Los retos y desafíos de la ciberseguridad y ciberdefensa en el ámbito de la formación y el entrenamiento

El ciberespacio, un nuevo terreno de juego para los delincuentes, los organizados o los individualistas, para terroristas y mafias, como nuevo campo de batalla de estados y naciones o como un espacio de manifestación y activismo de los nuevos movimientos sociales. Un entorno donde sólo los mejor preparados tendrán la capacidad de dar respuesta a los desafíos y retos que presenta.

En este artículo los autores enuncian algunos de los retos más importantes, asociados a la tecnología, la legislación y los que afectan a la formación de los profesionales.

Samuel Álvarez González
Ingeniero de Telecomunicación
Miembro del Grupo de Trabajo de Defensa y Seguridad del COIT.
Director General (CEO) del grupo In-Nova

Esther Álvarez González
Ingeniera de Telecomunicación
Presidenta de la Fundación In-Nova

El ciberespacio, un tablero de juego donde detrás de un *nickname* y un computador, a partir de un solo individuo, con pocos recursos económicos, o un estado con toda una división de decenas de miles de ingenieros, puede pergeñarse un acto ilegal o que atente contra la soberanía nacional de un país. Todo esto, gracias al poder escudarse en las particularidades y características de este nuevo espacio, como son el anonimato, la asimetría de los acontecimientos, la rapidez de los sucesos con su "tiempo real", la falta de conocimientos y experiencia de quienes defienden las redes y los sistemas, la falta de regulación nacional e internacional, la no existencia de fronteras y la falta en general de coordinación internacional.

Sin duda, este nuevo espacio, el ciberespacio, o el llamado el quinto dominio, si del ámbito de la guerra se trata, presenta unos retos para la sociedad, para los países y por lo tanto para las fuerzas y cuerpos de seguridad, ciudadanos y la industria. También presenta unos desafíos, en algunos casos humanos, otras veces legislativos y otros finalmente tecnológicos, que debemos conocer, abordar, planificar y resolver.

Desafortunadamente aún son pocos los que reconocen la criticidad de dominar este espacio, y por lo tanto, de ser independientes tecnológicamente como país y, lamentablemente, son menos los que intentamos sensibilizar sobre la importancia de reforzar nuestras capacidades, tanto civiles, militares, como por supuesto industriales: *en definitiva, más y mejores profesionales especializados.*

Al igual que no se concibe una Armada sin barcos, para proteger nuestras aguas y ayudar a proteger otras, o nuestro Ejército del Aire sin aviones, para proteger nuestro espacio aéreo, no podemos imaginarnos un ejército que debe proteger un activo extremadamente crítico como es el ciberespacio sin tener en posesión ni de barcos, ni de aviones, ni de un tejido de profesionales que pueda dar respuesta a la cantidad de retos que este escenario nos plantea.

El ciberespacio actualmente nos desafía con tres grandes retos: *1) tecnológicos, 2) jurídicos y éticos y 3) formación, entrenamiento y personal cualificado.* Estos últimos, tremendamente condicionados e imbricados a los dos primeros. Es por ello que ambos deben ser también esbozados.

Retos tecnológicos

Respecto al primero, los *retos tecnológicos*, quizás sean los más evidentes. Si tenemos en cuenta el incremento exponencial de las personas y las cosas que se conectan a internet el panorama en pocos años es impresionantemente vasto. ¿Seremos capaces de manejar tanto volumen de información de forma segura?, ¿y además en tiempo real?. ¿Tendremos capacidad para gestionar Zettabytes en un par de años?, ¿o Yottabytes?. La respuesta es: "ahora no", y el estado de la técnica representa un gran riesgo de que podamos hacerlo en los próximos años de una forma ágil… y segura. Lo que sí es cierto es que la asimetría es evidente, mientras que el ciberespacio se expande, crece, y por lo tanto la masa crítica de cosas y personas sobre las que podemos actuar, sobre un "internet", es mucho mayor, no lo acompañamos con un crecimiento sobre conocimientos, herramientas y capacidad de ges-

tión de todo lo que ahí se comparte. Sin embargo, lo que sí crece es la capacidad de hacer más daño, ser más lesivo, en un cibermundo donde cada vez hay más posibles víctimas y menos agentes en la misma proporción de crecimiento que la protejan y la regulen (Fig. 1).

