Jornada - Debate en el Coitt
" El Ingeniero de Seguridad"

Colegio Oficial Asociación Española Ingenieros Técnicos de Telecomunicación

udima UNIVERSIDAD A DISTANCIA DE MADRID

Asociación Nacional de Tasadores y Peritos Judiciales Informáticos

El pasado día 23 de Mayo se realizó en la Sede Central del COITT, una Jornada-Debate sobre "EL INGENIERO DE SEGURIDAD" en donde se dieron cita profesionales del sector en torno a una mesa compuesta por prestigiosos ponentes relacionados con el Anteproyecto de la Ley de Seguridad Privada.

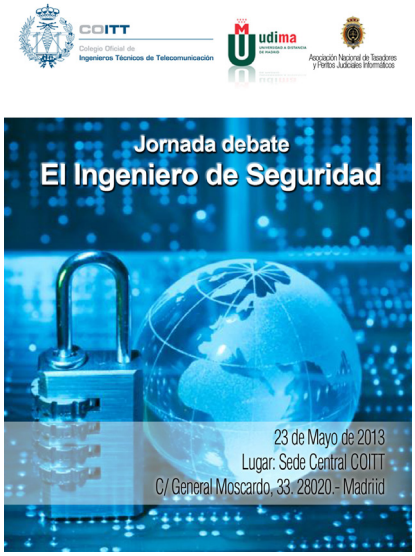
La inauguración de la mesa corrió a cargo del Decano del COITT **D. Jose Javier Medina**, quien disertó sobre la normativa futura y el nuevo campo que se abrirá para los Ingenieros en Telecomunicaciones, recalcando la importancia de las comunicaciones y la importancia de contar con profesionales capacitados.

Llego el turno del más esperado, El Comisario Jefe de la Unidad de Control de Seguridad Privada, **D. Esteban Gándara**, quien nos explicó de manera detallada, el ámbito de aplicación, las actividades compatibles, las prohibiciones, los requisitos generales, los servicios, las responsabilidades y sobre todo las sanciones para Técnicos, Ingenieros, Empresas y clientes.

Nos quedamos con los cuatro puntos que más nos afectan y que son:

Aplicación de la Ley al Ingeniero.
Artículo 3. Ámbito de aplicación.

2. Igualmente, en la medida que resulte pertinente en cada caso, se aplicarán a los establecimientos obligados a disponer de medidas de seguridad, a los usuarios de los servicios de seguridad privada, a los ingenieros y técnicos de las empresas de seguridad, a las empresas



prestadoras de servicios de seguridad de la información y las comunicaciones inscritas en el registro correspondiente, a las centrales de alarma de uso propio y a los centros de formación de personal de seguridad privada.

Acreditación del Ingeniero.
Artículo 19. Requisitos generales de las empresas.

1.c) Igualmente, los ingenieros y técnicos de las empresas de seguridad privada deberán disponer de la correspondiente acreditación expedida por el Ministerio del Interior, conforme a lo que reglamentariamente se establezca.

Servicios del Ingeniero.
Artículo 46. Servicios de instalación y mantenimiento.

1. Los servicios de instalación y mantenimiento

de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, consistirán en la ejecución, por técnicos acreditados, de todas aquellas operaciones de instalación y mantenimiento de dichos aparatos, equipos, dispositivos o sistemas, que resulten necesarias para su correcto funcionamiento y el buen cumplimiento de su finalidad, previa elaboración, por parte de ingenieros acreditados, del preceptivo proyecto de instalación, cuyas características se determinarán reglamentariamente.

Responsabilidad sobre el Ingeniero.

Artículo 56. Infracciones de las empresas que desarrollen actividades de seguridad privada, de sus representantes legales y de los despachos de detectives privados.

1. Infracciones muy graves:

b) La contratación o utilización, en servicios de seguridad privada, de personas que carezcan de la habilitación o acreditación correspondiente.

Artículo 57. Infracciones del personal que desempeñe funciones de seguridad privada. El personal que desempeñe funciones de seguridad privada, así como los ingenieros y técnicos, podrán incurrir en las siguientes infracciones:

Muy grave:

i) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, sin disponer de la acreditación correspondiente expedida por el Ministerio del Interior.

Grave:

m) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, no ajustados a las normas técnicas reglamentariamente establecidas.

1. Por la comisión de infracciones muy graves:

a) Multa de 30.001 a 600.000 euros.

b) Revocación de la autorización, que comportará la prohibición de volver a obtenerla por un plazo de entre uno y dos años.

c) Prohibición para ocupar cargos de representación legal en empresas de seguridad privada por un plazo de entre uno y dos años.

1. Por la comisión de infracciones muy graves:

a) Multa de 6.001 a 30.000 euros.

b) Revocación de la habilitación o acreditación, que comportará la prohibición de volver a obtenerla por un plazo de entre uno y dos años.

