#CyberSBC2023

3 al 13 julio de 2023

León, España

https://www.incibe.es/eventos/summer-bootcamp

Organizado por:

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA Más derechos para más gente

Con la colaboración de:

Canadá

AYUNTAMIENTO DE LEÓN

LEÓN CON SEGOS

universidad de León

INFORMACIÓN GENERAL

Objetivos:

- **Formar y adiestrar** en las últimas técnicas para la lucha contra los ciberdelitos, la gestión de incidentes de ciberseguridad y los aspectos legislativos a tener en cuenta en todos ellos.
- **Mejorar** la coordinación en la gestión de incidentes y ciberdelitos.

Formato práctico:

- Idiomas de impartición **español e inglés.**
- Evento de carácter **internacional y gratuito.**
- **Formación exclusiva** y puntera de máxima calidad.
- Temáticas novedosas y **últimas tendencias** en detección de ciberdelitos.
- **Talleres prácticos** impartidos por los mejores profesionales.
- Oportunidad para generar ***networking*** **de alto nivel** entre los asistentes.

Público objetivo:

- **Fuerzas y Cuerpos de Seguridad del Estado (FCS):** miembros de Fuerzas y Cuerpos de Seguridad que trabajen en unidades operativas relacionadas con la ciberseguridad.
- **CSIRT o CERT:** personal técnico que trabaje en Centros de Respuesta a Incidentes de Seguridad.
- **Fiscal, jueces y magistrados:** personal perteneciente a las carreras judicial, fiscal y abogados del Estado que trabajen en casos de cibercrimen o ciberseguridad.
- **PM:** *Policy Makers,* actores políticos, reguladores o legislativos: personal que trabaje en áreas relacionadas con los aspectos jurídicos y normativos de la ciberseguridad, formuladores de políticas estrategias de ciberseguridad y diplomacia.

Más información en:
https://www.incibe.es/eventos/summer-bootcamp

CARACTERÍSTICAS DEL EVENTO

Programa internacional de capacitación especializado en ciberseguridad.

5 tracks | 182 horas lectivas

- Programa de **37 horas** dirigido a **miembros de Fuerzas y Cuerpos de Seguridad** que trabajen en unidades operativas relacionadas con la ciberseguridad (FCS).
- Programa en español de **37 horas** dirigido a **personal técnico que trabaje en Centros de Respuesta a Incidentes de Seguridad** (CSIRT).
- Programa en inglés de **37 horas** dirigido a **personal técnico que trabaje en Centros de Respuesta a Incidentes de Seguridad** (CSIRT).
- Programa de **17 horas** dirigido a **personal en activo perteneciente a la carrera judicial.**
- Programa de **17,5 horas** dirigido a **personal en activo perteneciente a la carrera fiscal.**
- Programa de **36,5 horas** dirigido a **personal de organismos reguladores o legislativos que trabajen en áreas relacionadas con los aspectos jurídicos y normativos de la ciberseguridad** (*Policy Makers*).

PROGRAMAS FORMATIVOS

Talleres impartidos por **expertos de primer nivel** en aspectos relevantes y actuales para cada una de las 5 especializaciones.

Investigación policial (FCS):

Temática	Duración estimada
OSINT para investigaciones policiales	5 horas
Uso de la inteligencia artificial y Machine Learning por cibercriminales	5 horas
Colección y análisis de evidencias digitales en la nube	5 horas
Investigaciones de fraudes bancarios, BEC, *sim swapping* y fraude del CEO	5 horas
Operaciones criminales de los IAB (Initial Access Brokers)	5 horas
Agente encubierto en línea	2,5 horas
Investigaciones policiales sobre material de abuso infantil	2,5 horas
Ciberpatrullaje en investigaciones policiales	2,5 horas
Ciberseguridad conductual	2,5 horas
Ciberdelincuencia desde el punto de vista del microataque	2 horas

Operaciones CSIRT:

Temática	Duración estimada
Colección, procesamiento y distribución de *feeds* de ciberinteligencia	5 horas
Técnicas de ciberpatrullaje para CSIRT	5 horas
Respuesta a incidentes en la nube	2,5 horas
Detección, monitoreo y respuesta a incidentes	5 horas
Análisis de logs en la respuesta a incidentes (Windows/unix logs)	5 horas
Inteligencia sobre ciberamenazas (CTI)	5 horas
Análisis de correos electrónicos en la respuesta a incidentes	2,5 horas
KPI para servicios de los CSIRT	2,5 horas
Análisis de *malware* para la respuesta a incidentes	2,5 horas
Comunicación técnica para tomadores de decisiones	2 horas

Programa de jueces:

Temática	Duración estimada
Inteligencia artificial policial: vigilancia masiva y policía predictiva	3 horas
Registros policiales 2.0	2 horas
Trazabilidad de activos digitales y criptomonedas	2 horas
Contenidos ilícitos y afectación de la Seguridad Nacional	2 horas
Novedades regulatorias tecnológicas en el ámbito de la UE: el Reglamento de Servicios Digitales y las órdenes de actuación contra contenidos ilícitos	2 horas
La cooperación internacional en la investigación para la persecución de los ciberdelitos	2 horas
Visión general sobre los drones: fines preventivos, de investigación criminal y como herramienta de la Administración	2 horas
Retos del Derecho colombiano frente a la ciberdelincuencia: persecución y responsabilidad penal	2 horas

Programa de fiscales:

Temática	Duración estimada
Técnicas OSINT en procesos judiciales	6 horas
Cadena de custodia y evidencia electrónica en nuevas tecnologías	4 horas
Obtención transnacional de evidencias electrónicas	1 hora
Criptomonedas	1 hora
Nuevas formas de defraudación a través de la red (instrumentos de pago)	1,5 horas
Medidas cautelares: retirada de contenidos relacionados con el abuso sexual y crímenes de odio	1 hora
Preservación de evidencias	1 hora
Colaboración con los proveedores de servicios y reglamento de Servicios Digitales	2 horas

Formuladores de políticas:

Temática	Duración estimada
Perspectiva de género en la ciberdiplomacia y las estrategias nacionales de ciberseguridad (OEA)	2 horas
Desarrollo de estrategias de ciberseguridad (Catálogo de opciones de proyectos para el ciclo de la Estrategia de Ciberseguridad Nacional (NCS)	2 horas
Lecciones aprendidas sobre ciberseguridad y política digital en América Latina	2,5 horas
Ciberseguridad y herramientas digitales de la UE - SEAE	2 horas
Actores internacionales: análisis general	1 hora
Diplomacia tecnológica con casos simulados	2 horas
El rol de los formuladores de políticas en la gestión de incidentes	3 horas
Mesa redonda: prioridades para la ciberseguridad en un mundo global	2 horas
Opciones de sostenibilidad y creación de fondos de ciberseguridad	2,5 horas
Servicios públicos digitales y ciberseguridad	2,5 horas
Rol de la ciberdiplomacia en la gestión de crisis cibernética	4 horas
Gobernanza y normativa internacional en ciberseguridad	2,5 horas
Alianza Digital Lat-EU	2,5 horas
Pespectiva de género y estrategias globales de ciberseguridad	2,5 horas
Retos globales de protección de ciberseguridad en organizaciones	2,5 horas

*Estos programas son orientativos y están sujetos a modificaciones.

PROGRAMAS DE EMPRENDIMIENTO

Jornada Lean Startup – Colaboración INCIBE - TEC Monterrey

Programa destinado a **alumnos de maestría seleccionados desde TEC Monterrey** a fin de realizar un proyecto empresarial basado en la metodología Lean Startup.

Programa

- Presentación del programa e introducción a un proyecto empresarial.
- Qué es LeanStartUp.
- Modelo CANVAS: propuesta de valor y cliente.
- PMV.
- Marketing digital y métricas.
- Inversión y financiación.
- Retos innovadores destinados al desarrollo de un conjunto de actuaciones dirigidas a impulsar la I+D+i en materia de ciberseguridad.
- Elevator Pitch (story telling).

Jornadas Startups – Colaboración INCIBE – OEA

Programa en colaboración con la OEA que permite **consolidar poyectos y ampliar el ámbito de repercusión de sus iniciativas** mediante estrategias que permitan la replicabilidad nacional, regional y/o internacional de sus propuestas.

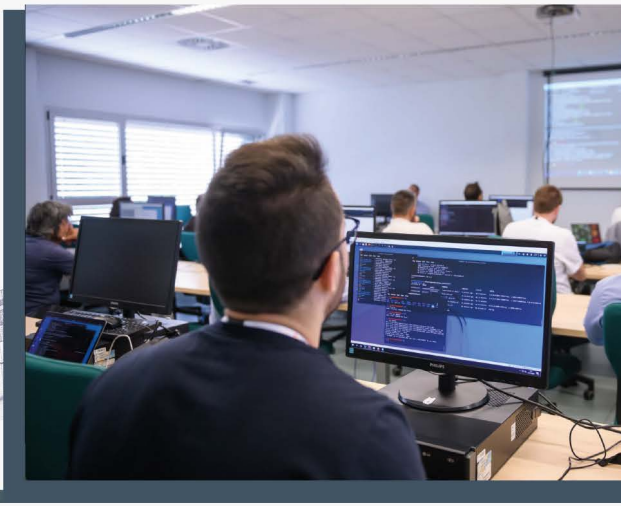
Programa

- Estrategia en la empresa.
- Internacionaliza tu *start-up* de ciberseguridad para conseguir crecimientos exponenciales.
- La protección del conocimiento y la innovación mediante la propiedad industrial e intelectual.
- Encuentro con alumni.
- Retos innovadores destinados al desarrollo de un conjunto de actuaciones dirigidas a impulsar la I+D+i y la creación de productos y soluciones en el ámbito de la ciberseguridad.