Si tuviéramos que sintetizar en dos ideas dónde está el principal reto tecnológico en el ámbito del ciberespacio recurriríamos a dos conceptos: *BIG DATA* y *Sistemas en Tiempo Real* (tanto software como hardware). Los grandes volúmenes de información, tanto en tránsito (en comunicación) como almacenados e indexados, requieren de ser gestionados, no sólo desde un punto de vista estático (procesos de minería de datos, análisis de información sobre fuentes abiertas, procesado y explotación de grandes bases de información, etc.), sino dinámico, requiriendo en muchos casos, sobre todo en los que a ciberseguridad se refiere, de la toma de decisiones en el momento: en tiempo real. Si la labor de inteligencia tradicional sobre indicios, tendencias, costumbres, comportamientos, etc., antes se podía realizar con más tiempo, con dedicación de horas/hombre cualificadas, hoy en día, en el mundo ciber, la denominada ciberinteligencia debe generar un output "para ya, ahora, en este momento". ¿Estamos preparados para esto?, ¿la tecnología, las herramientas, la industria, los profesionales nos brindan ya soluciones para esta labor tan crítica?. La respuesta es clara: tenemos mucho camino aún por recorrer, muchos proyectos de I+D por promover, mucho tejido industrial por desarrollar y muchos profesionales que formar y entrenar.

En la figura 2, se analizan aquellos factores impulsores (parte superior) o limitantes (parte inferior) que actualmente tenemos respecto al reto del BIG DATA y en la siguiente imagen se caracterizan en qué seis bloques el BIG DATA y Tiempo Real son de especial relevancia en el mundo de la ciberseguridad y ciberdefensa.

Retos Jurídicos y Éticos

Legislación, derechos humanos, principios éticos, cooperación internacional, son algunos de los conceptos que constituyen el entramado al que podríamos denominar ¿ciberderecho?, ¿ciberética?. Con objeto de contextualizar este tipo de retos lo más fácil es hacerlo plausible para todos con algunas preguntas: ¿es posible desde las leyes perseguir, procesar, juzgar y condenar un ataque contra la propiedad industrial, producido desde Corea del Norte hacia una empresa norteamericana?, ¿un ataque a una empresa de tecnología militar, con objeto de robarle información

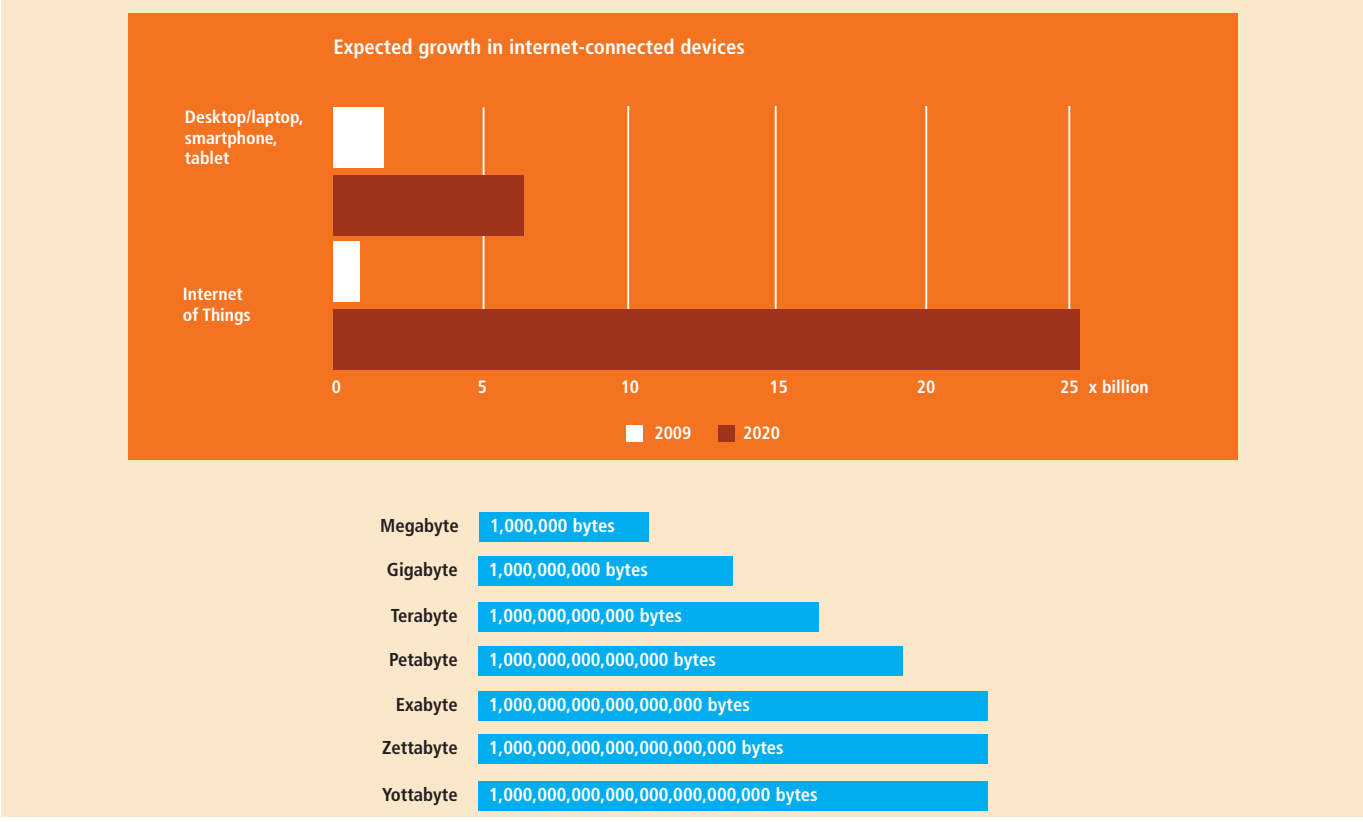
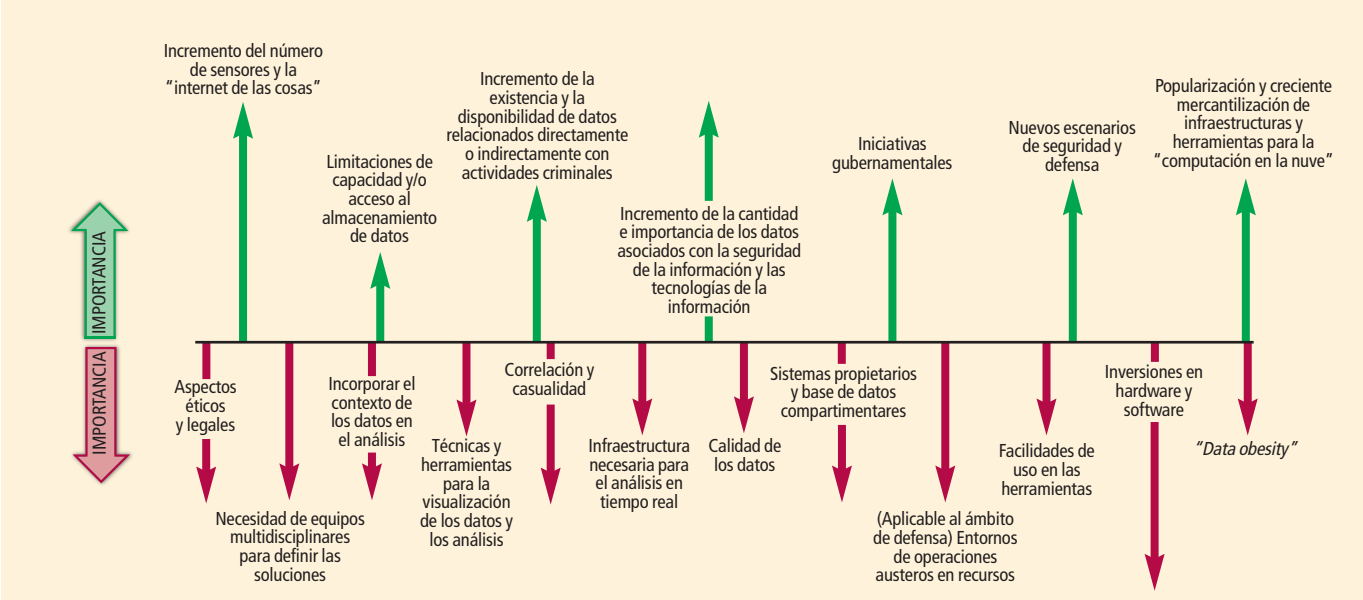


Figura 1. Perspectivas de crecimiento en los dispositivos conectados a internet.
(Fuente: http://www.gartner.com/newsroom/id/2684915)



Factores impulsores y limitadores en la aplicación del Big Data.
(Fuente: IEES. Instituto Español de Estudios Estratégicos. "Big Data en los Entornos de Seguridad y Defensa". 2013)

Figura 2. Desafíos del BIG DATA en la Ciberseguridad.
(Fuente: IEES. Instituto Español de Estudios Estratégicos. "Big Data en los Entornos de Seguridad y Defensa". 2013)

sobre tecnología punta, capaz de darle al primero que la tenga, una hegemonía en un territorio, a nivel mundial, es una acto de ciberdelincuencia o de ciberguerra (ataque entre estados)?, ¿cómo se gestionan los conceptos como "indicio", "prueba", "cadena de custodia" dentro del ámbito de la ciberseguridad, o mejor aún, de la ciberguerra?. ¿Cómo es de evidenciable quién está detrás de un ataque contra un estado?.

Sólo es necesario hacer un poco de historia para encontrar en el pasado reciente algunos acontecimientos representativos, como Tallin (2007), el caso Stuxnet, Flame o similares. ¿Aparentemente patrocinados por los estados, contra otros estados o industrias críticas, pero sin pruebas o evidencias claras de ello?. Al final, en todo momento, se habla en términos de presunción: "presuntamente fue". Pero aquí debemos también plantear preguntas como: ¿bajo qué regulación o legislación un estado puede *ciberatacar* a otro?, ¿con qué consecuencias sabiendo que uno de los principales objetivos de los ciberataques entre estados ha sido el ciberespionaje?, ¿cómo se abordará el tratamiento sobre un aspecto de los derechos humanos?.

Si bien es cierto en los últimos años podemos palpar avances tanto en la legislación nacional e internacional, en materia de ciberdelincuencia o ciberterrorismo, así como en la cooperación internacional entre los estados con la sufi-

ciente afinidad. No obstante, la inexistencia de fronteras de la "Red" muestra el gran desnudo que hoy sigue al descubierto en este ámbito, requiriéndose de soluciones con *carácter global* que ayuden a perseguir los actos delictivos o dañinos que desde un punto de vista de la Seguridad toda la población exige.

Desde un punto de vista de la Seguridad Nacional, como foco en la protección de infraestructuras críticas, esta cuestión de la legalidad o la ética es aún más peliaguda y en estado indeterminado. A pesar de los pocos tratados internacionales existentes, o de la doctrina o principios que cada país diseña de "puertas adentro", a nivel internacional y desde una óptica pura de la Guerra (Ciberdefensa y Ciberguerra), la situación requiere de soluciones de coordinación y normativa internacional como ya en otros ámbitos existe. El caso que más atañe a España es la propia OTAN, quien para escenarios operacionales tradicionales trabaja bajo una doctrina y unas "reglas del juego" que debe definir, de forma eminentemente apremiante, para el mundo del Ciberespacio. El Centro de Excelencia de Ciberdefensa de Estonia, promovido también por España, tiene entre otros objetivos esta labor. Misión que no podrá encontrar el buen fin sin profesionales, personas y especialistas que cooperen, desde lo técnico a lo jurídico, y viceversa, y sea coronado por acuerdos multilaterales que impacten en leyes y sus consecuencias, desde un punto de vista global.

Retos sobre el impacto en la formación y el entrenamiento

Qué duda cabe que el talento, el profesional especialista, y por lo tanto los procesos de formación, de adiestramiento, constituyen los puntales, los pilares que darán consecuencia a los retos de partida esbozados anteriormente, tanto los tecnológicos como los jurídicos y éticos.

Formación

A pesar de la cantidad de ingenieros que ven la luz en nuestro país, de las diferentes disciplinas tecnológicas y diversidad de centros de educación superior, apenas existen en los grados universitarios, con contundencia, una rama en profundidad que aborde o resuelva muchas de las preguntas compartidas en este artículo.

Por otro lado, si nos vamos a los posgrados, al grado de master, formación continua o cualquier otra fórmula de acción formativa con enfoque a la I+D o con enfoque de aplicación profesional e industrial, tampoco nos encontramos, de forma aunada, un plan de carrera estructurado que sea capaz de garantizar una hoja de ruta que logre satisfacer los perfiles y profesionales que el ciberespacio necesita ahora, no dentro de diez años, para aportar Seguridad. Sí existen masters, especializaciones, que apoyan esta necesidad profesional, pero insuficiente dentro del volumen de demanda acuciante que requiere la realidad de la amenaza. No hay más que atender y escuchar al mercado para identificar una gran oportunidad, un gran océano azul de nuevas opciones profesionales. La figura 3, ilustra cómo, en los últimos años, la principal preocupación de directivos de empresas es la ciberseguridad, como uno de sus principales riesgos (por encima de lo que supondría la ruptura de su cadena de suministro o lo que provocarían las catástrofes naturales).

Adicionalmente no podemos dejar de lado la aplicación militar de estos conocimientos. Al final, la Seguridad la proveen y gestionan personas, empresas, estados y cualquier tipo de organización conectada a la red, con el objeto de mantener la integridad de sus infraestructuras físicas y lógicas, y de la información que albergan. Interviniendo en todo el ciclo de vida de los sistemas y componentes que de forma directa o indirecta pueden

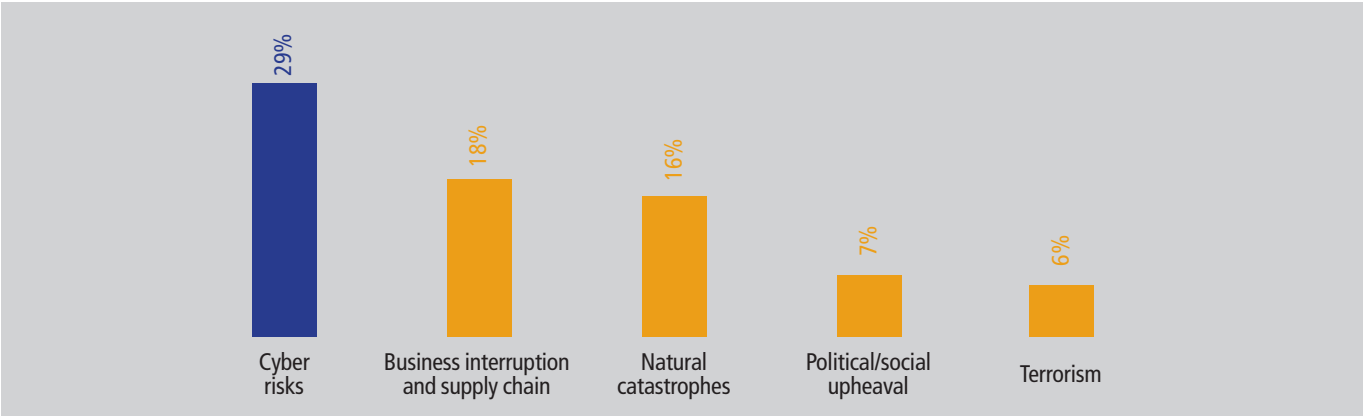


Figura 3. Riesgos mundiales, tal y como son percibidos por los directivos de todo el mundo.
(Fuente: ALLIANZ-2015)

llegar a ser comprometidos; desde el diseño y desarrollo de aplicaciones seguras, pasando por las comunicaciones seguras y privadas (inalámbricas y alámbricas), continuando con la protección de equipos y sistemas comunicados entre sí y hasta la correcta gestión de los usuarios que las explotan. Todo, bajo el paradigma de la prevención, el análisis dinámico de los riesgos, identificación de las amenazas, y en caso de incidente, de la capacidad de recuperar la productividad de los sistemas (resiliencia) y de tomar las decisiones oportunas, como lecciones aprendidas, para minimizar el riesgo de que vuelvan a acontecerse. Sin embargo, en el ámbito militar tenemos otros retos adicionales, y es disponer de capacidad de anticipación y de respuesta.

Por ejemplo, si nos referimos al caso de España, nos encontramos con el Mando Conjunto de Ciberdefensa (MCCD), dependiente del Estado Mayor de la Defensa (EMAD), creado a finales de 2013 para dar respuesta operativa a situaciones que puedan comprometer la seguridad nacional, a través del compromiso de las protecciones críticas que están bajo su competencia. Por lo tanto, además de lo descrito en el párrafo anterior sobre el ciclo de vida, dentro del sesgo militar (ciberdefensa y ciberguerra), se requieren otras capacidades adicionales para desempeñar su misión, que son la capacidad de Defensa, de Explotación (inteligencia) y de Ataque (Defensa Activa). En total, una amalgama de capacidades que impactan de lleno en la necesidad no sólo de especialistas y expertos militares, sino de aliados, de profesionales e industria que les apoye, y desde un punto de vista de independencia tecnológica y de la verdadera defensa de la soberanía nacional, respecto al resto del mundo, pertinente que esas capacidades las pudiéramos encontrar dentro de nuestro mercado interno: ese es el reto.

Analizando como ejemplo el Plan de Carrera necesario para dar respuesta a la necesidad de los empleos que tiene el Mando Conjunto de Ciberdefensa, en la figura 4 se determinan los cursos y acciones de formación necesarias desde un punto de vista técnico, especial o generalista y mediante tres niveles de formación: inicial, avanzada o asociada al puesto de trabajo.

Puesto que no es lo mismo un auditor de seguridad, que un supervisor de la misma, o un gestor de incidentes o un perfil de monitorización de procesos, o aquel que realiza análisis forense, o el que analiza malware, etc., se requiere en cada caso el diseño del correspondiente plan de carrera donde se garanticen cuestiones como: maximización de capacidades, y mecanismos de incorporación y redundancia de conocimiento de cara las situaciones de

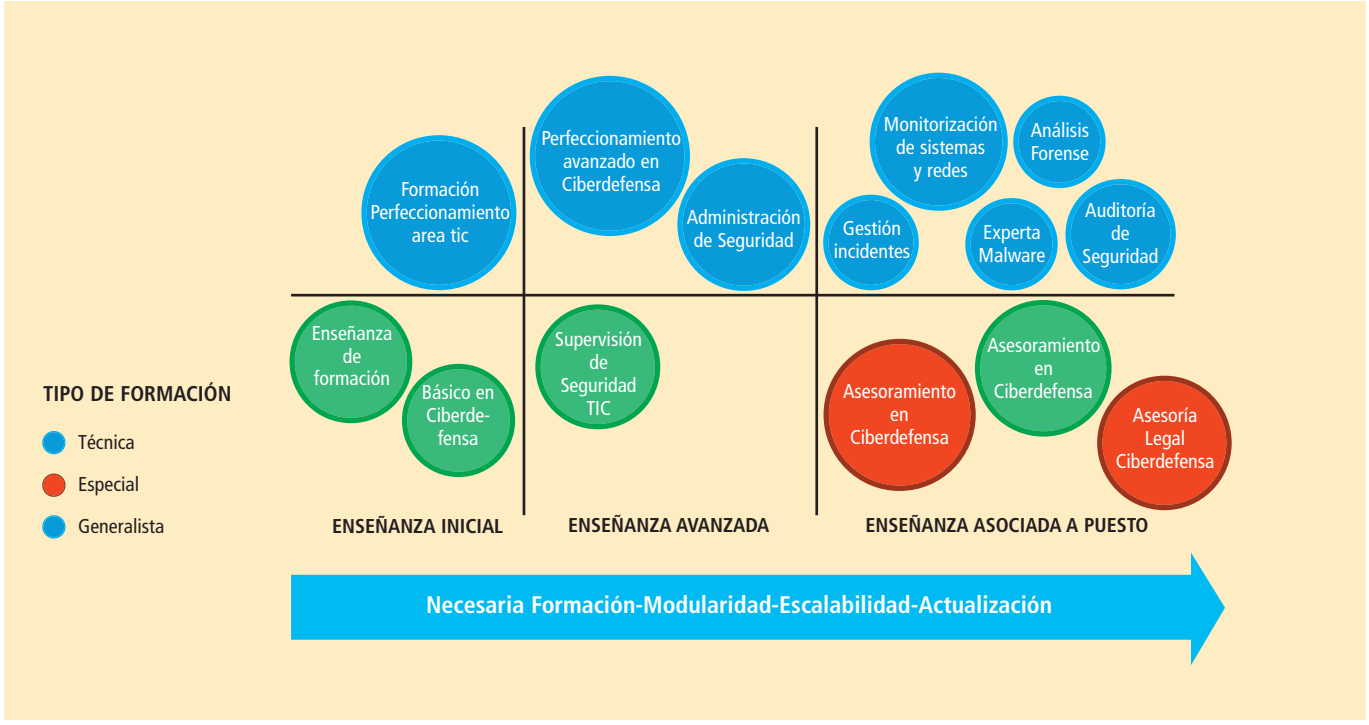


Figura 4. Esquema del plan de formación en ciberdefensa.
(Fuente: Mando Conjunto de Ciberdefensa (MCCD) de España)

rotación de personal, y que en el caso de la carrera militar es muy acusado.

Con ánimo de aterrizar ideas de temáticas de base, que deben poder hilar diferentes recorridos de formación y con un enfoque totalmente aplicado, a continuación planteo algunas de ellas, con identidad y suficiencia para consolidar una acción formativa de profundidad: seguridad del software, seguridad en las comunicaciones, análisis dinámico del riesgo y detección de amenazas, análisis de redes y malware, arquitecturas y redes seguras, análisis forense, criptografía, hacking ético, diseño e implementación de ciberarmas, ingeniería social, aspectos legales, jurídicos y éticos, ciberinteligencia y fuentes abiertas, diseño de bases de datos seguras, amenazas avanzadas persistentes (APTs), la ciberdefensa operacional, ataques de negación de servicio, honeynets, big data, inteligencia artificial, etc.

Adicionalmente, en el mundo de profesional que rodea a los sistemas de información, las tecnologías de la comunicación y la seguridad de las mismas, podemos encontrar diferentes certificaciones, tanto profesionales como orientadas a la organización, las cuales plantean un refuerzo clave, normalizado, en cuestión del manejo de la seguridad en general o la correcta gestión de las tecnologías de la información. Algunas de ellas, las más conocidas, certificaciones como las que engloba ISACA: CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified In the Governance of Enterprises IT), CRISC (Certified in Risk and Information Systems Control) u otras como: ITIL (IT Infrastructure Library, biblioteca de infraestructura de TI), la propia ISO 27000, Ec-council, GIAC, CompTIA, CWNP, CISSP, etc.

En la figura 5, se ilustra, en función de las capacidades operativas del ámbito de la ciberseguridad y ciberdefensa (Defensa, Gestión, Análisis y Respuesta) el conjunto de capacidades formativas y retos agregados de conocimiento que no pueden ser ajenos en el reto de consolidar planes de carrera especializados para profesionales de nuestro sector.

Entornos de entrenamiento, simulación y experimentación

Qué duda cabe que los conocimientos relativos al ámbito de la Ciberseguridad y Ciberdefensa deben ser adquiridos mediante la propia aplicación de los contenidos. Pero claro, ¿dónde puedo practicar un ciberataque?, ¿en qué lugar puedo realizar un ataque de negación de servicio sin afectar a nadie?, ¿dónde pruebo una amenaza que termino de descubrir?, ¿en qué entorno pongo en

Figura 5. Capacidades formativas.
(Fuente: Profesor Bernardo Alarcos. Universidad de Alcalá)

práctica un protocolo de ataque?, ¿de qué manera puedo caracterizar el patrón de ataque de una amenaza?... en definitiva, ¿en qué entorno y con qué herramientas puedo experimentar con todos los conocimientos adquiridos?, y, ¿en qué entornos puedo entrenar y adiestrar a un equipo de personas que actúan de forma coordinada ante una amenaza?. Todas estas preguntas tienen una única respuesta: un entorno de experimentación y simulación de ciberseguridad y ciberdefensa.

En definitiva, acompañado a la propia formación técnica, jurídica o administrativa relativa a la el mundo ciber en general se requiere de una infraestructura científica y tecnológica capaz de albergar las capacidades suficientes como para, no sólo poner en práctica los conocimientos adquiridos, sino poder desarrollar nuevas experimentaciones en relación a ello. Al menos, estas capacidades deberían ser:

- Capacidades de Experimentación Básicas: gestión y monitorización de eventos de seguridad, correlación de eventos, detección de intrusos y control de acceso a datos y redes, sistemas de auditoria de vulnerabilidades y herramientas de hacking ético y herramientas de bastionado y parcheo.
- Capacidades de Experimentación Avanzadas: simuladores, sistemas anti-fuga de datos, análisis forense y sistemas robustos.
- Capacidades de Experimentación en Nuevas Tecnologías: neutralización de botnets, gestión dinámica de riesgos, mitigación de ataques DDoS y ataques contra dispositivos de enrutamiento de redes de comunicaciones.

