dado que la interrupción o perturbación severa de su funcionamiento, ocasionaría graves efectos sobre el normal desarrollo de las actividades básicas de la sociedad, por lo que una eventual operación terrorista podría "tener efectos potencialmente devastadores a todos los niveles de seguridad si se origina un ataque combinado (físico y cibernético) o un efecto de cascada (por un efecto sinérgico entre industrias de infraestructuras interdependientes)" (Miranzo y del Rio, 2014, p. 342). Ello se debe a que, cuando fueron diseñados, este tipo de infraestructuras no contaban con la necesidad de articular mecanismos de seguridad ante eventualidades que no tuvieran una naturaleza meramente física, tales como un desastre natural o una acción terrorista.

No obstante, en la actualidad, estas infraestructuras se han tornado más complejas, lo que ha redundado en el aumento de su vulnerabilidad y sensibilidad. Es por ello que la protección de las infraestructuras críticas solo puede realizarse convenientemente a través de un planeamiento integral, que abarque el conjunto de riesgos y amenazas a través de la cooperación público-privada, a sabiendas de que "el aspecto cibernético es una nueva capacidad de causar daño que no ha pasado desapercibida para los grupos terroristas y del crimen organizado, que lo han incluido como una clara alternativa para la comisión de sus atentados y delitos" (Caro, 2014, p. 8).

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

3. Formación especializada en materia de ciberdelincuencia: La propuesta de la Universidad Nebrija

3.1. La formación como línea de acción de la Estrategia de Ciberseguridad Nacional de 2013

Una vez expuestas de forma breve algunas de las claves acerca de los límites jurídicos y dimensiones reales del fenómeno de la ciberdelincuencia en España, cabe preguntarse por las políticas adoptadas durante los últimos años por el poder ejecutivo para hacer frente a esta amenaza. Ante las preocupantes tendencias situadas anteriormente, que parecen expresar la consolidación del fenómeno de la ciberdelincuencia y su configuración como una problemática de creciente magnitud para la seguridad de los españoles, la ya citada Estrategia de Ciberseguridad Nacional representa, con todo y sus posibles carencias (Fojón, 2013), el documento que sirve como base de la política de ciberseguridad del Gobierno de España.

Entre los objetivos que plantea, teniendo en consideración el propósito del presente trabajo, es pertinente destacar algunos como "potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio" (Departamento de Seguridad Nacional, 2013, p. 24), o "alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad" (Departamento de Seguridad Nacional, 2013, p. 26). Asimismo, y con la finalidad de sentar los ejes de trabajo necesarios para alcanzar tales objetivos, el mencionado documento recoge toda una serie de líneas de acción en materia de ciberseguridad nacional, entre las cuales es oportuno reseñar las siguientes:

- Línea de acción 4, relativa a la capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia, que incluye la necesidad de "ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia, así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad" (Departamento de Seguridad Nacional, 2013, p. 35).

- Línea de acción 6, referida a la adquisición de conocimientos y competencias e I+D+i, que plantea entre sus tareas "extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con universidades y centros especializados" (Departamento de Seguridad Nacional, 2013, p. 37).

Al calor de lo anteriormente expuesto, se evidencia que algunas de las principales prioridades de las autoridades españolas en relación a la ci-

berdelincuencia como fenómeno de una creciente entidad, sofisticación e impacto en la sociedad española se refieren, en lo fundamental, a la adquisición de mayores capacidades en un sentido general por parte de los organismos competentes en la prevención, investigación y persecución del ciberdelito.

A este respecto, la adecuada cualificación del personal dedicado a dichas labores representa una tarea de relevancia estratégica, especialmente en el seno de los organismos que gozan de prerrogativas en este campo, las fuerzas y cuerpos de seguridad del Estado, pero también en otras agencias estatales vinculadas de forma más o menos directa con la ciberseguridad, e incluso en el mundo empresarial. Huelga decir que, ante tal necesidad, las entidades universitarias juegan un papel de importancia mayúscula como instituciones respaldadas y reconocidas por la administración en la función docente, mediante la oferta de programas e itinerarios formativos de nivel superior, y como centros con capacidad de vehicular el trabajo de grupos de investigación.

3.2. La formación sobre ciberseguridad en España: Estado de la cuestión

Ya descrito someramente, el fenómeno de la ciberdelincuencia y la importancia otorgada por el gobierno de España a la generación de medios para la lucha efectiva contra este, puede decirse que la capacitación de especialistas en materia de ciberseguridad pasa a ser una tarea de relevancia estratégica, pudiendo afirmarse que "es una cuestión de seguridad nacional tener profesionales con una sólida formación en ciberseguridad trabajando en todos los sectores de la nación, tanto privados como públicos, en el desarrollo y en el mantenimiento de sistemas informáticos" (Hidalgo, 2013, p. 48).

Teniendo en cuenta la simbiótica relación existente entre la Administración Pública, las organizaciones empresariales y las instituciones académicas; en relación a la seguridad en el ciberespacio, no es de extrañar que durante los últimos años se haya experimentado un aumento inusitado de la oferta formativa en materia de ciberseguridad, fundamentalmente a nivel de estudios de posgrado.

Así, en palabras del Instituto Nacional de Ciberseguridad (INCIBE), adscrito al Ministerio de Industria, Energía y Turismo,

> *"mientras que la presencia de programas o asignaturas específicas en seguridad era anecdótica hace tan solo unos años, en el curso académico 2014/15 se han identificado 83 programas de posgrado sobre Seguridad y Fiabilidad, de los que 26 llevan el título de Máster en Ciberseguridad". (INCIBE, 2016b, p. 15).*

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

Según este mismo organismo, en España un total de 78 instituciones de diferente naturaleza, siendo 26 de ellas universidades, imparten acciones formativas en materia de ciberseguridad durante el año 2017 (INCIBE, 2017a), con un total de 45 acciones formativas de posgrado, de las cuales 19 se imparten presencialmente, 21 de manera online y 5 bajo la modalidad semipresencial (INCIBE, 2017b).

Sin embargo, tal y como indica el INCIBE, no son pocos los problemas existentes a la hora de diseñar una oferta formativa ajustada a las necesidades profesionales de los alumnos para su incorporación al mercado laboral: Brecha entre los requerimientos de las empresas y las características de los candidatos, la constante transformación del sector, la dificultad de los alumnos de adquirir experiencia práctica previa, o la inexistencia de una metodología clara; son solo algunas de las dificultades existentes a este respecto, por lo que el INCIBE concluye que "se hace indispensable la adecuación de los programas formativos, o la creación de otros nuevos específicos, para acercar de la mejor forma posible la oferta a la necesidad real del mercado" (INCIBE, 2016b, p. 26).

Por otro lado, cabe destacar la importancia de la labor realizada por el propio INCIBE en el ámbito de la formación no reglada en ciberseguridad, siendo promotora de eventos específicos sobre la materia tales como el **CyberCamp,** encuentro encaminado a identificar, atraer, y gestionar la generación de talento para su aprovechamiento en el sector privado; o el **Summer BootCamp,** iniciativa de alcance internacional específicamente destinada a la capacitación y adiestramiento de los especialistas de las FCSE y del personal técnico de entidades públicas en seguridad informática. Del mismo modo, hasta la finalización del año 2016, INCIBE contó con un programa de becas dotado de 400 000 euros para alumnos de un total de 25 acciones formativas que van desde cursos de posgrado a certificaciones, así como ayudas a la investigación avanzada en ciberseguridad para organismos públicos de investigación y universidades públicas y privadas en 2 modalidades no excluyentes: Las ayudas para contratos predoctorales dirigidas al personal investigador en formación que desee realizar una tesis relacionada con la ciberseguridad; y las ayudas dirigidas a la contratación de doctores y su incorporación al Sistema Español de Ciencia, Tecnología e Innovación, formado por agentes públicos y privados dedicados a la I+D+i en España. Asimismo, INCIBE oferta cursos breves gratuitos en formato online orientados a un amplio público de las FCSE, del mundo empresarial, etcétera.

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

3.3. La Universidad Nebrija: Una institución comprometida con la formación en materia de seguridad

La Universidad Nebrija, fundada en 1995, es una universidad privada que toma su nombre haciendo homenaje a una de las grandes figuras de las letras españolas, el humanista sevillano Antonio Martínez de Cala y Xarava, más conocido como Antonio de Nebrija. En la actualidad, la Universidad Nebrija oferta 64 carreras universitarias y 60 programas de posgrado en las áreas de la Ingeniería, la Arquitectura, las Ciencias Sociales, el Turismo, las Ciencias de la Salud, las Ciencias de la Comunicación, las Artes Escénicas, las Bellas Artes, las Lenguas y la Educación; a través de las diversas facultades, escuelas y centros adscritos. Cabe destacar que, durante el pasado curso 2015/2016, se formaron en la Universidad Nebrija un total de 7 375 estudiantes, de los cuales 2 785 eran alumnos extranjeros, confirmando su clara vocación y orientación internacional.

Por otro lado, dado las necesidades específicas de quienes por circunstancias personales y/o profesionales encuentran grandes dificultades a la hora de seguir un programa formativo de tipo presencial, en 2012 la Universidad Nebrija lanzó el **Global Campus Nebrija**, medio por el cual se imparten titulaciones bajo un modelo de aprendizaje a distancia en el que durante el curso 2015/2016 participaron 2 381 alumnos a través de 26 programas formativos (Universidad Nebrija, 2016).

Durante los últimos años, y dado el creciente interés del público general en las materias vinculadas a la seguridad, la Universidad Nebrija ha realizado una clara y fuerte apuesta por ofertar programas académicos que supongan un salto cualitativo en la formación en materia de seguridad, tanto para quienes buscan iniciar su carrera profesional en este sector, ya sea en su vertiente pública como privada, como para aquellos que, contando con una trayectoria en el mismo, requieren de una actualización y acreditación de sus conocimientos.

A este respecto, destaca el Grado en Seguridad, título oficial universitario con una duración de 4 años e impartido íntegramente en modalidad online. Dicha titulación, habilitante para la obtención de la licencia de director de seguridad y jefe de seguridad por el Ministerio del Interior, ofrece al alumnado una formación eminentemente multidisciplinar, abarcando los diferentes campos de estudio relacionados con la seguridad en un sentido amplio, y contemplando además la realización de prácticas profesionales en empresas de seguridad privada y en instituciones públicas, donde existe la posibilidad de convalidar por el ejercicio profesional de cada estudiante. De este modo, el Grado en Seguridad se configura como un medio de gran utilidad para un número cada vez mayor de integrantes de las fuerzas armadas y de las fuerzas y cuerpos de seguridad del Estado, especialmente para aquellos que buscan un nuevo impulso en su carrera

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

profesional. Además del Grado en Seguridad, la Universidad Nebrija oferta el Máster en Seguridad y Defensa, título oficial universitario impartido tanto presencialmente como a distancia y respaldado por la Cátedra Nebrija-Santander en Análisis y Resolución de Conflictos.

Aunque los aspectos vinculados a la ciberseguridad son objeto de estudio desde una perspectiva general en los programas formativos citados anteriormente, dada la complejidad de un fenómeno como el de la ciberdelincuencia y su creciente magnitud e impacto, se torna imprescindible articular una oferta formativa del más alto nivel y que provea de una capacitación profesional plena en su adecuado tratamiento. En consecuencia, la Universidad Nebrija lanzó en el curso 2016/2017 la primera edición del Máster en Ciberdelincuencia con el apoyo de la Fundación Policía Española, el Cuerpo Nacional de Policía y de Telefónica España; con la aspiración fundamental de realizar una aportación a la altura de las necesidades actuales en el terreno de la ciberseguridad y facilitar a sus alumnos los conocimientos y competencias necesarias para encarar de forma resuelta el fenómeno de la ciberdelincuencia en España. A continuación, se exponen algunos de los pormenores de este programa formativo de posgrado.

3.4. El Máster en Ciberdelincuencia de la Universidad Nebrija: Conocimientos y competencias

El Máster en Ciberdelincuencia de la Universidad Nebrija ofrece la valiosa oportunidad a sus participantes de adquirir un conocimiento detallado del fenómeno del ciberdelito, de sus agentes, del entorno en el que sucede y de su tratamiento; antes, durante y tras su comisión. Con este posgrado oficial, el egresado de la Universidad Nebrija contará con un alto grado de especialización en lo que a los principales riesgos y amenazas en el ámbito de la ciberseguridad se refiere, y contará con la capacidad necesaria para implementar los procedimientos requeridos en el análisis e investigación de las diferentes modalidades de ciberdelito, en cuestiones tales como: Los ciberataques en diferentes sistemas operativos, el análisis de vulnerabilidades, la redes y el software de aplicación, los sistemas web o las bases de datos.

Todo ello con el objetivo principal de brindar al estudiante una base teórico-práctica que, a la hora de plasmar los conocimientos y habilidades adquiridos en su desempeño profesional, le permitan tomar decisiones proactivas y reactivas frente a posibles fallos de ciberseguridad, formando robustos equipos directivos, partiendo de un conocimiento preciso acerca de la legislación en materia de sistemas de información y contando con un manejo solvente de las metodologías y técnicas necesarias para gestionar, planificar, diseñar e implementar los procedimientos necesarios para optimizar la seguridad de los diferentes activos, teniendo siempre en consideración el carácter cambiante y adaptativo de las amenazas en este ámbito.

