28 y 29 de enero
4, 5, 11 y 12 de febrero

CURSO DE CONTRAINTELIGENCIA Y SEGURIDAD

INTELIGENCIA
MÁS LIDERAZGO

+32 639 834 504 | www.inteligenciayliderazgo.com | info@inteligenciayliderazgo.com

EL CURSO

La contrainteligencia podría definirse como un conjunto de acciones diseñadas por un serviciode inteligencia u organización con el fin de obstruir aquellas fuentes de información que puedan ser utilizadas en nuestra contra por un enemigo potencial y contrarrestar las actividades de servicios de inteligencia u organizaciones hostiles.

No debemos obviar que nuestros competidores o adversarios también disponen de equipos de inteligencia dispuestos a obtener datos sobre nuestras capacidades y vulnerabilidades, por lo que la contrainteligencia actuaría privándole de esas fuentes y protegiendo nuestra organización de amenazas externas, competencias desleales o sabotajes.

En resumen, es ese aspecto de la inteligencia que abarca todas las actividades que se dedican a eliminar o reducir la efectividad de las operaciones de inteligencia hostiles, y a la protección de la información propia contra el espionaje. Inteligencia y contrainteligencia están tan íntimamente ligadas, que una no existiría sin la otra.

PERFIL DEL ALUMNO

Personal de cualquier sector profesional que necesite llevar a cabo obtención de información, análisis y elaboración de inteligencia en apoyo de los procesos de planificación y toma de decisiones de su organización.

Los conocimientos adquiridos son de aplicación en inteligencia competitiva y económica, inteligencia criminal, terrorismo, ciberinteligencia, ciberseguridad, seguridad y defensa.

EL PROFESORADO ESTÁ COMPUESTO POR PROFESIONALES DE CONTRASTADA EXPERIENCIA EN INTELIGENCIA, TANTO CIVIL COMO MILITAR

OBJETIVOS GENERALES

A los asistentes se les proporcionarán los conocimientos necesarios sobre las actividades de contrainteligencia en apoyo a la seguridad en cualquier tipo de organización, así como los fundamentos sobre operaciones de influencia y la manera de contrarrestarlas.

La clave es una correcta elaboración del modelo de la amenaza como punto de partida para la evaluación de riesgos y la correspondiente implantación de las medidas de seguridad, así como el desarrollode los indicadores precisos para llevar a cabo una monitorización y control de las amenazas.

Los asistentes aprenderán cómo aplicar una gama de técnicas de análisis para mejorar la solidez, precisión, fiabilidad y calidad de los productos de contrainteligencia que elaboren.

Estas técnicas son un conjunto de metodología que permite llevar a cabo un proceso, paso por paso, para realizar un diagnóstico correcto del problema objeto de análisis, identificar los factores y variables clave y los precursores de cambio, elaborar y contrastar los posibles escenarios futuros de un asunto y desarrollar los indicadores precisos para llevar a cabo una monitorización y control del mismo.

OBJETIVOS ESPECÍFICOS

- Definir que es contrainteligencia y su finalidad.
- Comprender la interrelación entre contrainteligencia y seguridad.
- Diferenciar entre amenaza y riesgo.
- Elaborar un modelo de amenaza.
- Llevar a cabo el proceso de gestión del riesgo siendo capaces de realizar una evaluación de amenazas y riesgos.
- Aplicar diferentes técnicas de análisis para la evaluación de amenazas y riesgos.
- Definir que son las operaciones de Influencia y desinformación.
- Comprender la aplicación de la psicología social a las operaciones de influencia y desinformación.
- Aplicar técnicas para el análisis de operaciones de influencia y desinformación.
- Conocer los fundamentos de la comunicación estratégica.
- Identificar y analizar campañas de influencia
- Elaborar indicadores para monitorizar la evolución de una amenaza.
- Deducir la influencia que tiene en el proceso de toma de decisiones los procesos de evaluación de la amenaza y del riesgo.
- Comprender como se interrelacionan contrainteligencia, OPSEC y SEGINFO.

METODOLOGÍA DOCENTE Y CERTIFICACIÓN

CONVOCATORIA: 28 y 29 de enero y 4, 5, 11 y 12 febrero de 2021.

HORARIO: de 16,30 a 20,30horas.

MODALIDAD: presencial-virtual a través de la plataforma ZOOM.

NÚMERO DE HORAS: 24 horas presenciales virtuales. 100 horas de carga lectiva.

METODOLOGÍA: eminentemente práctica, combinándose clases teóricas con los correspondientes ejercicios.

