

# **CLAVES DE CIBERSEGURIDAD**

## **PARA DIRECTIVOS Y MANDOS INTERMEDIOS**





## Qué es

La COVID-19 ha creado una tormenta casi perfecta en el ciberespacio. El incremento de la cibercriminalidad ha puesto en jaque a todos los actores públicos y privados. En estos meses, la ciberseguridad ha aparecido como elemento principal ante la exposición a nuevos fenómenos como el del teletrabajo, la educación o el ocio a través de las pantallas.

Pero antes de la pandemia, el mundo de la ciberseguridad ya se había convertido en un campo realmente complejo de abarcar para conocer todo lo que ocurre en torno a él.

A lo largo de este curso **se adquirirán las competencias o capacidades básicas para poder hacer frente a los retos más comunes que se nos pueden presentar en temas de ciberseguridad.** Riesgos como la ingeniería social, el malware, la gestión de contraseñas, etc. serán abordadas de una manera práctica.

Se conocerán las medidas organizativas básicas, desde una perspectiva formativa para aplicarlas en nuestras empresas o negocios, **sin perder de vista el desarrollo de la cultura y el elemento de la concienciación**, también conocido como “awareness” como punto de partida para evitar la mayor parte de incidentes que suelen ser provocados por los propios empleados.

## Dirigido a profesionales que quieren

**Saber proteger** su puesto de trabajo y el de su equipo

Saber que **la información de sus clientes está segura**

**Crear cultura** en ciberseguridad dentro de su empresa

Conocer cómo **protegerse cuando se trabaja en remoto**



## Estructura

Se trata de un itinerario formativo de **20 horas de duración**, impartidas durante 5 semanas, con 16 horas en presencia virtual (Zoom) y 4 horas de contenido e-learning.





## Objetivos

1

Sensibilizar a los profesionales sobre la necesidad de **proteger** su **información** y la de sus empresas

2

Entender las **claves de la ciberseguridad** que influyen en la protección de la información.

3

Comprender cómo trabajan los **ciberdelincuentes** y cómo descubrirlos

4

Conocer **herramientas** que ayudan a proteger la información.

5

**Analizar los riesgos** y saber **gestionar los incidentes.**





## Contenidos

### **Clases en formato presencia virtual (Zoom)- 12 horas.**

- ✔ Manejando a la persona: la ingeniería social – 1 h.
- ✔ Evolución de las amenazas y riesgos (I) – 1 h.
- ✔ Evolución de las amenazas y riesgos (II) – 1 h.
- ✔ Utilizando los servicios de manera segura – 1 h.
- ✔ Ataques y controles para proteger los activos – 1 h.
- ✔ Herramientas para proteger la información (I) – 1 h.
- ✔ Herramientas para proteger la información (II) – 1 h.
- ✔ Herramientas para proteger la información (III) – 1 h.
- ✔ Respuesta a incidentes: cómo reportar un incidente – 1 h.
- ✔ Análisis de riesgos y gestión de incidentes desde una perspectiva más técnica (I) – 1 h.
- ✔ Análisis de riesgos y gestión de incidentes desde una perspectiva más técnica (II) – 1 h.
- ✔ Análisis de vulnerabilidades – 1 h.

### **Taller sobre ciberseguridad (Zoom) – 4 horas.**

- ✔ Taller sobre herramientas de protección – 2 h.
- ✔ Taller de detección de vulnerabilidades, análisis de riesgos y gestión de incidentes – 2 h.



## Contenidos



### **Contenido e-learning – 4 horas**

- ✔ Introducción a la ciberseguridad
- ✔ Contexto actual de la ciberseguridad y objetivo de los ciberdelincuentes
- ✔ ¿Qué amenazas afectan a la información de las empresas?
- ✔ Ciberseguridad como elemento diferenciador y dependencia tecnológica
- ✔ ¿Qué es la ingeniería social y por qué la usan los ciberdelincuentes?

## Equipo docente

Los profesores de nuestro Partner Académico se distinguen por ser expertos de prestigio en sus campos respectivos. Con una experiencia profesional sólida.



### **Marco Antonio Lozano Merino**

Coordinador de Servicios de Ciberseguridad del INCIBE.  
Especialista en ciberseguridad y seguridad en TI e IICC



# Calendario

Las clases online síncronas se impartirán los lunes, miércoles y jueves de 18 a 19 horas y los talleres de 18 a 20 horas.

El programa se iniciará el 1 de marzo y finalizará el 31 de marzo.

Marzo 2021						
Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

18:00 - 19:00	<b>1</b>	<b>Manejando a la persona: la ingeniería social</b>
18:00 - 19:00	<b>3</b>	<b>Evolución de las amenazas y riesgos (I)</b>
18:00 - 19:00	<b>8</b>	<b>Evolución de las amenazas y riesgos (II)</b>
18:00 - 19:00	<b>10</b>	<b>Utilizando los servicios de manera segura</b>
18:00 - 19:00	<b>11</b>	<b>Ataques y controles para proteger los activos</b>
18:00 - 19:00	<b>15</b>	<b>Herramientas para proteger la información (I)</b>
18:00 - 19:00	<b>17</b>	<b>Herramientas para proteger la información (II)</b>
18:00 - 19:00	<b>18</b>	<b>Herramientas para proteger la información (III)</b>
18:00 - 19:00	<b>22</b>	<b>Análisis de riesgos y gestión de incidentes desde una perspectiva más técnica (I)</b>
18:00 - 19:00	<b>24</b>	<b>Análisis de riesgos y gestión de incidentes desde una perspectiva más técnica (II)</b>
18:00 - 19:00	<b>25</b>	<b>Análisis de vulnerabilidades</b>
18:00 - 20:00	<b>29</b>	<b>Taller sobre herramientas de protección</b>
18:00 - 20:00	<b>31</b>	<b>Taller de detección de vulnerabilidades, análisis de riesgos y gestión de incidentes</b>



## 05 – Condiciones económicas

El importe de la matrícula para realizar este programa es de **1.500 €** (más IVA)

## 06 – Contacto

Para cualquier tipo de información puedes ponerte en contacto con el equipo de CEOE Campus



Nuria Torrijos

**Email:** [ntorrijos@ceoecampus.es](mailto:ntorrijos@ceoecampus.es)

**Tel.** +34 616 863 512



Óscar Charneco

**Email:** [ocharneco@ceoecampus.es](mailto:ocharneco@ceoecampus.es)

**Tel.** +34 915 663 476



# CEO Campus