Cybersecurity
Summer
BootCamp

2017

TEMARIO
Policy Makers (extensivo)

Cybersecurity Summer BootCamp 2017
18-29 julio - León (España)
www.incibe.es/summer-bootcamp

Organizado por:

Gobierno de España – Ministerio de Energía, Turismo y Agenda Digital
incibe_ Instituto Nacional de Ciberseguridad
OEA OAS

Con la colaboración de:

universidad de León
Ayuntamiento de León
León Cuna del Parlamentarismo
Gobierno de España – Ministerio de Asuntos Exteriores y de Cooperación
Santander
BID Banco Interamericano de Desarrollo
EUROPOL EC3 European Cybercrime Centre
INTERPOL

PROFESORES

David Cantón

Jesús Feliz

Aisler Martínez

Taller 16

Fundamentos básicos de ciberseguridad

Duración: 5 horas

Descripción

Tiene por objeto servir de introducción a los conceptos y problemáticas que la ciberseguridad plantea y su tratamiento en la labor de Policy Makers. Concretamente, se plantea como formación básica de soporte para facilitar la comprensión e interpretación de los conceptos e informes relacionados con ciberdelitos.

Temario

El taller estaría divido en tres partes:

- Ciberseguridad: A qué nos enfrentamos. (2 horas)
  - Vulnerabilidad y amenaza
  - Ciberdelitos y ciberciminalidad: incidentes de seguridad.
  - Criptografia/cifrado
  - Sistemas de anonimización: VPN, Deep Web, red TOR y similares.
  - Delitos tradicionales potenciados por sistemas de información.
  - Principales actores en la detección, prevención, respuesta y recuperación frente a ciberataques.
  - Problemática de la investigación en internet desde una perspectiva técnica.

- Introducción a la ciberseguridad: tecnologías. (2 horas)
  - Evolución y contexto tecnológico actual
  - Redes y sistemas operativos
  - Virtualización
  - Cloud pública y privada

- Introducción al análisis forense digital. (1 hora)
  - Se explicará en qué consiste un análisis forense digital, las fases del mismo y los conceptos técnicos que los asistentes al taller pueden necesitar conocer en su día a día.

PROFESOR

Vicente Moret

Taller 17.1

Aspectos regulatorios de la ciberseguridad (I). Normativa aplicable

Duración: 5 horas

Temario

- **Marco normativo internacional aplicable**
  - Introducción sobre el distinto tratamiento jurídico de la ciberdelincuencia, el ciberterrorismo y la ciberguerra. Precisiones conceptuales
  - El derecho procesal y el derecho penal ante el reto de la ciberseguridad
  - El derecho internacional humanitario y la ciberseguridad
  - Convenios y acuerdos internacionales
    - El Convenio del Consejo de Europa sobre ciberdelincuencia (Budapest 2011)
    - El Convenio del Consejo de Europa sobre la prevención del terrorismo (Varsovia 2005)
    - El Manual de Tallin
    - UN y la ciberseguridad
  - Normativa Europea
    - Estrategia de Ciberseguridad de la Unión Europea (2013)
    - La Directiva 2013/40/UE
    - La Directiva NIS (2016)

- **La territorialidad en Internet:** aspectos de derecho internacional aplicados a la investigación de ciberdelitos: la jurisdicción, la competencia y la cooperación internacional.
  - Mecanismos de asistencia mutua entre autoridades.
  - Acceso a información alojada en infraestructuras situadas en otros Estados.
  - Bases de datos multinacionales.
  - Organismos internacionales
  - La cooperación con entidades privadas de otros Estados.

PROFESORES

Jorge Villarino

Pablo García Mexía

Taller 17.2

Aspectos regulatorios de la ciberseguridad (II). Derechos y libertades de las personas

Duración: 5 horas

Descripción

El taller comenzará explicando el contexto en el que surgen los derechos de última generación y señalando qué derechos se incluyen en este concepto y qué características tienen.

Seguidamente se tratará el derecho de acceso a internet y si se puede catalogar como un derecho fundamental. Se incluirá una referencia a los principales textos normativos en los que se ha considerado un derecho. A continuación se tratará el principio de neutralidad en la red y la internet abierta. Se tratará la evolución histórica de estos conceptos y la situación actual, incluyendo el posicionamiento de las autoridades norteamericanas y europeas.

En la siguiente parte del taller se estudiarán los principales conflictos entre derechos fundamentales en la Red. Se tratarán –a través de casos reales en Europa y Estados Unidos– las principales características de la libertad de expresión en Internet, así como sus límites y sus sistemas de protección. Igualmente se analizará la evolución del conflicto entre libertad y seguridad, y en concreto, hasta qué punto se puede limitar la libertad en Internet en virtud de la seguridad. Esta parte terminará con una breve referencia a los Equipos de Respuesta ante Emergencias Informáticas (CERTs).

La tercera y última parte del taller se centrará en algunos de los principales retos que afronta la privacidad desde la perspectiva del nuevo Reglamento General de Protección de Datos. Se verán los aspectos técnicos y legales de Big Data y Analytics, así como las fugas de información y las obligaciones que deben cumplir las organizaciones; las transferencias internacionales de datos, incluyendo el nuevo régimen de transferencias a los Estados Unidos y el papel que pueden jugar las BCR; las medidas técnicas y organizativas que deben ser implantadas por las organizaciones, incluyendo el papel de la privacidad desde el diseño y por defecto, las PIAs y los delegados de protección de datos.

Temario

- El desarrollo de los derechos “de cuarta generación”.
- El derecho de acceso a Internet: la neutralidad de la red y la internet abierta.
- Las libertades fundamentales en el ciberespacio: expresión vs información. Libertad vs seguridad. Los CERTs.
- Intimidad, privacidad y protección de datos: fronteras territoriales en un mundo sin barreras y conectado.
    - Big Data y analytics: aspectos técnicos y legales
    - Fugas de información
    - Del Safe Harbour al Privacy Shield: las transferencias internacionales de datos. Las BCR.
    - Medidas técnicas y organizativas a implementar en las organizaciones. Privacidad desde el diseño y por defecto. PIAs. El DPO.

PROFESORES

Marco A. Lozano

Alejandro Diez

Taller 18 (1/4)

La ciberseguridad en la empresa - Primera parte (Marco A. Lozano y Alejandro Diez)

Duración: 1 hora 30 minutos

Temario

- Fundamentos y estándares de la seguridad de la información: Sistemas de Gestión de la Seguridad de la Información (SGSI) y auditoría de sistemas de información. Gestión de riesgos y la metodología para la gestión del cumplimiento normativo
- Nivel de adopción real de las medidas básicas de protección para la pyme
- Ejemplos de regulación y autorregulación sectorial:
  - PCI-DSS, entorno financiero
  - Tecnologías incipientes (Cloud Computing, IoT, RFID, etc.)

PROFESOR

Rafael García del Poyo

Taller 18 (2/4)

La ciberseguridad en la empresa – Segunda parte (Rafael García del Poyo)

Duración: 3 horas 30 minutos

Descripción

La ciberseguridad es un área que en los últimos tiempos está siendo objeto de análisis, inversión y asignación de recursos por parte de todo tipo de compañías, tendencia que tiene visos de ser más relevante día a día, más si cabe tras los últimos acontecimientos acaecidos a nivel mundial que han puesto en jaque a muchas grandes empresas que son, las que en un principio, mejor preparadas se encuentran tanto técnica como organizativamente, para enfrentarse a este tipo de acontecimientos.

En cualquier caso, la presente sesión no tiene como único fin el centrarse exclusivamente en la regulación aplicable a día de hoy a nivel nacional en lo referente a la ciberseguridad, sino dar una visión legal y eminentemente práctica sobre otros aspectos directa o indirectamente relacionados y demandados por parte de las empresas tomando como base las gestión de riesgos empresariales desde la perspectiva de la ciberseguridad. Entre los cuales cabría destacar la delimitación de la responsabilidad de las compañías y sus administradores/directivos así como la implementación de programas de prevención de delitos o *compliance*.