AULA VIRTUAL

En el área personal del Aula Virtual, el alumno encontrarla el manual del curso, material didáctico complementario, documentación, bibliografía y ejercicios, que deberá enviar a los profesores para su corrección.

CERTIFICACIÓN

Los alumnos deben asistir a un 75% de las sesione presenciales-virtuales y realizar todos los ejercicios y controles de evaluación y seguimiento.

Posteriormente, recibirán un diploma-certificado de las materias cursadas en la acción formativa, el cual podrán incorporar a su currículum. Este certificado se descargará del Aula Virtual una vez cumplidos todos los requisitos.

INTELIGENCIA MÁS LIDERAZGO

CONDICIONES DE PAGO

PRECIO:
El precio de curso es de 300 euros

MATRICULACIÓN
La matriculación del curso se realizará mediante un único pago del importe del mismo.

DESCUENTO
Los alumnos pertenecientes a Fuerzas y Cuerpos de Seguridad, Fuerzas Armadas y miembros de las entidades colaboradoras tendrán derecho a un descuento del 15%

FORMA DE PAGO
Mediante transferencia bancaria, tarjeta de crédito y Paypal.

DEVOLUCIÓN
Si el alumno cancela la asistencia al curso con más de siete (7) días de antelación, se devolverá integro el importe abonado. Si la cancelación se produce con menos de siete (7) días de antelación, se devolverá solamente el 50% del importe abonado.
En caso de no alcanzarse un número mínimo de asistentes, el curso podrá ser suspendido. En tal caso, los alumnos matriculados recibirán el reembolso completo.

BONIFICABLE
Este curso curso cumple los requisitos para ser bonificable para empresas por la FUNDAE.

INTELIGENCIA MÁS LIDERAZGO

PROGRAMA

CLASES PRESENCIALES: 26 HORAS
DURACIÓN TOTAL: 100 HORAS

Introducción a Contrainteligencia.
- Conceptos básicos. El ciclo de contrainteligencia.
- Actividades y operaciones de Contrainteligencia.
- Relación de contrainteligencia con seguridad.

Amenazas y Riesgos.
- Definición de amenaza y riesgo. Tipos.
- La amenaza TESSCO y su influencia en la actividad empresarial. Caso particular: el Insider.

Diseño del modelo de amenaza.
- Elaboración de un modelo de amenaza.

Evaluación de amenazas y riesgos.
- Metodología para el Análisis de Riesgos. El proceso de gestión del riesgo.
- Análisis de riesgos y el proceso de
- contrainteligencia.

Contribución de contrainteligencia a OPSEC y protección de la información.
- Concepto. El proceso OPSEC.
- La Seguridad de la Información (SEGINFO). En las personas, en los documentos, en las instalaciones, en los Sistemas y en las Empresas.

El análisis en Contrainteligencia y Seguridad.
- Técnicas de análisis en Contrainteligencia y Seguridad.
- Técnicas contrarias de análisis. El Red Teaming.
- Concepto de Red Teaming. Clasificación de las
- técnicas de Red Teaming.
- Otras Técnicas: What if, Quadrant Crunching,
- Premorten, Detección de Decepción.

Operaciones de Influencia.
- Concepto y definiciones.
- Entorno operativo.
- Tipos de operaciones:decepción, ataques de reputación y manipulación de información.
- Técnicas para detección de operaciones de influencia.
- **Elaboración de contramedidas.**

Caso especial: las Operaciones de Decepción.

Apoyo de contrainteligencia a la activida empresarial.
- Internacionalización de la empresa.
- Seguridad en la cadena de suministros.
- Protección contra ataques de reputación.
- La protección contra la obtención ilegal de información: espionaje.
- Decepción en la actividad empresarial.

Contrainteligencia en el Ciberespacio.
- Enfoque de contrainteligencia para la Ciberinteligencia.
- El apoyo a ciberseguridad.

Consideraciones legales.

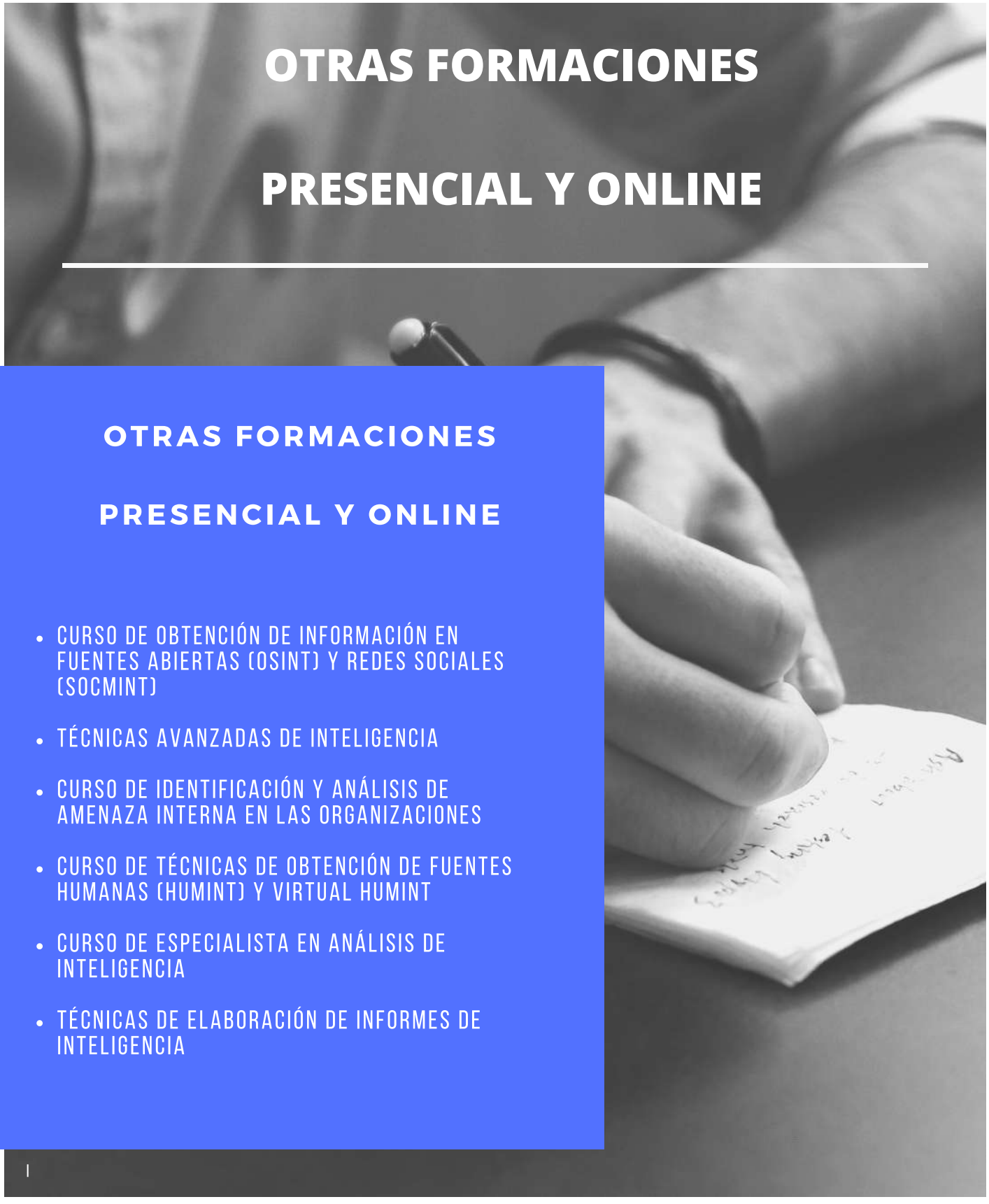
Elaboración de productos de contrainteligencia.
- Tipos de productos y su difusión.
- Normas para la elaboración de productos.

Ejercicios prácticos.
- Planificación de una campaña de decepción.
- Contramedidas OPSEC.
- Detección y análisis de campañas de desinformación en el ciberespacio.
- Detección de la decepción.

INTELIGENCIA MÁS LIDERAZGO

OTRAS FORMACIONES

PRESENCIAL Y ONLINE



OTRAS FORMACIONES

PRESENCIAL Y ONLINE

- CURSO DE OBTENCIÓN DE INFORMACIÓN EN FUENTES ABIERTAS (OSINT) Y REDES SOCIALES (SOCMINT)
- TÉCNICAS AVANZADAS DE INTELIGENCIA
- CURSO DE IDENTIFICACIÓN Y ANÁLISIS DE AMENAZA INTERNA EN LAS ORGANIZACIONES
- CURSO DE TÉCNICAS DE OBTENCIÓN DE FUENTES HUMANAS (HUMINT) Y VIRTUAL HUMINT
- CURSO DE ESPECIALISTA EN ANÁLISIS DE INTELIGENCIA
- TÉCNICAS DE ELABORACIÓN DE INFORMES DE INTELIGENCIA

INTELIGENCIA MÁS LIDERAZGO

MÁS INFORMACIÓN: 639 834 504

WWW.INTELIGENCIAYLIDERAZGO.COM INFO@INTELIGENCIAYLIDERAZGO.COM