Para tales fines, el Máster en Ciberdelincuencia de la Universidad Nebrija se encuentra orientado a ofrecer las siguientes competencias:

- La obtención, mantenimiento y procesamiento de evidencias digitales, utilizando procedimientos y herramientas específicas.
- El desarrollo de técnicas y el uso de herramientas que exploten al máximo tanto habilidades como conocimientos para la realización de pruebas de intrusión a sistemas y redes.
- La adquisición de una visión general e introductoria al mundo de la ciberseguridad, explicando los ataques más relevantes y cómo mitigarlos.
- La comprensión de los fundamentos de la monitorización y correlación de eventos de seguridad, mediante el estudio, la elaboración e interpretación de informes reales.
- La elaboración de desarrollos en programación segura y el mejoramiento de tus habilidades en auditoría de seguridad en el análisis y evaluación del código fuente de las aplicaciones.
- La implementación de auditorías de seguridad, analizando los hechos y la información de seguridad recopilada, así como la aplicación de la ingeniería inversa y la ciberinteligencia.
- La realización de un correcto análisis forense.
- La aplicación de la seguridad ofensiva desde las metodologías de un ciberataque.

Para cumplir con dichos requerimientos formativos, el itinerario formativo ofrecido por el Máster en Ciberdelincuencia de la Universidad Nebrija se articula mediante un total de 8 bloques, cada uno de los cuales cuenta con una carga lectiva de 6 créditos ECTS y 45 horas de clase. Además de cada uno de los módulos formativos, el Máster en Ciberdelincuencia contempla la necesidad de que cada uno de los estudiantes cumpla satisfactoriamente un periodo de prácticas en organizaciones empresariales u organismos públicos. Por último, deberán elaborar y presentar de manera individual un proyecto de investigación en calidad de trabajo de fin de Máster, orientado a profundizar en uno o en varios aspectos de los contenidos del programa, siempre bajo la dirección de un tutor con experiencia en la materia.

El Bloque I, titulado “Ciberseguridad y agentes de la amenaza”, se encuentra dirigido a ofrecer a los estudiantes una introducción a los principales conceptos del ciberespacio y la ciberseguridad, sus características,

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

objetivos y funciones; y una introducción a la ecuación del riesgo con sus diversos componentes, vulnerabilidades y amenazas, finalizando con una descripción de los principales agentes que se identifican actualmente en este espacio cibernético (hackers, ciberactivistas, cibercriminales, ciberterroristas y Estados). Por otro lado, este primer bloque se dedica a una revisión del estado del arte de la ciberseguridad mediante un repaso de las principales estrategias nacionales y conjuntas de ciberseguridad con especial énfasis en la estrategia española finalizando con la presentación del denominado Esquema Nacional de Seguridad (ENS).

Asimismo, se expone una diferenciación entre incidentes, eventos y ataques, así como una breve presentación de uno de los activos a proteger de los ciberataques, las denominadas infraestructuras críticas para, posteriormente, presentar una tipología de los diferentes delitos cibernéticos y la evolución del cibercrimen caracterizada por los nuevos delitos recogidos en la reforma del Código Penal. Finalmente, este primer bloque está dedicado a los modernos riesgos y amenazas, en particular el denominado CaaS, o crimen como servicio, los mercados digitales de servicios ocultos, los sistemas de anonimización y los vectores de ataque con especial énfasis en las APT (amenazas persistentes avanzadas).

El Bloque II, titulado "Marco jurídico: aspectos transversales", se concibe como una introducción a los aspectos jurídicos de la interacción entre derecho y tecnología, ofreciendo una amplia descripción de la legislación internacional y europea referida al fenómeno del ciberdelito, así como a la aproximación a este realizada por el ordenamiento jurídico español, tanto desde la perspectiva del derecho penal y procesal, como desde otras disposiciones legislativas de carácter sectorial en relación a cuestiones como la privacidad, la protección de datos y el comercio electrónico.

Este segundo bloque sirve de reflexión acerca de la ausencia de una reacción temprana del legislador ante los hitos informáticos de nuestra historia reciente. Así, mientras las fuerzas y cuerpos de seguridad del Estado hacen un ímprobo esfuerzo por ponerse al día en materia de persecución de la criminalidad informática, estos han resultado en gran medida baldíos, al no verse respaldados por una normativa que permita desarrollar sus investigaciones con el adecuado paraguas legislativo. Por ello, este bloque aborda las diferentes dificultades existentes ante la falta de un cambio de modelo orgánico procesal que haga verdaderamente eficaces los avances en materia legislativa, y que a la postre supone considerables problemas a la hora de llevar a la práctica sus disposiciones. Entre ellas, destaca el desarrollo del llamado "deber de colaboración" que se impone a empresas y particulares que tengan una especial e íntima relación con las tecnologías utilizadas para la comisión de los delitos o para la protección de la impunidad de los delincuentes, cuestión que es tratada en este segundo bloque.

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

El Bloque III, planteado como "Taller tecnológico de la ciberdelincuencia", gira en torno a algunos de los fundamentos tecnológicos de la ciberseguridad y del ciberdelito, presentando en primera instancia una introducción a la arquitectura de los ordenadores y a los sistemas operativos, mostrando cómo está estructurado un ordenador convencional, qué elementos tiene, cómo se comporta, cómo interactúa y cómo funciona para, posteriormente, mostrar una visión general de qué es un sistema operativo y cuáles son sus funciones principales, para entender los fundamentos de los sistemas actuales. Acto seguido, los estudiantes se familiarizan con 3 de los sistemas de archivos más utilizados hoy en día, profundizando en las estrategias que adoptan los ordenadores para manejar estos archivos, así como las ventajas e inconvenientes que presenta cada uno. Para finalizar, en este bloque se estudian los cimientos de la mayor parte de las redes actuales, tanto locales como globales (por ejemplo, Internet), se explica cómo y porqué funcionan para, finalmente, estudiar las redes wifi. En esta última parte se muestran las fortalezas y las debilidades de la tecnología wifi, así como las distintas formas de atacarla y, por lo tanto, dotarla de la seguridad conveniente.