OTRAS ACTIVIDADES

Actividades para potenciar el *networking* entre los asistentes y las necesidades de colaboración entre los mismos.

- ***Role – Play:* casos prácticos y colaborativos** en los que intervienen perfiles de las 5 especialidades dando su punto de vista para la resolución de un incidente.



- **Actividades de ocio: visitas guiadas** por la ciudad de León y a los monumentos más emblemáticos, fomentando la difusión en redes sociales de las actividades.

Charlas de expertos en diferentes temáticas actuales, investigaciones en curso y nuevas herramientas relacionadas con la ciberseguridad y otras áreas.

RESULTADOS DEL EVENTO

Formato presencial con **210** participantes de **20** países

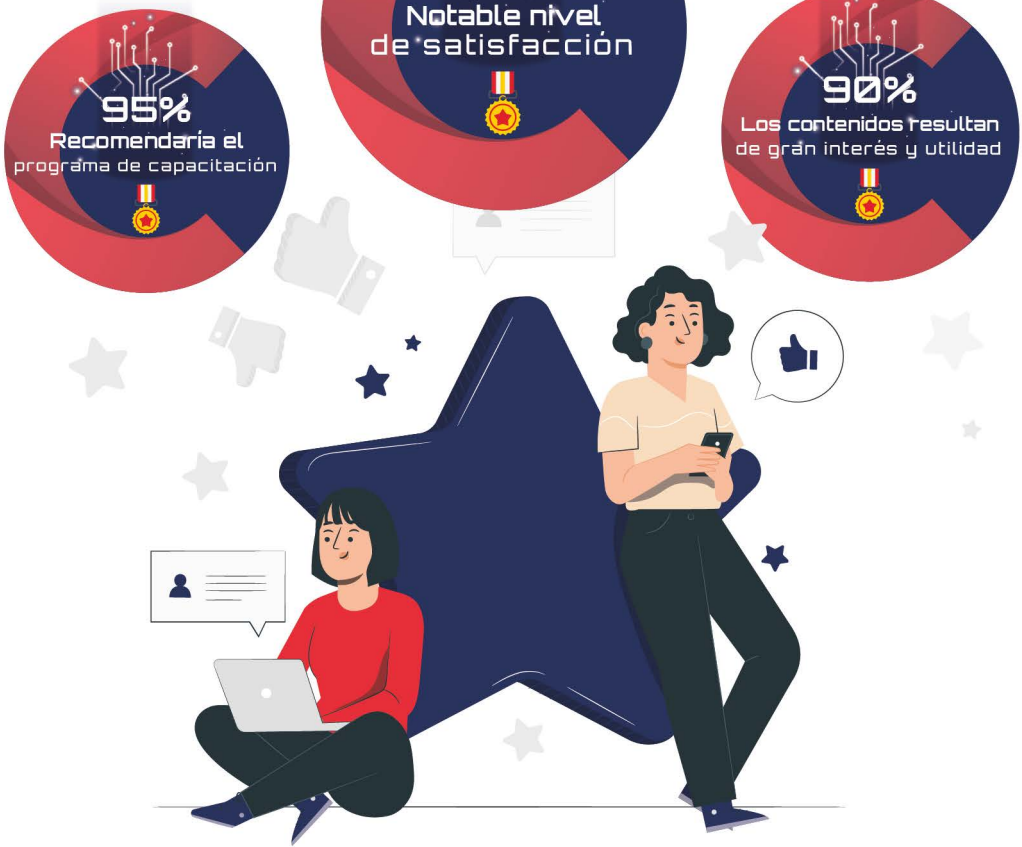
4 horas de ***keynotes*** **y sesiones magistrales**

Formación específica

- Investigación policial: **35 horas** de formación.
- Operaciones CSIRT: **37,5 horas** de formación.
- Fiscal, jueces y magistrados: **17 horas** de formación.
- Actores políticos, reguladores o legislativos: **22 horas** de formación.

42 ponentes y **8** ***keynotes*** **internacionales**

Feedback
de los alumnos:



#CyberSBC2023

https://www.incibe.es/eventos/summer-bootcamp

Organizado por:

Con la colaboración de: