Introducción de las Enseñanzas de Seguridad Informática en los Planes de Estudio de las Ingenierías del Siglo XXI

Jorge Ramió Aguirre
Dpto. de Lenguajes, Proyectos y Sistemas Informáticos
Universidad Politécnica de Madrid
Escuela Universitaria de Informática. Ctra. de Valencia km 7
28031 Madrid – España
Coordinador de la Red Temática CriptoRed
e-mail: jramio@eui.upm.es

Resumen

Las denominadas NTIs, *Nuevas Tecnologías de la Información*, están cambiando nuestra forma de ver y enfrentarnos al mundo. Es tal la cantidad de información que ya estamos intercambiando y procesando, que comienza a tenerse en cuenta, después de muchos años, que uno de los pilares en los que debe descansar el desarrollo tecnológico en este nuevo siglo será el de la seguridad informática, en el sentido más amplio de la palabra. Sin embargo, y a pesar de interesantes esfuerzos e iniciativas docentes más o menos espontáneas en las universidades españolas, ha llegado el momento de plantearse la necesidad de cubrir este área de conocimiento en algunas de las ingenierías que demanda la sociedad. El artículo, tras el análisis de datos concretos en este área, presenta un primer borrador de curriculum específico para este perfil y que deriva en la propuesta de una nueva titulación con el nombre de *Ingeniero en Seguridad Informática*.

1. Introducción

El estudio, gestión y mantenimiento de sistemas en ingeniería en los que un factor de importancia vital resulta ser la seguridad informática, ha experimentado un espectacular auge en estos últimos años, siendo un perfil de ingeniero muy cotizado en el mercado laboral. Una afirmación como ésta, que hoy a nadie o a casi nadie le puede parecer extraña, remontándonos tan sólo una década atrás, en el comienzo de los noventa, bien podría haber sido calificada de exagerada o, en el mejor de los casos, alejada de la realidad.

¿Qué ha sucedido en estos últimos diez años para que, al menos quienes trabajamos en el entorno de la educación superior y las empresas y organismos relacionados con las NTIs, podamos tener esta nueva visión? Qué duda cabe que el cambio más importante que la sociedad ha experimentado en esta década que acabamos de dejar es el surgimiento y posterior desarrollo de Internet, hoy considerada ya como la red global de comunicaciones a nivel mundial y el futuro motor de la economía de mercados abiertos.

Este espacio conjunto que comparten las ciencias de las telecomunicaciones e informática, comúnmente llamada Telemática, nos ofrece una amplia oferta de servicios y potencialidades nuevas aún por descubrir. No obstante, esto no hace sino agudizar los problemas de seguridad –ya existentes anteriormente en menor proporción y en la práctica menospreciados- asociados con las *vulnerabilidades* y *amenazas* que van implícitas en un entorno abierto como éste. Las máximas de que no existe una red segura y que un canal de información es, simplemente por definición, inseguro, plantea un buen número de situaciones en las que la seguridad y la protección de la información juegan un papel fundamental en este nuevo entorno de comunicaciones.

Las herramientas que permitirán salvaguardar los datos de intrusos y proteger nuestra intimidad son las denominadas técnicas criptográficas. No hay que perder de vista, sin embargo, que la criptografía es sólo una de las muchas facetas de la denominada seguridad informática o su término anglosajón *computer security*. Términos como comercio electrónico, firma digital, autoridades de certificación, navegación segura por Internet,

derecho informático, protección de datos, auditoría informática, planes de contingencia, etc. comienzan a resultar familiares, incluso para los no profesionales, y conforman un perfil de conocimientos requeridos a los ingenieros que estamos hoy formando en nuestras universidades.

2. El perfil de Seguridad Informática

La Seguridad Informática es un concepto mucho más amplio que lo esbozado en el punto anterior. Abarca desde los principios básicos de la Matemática Discreta, la Teoría de la Información y el estudio de la Complejidad de los Algoritmos, fundamentos éstos que permiten el estudio, diseño e implementación de Sistemas de Cifra, Firma Digital, aplicaciones sobre Redes y Protocolos Criptográficos –parte de la denominada Seguridad Lógica- hasta los Planes de Contingencia y Recuperación, Políticas de *Backup*, Políticas de Acceso y Protección Física de los datos dentro del sistema informático –que corresponden por su parte a la denominada Seguridad Física- teniendo además como disciplinas relacionadas y afines por ejemplo las del Derecho Informático, Auditoría Informática y Peritaje.

Este importante abanico de temas comunes a la Seguridad Informática, complementarios entre sí y de gran actualidad, nos lleva a una simple y no menos importante reflexión: su necesaria introducción a través de sendas asignaturas en los curricula de las enseñanzas de ingeniería, al menos en aquellas relacionadas con la informática y las telecomunicaciones. Y esto es sólo la punta del iceberg; en realidad lo que está demandando esta nueva sociedad de la información es que las universidades también formemos ingenieros con estos perfiles específicos, que encontrarán un campo laboral tan importante como lo han tenido hasta hoy aquéllos con una formación orientada hacia la gestión de bases de datos, el desarrollo de nuevas metodologías, el mantenimiento y gestión de redes, la planificación y gestión de proyectos o la ingeniería del software.

3. Integración de la Seguridad Informática en los curricula

Como primer material de referencia podemos recoger lo que algunos expertos norteamericanos ya vislumbraban –aunque con un enfoque menos *agresivo* que el planteado en este artículo- hace dos años. En su artículo "*Integrating Security into the Curriculum*" [1] *Irvine, Chin* y *Frincke* proponen dos enfoques:

- "La Seguridad Informática podría ser el objetivo principal de un curriculum que debería investigar los fundamentos y enfoques técnicos de la seguridad con una profundidad considerable.
- Un curriculum de ingeniería relacionado con las ciencias de la computación podría elegir la Seguridad Informática como una propiedad importante a ser considerada a lo largo de todos los estudios."

Sin temor a equivocarnos, esta tendencia insinuada por estos destacados investigadores en su informe, es la que la amplia mayoría de los centros de educación superior en España han comenzado a tener en cuenta desde hace algo más de 5 años. Si nos remitimos al estudio sobre la "*Enseñanza de la Criptografía y Seguridad de la Información en España: primer Informe sobre perfiles de asignaturas*" [2], vemos que una de sus conclusiones más relevantes y sorpresivas al menos en ese momento en que se desconocía ese dato, fue la observación de un crecimiento de tipo exponencial en la oferta de asignaturas de este perfil a partir del año 1995: en tan sólo 10 años las universidades españolas pasaron de una oferta única a cerca de 40 asignaturas directamente relacionadas con la seguridad informática, la gran mayoría de ellas orientadas hacia la criptografía.

¿Casualidad, moda? En absoluto. Podríamos afirmar que, en este caso nuestras universidades, como siempre debería ser, han ido por delante de las innovaciones tecnológicas y las demandas del mercado, aunque esto no quiera decir que el enfoque de sus enseñanzas en este apartado sea, necesariamente, lo que el sector productivo y empresarial demanda en estos momentos. Lo que sí está claro es que en la actualidad, la práctica totalidad de las carreras de ingeniería informática y un buen número de las ingenierías de telecomunicaciones presentan como oferta docente una o más asignaturas de pregrado dedicadas a la seguridad informática, siendo también significativo el número creciente de asignaturas y formación de postgrado.

Entre otras cosas, esto ha dado lugar a que se celebren en España las Reuniones bienales de Criptografía, cuya VI edición acaba de celebrarse

en el año 2000 en Tenerife y en las que se presentan sobre 30 ponencias de investigación y desarrollo en este área, el nacimiento y los primeros pasos de una Asociación Española de Criptología y Seguridad de la Información, diversos portales en Internet, muchos de ellos conocidos en toda Iberoamérica y con un número muy alto de suscriptores, el éxito de público –en su mayoría ingenieros jóvenes de empresas- en las presentaciones que otras empresas del sector de la seguridad realizan con una periodicidad muy alta sobre temas de firma digital, comercio electrónico, seguridad en Internet, protección de la información, etc., el hecho de contar con una revista de Seguridad en Informática y Comunicaciones SIC que se edita cada dos meses y que acaba de cumplir 10 años, la celebración en nuestro país de diversos congresos, seminarios y cursos sobre seguridad y criptografía, los grupos de trabajo en seguridad de RedIRIS y, por último, el nacimiento de CriptoRed, la Red Temática Iberoamericana de Criptografía y Seguridad de la Información, un sitio en la red en el que los profesores, investigadores y profesionales del sector, agrupados en una comunidad virtual de científicos, aportan información y contenidos docentes de libre distribución para beneficio propio de sus miembros y el de muchos miles de alumnos, ingenieros e internautas en general en toda Iberoamérica. Pocos países pueden mostrar un empuje tan sostenido en esta materia.