El Bloque IV, titulado "Gestión de proyectos de investigación aplicado a la ciberdelincuencia", inicia a los estudiantes del Máster en los principios fundamentales de la investigación tecnológica, sus consideraciones generales y bases para su desarrollo, analizando los aspectos relacionados con la verificación de los hechos y la obtención de evidencias para la investigación. A tal fin, se exponen los primeros aspectos a considerar con la investigación como son la identificación del titular dominio o webmaster, la localización e investigación de páginas web, los requerimientos de datos al administrador web, metadatos, descarga de páginas y captura de información y requerimientos policiales para solicitud de datos; todo ello desde el prisma de garantizar su validez en el proceso judicial. También se muestra la importancia de las evidencias en el marco de la investigación tecnológica y se profundiza en aspectos relacionados con los proveedores de servicio de Internet y de telecomunicaciones, evidencia de los datos de tráfico, estudio de datos, localización, ubicación, línea de acceso y titular, resolución IP, determinación de terminal y usuario, diferenciación entre dispositivos y elementos tecnológicos de las telecomunicaciones (tarjeta SIM, antenas BTS, etcétera) y la trazabilidad de usos de terminales móviles en el tiempo y en el espacio. Como último aspecto de este cuarto bloque, se analizan las tecnologías emergentes y las vulnerabilidades en la gestión de la información.

El Bloque V, titulado "Auditoria forense de la ciberdelincuencia", introduce a los estudiantes en la utilización de las principales técnicas del proceso de análisis forense digital en diferentes sistemas operativos, así como de los procedimientos antiforenses. Para ello, en primer lugar, se define de forma precisa qué es una auditoría, y cuál es su misión en las organiza-

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

ciones, tomando como base estándares y guías aceptadas, que han sido reconocidas internacionalmente. En ese sentido, este V bloque profundiza en la auditoría de sistemas de información como actividad vinculada a la ciberdelincuencia, revisando los aspectos fundamentales de esta primera: Tipos de trabajos, evidencias, técnicas asistidas por ordenador, diligencia profesional, irregularidades, ciclo de vida y privacidad; así como otros aspectos significativos.

Por otro lado, se revisan los aspectos fundamentales en la prevención y detección de toda clase de delitos, entre los que se encuentran los relacionados con la ciberdelincuencia. En base a mejores prácticas internacionales, se exponen modelos para la identificación, evaluación y gestión eficaz de riesgos, así como el establecimiento de un efectivo control interno que permita garantizar entre otros objetivos la salvaguarda de activos. Además, en un plano puramente práctico, este quinto bloque concreta procedimientos de trabajo para realizar auditorías específicas en la lucha contra la ciberdelincuencia, como, por ejemplo: Procedimiento de virus y otros códigos maliciosos, cortafuegos, análisis de vulnerabilidades, control de cambios en software o procedimiento de gestión de claves. Para terminar este bloque, se realizan análisis específicos de ciberseguridad, entre los que se encuentran los análisis forenses, de malware, caja blanca, caja negra, o fuentes abiertas.

El Bloque VI, titulado "Entorno y equipo de investigación de ciberdelincuencia", aborda, además de las técnicas de ciberataques y de las medidas de análisis de vulnerabilidades, la implementación de diferentes tipos de auditorías de ciberseguridad (caja blanca, caja negra, cumplimiento, test de penetración, "Red Team"). En este sexto bloque los estudiantes también tienen ocasión de explorar las metodologías y buenas prácticas asociadas a las auditorías de ciberseguridad (OSSTMM, OWASP, ISSAF, NIST 800-115, etcétera), y de obtener un conocimiento profundo sobre la diversidad de herramientas de necesario manejo en el diseño de auditorías de ciberseguridad, y los entornos en los que estas deben ser realizadas más habitualmente (Windows, Linux, etcétera).

El Bloque VII, titulado "Metodología de la investigación policial aplicada a la ciberdelincuencia", profundiza en los aspectos metodológicos del proceso de investigación en las diferentes tipologías delictivas, vinculadas de una manera u otra con el ciberespacio, tanto en lo referido a los delitos informáticos de más reciente aparición como a los delitos tradicionales, abordando los ataques contra sistemas informáticos, los delitos contra la propiedad intelectual e industrial, la explotación sexual infantil o las diferentes modalidades de fraude informático, entre otros; pero también, la metodología de la investigación y la obtención de evidencias electrónicas en delitos tradicionales como homicidios, el blanqueo de capitales, la violencia doméstica, etcétera. Para finalizar este séptimo bloque, se exponen

otras cuestiones de vital importancia para la investigación policial de las modalidades delictivas anteriormente citadas, tales como la investigación en redes sociales, la adquisición de evidencias electrónicas en el registro domiciliario, o los pormenores de la coordinación nacional e internacional entre diferentes cuerpos policiales en la lucha contra la ciberdelincuencia.

Por último, el Bloque VIII, titulado "Ciberterrorismo", ofrece a los estudiantes una aproximación a las particularidades y aspectos jurídicos del ciberterrorismo, partiendo de la diferenciación de este con otras modalidades y fenómenos como la ciberguerra. Partiendo de las peculiaridades que caracterizan el uso de Internet con fines terroristas, este octavo y último bloque hace un especial énfasis en la prevención y persecución de ciberoperaciones contra infraestructuras críticas, aquellas infraestructuras estratégicas cuyo funcionamiento es vital sin existir soluciones alternativas, haciendo que su perturbación o destrucción suponga un grave impacto sobre los servicios esenciales que mantienen las funciones sociales básicas, la salud, la seguridad, el bienestar económico-social de los ciudadanos y el adecuado funcionamiento de las administraciones públicas. Tratándose de instalaciones, redes, sistemas y equipos físicos basados en las tecnologías de la información; se procede a capacitar a los estudiantes en la obtención de información de fuentes abiertas ante este tipo de amenazas, a través de análisis de casos prácticos que les permitan extraer conclusiones derivadas de la experiencia real en la protección de infraestructuras críticas.

En lo que se refiere al profesorado, la Universidad Nebrija ha contado para el diseño del Máster en Ciberdelincuencia con un equipo de profesionales de prestigio de muy diversa procedencia, pero que comparten su dedicación y alto grado de especialización en el ámbito de la ciberseguridad. De este modo, el equipo docente del Máster en Ciberdelincuencia se nutre de profesores de una dilatada experiencia en diferentes organismos públicos como: Ingeniería de Sistemas para la Defensa (ISDEFE), empresa especializada en consultoría tecnológica adscrita al Ministerio de Defensa, y que forma parte del sector público estatal español; el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), organismo dependiente del Ministerio del Interior encargado del impulso, coordinación y supervisión de las actividades encomendadas a la Secretaría de Estado de Seguridad en relación a la protección de infraestructuras críticas en el territorio nacional; o de diversas instancias del Cuerpo Nacional de Policía, tales como la Unidad de Investigación Tecnológica o la Comisaría General de Información. Este equipo docente realiza su labor bajo la dirección de Bernardino Cortijo, excomisario del Cuerpo de Policía Nacional y actual Director de Seguridad Corporativa de Telefónica.

Dado que esta primera edición del Máster en Ciberdelincuencia se encuentra específicamente dirigida a miembros de las fuerzas y cuerpos de seguridad del Estado, quienes no cuentan por lo general con la disponibilidad

suficiente como para asegurar el seguimiento de un programa de posgrado de manera presencial, este adopta un formato semipresencial. De este modo, partiendo del planteamiento del anteriormente mencionado Global Campus Nebrija, el Máster en Ciberdelincuencia se imparte mayoritariamente a distancia, contando con un campus virtual basado en Blackboard, una de las plataformas comerciales educativas más extendidas del mercado a nivel mundial. La plataforma Blackboard integra toda una serie de aplicaciones que garantizan una experiencia de enseñanza y aprendizaje plena y dinámica, de las cuales se hace uso en el Máster en Ciberdelincuencia no solo como instrumentos para desarrollar la labor docente, sino también como medios de evaluación.

Además de almacenar los contenidos de las asignaturas, en el campus virtual los alumnos pueden encontrar diversos foros en los que se desarrollan casos prácticos y debates dirigidos por el profesor pertinente, en los cuales la participación de estos primeros es parte de los criterios de evaluación final de la asignatura. Asimismo, los alumnos realizan los exámenes parciales en esta misma plataforma, y a través de ella participan en las 2 sesiones síncronas en formato de videoconferencia contempladas para cada una de las asignaturas, en las cuales el profesor expone la materia de estudio e interactúa con los alumnos participantes resolviendo sus posibles dudas o peticiones. En todo caso, en el marco de cada asignatura se celebra un número considerable de sesiones de carácter presencial con el objetivo de facilitar la adquisición de conocimientos y competencias en las áreas de mayor dificultad técnica, y en las que una reforzada interactuación alumno-profesor pasa a ser imprescindible para garantizar un aprendizaje adecuado.

Llegados a este punto, es pertinente preguntarse qué tipo de expectativas pueden tener los alumnos del Máster en Ciberdelincuencia en cuanto a su futuro profesional. A este respecto, cabe destacar que una de las principales características que define los programas formativos ofertados por la Universidad Nebrija es su orientación a la empleabilidad de sus egresados, política por la cual se hace énfasis en un diseño eminentemente práctico de estos. No obstante, el subsector de la ciberseguridad en España guarda importantes particularidades que es necesario abordar para explorar con rigor el futuro laboral de los especialistas en ciberseguridad general, y los egresados del Máster en Ciberdelincuencia de la Universidad de Nebrija en particular.

3.5. El subsector de la ciberseguridad en España: Particularidades y carencias

Tal y como se ha expuesto, el Máster en Ciberdelincuencia de la Universidad Nebrija se configura como una propuesta formativa con una clara orientación hacia la profesionalización. Es por eso que una de las princi-

pales preocupaciones de la universidad es dotar a los estudiantes de los conocimientos, competencias y experiencia requeridos para una exitosa y pronta incorporación al mercado laboral. Siendo el de la informática uno de los sectores de mayor dinamismo y cambio, es preciso introducir determinadas claves acerca del subsector de la ciberseguridad en España para comprender de forma integral como la universidad puede satisfacer las necesidades del mercado a través de sus programas formativos.

Es importante subrayar que, con carácter general, durante los últimos años se ha experimentado un crecimiento sin parangón en la demanda de perfiles especializados en ciberseguridad. Ello no es producto de la casualidad: Según datos del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) del Ministerio de Industria, Energía y Turismo, en 2014 las 533 empresas que componían el subsector de la ciberseguridad facturaron un total de 598,2 millones de euros y dieron empleo a 5 808 personas en España. Asimismo, durante el periodo comprendido entre 2014 y 2019, las estimaciones del ONTSI señalaban que el gasto por parte de empresas en productos y servicios de ciberseguridad pasaría de 744 a 1 014 millones de euros, es decir, un ascenso del 36% (ONTSI, 2015). Tales cifras son buena muestra de la cada vez mayor preocupación y concienciación de las empresas con las problemáticas vinculadas a la ciberseguridad, especialmente ante el fuerte incremento de las incidencias producidas durante esos mismos años, que pasaron de 13 301 en 2014 a 39 985 en 2015, es decir, una variación de más del 200%, siendo los ataques de una criticidad alta los más habituales.

Al igual que el conjunto de campos que componen el sector de las tecnologías de la información, las estimaciones existentes apuntan a que durante los próximos años se producirá un crecimiento sostenido de la demanda de especialistas en ciberseguridad en España de aproximadamente un 12%. Sin embargo, según el INCIBE,

> *"la descripción del escenario se completa con un volumen importante de puestos de ciberseguridad que quedan sin ser cubiertos, en parte motivado por la falta generalizada de profesionales en el ámbito de las TIC y en particular por la escasez de competencias del profesional de la ciberseguridad". (INCIBE, 2016b, p. 17).*

Esta falta de adaptación de las competencias y conocimientos de los candidatos se encuentra directamente relacionada con la falta de definición que la ciberseguridad aún adolece como ocupación profesional, que solo recientemente ha comenzado a ser objeto del interés por parte de las administraciones públicas y las empresas como actividad con entidad propia dentro del sector de las tecnologías de la información y la comunicación.

Ante tal panorama, cabe preguntarse acerca del estado actual de la especialización en ciberseguridad como ocupación profesional. Según el Ser-

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

vicio Público de Empleo Estatal (SEPE), organismo adscrito al Ministerio de Empleo y Seguridad Social que en 2014 abordaría por vez primera el análisis del subsector, la ocupación de especialista en ciberseguridad quedaría encuadrada en el subgrupo 2729 de la Clasificación Nacional de Ocupaciones del Instituto Nacional de Estadística de 2011, denominada "Especialistas en bases de datos y en redes informáticas no clasificados bajo otros epígrafes" y perteneciente al grupo 27 de "profesionales de las tecnologías de la información". No obstante, debido a la vaguedad de tal designación, las ofertas de empleo referidas a los especialistas de ciberseguridad reciben muy diferentes denominaciones, no existiendo una única forma de aludir a tal ocupación. De este modo, entre las ofertas de empleo recogidas de Internet por el SEPE, existen hasta un total de 13 denominaciones distintas utilizadas para referirse al perfil del especialista en ciberseguridad: Administrador de seguridad de red, consultor de seguridad y hacking ético, experto en seguridad informática, analista de seguridad, entre otras.