2. Por la comisión de infracciones graves:

a) Multa de 1.501 a 6.000 euros.

b) Suspensión temporal de la habilitación o acreditación por un plazo de entre seis meses y un año.

2. Por la comisión de infracciones graves:
Multa de 5.001 a 20.000 euros.

Entendiendo como el mejor valor la capacitación universitaria, se encontraba en la mesa también el Vicerrector de la Universidad UDIMA, **D. Juan Luis Rubio**, quien explicó que como Universidad de referencia en la formación en TICs, estaba mentalizada con el anteproyecto de la Ley de Seguridad Privada y mostró a los asistentes la oferta personalizada a este colectivo, informando de la creación de un CSIRT Universitario (Computer Security Incident Response Team), Equipo de Respuesta ante Incidencias de Seguridad) Con el objeto de dar respuesta a incidentes de seguridad en tecnológicas de la información que contara con un laboratorio informático y telemático forense propio con distintas áreas, gestionado por un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidentes de seguridad en los sistemas de información, ya que existe una gran cantidad de pérdidas causadas por los virus, las vulnerabilidades, los casos de acceso no autorizado a información, el robo de información protegida, etc.

Este CSIRT Universitario, recibirá, analizará y responderá informes de incidentes recibidos desde miembros de su comunidad formada por empresas que se asociasarán al mismo coordinando la respuesta de cualquier incidente de Seguridad, evento real o sospechoso relacionado con la seguridad de un sistema informático o red.

Las funciones, serán:
• Ayudar al público objetivo a atenuar y prevenir incidentes graves de seguridad.
• Ayudar a proteger informaciones valiosas.
• Coordinar de forma centralizada la seguridad de la información.
• Guardar evidencias, por si hubiera que recurrir a pleitos.
• Apoyar y prestar asistencia a empresas para recuperarse de las consecuencias de los incidentes de seguridad.
• Dirigir de forma centralizada la respuesta a los incidentes de seguridad - Promover confianza, que alguien controla la situación
• Avisos de seguridad
• Búsqueda de vulnerabilidades
• Auditorias o evaluaciones de seguridad
• Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras
• Desarrollo de herramientas de seguridad
• Propagación de información relacionada con la seguridad
• Gestión de incidentes de seguridad (análisis, respuesta, soporte y coordinación de incidentes de seguridad)
• Gestión de vulnerabilidades (análisis, respuesta y coordinación de vulnerabilidades detectadas)

Ya se han realizado acuerdos con empresas para la formación de un grupo de 25 investigadores informáticos

forenses, que estudiara el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas; y una capacitación mediante becas para formar a 150 expertos en Seguridad Informática forense que quedaran contratados en dichas empresas.

El siguiente ponente fue **D. Enrique Belda Esplugue**s, *Subdirector General de Sistemas de Información y Comunicación para la Seguridad*; quien debatió sobre la importancia de las certificaciones necesarias, la problemática existente en el ámbito de esta Sociedad de la Información y la importancia de unir la Seguridad Física y Lógica. Su trabajo diario para sumar fuerzas entre los profesionales de las entidades públicas y privadas, llevan a una multiplicación y construir unas trabas más potentes para los verdaderos enemigos que aprovechando el ciberespacio, gozan de una invisibilidad difícil de detectar unida a un limbo legislativo sin fronteras, que es aprovechado para cometer todo tipo de acciones delictivas.
La siguiente ponencia corrió a cargo de **D. Luis Fernando Hernández García**, *Teniente Coronel de la Jefatura de Información*, quien dejó perplejos a los asistentes mostrándoles la cara oculta de Internet, y el nuevo reto a los que se encuentran los profesionales de la seguridad física, corporativa y empresarial.

Dejo patente, que el tradicional marco colaborativo ente las Seguridades FISICA y LOGICA, es más que necesario para que mediante un trabajo en equipo ambas partes formen un equipo indisoluble para una Seguridad Real.
El conoce muy bien por su trabajo diario que los grupos terroristas y las organizaciones afines, para la consecución de sus objetivos, si se han profesionalizado en las TICs y utilizan Internet, los sistemas informáticos, aplicaciones, programas y herramientas como instrumento de comisión de los delitos. Enfatizó que no podemos perder más tiempo ante esta amenaza emergente que está en las agendas de los gobiernos como amenaza principal que no cuenta con profesionales capacitados y se ha convertido en el cuarto modelo más lucrativo para los criminales después de la venta de armas, prostitución, juego ilegal; escalando puestos, superando conceptos y obteniendo resultados cuya realidad supera la ficción.
El binomio Ciberamenazas &Ciberseguridad, preocupa a los profesionales de la seguridad lógica y aun no han reaccionado los profesionales de la seguridad física