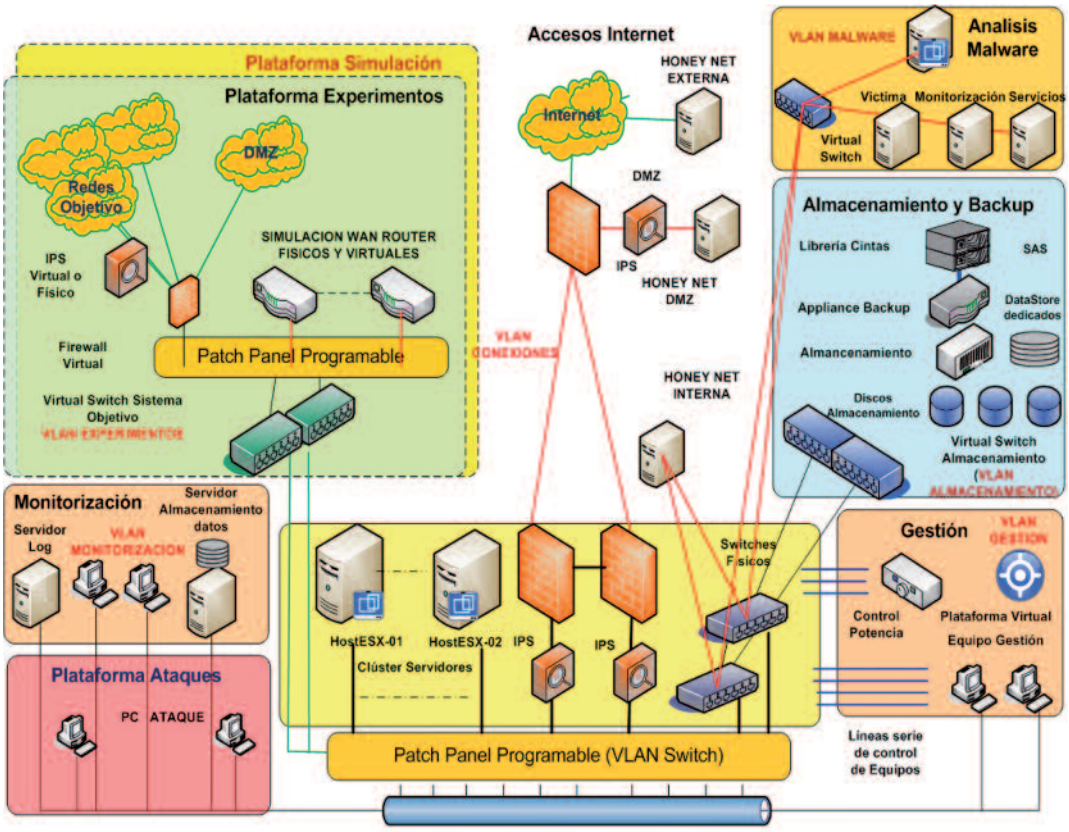


Figura 6. Modelo general de Centro de Experimentación en Ciberdefensa.
(Fuente: Ministerio de Defensa de España)

- Inteligencia: recolección de información de fuentes abiertas, filtrado de datos y alerta temprana.
- Capacidades de Experimentación en Ciberarmas: investigación y desarrollo de malware, automatización de malware, análisis de vulnerabilidades en software (certificación de desarrollos seguros) y malware y utilización de vulnerabilidades (creación de exploits).
- Capacidades para diseñar y ejecutar Juegos de Guerra (CyberRange): diseño de red para juegos de guerra, desde escenarios, teatro de operaciones y todo el entorno necesario para la realización de un entrenamiento/adiestramiento de personal.

Al final se trata de tener un laboratorio, un centro real donde poder realizar todo de tipo de pruebas sobre herramientas de utilidad, con capacidad de análisis, acción y reacción en el mundo del ciberespacio. Compuesto de hardware y de software, un centro de experimentación representa un polígono cerrado de comunicación, una red totalmente aislada, sobre la cual pueden recrearse escenarios y situaciones reales sobre las que se tiene control y monitorización constante. A modo ilustrativo y como caso de ejemplo del Ministerio de Defensa de España, en la figura 6, se muestra un esquema general de lo que puede ser un centro de experimentación de esta naturaleza.

The challenges of cyber-security and cyber-defense in the field of education and training

Cyberspace is the new playground for criminals, be they organized or working alone, operating as terrorists or as part of criminal mafias, making cyberspace the newest battleground for states and nations, or alternately it acts as a novel space for free expression and the activism of new social movements. Undoubtedly, this is an environment in which only the best prepared will be capable of facing the challenges and dangers it presents.

In this article, the authors highlight some of the most important challenges associated with technology, related legislation, and factors affecting professional development.