Todo esto no puede ser mera coincidencia. Lo que hace años atrás comenzó como una tendencia docente con un enfoque netamente académico, hoy en día se ha convertido en un perfil profesional muy deseado en el sector productivo y empresarial, con la particularidad de que éste no se conforma sólo con profesionales que tengan conocimientos en una o dos materias de las que hablábamos en párrafos anteriores: es menester contar con un técnico que domine una mayoría de ellas y esto, aunque nos pese al sector educativo en el que se encuentra el autor, no lo estamos ofreciendo actualmente a la sociedad.

El efecto no se ha hecho esperar y es así como varias empresas del sector –algunas incluso sólo de formación- ofrecen estas enseñanzas como un compendio de asignaturas de seguridad y redes a ingenieros y técnicos que necesitan conocer todo este entremado relacionado con la problemática de la seguridad en general.

Si, por nombrar sólo algunos, tenemos en cuenta también documentos tan importantes y *vinculantes* como la nueva *Ley Orgánica de Protección de Datos* [3] LOPD aprobada en España en diciembre de 1999 en la que, entre otras muchas cosas, se definen las figuras del *Responsable de Fichero* y el *Encargado de Tratamiento* y, además, el Real Decreto 994/1999 por el que se aprueba el *Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal* [4], en el que se define al *Responsable de Seguridad* como la "*persona o personas a las que el responsable de fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables*", podemos concluir que ya no sólo es el sector empresarial quien nos pide a los centros de enseñanza superior este perfil de ingeniero, sino el poder legislativo quien ha regulado al respecto y esto es un tema muy serio como para que las universidades no se hagan eco de tal demanda.

Es más, en el reciente Informe "*¿Qué les preocupa a los responsables de seguridad?*" publicado en la mencionada revista SIC [5] queda patente el problema cuando destacados expertos en la materia de diversas empresas en España indican la necesidad de disponer de profesionales cualificados y especializados, actualmente muy escasos, y la importancia de una formación continuada y del reciclaje de estos profesionales.

4. El Ingeniero en Seguridad Informática

Llegados a este punto, es preciso aclarar que el planteamiento que aquí se propone como formativo específico de la malla curricular del ingeniero tendrá -como era de esperar- algunos detractores y, además de ello, es posible que sea incluso en cierto grado utópico. No obstante, hay que tener en cuenta que aquí no se pretende otra cosa que hacer un llamado de atención que invite a reflexionar a quienes corresponda, sin entrar en aspectos docentes más específicos. Estos otros temas pueden ser fruto de un estudio posterior, con una clara orientación académica y dirigida tal vez hacia otro ámbito.

Vamos a plantear dos tipos de titulación, acorde con la realidad educacional en España: la del Ingeniero Superior en Seguridad Informática (ISSI) de 5 años y la del Ingeniero Técnico en Seguridad Informática (ITSI) de 3 años. En las

siguientes tablas se propone un conjunto de asignaturas obligatorias específicas del perfil y que conforman, por sí solas, aproximadamente el 35 % del curriculum de formación obligatoria del ingeniero, tanto en titulación superior ISSI como en la técnica ITSI.

Curso	Cuatrimestre	Asignatura	Créditos	Total
3º	Primer	Fundamentos de Matemática Discreta	3,0	
		Temas Avanzados de Matemática Discreta	4,5	7,5
3º	Segundo	Algorítmica Aplicada a la Criptografía	4,5	
		Fundamentos de la Seguridad Informática	4,5	
		Seguridad Física	4,5	13,5
4º	Primer	Derecho Informático	6,0	
		Criptografía	4,5	
		Algoritmos Criptográficos	4,5	15,0
4º	Segundo	Virus Informáticos	4,5	
		Seguridad en Lenguajes y Bases de Datos	4,5	
		Seguridad en Sistemas Operativos	6,0	15,0
5º	Primer	Autoridades de Certificación	4,5	
		Protocolos de Seguridad en Redes	6,0	
		Administración de Sistemas	4,5	
		Autenticación	4,5	19,5
5º	Segundo	Comercio Electrónico	4,5	
		Protocolos Criptográficos	4,5	
		Auditoría y Peritaje Informático	4,5	
		Tecnologías de Tarjetas Inteligentes	3,0	
		Temas Avanzados de Seguridad Informática	3.0	19,5
			TOTAL	**90,0**

Tabla 1. Componente obligada específica en la titulación de ISSI.

Curso	Cuatrimestre	Asignatura	Créditos	Total
2º	Primer	Fundamentos de Matemática Discreta	3,0	
		Fundamentos de la Seguridad Informática	4,5	7,5
2º	Segundo	Derecho Informático	6,0	
		Seguridad Física	4,5	
		Virus Informáticos	4,5	15,0
3º	Primer	Criptografía	6,0	
		Seguridad en Sistemas Operativos	4,5	
		Seguridad en Bases de Datos y Lenguajes	4,5	
		Auditoría y Peritaje Informático	4,5	19,5
3º	Segundo	Autoridades de Certificación	4,5	
		Autenticación y Protocolos de Seguridad en Redes	7,5	
		Comercio Electrónico	4,5	
		Administración de Sistemas	4,5	21,0
			TOTAL	**63,0**

Tabla 2. Componente obligada específica en la titulación de ITSI.

En cuanto a aquellas materias obligadas y reguladas por BOE, evidentemente no haremos comentario alguno. Sus descriptores y objetivos están bien definidos y son contenidos necesarios para la formación del Ingeniero Informático y de Telecomunicaciones. Sin embargo, habrá que hacer un esfuerzo de síntesis en aquellos créditos troncales y obligatorios para ajustar esta carga lectiva a sus valores estándar. Es una tarea difícil pero no por ello imposible. En estas enseñanzas estamos ya acostumbrados a cambiar los planes de estudio cada 7 ú 8 años, no por gusto sino por la imperativa necesidad de adecuar los estudios a los nuevos tiempos y técnicas.

Aunque lo normal es *construir la casa por los cimientos y no por el techo* y, en lo que a este estudio respecta deberíamos plantear primero los objetivos generales y específicos de esta nueva titulación para luego establecer la

denominada malla curricular del estudiante, vamos a darnos la libertad de comenzar al revés, planteándonos así en primer término aquellos conocimientos que nos demanda la sociedad.

En la Tabla 1 se muestra la propuesta de distribución curricular para las asignaturas específicas del perfil propuesto en la Ingeniería Superior en Seguridad Informática ISSI, con un total de 90 créditos. Supondremos todas las asignaturas con carácter cuatrimestral.

Aunque pueda resultar obvio, es menester recordar que 1 crédito es equivalente a 10 horas de clase; es decir, una asignatura con 4,5 créditos significa 45 horas de clase, distribuidas entre clases teóricas y prácticas. Por lo tanto, si dedicásemos de esa cantidad 3 créditos a teoría (y por tanto 1,5 a prácticas) en un cuatrimestre, ello representa dos horas de clase en aula a la semana, un módulo suficientemente adecuado para la mayoría de las asignaturas.

Fundamentos de Matemática Discreta • Cuerpos finitos • Operaciones en aritmética modular • Algoritmos en aritmética modular	**Temas Avanzados en Matemática Discreta** • Cálculos en Campos de Galois • Factorización de polinomios en GF • Curvas elípticas aplicadas a la criptografía
Algorítmica Aplicada a la Criptografía • Clasificación de los problemas • Complejidad algorítmica • Problemas típicos usados en criptografía	**Fundamentos de la Seguridad Informática** • Conceptos de seguridad informática • Historia de la criptografía, sistemas de cifra • Teoría de la información y codificación
Seguridad Física • Planes de contingencia • Políticas de seguridad en la empresa • Política y control de accesos	**Derecho Informático** • Protección de datos • Ley de firma digital y comercio electrónico • Deontología del Ingeniero en Seguridad
Criptografía • Cifrado simétrico y asimétrico • Autenticación y firma digital • Criptosistemas híbridos	**Algoritmos Criptográficos** • Análisis de algoritmos de cifra y firma • Análisis de funciones hash • Estudio de la fortaleza de los algoritmos
Virus Informáticos • Clasificación y características de los virus • Medidas de protección y eliminación • Análisis de algoritmos malignos	**Seguridad en Lenguajes y Bases de Datos** • Seguridad en Java • Protección de datos en SGDB • Seguridad en bases de datos distribuidas
Seguridad en Sistemas Operativos • Sistemas Operativos seguros: libro naranja • Seguridad en Windows NT y Novell • Seguridad en entornos Unix y Linux	**Autoridades de Certificación** • Concepto, definiciones y políticas de una AC • Certificados digitales X.509 • Implementación de una AC
Protocolos de Seguridad en Redes • Seguridad en Internet y en Intranet • Plataformas seguras: SHTTP, SSL, TLS, IPSec • Cortafuegos	**Administración de Sistemas** • Gestión y fortificación de la máquina • Detección de intrusiones • Herramientas de control y auditoría de la máquina
Autenticación • Kerberos, SSH • Autenticación X.509 • Autenticación con marcas de agua	**Comercio Electrónico** • Normas del mercado, inicio de actividades • Norma SET. Instalación del servicio • Tipos de comercio: B2B, B2C
Protocolos Criptográficos • Transferencia trascordada • Protocolos de conocimiento nulo • Aplicaciones a la resolución de problemas	**Auditoría y Peritaje Informático** • Técnicas de auditoría • Auditoría de sistemas y seguridad • Auditoría jurídica
Tecnologías de Tarjetas Inteligentes • Estándares de interconexión • Estructura interna de las tarjetas y tipos • Funcionalidades criptográficas	**Temas Avanzados en Seguridad Informática** • Criptografía cuántica, visual, etc. • Autenticación con parámetros biométricos • Nuevos algoritmos; esquemas de seguridad

Tabla 3. Descriptores de las asignaturas de la componente obligada específica en las titulaciones propuestas.