En cuanto al perfil del especialista en ciberseguridad, según el SEPE, en la totalidad de las demandas de empleo monitorizadas vienen descritas las competencias generales del profesional de la ciberseguridad que se valoran, entre las cuales destacan la capacidad de aprendizaje autodidacta, la colaboración y el compromiso, la innovación, la creatividad, la orientación al logro de resultados, la disponibilidad, la adaptabilidad y la flexibilidad, la capacidad de integración en equipos multidisciplinares, así como la iniciativa y el dinamismo. A su vez, el SEPE enumera las competencias específicas que estos profesionales deben cumplir: El especialista en ciberseguridad requiere competencias para manejar sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones; implantar protocolos criptográficos y herramientas de seguridad basadas en dichos protocolos; analizar y detectar amenazas de seguridad y desarrollar técnicas de prevención; conocer e interpretar la normativa de centros de respuesta a incidentes; seguridad en centros financieros y de negocio, seguridad en infraestructuras de defensa y auditoría de sistemas; crear y desarrollar proyectos de seguridad informática y de las comunicaciones; análisis forense y análisis malware.

En cuanto a los conocimientos requeridos, el informe del SEPE indica que algunos con lo que los candidatos deben contar están relacionados con diferentes entornos tecnológicos y otras arquitecturas tecnológicas de propósito general; análisis forense; análisis de malware; análisis y evaluación de vulnerabilidades técnicas para el descubrimiento y explotación de vulnerabilidades tanto en servidores como en puestos; y, por último, la adecuada gestión de incidentes. Asimismo, el SEPE indica que las empresas buscan perfiles con experiencia en el ámbito de las políticas y normativas de seguridad; del diseño y desarrollo de proyectos, planes, programas y herramientas de seguridad que den soporte o automaticen parte de las

tareas a realizar; de la Implantación de Sistemas de Gestión de la Seguridad en la Información; y de la gestión de seguridad, siendo además un requisito imprescindible contar con un elevado nivel del idioma inglés (SEPE, 2014).

3.6. La segunda edición del Máster en Ciberdelincuencia: Una apuesta por la especialización

El constante estado de transformación por el cual atraviesa el subsector de la ciberseguridad en España, obliga a que cualquier propuesta formativa en este campo sea sometida a un proceso de permanente revisión y actualización. De otro modo, la caducidad de sus contenidos ante el imparable proceso de cambio tecnológico y delincuencial conducirá a la obsolescencia de sus contenidos, y, por ende, a una capacitación insuficiente de sus egresados, por lo que su empleabilidad se verá sensiblemente mermada. Ante este riesgo, y aun tratándose el Máster en Ciberdelincuencia de una iniciativa joven, la Universidad Nebrija apuesta por mantener debidamente actualizada su oferta formativa en pos de garantizar que esta se encuentra debidamente adaptada a las presentes condiciones del mercado laboral.

Dado que, tal y como se ha expuesto a lo largo del presente trabajo, las empresas son, junto a las administraciones públicas, actores de importancia estratégica en lo que al fenómeno de la ciberdelincuencia se refiere, y que las necesidades de unos y otros guardan sus particularidades en términos de la capacitación de su personal, se torna imprescindible ofrecer itinerarios formativos especializados que permitan satisfacer en mayor medida las necesidades específicas de cada uno de ellos. Así, la segunda edición del Máster en Ciberdelincuencia parte de un bloque de asignaturas de carácter troncal y obligatorio para el conjunto de los alumnos: “Ciberseguridad y agentes de la amenaza”, “Marco jurídico: Proceso penal, aspectos transversales y agente encubierto”, “Taller tecnológico de ciberdelincuencia”, “Gestión de proyectos de investigación aplicado a la Ciberdelincuencia”, “Auditoria forense de la ciberdelincuencia”, “Entorno y equipo de investigación de ciberdelincuencia”; pero, al mismo tiempo, ofrece 2 itinerarios formativos en especializaciones a elegir por el estudiante:

- El itinerario enfocado a FCSE, por un lado, que se mantiene con una estructura idéntica a la del Máster en su primera edición, con las asignaturas específicas de “Metodología de la investigación policial aplicada a la ciberdelincuencia”, y de “Ciberterrorismo”.

- El itinerario orientado al ámbito empresarial, por otro lado, que ofrece la posibilidad a los estudiantes de elegir 2 de 3 asignaturas específicas: “Compliance: Prevención de delitos empresariales”, “Responsabilidad social corporativa. Reputación”, y “Ciberinteligencia”.

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

De este modo, y dadas las particularidades del subsector de la ciberseguridad anteriormente expuestas, la Universidad Nebrija articula un innovador programa formativo capaz de satisfacer las necesidades de un amplio abanico de profesionales, atendiendo siempre a las particularidades que guardan los 2 campos de aplicación a los que se encontrará orientado el Máster en su segunda edición. De este modo, al margen de los contenidos del itinerario orientado a FCSE, que ya han sido expuestos en páginas anteriores, el segundo de los itinerarios aborda algunas de las tendencias más significativas y de mayor proyección en el ámbito empresarial, como es el "compliance", que vela con el cumplimiento estricto de las complejas legislaciones vigentes en todo tipo de sectores económicos; la responsabilidad social corporativa y los aspectos vinculados a la reputación de las organizaciones empresariales en el ciberespacio; o la ciberinteligencia, es decir, la aplicación de los métodos y procedimientos asociados tradicionalmente al análisis de inteligencia para prevenir e identificar los riesgos y amenazas informáticas. En definitiva, esta II edición del Máster en Ciberdelincuencia trata de dar una mejor respuesta a las necesidades de las empresas, con el fin de garantizar en última instancia la empleabilidad de sus egresados.

4. Reflexiones finales

La formación y la capacitación del personal implicado directamente en la lucha contra la ciberdelincuencia es una labor fundamental que implica a administraciones públicas, organizaciones empresariales e instituciones académicas. Sin embargo, todo programa formativo que se dirija a capacitar a sus participantes en las técnicas y procedimientos requeridos para el adecuado tratamiento de la ciberdelincuencia nace condenado a la obsolescencia en un periodo de tiempo cada vez más breve. Ello se debe, en primer lugar, al carácter cambiante de la amenaza, cuya sofisticación, complejidad y dimensiones aumenta día tras día, lo que conlleva a una aparición continua de nuevas técnicas y procedimientos para eludir las medidas de seguridad de los sistemas informáticos a los que, normalmente, los especialistas en ciberseguridad únicamente pueden responder de manera reactiva. Mientras tanto, como se ha procurado mostrar a lo largo del presente trabajo, los ciberdelincuentes realizan a menudo sus actividades en una situación de impunidad, al tiempo que un número creciente de usuarios comunes, administraciones públicas y empresas, son víctimas con mayor frecuencia de diferentes modalidades delictivas que causan un mayor perjuicio económico y un preocupante clima de alarma social en la sociedad española.