por su desconocimiento en la materia CIBER, siendo sus campos el espionaje, sabotaje, caos invisible e incluso la guerra. Los profesionales de la seguridad física, tienen a su cargo objetivos golosos para estos delincuentes del siglo XXI, como las infraestructuras críticas y estratégicas y conocen que pueden adueñarse de cualquier sistema o instalación sin pasar delante de los vigilantes armados.
El CCN-CERT aviso del alto nivel de ataques cibernéticos contra instituciones, organizaciones, infraestructuras criticas, empresas y organismos públicos y privados, de la necesidad de sensibilización y preparación de profesionales de la seguridad; ilustrándonos de algunos ciberataques reales, como Stuxnet, la Operación Shady Rat, Duqu, Flame, Gauss y otros más que comprometían millones de ordenadores capaces de realizar capturas de pantalla, activar micrófonos, enviar a otros ordenadores bases de datos y archivos con material y contenido sensible, grabar conversaciones y remitir mensajes instantáneos entre otras cosas.

No quiso pasar por alto que toda organización y sobre todo sus responsables de seguridad deben de priorizar la Gestión del Conocimiento dentro de su estructura. Es vital la clasificación, Custodia, Acceso y Difusión de la información sensible ya que la máxima es que solo se tiene que tener acceso a la información que se debe conocer. Hay que realizar un estudio real de nuestras debilidades corporativas para no caer en manos de algún desaprensivo que se escuda en el anonimato de la red.

La unidad que dirige cuenta con reconocidos profesionales, pero lanza un llamamiento a la colaboración de todos los agentes implicados en la Seguridad tanto Lógica como Fisica.

El responsable de la Comisión de Emprendedores del Colegio y vocal de la AEGIT, **D. Esteban González Peinado**, recalco la misión del Ingeniero de Seguridad desde su prisma del Colegio Profesional El IS debe adaptar los medios de seguridad al riesgo y bienes a proteger proporcionalmente, considerando que la protección local y el medio de transmisión hasta la CR deben ser lo suficientemente confiables integrados y adecuados con un criterio normativo, fundamentado en una formación y conocimiento homologada y contrastada suficientemente, dando lugar este saber hacer contrastado, a una habilitación emitida por una entidad certificada y un registro oficial de esa habilitación en la autoridad correspondiente que permita la adecuación de un régimen sancionador por el no cumplimiento determinados requisitos de suficiencia técnica y su adecuación.

• Unas funciones claramente diferenciadoras como Dirección técnica.
•Proyecto (diseño) de los sistemas de seguridad, según las normas EN-UNE de aplicación, que incluirá memoria, medición y valoración de los costes de la instalación
•Documentación técnica y gráfica del proyecto
•Realizar previamente el análisis de los riesgos
•Planificación de la instalación de los sistemas
•Supervisión del proceso de instalación que realizará personal técnico con la formación y experiencia adecuada
•La Certificación de que lo instalado satisface a lo proyectado.
•Documentación y registros de los cambios posteriores.
•Planificación y Control del Servicio de Mantenimiento
•Asesorar a la empresa en la selección, homologación y adquisición de los componentes de los sistemas de seguridad a instalar y sobre las tecnologías más adecuadas y avances.

El último ponente de la Jornada fue **D. Angel Bahamontes Gómez**, *Presidente de la ANTPJI*, que agradeció al COITT su invitación a estas Jornadas, y al Ministerio del Interior por el esfuerzo de integrar en el anteproyecto de la Nueva Ley de Seguridad Privada a los profesionales de la Seguridad Informática, entendiendo que la suma de todos hace una fortaleza real ante los delincuentes sean

del tipo que sea. Los expertos en Seguridad Informática son los profesionales más demandados en la actualidad, puntualizo, y la demanda de grandes empresas concienciada con la seguridad informática, así lo atestiguan, no solo son demandados en el ámbito empresarial, sino en la administración de la Justicia, ya que es raro que cualquier litigio no tenga un componente tecnológico.

Como entidad líder en la Informática Forense, sigue la política de establecer acuerdos y sinergias que beneficien el conjunto de las empresas y por ende de la sociedad. La Seguridad Física y la Seguridad Lógica, están condenadas a establecer acuerdos de colaboración estratégica, de compartir conocimientos y experiencias a favor de la una Sociedad necesitada de Protección y Seguridad.

El tiempo se agotaba y tras la entrega por parte del Colegio de los títulos de Socio de Honor a:
D. Enrique Belda Esplugues,
D. Esteban Gándara Trueba y a
D. Luis Fernando Hernandez García, en reconocimiento a su trayectoria profesional y su apoyo a la institución se ofreció un cóctel a los asistentes que salieron con ideas muy claras de lo que será la nueva Ley de Seguridad Privada y su diploma acreditativo de las Jornadas.