Temario

- Las nuevas relaciones laborales en las empresas digitalizadas y el control empresarial
  - Introducción
  - Breve reseña sobre los derechos fundamentales del trabajador en el marco de las relaciones laborales y sus límites
  - Criterio de proporcionalidad
  - Nuevas medidas en auge implementadas durante los últimos años
    - La utilización y monitorización del correo electrónico y herramientas informáticas puestas a disposición de los trabajadores
    - La instalación de cámaras de videovigilancia y circuito cerrado de televisión
    - La instalación de dispositivos de acceso mediante la utilización de datos biométricos
    - La implantación y utilización de dispositivos de geolocalización
  - Uso de redes sociales personales y profesionales e implicaciones en el ámbito laboral

PROFESOR

Rafael García del Poyo

Taller 18 (3/4)

La ciberseguridad en la empresa – Segunda parte (Rafael García del Poyo)

Temario

- Gestión de riesgos y la metodología para la gestión del cumplimiento normativo
  - Introducción
  - Identificación de los riesgos en función del marco regulatorio
  - Especial referencia a la protección de datos de carácter personal
  - Identificación de riegos operacionales y reputacionales
  - Identificación de las necesidades de una compañía y preparación de guías o manuales internos y procedimentación de las actuaciones a llevar a cabo.
- La ciberseguridad en medios sociales y la reputación empresarial
  - Introducción
  - Identidad digital
  - Principales riesgos en la gestión de las redes sociales e impacto en la reputación de las compañías
  - Esfera pública y esfera privada
  - Protección de datos de carácter personal y nuevo Reglamento Europeo de Protección de Datos
  - *Big data* e *Internet of Things*
  - Personas jurídicas
    - Derecho al olvido
    - Derecho al honor
  - Breve referencia a la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
  - Gestión de un incidente
  - Implantación de políticas para uso responsable de redes sociales para los empleados

PROFESOR

Rafael García del Poyo

Taller 18 (4/4)

La ciberseguridad en la empresa – Segunda parte (Rafael García del Poyo)

Temario

- La responsabilidad penal de las personas jurídicas: *compliance*
  - Introducción
  - Evolución histórica de la responsabilidad penal de las personas jurídicas
  - Novedades introducidas por medio de la Ley Orgánica 1/2015
  - Análisis de la Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del código penal efectuada por ley orgánica 1/2015
  - Programas de *compliance* ¿Qué son?
  - Diferencias entre *compliance* y responsabilidad social corporativa
  - Fin de un programa de *compliance* empresarial
  - *Compliance officer*: Obligaciones y responsabilidades
  - Contenido de un programa de compliance
  - Establecimiento de procedimientos y medidas de control
  - Detección, notificación y gestión de una incidencia
  - Normalización y estándares internacionales – ISO / Normas UNE
- La responsabilidad de administradores y directivos
  - Introducción
  - Nuevo régimen de responsabilidad de los administradores
  - Deberes de los administradores y directivos
  - Régimen de responsabilidad civil
  - Acciones de responsabilidad y otros supuestos
  - Diferencias entre administradores de hecho y de derecho
  - Medidas de prevención
  - Seguros de administradores y directivos (seguros de D&O)
- Los ciberseguros
  - Introducción
  - ¿Qué son?
  - Situación actual de los ciberseguros en España y en otras jurisdicciones
  - A quien van dirigidos y necesidades de los asegurados
  - ¿Que se pretende proteger?
  - Blockchain y Smart Contracts

PROFESORES

Javier I. Zaragoza

Jorge Bermúdez

Taller 19 (1/2)

Ciberdelincuencia y criminalidad digital global

Horas taller: 5 horas

Descripción

El desarrollo de las tecnologías de la información y de la comunicación ha modificado profundamente las reglas de convivencia y pautas de comportamiento de nuestra sociedad. La implementación de estos nuevos medios de comunicación, de la misma manera que ha traído efectos positivos para todos los ciudadanos, también ha supuesto la aparición de nuevas conductas delictuales desconocidas hasta la fecha en nuestro ordenamiento jurídico. El legislador, a estos efectos, ha realizado un encomiable esfuerzo para adaptar nuestro Código Penal a la nueva naturaleza de estos delitos introduciendo tipos penales realmente novedosos (stalking, sexting, childgrooming) y adaptando tipos penales ya existentes –como la estafa- a la nueva realidad social.