En el actual momento histórico, en el que la tendencia general es de una progresiva informatización de las sociedades, y de una creciente dependencia individual y colectiva respecto a las innovaciones tecnológicas, todo indica que la importancia de estas nuevas formas de delincuencia

aumentará exponencialmente en el futuro próximo. Además de la cuestión meramente técnica, del carácter cambiante de la ciberdelincuencia se desprende una dificultad añadida en su prevención y persecución: La perfectibilidad de los instrumentos legales y jurídicos de los que se dispone en la actualidad. En muchas ocasiones, la judicatura y el legislador no se encuentran convenientemente preparados para enfrentar los retos derivados del mundo digital, por lo que los ciberdelincuentes mantienen sus actividades en un espacio de cierto vacío legal, lo cual favorece que estos hechos no sean debidamente perseguidos.

Como se ha apuntado a lo largo del presente trabajo, uno de los elementos caracterizadores del subsector de la ciberseguridad en España es la insatisfacción de las necesidades de las organizaciones empresariales ante la escasez de profesionales debidamente formados en este terreno frente a una demanda creciente. Ello debería hacer reflexionar al conjunto de la comunidad académica dedicada a la docencia en materia de ciberseguridad, en la medida que esta insuficiencia de profesionales capacitados coincide con el periodo en el que más universidades han impulsado sus propios programas de posgrado dedicados a la ciberseguridad. Esta incongruencia debe llevar a reconsiderar la ciberseguridad no solo desde un plano técnico, sino ocupacional: Definir con precisión los conocimientos y competencias con las que un profesional de la ciberseguridad debe contar para incorporarse de manera exitosa al mercado de trabajo hoy ya no es suficiente, siendo cada vez más necesario prospectar para identificar los requisitos que serán necesarios en el futuro próximo.

Siguiendo en el plano formativo, se torna también imprescindible articular los mecanismos oportunos que permitan la constante actualización de conocimientos y competencias de los especialistas en ciberseguridad, pues solo contando con un conocimiento preciso de las dimensiones jurídicas y técnicas del fenómeno de la ciberdelincuencia y con un manejo solvente de las nuevas herramientas informáticas requeridas para su prevención y persecución, será posible que vulnerabilidad de los diferentes actores expuestos a los riesgos y amenazas que alberga el ciberespacio se mantenga en umbrales aceptables. En todo caso, la preocupación en este campo no debe girar únicamente en torno a la actualización de los contenidos, sino también el plano metodológico debe ser objeto de constantes esfuerzos para su mejoramiento, procurando en todo momento garantizar las mayores cotas de flexibilidad posibles que, sin ir en detrimento del rigor y la exhaustividad, permitan a aquellos profesionales que ya han iniciado su carrera profesional seguir convenientemente cualquier iniciativa formativa.

Teniendo en consideración todo lo anterior, el Máster en Ciberdelincuencia de la Universidad Nebrija, pese a ser una iniciativa de reciente creación, nace con la aspiración de configurarse en el futuro como uno de los programas de posgrado más destacados del panorama de la oferta formativa

en materia de ciberseguridad en España, satisfaciendo las necesidades de instituciones y empresas, y ofreciendo a sus estudiantes la oportunidad de aprender junto a algunos de los profesionales más destacados y experimentados del subsector de la ciberseguridad. A tal efecto, y más allá de resultados inmediatos, la propuesta de la Universidad Nebrija pasa por profundizar su oferta formativa en el ámbito de la ciberseguridad y se articula como una apuesta a largo plazo, conjugando en todo momento rigor, innovación, y empleabilidad.

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

Bibliografía

Boletín Oficial del Estado. (2015). Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE num. 77, 31 de marzo de 2015. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=-BOE-A-2015-3439

Caro, M. J. (2014). La protección de las infraestructuras críticas. Instituto Español de Estudios Estratégicos, Documento de análisis, 27 de julio de 2011. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_analisis/2011/ DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf

Centro Criptológico Nacional (2016). Ciberamenazas 2015/ tendencias 2016. Resumen ejecutivo. 7 de abril de 2016, p. 7. Recuperado de: https://www.ccn-cert.cni.es/pdf/informes-de-ciberseguridad-ccn-cert/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015-tendencias-2016-resumen-ejecutivo/file.html

Consejo de Europa (2001a). Convenio sobre la ciberdelincuencia. Informe explicativo. Serie de tratados europeos (185), Budapest. Recuperado de: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403

Consejo de Europa (2001b). Convenio sobre la ciberdelincuencia. Serie de tratados europeos (185), Budapest. Recuperado de: https://rm.coe.int/ CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=-09000016802fa41c

Consejo de Europa (2003). Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. European Treaty Series (189), Budapest. Recuperado de: https://rm.coe.int/CoERMPublicCommonSearch Services/DisplayDCTMContent?documentId=090000168008160f

Departamento de Seguridad Nacional (2013). Estrategia de Ciberseguridad Nacional. Presidencia del Gobierno, Gobierno de España. Recuperado de: http://www.dsn.gob.es/es/file/146/download?token=KI839vHG

Europol (2016). The Internet Organized Crime Threat Assessment (IOCTA). Centro Europeo contra la Cibercriminalidad, La Haya, Países Bajos. Recuperado de: https://www.europol.europa.eu/sites/default/files/documents/ europol_ iocta_web_2016.pdf

Fojón, E. (2013). La Estrategia de Ciberseguridad Nacional... aún queda mucho trabajo por hacer. Real Instituto Elcano. Recuperado de: http://www.blog.rielcano.org/la-estrategia-de-ciberseguridad-nacionalaun queda-mucho-trabajo-por-hacer/

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270

Gollnick, C. y Wilson, E. (2016). Separating Fact from Fiction: the Truth about Dark Web. Termium labs. Recuperado de: https://go.pardot.com/l/190892/2016-10-31/65l87

Hidalgo, J. T. (2013). Principios de una cultura nacional de ciberseguridad, en: Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: Un reto prioritario. Escuela de Altos Estudios de la Defensa, monografía 137. Recuperado de: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NECESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf

INCIBE. (2016a). Tendencias en el mercado de la ciberseguridad. Instituto Nacional de Ciberseguridad, Ministerio de Industria, Energía y Turismo. Recuperado de: https://www.incibe.es/sites/default/files/estudios/tendencias_ en_el_mercado_de_la_ciberseguridad.pdf

