Policy Makers Intensivo-semana 2

Organizado por:

Gobierno de España · Ministerio de Economía y Empresa · incibe_ Instituto Nacional de Ciberseguridad · OEA OAS

Con la colaboración de:

Gobierno de España · Ministerio de Asuntos Exteriores, Unión Europea y Cooperación · universidad de león · Ayuntamiento de León · León · Santander · IDB Inter-American Development Bank · Canada · aws · EUROPOL EC3 European Cybercrime Centre · INTERPOL

PROFESORES

Juan Delfín Peláez

Beatriz García del Pozo

Introducción a la ciberseguridad: conceptos generales

Descripción

Introducción de la ciberseguridad y conceptos generales de la seguridad de la información, en el contexto actual de incidentes y delitos de ciberseguridad a nivel nacional e internacional. Como objetivos en este taller se encuentran conocer las principales medidas de protección de carácter técnico y organizativo y asegurar la privacidad y seguridad en internet y en los dispositivos móviles.

Temario

- Introducción a la ciberseguridad. Conceptos generales.
- Situación actual de incidentes y delitos de ciberseguridad.
- Principales medidas de protección.
- Privacidad y seguridad en internet.
- Talleres prácticos:
  - Cómo configurar la privacidad y seguridad en google, gmail.
  - Cómo configurar la privacidad y seguridad en RRSS.
  - Cómo configurar la privacidad y seguridad en dispositivos móviles.
  - Cómo cifrar datos y comunicaciones para garantizar la privacidad.

PROFESORES

Rafael García del Poyo

Derechos y libertades

La ciberseguridad en las organizaciones

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.

El objetivo de esta sesión no sólo se centra en la regulación aplicable a día de hoy a nivel nacional en lo referente a la ciberseguridad, sino también pretende aportar una visión jurídica y eminentemente práctica sobre otros aspectos directa o indirectamente relacionados y demandados por parte de las empresas tomando como base la gestión de riesgos empresariales desde la perspectiva de la ciberseguridad. Nos centraremos en destacar la delimitación de la responsabilidad de las compañías y sus administradores/directivos así como la implementación de programas de prevención de delitos o de "compliance".

Temario

- La gestión del riego en las organizaciones y la responsabilidad penal de las personas jurídicas.
- La responsabilidad de administradores y directivos.
- La responsabilidad laboral de los empleados.
- La responsabilidad legal y deontológica por fugas de información.

PROFESORES

Cristina Gutiérrez

Derechos y libertades

Situaciones de riesgo online para menores y su tratamiento a través de la Línea de Ayuda de IS4K

Descripción

El taller tiene por objeto ofrecer una introducción a Internet Segura for Kids, el Centro de Seguridad para Menores en Internet de España operado por INCIBE, y de forma específica a su servicio de Línea de Ayuda, en el que se proporciona asesoramiento y asistencia psicosocial y en aspectos preventivos y reactivos sobre Internet y las situaciones de riesgo que experimentan niños y adolescentes. En este sentido, se abordarán las principales temáticas de riesgos que aborda el servicio a través del tratamiento de casos de estudio y se comentarán otros casos de referencia tratados dentro de la red europea INSAFE, red de centros de concienciación y líneas de ayuda a la cual pertenece IS4K.

Temario

- Introducción: IS4K dentro de la Red INSAFE
- Funcionamiento de la Línea de Ayuda
  - Elementos organizativos y funcionales
  - Principales resultados
- Casos de estudio de la Línea de Ayuda IS4K
  - Planteamiento del caso
  - Flujo de atención
  - Planteamiento para la prevención y respuesta
- Otros casos de estudio a través de la Red INSAFE

PROFESORES

Alejandra Frías

Derechos y libertades

La importancia de la ordenación institucional de la ciberseguridad

Descripción

Garantizar la seguridad en el ciberespacio se ha convertido en objetivo prioritario de todas las agendas gubernamentales. Este taller pretende abordar la necesidad, de todos los Estados, de contar con un esquema claro de gobernanza de la Ciberseguridad.

Temario

- Una parte general:
  - El marco gubernamental de la Ciberseguridad derivado de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, (NIS).
  - Referencia a diferentes Estrategias nacionales de Ciberseguridad.
- Una parte especial, dedicada al análisis del contexto institucional de la Ciberseguridad en España:
  - La Estrategia de Seguridad Nacional: el Consejo de Seguridad Nacional.
  - La Estrategia de Ciberseguridad Nacional: el Consejo Nacional de Ciberseguridad.
  - El Plan Nacional de Ciberseguridad.
  - Los Planes Derivados de Ciberseguridad: el Plan Derivado contra la Ciberdelincuencia y el Ciberterrorismo como herramienta en la lucha contra el Cibercrimen.

PROFESORES

Jorge Villarino

Derechos y libertades

Los derechos y libertades de las personas en un mundo digital

Descripción

Este taller estará dividido en dos partes: en la primera se analizará Internet como Red Abierta y el fenómeno de la manipulación de información, así como determinados conceptos básicos para los derechos fundamentales en Internet; y en la segunda, nos centraremos en algunos aspectos de la protección de datos, fundamentalmente enfocados a los instrumentos y problemáticas derivadas de la ausencia de fronteras.

Temario

- La Internet abierta y los derechos de última generación
- La libertad de acceso a la información en Internet. El binomio libertad de expresión vs derecho a la información veraz: la manipulación de contenidos y las acciones de desinformación en un mundo conectado.
- La neutralidad de la Red
- Tecnologías disruptivas y acceso a la Red
- Intimidad, privacidad y protección de datos: Europa vs EE.UU. Fronteras territoriales en un mundo sin barreras y conectado. La protección de la identidad.
- Las transferencias internacionales de datos: el *Privacy Shield*.
    - El régimen en el RGPD.
    - Países con nivel adecuado de protección: especial consideración a Argentina y Uruguay.
    - Las Binding Corporate Rules (BCR).
    - Casos de estudio: Facebook y Microsoft.

PROFESOR

Vicente Moret

Francisco Pérez Bes

Ordenación institucional en Ciberseguridad

La importancia de la ordenación institucional de la ciberseguridad

Descripción

El objetivo de este taller es conocer los distintos aspectos regulatorios de la ciberseguridad, tanto a nivel internacional como español. Se pretende dotar de un conocimiento detallado de las distintas normas y convenios vigentes en esta materia, así como abordar los aspectos más jurídicos de los conflictos en el ciberespacio.

Temario

- La gobernanza de la ciberseguridad.
  - Estado actual de la cuestión.
  - La ciberseguridad como elemento central de la seguridad nacional
  - La gobernanza de la seguridad en España
- El marco normativo de la ciberseguridad
  - Tratamiento jurídico de la ciberdelincuencia, el ciberterrorismo, y el ciberconflicto. Precisiones conceptuales.
  - El derecho penal, el derecho procesal y la ciberseguridad.
  - El Convenio del Consejo de Europa sobre ciberdelincuencia (Budapest 2011)
  - El Convenio del Consejo de Europa sorne prevención del terrorismo (Varsovia 2005).
- La Unión Europea y la ciberseguridad
  - La estrategia de ciberseguridad de la UE (2013)
  - La Directiva 2013/40 relativa a ataques contra los sistemas de información
  - La Directiva NIS (2016)
  - El RGPD
  - Las fake news y la UE
  - Directiva 2016/681 sobre registro de pasajeros
- La territorialidad en internet
  - Jurisdicción y competencia
  - La cooperación internacional
- El ciberconflicto
  - El derecho internacional humanitario y el ciberespacio
  - Naciones Unidas y la ciberseguridad
  - La OTAN y sus estructuras de ciberdefensa
  - El Manual de Tallin
  - La organización de la ciberdefensa en España

PROFESOR

Horacio Azzolín

Roberto Valverde

Medidas de investigación tecnológica

Medidas de investigación tecnológica

PROFESOR

Manuel de Campos

XXXXX

Gestión de evidencias tecnológicas

Fundamentos prácticos de la investigación tecnológica

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 buscará dejar en claro 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 quien debe obtenerla, cual es su adecuado tratamiento, las características especiales de su cadena de custodia y finalmente su valoración en juicio.

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

Antonio López

XXX

Fundamentos prácticos en la Investigación Tecnológica

PROFESORES

Jorge Bermúdez

Javier Zaragoza Tejada

Cibercrimen

Descripción

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.

Temario

- Introducción a la investigación de delitos cometidos a través de la red. El problema de la transnacionalidad. La feudalización de la red. Mecanismos de cooperación internacional.
- Demarcación y planta de los juzgados y tribunales españoles. La jurisdicción universal. El principio de ubicuidad. La comunicación personal como primera forma de cooperación.
- Introducción al derecho penal sustantivo. Nuevos tipos penales.
- Estafas informáticas. Phishing.
- Las criptomonedas desde el punto de vista legal. Incautación y realización de las mismas.
- El blanqueo de capitales a través de intermediarios en internet (exchangers). La nueva directiva europea del 19 de abril del 2018.
- El Stalking o delito de hostigamiento.
- El acoso a menores a través de la red. Childgrooming y novedades jurisprudenciales (referencia al pleno no jurisdiccional del 8 de noviembre del 2017)
- Elaboración, posesión y distribución de pornografía infantil en la red.
- El delito de daños informáticos. Ataques contra infraestructuras críticas. El ciberterrorismo. Enaltecimiento en la red.
- El descubrimiento y revelación de secretos. El delito de sexting del artículo 197.7
- Modificaciones legislativas necesarias.

PONENTE

Carlos Álvarez

Seminario ICANN

Duración seminario: 5 horas

Descripción

El entrenamiento ofrece estrategias, técnicas y herramientas a los investigadores, fiscales y otros agentes de la ley, que los profesionales en seguridad operacional y threat research utilizan para identificar diferentes formas de actividad maliciosa o delictiva que haga uso de recursos del Sistema de Nombres de Dominio (DNS). El objetivo es familiarizar a los asistentes con el DNS, permitirles conocer los tipos de información que están disponibles en el DNS y cómo acceder a ella para identificar infraestructura delictiva o identificar a los responsables de determinada actividad, cuando esto es posible.