Si bien es deseable que el Ingeniero Técnico tenga los mismos conocimientos que el Superior, esto es imposible en tanto ese título tiene una duración de sólo 3 años. Teniendo en cuenta esta limitación de tiempo de estudio y, por otra parte, el enfoque eminentemente

práctico de esta titulación de primer ciclo, se propone en este caso un total de 63 créditos repartidos como se indica en Tabla 2.

La Tabla 3, a modo de ejemplo y como una primera aproximación, enumera descriptores de las asignaturas que forman el perfil de la nueva titulación, y que serán similares en contenido y en carga docente tanto en ISSI como en ITSI.

5. Conclusión

La necesaria adaptación de los curricula en las enseñanzas de ingeniería a los avances de la tecnología, nos pone a veces ante el umbral de tomar decisiones de gran trascendencia y, por tanto, expuestas a todo tipo de críticas y opiniones encontradas. No obstante, y pese a ello, en este artículo se ponen sobre la mesa datos concretos sobre el empuje de las nuevas tecnologías de la información y la imperiosa necesidad de ofrecer al mercado laboral un perfil de ingeniero cuyo papel fundamental, además de otros propios de su formación en informática, telecomunicaciones y redes, sea el de la seguridad informática en el contexto amplio que aquí se ha presentado.

El devenir de los tiempos es cada vez más acelerado y la universidad comienza a correr el riesgo, principalmente ante el sector industrial y empresarial, de no ser el referente idóneo de formación en tanto éstos deben suplir por su cuenta esta formación, en muchos casos de alta complejidad tecnológica, a través de cursos extra universitarios.

La *apuesta* por una titulación universitaria nueva –y ya no sólo un perfil- en Seguridad Informática es evidentemente muy fuerte y, como ya se ha comentado, a más de alguno podrá parecerle desmesurada; no obstante, en la opinión del autor y a la luz del análisis de lo acontecido en estos últimos diez años en este sector, no ofrecer este tipo de formación superior desde nuestras universidades bien podría considerarse como la pérdida de una gran oportunidad. Quedan muchas cosas pendientes: especialización del profesorado, evaluación de costes, completar el curriculum con troncalidad en ingeniería, contrastar con otras universidades, etc. No obstante, es muy posible que dentro de algunos años escuchemos hablar del *Computer Security Engineer* mientras aquí todavía estemos dándole vueltas al tema. No sería aventurado decir que la adecuación de los planes de estudio de las ingenierías a las nuevas tecnologías de la información es sólo una cuestión de tiempo.

Referencias

[1] Cynthia E. Irvine, Shiu-Kai Chin, Deborah Frincke. *Integrating Security into the Curriculum.* Computer IEEE, December 1998, pp. 25-30.

[2] Ramió A. Jorge, Caballero G. Pino. *Enseñanza de la Criptografía y Seguridad de la Información: primer Informe sobre perfiles de asignaturas.* Revista Seguridad en Informática y Comunicaciones SIC, nº 34, Abril de 1999, pp. 85-90.

[3] LOPD: Ley Orgánica 15/1999, de 13 de diciembre de *Protección de Datos de Carácter Personal*. BOE núm. 298, de 14 de diciembre de 1999.

[4] Real Decreto 994/1999, de 11 de junio, por el que se aprueba el *Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal*. BOE núm. 151, de 25 de junio de 1999.

[5] *¿Qué les Preocupa a los Responsables de Seguridad?* Revista Seguridad en Informática y Comunicaciones SIC, nº 41, Septiembre de 2000, pp. 40-49.

Referencias en Internet

[1] CriptoRed: Red Temática Iberoamericana de Criptografía y Seguridad de la Información http://www.criptored.upm.es

[2] Asociación Española de Criptología y Seguridad de la Información http://aecsi.rediris.es

[3] Criptonomicón http://www.iec.csic.es/criptonomicon

[4] HispaSec http://www.hispasec.com

[5] Kriptópolis http://www.kriptopolis.com