INCIBE. (2016b). Punto de partida al Modelo de Gestión y Seguimiento del Talento en Ciberseguridad en España. Visión conjunta de la industria, sector académico e investigador y profesionales del sector. Instituto Nacional de Ciberseguridad, Ministerio de Industria, Energía y Turismo. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/modelo_gestion_talento_incibe_0.pdf

INCIBE. (2017a). Másteres en Ciberseguridad en España. Edición marzo de 2017. Instituto Nacional de Ciberseguridad, Ministerio de Industria, Energía y Turismo. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/catalogo_masteres_actualizado.pdf

INCIBE. (2017b). Instituciones que imparten formación en ciberseguridad en España. Edición marzo de 2017. Instituto Nacional de Ciberseguridad, Ministerio de Industria, Energía y Turismo. Recuperado de: https://www.incibe.es/sites/default/files/contenidos/notasprensa/doc/catalogo_instituciones_actualizado.pdf

Jané, C. (6 de febrero de 2017). Vengador Anonymous. El Periódico. Recuperado de: http://www.elperiodico.com/es/noticias/sociedad/grupo-vinculado-anonymous-tumba-parte-deep-web-5789582

Lodeiro, R. (2017). El uso de las nuevas tecnologías por el terrorismo yihadista. Cuadernos de la Guardia Civil, núm. 54, pp. 50-73.

Martín, E. (2017). Dark web y Deep web como fuentes de ciberinteligencia utilizando minería de datos. Cuadernos de la Guardia Civil, núm. 54, pp. 74-93.

Ministerio del Interior (2015a). Estudio sobre la criminalidad en España. Secretaria de Estado de Seguridad, Gabinete de Coordinación y Estudios. Recuperado de: http://www.interior.gob.es/documents/10180/3066430/Informe+Cibercriminalidad+2015.pdf/c10f398a-8552-430c-9b7f-81d9cc8e751b

Ministerio del Interior (2015b). Anuario estadístico del Ministerio del Interior 2014. Secretaría General Técnica. Recuperado de: http://www.interior.gob.es/ documents/642317/1204854/Anuario-Estadistico-2014_v201510.pdf/0c18a 800-f7f7-405c-9155-7391633618c8

Ministerio del Interior (2016). Anuario estadístico del Ministerio del Interior 2015. Secretaría General Técnica. Recuperado de: http://www.interior.gob.es/documents/642317/1204854/Anuario-Estadistico-2015.pdf/03be89e1-dd38-47a2-9ce8-ccdd74659741

Miranzo, M. y del Rio, C. (2014). La protección de infraestructuras críticas. UNISCI Discussion Papers, num. 35, p. 342. Recuperado de: http://revistas.ucm.es/index.php/UNIS/article/viewFile/46435/43628

Miró, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de actividades cotidianas para la prevención del Cibercrimen. Revista Electrónica de Ciencia Penal y Criminología, (13).

ONTSI. (2015). Caracterización del subsector y el mercado de la ciberseguridad. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información. Ministerio de Industria, Energía y Turismo. Recuperado de: http://www.ontsi.red.es/ontsi/es/estudios-informes/caracterizaci%C3%B3n-del-subsector-y-el-mercado-de-la-ciberseguridad-2015

PwC (2016). Encuesta sobre fraude y delito económico 2016. Resultados en España. Recuperado de: https://www.pwc.es/es/ publicaciones/transacciones/assets/pwc-forensic-encuesta-fraude-empresarial-y-delito-economico-2016-spain.pdf

Rayón, M. C. y Gómez, J.A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, núm. 47, pp. 209-234. Recuperado de: http://www.rcumariacristina. net:8080/ojs/index.php/AJEE/article/view/189/158

Salvador, L. de (21 de febrero de 2012). Redes de anonimización en internet: Cómo funcionan y cuáles son sus límites. Instituto Español de Estudios Estratégicos, Documento Opinión. Recuperado de: http://www.ieee.es/ Galerias/fichero/docs_opinion/2012/DIEEEO162012_RedesAnonimizacionInternet_LdeSalvador.pdf

SEPE. (2014). Los perfiles de la oferta de empleo 2014. Servicio Público de Empleo Estatal, Observatorio de las ocupaciones. Recuperado de: https://www.sepe.es/contenidos/observatorio/perfiles/pdf/Especialistas_ciberseguridad.pdf

Universidad Nebrija (2016). Memoria Nebrija 2015/2016. Servicio de Publicaciones de la Universidad Nebrija. España. Recuperado de: http://www.nebrija.com/memoria/2015-16/

Weimann, G. (2016). Terrorist Migration to the Dark Web. Perspectives on Terrorism, (10), issue 3, pp. 40-44.

CC BY

Anexo 1. Tipología de la ciberdelincuencia según el sistema estadístico de criminalidad

DENOMINACIÓN	CÓDIGO PENAL ESPAÑOL	TIPO HECHO SEC
Acceso e interceptación ilícita	Arts. CP 197 a 201 Arts. CP 278 a 286	Acceso ilegal informático.
		Descubrimiento/revelación de secretos.
		Otros relativos al mercado/consumidores.
Interferencia en los datos y en el sistema	Arts. 263 a 267 y 625.1.	Daños.
		Ataques informáticos.
Falsificación informática	Arts. CP 388 - 389, 399bis, 400 y 401.	Falsificación de moneda, sellos y efectos timbrados.
		Fabricación tenencia de útiles para falsificar.
		Usurpación del estado civil.
Fraude informático	Arts. CP 248 a 251 y 623.4	Estafa bancaria.
		Estafas con tarjetas de crédito, débito y cheques de viaje.
		Otras estafas.
Delitos sexuales	Arts. CP 181, 183.1 183.bis, 184, 185, 186, 189.	Exhibicionismo.
		Provocación sexual.
		Acoso sexual.
		Abuso sexual.
		Corrupción de menores/incapacitados.
		Pornografía de menores.
		Contacto mediante tecnología con menor de 13 años con fines sexuales.
Contra la propiedad industrial/intelectual	Arts. CP 270 a 277 y 623.5.	Delitos contra la propiedad intelectual.
		Delitos contra la propiedad industrial
Contra el honor	Arts. CP 205 a 210 y 620.2	Calumnias.
		Injurias.
Amenazas y coacciones	Arts. CP 169 a 172 y 620	Amenazas.
		Amenazas a grupo étnico, cultural o religioso.
		Coacciones.

Fuente: Estudio sobre la criminalidad en España, Ministerio del Interior, 2015.

ISSN: 2225-5648, Año 7, Vol. 1, p. 237-270