Por otra parte, la utilización de las nuevas tecnologías ha abierto un abanico impresionante en la investigación y esclarecimiento de los hechos criminales. Tras la última reforma operada en nuestra Ley de Enjuiciamiento Criminal se ha superado, de una vez por todas, el desfasado artículo 579, introduciéndose medios de investigación especialmente novedosos como el agente encubierto online.

El presente taller tiene por objeto principal explicar el nuevo fenómeno criminal que se ha originado a raíz del auge de las nuevas tecnologías, los nuevos tipos penales creados para luchar contra el mismo, las nuevas medidas de investigación tecnológicas usadas para ser esclarecidos, y la afectación a los derechos fundamentales que se pueden producir como consecuencia del uso de las mismas. Todo ello desde un punto de vista no solamente teórico sino también práctico a través de la exposición, y debate, de casos prácticos vividos por ambos ponentes durante el desarrollo de sus actividades profesionales

PROFESORES

Javier I. Zaragoza

Jorge Bermúdez

Taller 19 (2/2)

Ciberdelincuencia y criminalidad digital global

Horas taller: 5 horas

Temario

- Introducción a la ciberdelincuencia
  - Concepto
  - Evolución de las conductas delictivas
  - El papel de la Fiscalía en la lucha contra el ciberdelito
- Principales tipologías penales
  - La difusión inconsentida de imágenes íntimas. El sexting.
  - El nuevo delito de hostigamiento. El stalking
  - El acoso a menores a través de la red. El Childgrooming
  - El delito de daños informáticos. Ataques contra infraestructuras críticas. El ciberterrorismo.
  - El enaltecimiento de actos terroristas a través de la red. Su colisión con el derecho a la libertad de expresión. El nuevo tipo penal del autoadoctrinamiento.
  - Los delitos de odio y delitos de violencia de género cometidos a través de la red.
  - La protección de las víctimas de los delitos cometidos a través de internet. Retirada de contenidos y bloqueo de acceso.
- Nuevas medidas de investigación tecnológicas
  - Las nuevas medidas de investigación tecnológicas y su colisión con los derechos fundamentales. El derecho al entorno virtual.
  - La nueva regulación del agente encubierto online.
  - La investigación a través de la dirección IP. Regulación tras la reforma operada por Ley 13/2015.
  - Investigación de IMEI e IMSI
  - La nueva regulación del registro de dispositivos de almacenamiento masivo de información.
  - La colaboración de las entidades prestadoras de servicios.
  - La conservación rápida de contenidos a través de la red.

PROFESORES

Manuel Huerta de la Morena

Taller 20.1 (1/2)

Investigación tecnológica y evidencia digital (I) – Primera parte (Manuel Huerta)

Duración: 2 horas 30 minutos

Temario

- Fundamentos de la investigación tecnológica. Los requerimientos de la evidencia electrónica, La correcta identificación de los escenarios, los preceptos de la prueba Conservación, inalterabilidad y repetibilidad y la correcta comprensión de los antecedentes y los escenarios.
  - Aspectos procesales en la LECRim: el control remoto de dispositivos y el agente encubierto en la red. La contextualización de la evidencia como proceso de identificación o descarte de falsas evidencias. El control remoto y los accesos multiusuario en entornos corporativos y sistemas con mantenimiento remoto.
  - La retención de datos. Los procesos de adquisición de evidencias, la tipología de escenarios, tecnologías y técnicas de adquisición. El análisis y la conservación, la tecnología de automatización de proceso de evidencias, la simulación de escenarios y funcionamiento de sistemas.
- La gestión de las evidencias electrónicas El triaje de evidencias y las magnitudes de información.
  - Actuaciones tendentes a la identificación de terminal y usuario, y su valor en juicio. La contextualización de la actividad objeto de análisis, la vinculación entre terminal y usuario, autor o victima?
  - Fuentes y medios de prueba electrónicos. Como dotar de seguridad jurídica a los documentos electrónicos. La identificación de escenarios como fuentes de información, el enfoque de cara a las garantías jurídicas, indefensión y tutela judicial efectiva, el contraste de fuentes como garantía probatoria en procesos de comunicación efectiva con documentación electrónica. Contextualización de comunicaciones.
  - Régimen jurídico de la prueba electrónica en el proceso: verificación de los hechos, obtención y aportación de prueba electrónica. La existencia de prueba descontextualizada, sistemas de verificación de autoría y acción, La falsificación de evidencias, sistemas de descarte de intervención en evidencias por parte de terceros, Los indicios probatorios y la solicitud de requerimientos.
  - Los metadatos, las descargas y la certificación de contenidos y datos de tráfico: la fe pública digital. El papel de los proveedores en proceso de emisión de medios de prueba, El papel notarial en las evidencias electrónicas y peligros reales en la actividad notarial.
  - Riesgos asociados en la prueba electrónica y colisión con derechos fundamentales. La cadena de custodia. La cadena de custodia antes, durante y después del proceso de adquisición, La importancia del proceso de adquisición, El HASH y el ADN como parte de la cadena de custodia.
  - Análisis forense digital y su práctica por medio de expertos forenses ("computerforensics"): el informe forense y su valor en juicio. La moralidad e imparcialidad del investigador, la capacidad de investigación vs capacidad técnica, la importancia de las infraestructuras de laboratorio, La importancia del formato del informe forense tecnológico, su esquema y los puntos clave.

PROFESORES

César Lorenzana

Taller 20.1 (2/2)

Investigación tecnológica y evidencia digital (I) – Segunda parte (César Lorenzana)

Duración: 2 horas 30 minutos

Descripción

Durante el taller los alumnos deberán resolver un caso práctico en el que deberán analizar las evidencias iniciales, establecer las líneas de investigación, y desarrollar las mismas con el objetivo de establecer el caso planteado. Concretamente, se trata de desarrollar una investigación de un ataque distribuido de denegación de servicios (DDoS). El punto de partida de la investigación es la recogida de evidencias del ataque, y mediante la aplicación de la metodología de investigación el alumno podrá ir avanzando por diferentes líneas hasta finalizar con éxito la investigación e identificar al responsable

Temario

- Presentación, misiones, y capacidades Departamento de Delitos Telemáticos de la UCO (10 min)
- Descripción de la metodología de investigación (20 min)
  - Recogida de evidencias de los sistemas afectados (escena del crimen)
  - Actuaciones iniciales de obtención de información OSINT (sin control judicial)
  - Proceso de Investigación Tecnológica (determinación del lugar de conexión)
  - Proceso de Investigación Tradicional (determinación del posible responsable)
  - Recopilación de evidencias y construcción de imputaciones
- Presentación del caso práctico (2 horas)
  - Presentación del caso práctico
  - Difusión información y datos iniciales
  - Desarrollo de las líneas de investigación (aplicación de la metodología) con ejemplos prácticos.
  - Solución del caso (en caso de que los alumnos no lleguen a la solución, se describirá el proceso seguido para determinar el responsable)

PROFESOR

Manuel López Guerra

Taller 20.2 (1/2)

Investigación tecnológica y evidencia digital (II) – Primera parte (Manuel López Guerra)

Duración: 2 horas 30 minutos

Descripción

Caso práctico de una investigación llevada a cabo por la Policía Nacional

Temario

- Unidades especializadas de investigación: la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía (UIT)
- Presentación de un caso práctico.
  - Control remoto de dispositivo. Problemática.
  - Procedimiento de obtención y tratamiento de pruebas electrónicas en una diligencia de entrada y registro en el domicilio del autor de los hechos.
  - Implicaciones en los derechos fundamentales: secreto de las comunicaciones, comunicaciones secretas con un abogado, etc.
  - Análisis forense de evidencias desde el punto de vista policial.

PROFESOR

Manuel de Campos

Taller 20.2 (2/2)

Investigación tecnológica y evidencia digital (II) – Segunda parte (Manuel de Campos)

Duración: 2 horas 30 minutos

Descripción

En los últimos años las Nuevas Tecnologías han hecho irrupción en el campo del delito, provocando un drástico cambio de paradigma en materia de Investigación Criminal, ya que no sólo se ha modificado la modalidad de comisión de la mayoría de los delitos tradicionales, llevándola del campo físico al campo digital, sino que además, se han descubierto y generado nuevos delitos específicos cometidos en el ciberespacio a través de medios digitales. Esta circunstancia requiere un importante cambio en los métodos de investigación, cambio que debe abarcar todos los ámbitos relacionados con el crimen; y es aquí donde adquiere fundamental relevancia lo que se ha dado en llamar evidencia electrónica o evidencia digital y, dadas sus especiales características, todo lo relativo a su obtención, tratamiento, cadena de custodia y valoración en juicio.

El taller se orienta a establecer los conceptos de evidencia, evidencia digital o electrónica y prueba digital o electrónica, como así también los distintos aspectos de la prueba –elemento, sujeto, medio y objeto de prueba-, para luego desarrollar y profundizar respecto de la prueba digital, cómo y quién debe obtenerla, cuál es su adecuado tratamiento, las características especiales de su cadena de custodia y finalmente su valoración en juicio.

Temario

1. **Actuaciones tendentes a la identificación de terminal y usuario, y su valor en juicio.**
   Se tratarán las formas a través de las cuales se puede identificar una terminal y el usuario, ya que uno de los objetivos primordiales de toda investigación criminal es determinar “quien” es el autor del delito.
2. **Fuentes y medios de prueba electrónicos. Como dotar de seguridad jurídica a los documentos electrónicos.**
   Se verán las características particulares de las fuentes de evidencia digital, lo que se relaciona directamente con la manera de obtenerla –procesos de identificación, recolección o adquisición y conservación o preservación-, y cuáles son los aspectos de este tipo de prueba; como así también la definición de los roles de especialistas en la gestión de evidencias electrónicas.
3. **Régimen jurídico de la prueba electrónica en el proceso: verificación de los hechos, obtención y aportación de prueba electrónica.**
   Se debatirá el estándar mundial de buenas prácticas para el manejo de las evidencias digitales (identificación, recopilación, consolidación y preservación) y sus principios básicos –aplicación de métodos y procesos auditables, reproducibles y defendibles-.
4. **Los metadatos, las descargas y la certificación de contenidos y datos de tráfico: la fe pública digital.**
   Se tratará el concepto de metadato, sus registros, clasificación -metadatos de propósito general y de propósito específico-, esquemas de información, su utilidad en una investigación.
5. **Riesgos asociados en la prueba electrónica y colisión con derechos fundamentales. La cadena de custodia.**
   La obtención de información digital puede afectar el derecho a la privacidad, por lo que resulta fundamental encontrar el balance justo entre seguridad y privacidad, entre el objeto de la investigación digital y las garantías fundamentales y la forma adecuada de legislar al respecto. También se verá el valor de la cadena de custodia como garantía del derecho de defensa en juicio.
6. **Análisis forense digital y su práctica por medio de expertos forenses: el informe forense y su valor en juicio.**
   Se analizarán las características que presenta el adecuado tratamiento de la evidencia digital, capacidades requeridas, trabajo del experto, características del informe y su valor probatorio.

PROFESORES

Manuel Ransán

Alejandra Frías

Taller 21

Ciberseguridad y menores – Primera parte (Manuel Ransán)

Duración: 2 horas

Descripción

Se abordarán los fundamentos sobre las problemáticas relacionadas con el uso de Internet y las TIC por los menores. Se tratarán sus principales características y datos de situación, y se presentarán estrategias y recomendaciones para su prevención y respuesta en caso de incidente, tanto en el entorno familiar como en el escolar. También se analizar el papel de los Centros de Seguridad en Internet de la red europea INSAFE..

Temario

- Problemáticas vinculadas al uso de Internet por los menores
  - Contenidos inapropiados
  - Conductas peligrosas
  - Contactos dañinos
- Buenas prácticas para la prevención y respuesta
  - Entorno familiar
  - Entorno escolar
- Centros de Seguridad en Internet (IS4K) y la red INSAFE

Ciberseguridad y menores – Segunda parte (Alejandra Frías)

Duración: 3 horas

Temario

- La alfabetización digital y mediática
- La protección en la red de las personas menores de edad
- Los ciberdelitos que afectan a menores: el Convenio de Lanzarote y la Directiva 2011/93/UE