



**SÉ**

**INTERNACIONAL**

**Programa Internacional en  
CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES**

## INFORMACIÓN ACADÉMICA

### Justificación del programa

Las ciber amenazas tienen un potencial peligroso de revertir todo el progreso y los avances socio-económicos, militares y culturales que se han producido en las últimas décadas, gracias precisamente al desarrollo tecnológico del mismo ciberespacio. Los acontecimientos y estudios más recientes señalan el factor humano como el impulsor del asombroso crecimiento que se detecta en el negocio del cibercrimen. Estos mismos estudios apuntan a la necesidad de crear programas de formación en Ciberseguridad para Protección de datos personales, para ésta y futuras generaciones, en los ámbitos empresarial, gubernamental, militar y doméstico. Este es el objetivo de este workshop. En este curso se darán las bases para entender las claves del negocio del cibercrimen, reconocer fraude, adquirir conductas seguras en el ciberespacio y proteger los activos con los que trabajamos.

### Objetivo General

El Certificado en Ciberseguridad para Protección de datos personales tiene como objetivo formar a personal no técnico (Directores, Asesores, y personas no vinculadas directamente con el sector IT que requieren, debido a su responsabilidad, tener mayor conocimiento en ciberseguridad), mediante el conocimiento y aprendizaje de las amenazas que recaen sobre los sistemas de información. A partir de este programa el profesional no técnico será capaz de:

- Conocer las amenazas que se ciernen sobre los activos de información que maneja.
- Reconocer y detectar posibles puntos de entrada de los ciberataques.
- Reconocer el ciberfraude.
- Mitigar el impacto de un posible ciberataque.
- Proteger la integridad de los activos bajo su responsabilidad.
- Detectar y alertar sobre intrusiones a sus sistemas.

### Perfil del aspirante

- Titulados que deseen mejorar sus posibilidades laborales para alcanzar puestos de perfil más técnico y mejor remunerado
- Directores o técnicos de asesoramiento de dirección que lideren o asesoren equipos encargados de la ciber seguridad de una empresa.
- Directivos y Altos Directivos, que desempeñan cargos de responsabilidad en la dirección estratégica de las empresas y que deseen actualizar y perfeccionar su formación y eficacia en el ámbito de la ciber seguridad.
- Asesores y Consultores para el ámbito estratégico de la actividad empresarial en el contexto de la ciber inteligencia y la ciber seguridad.

Cualquier persona que desde el punto de vista no técnico requiera:

- Conocer las amenazas que se ciernen sobre los sistemas de información.
  - Conocer el impacto y los riesgos que suponen estas amenazas
  - Conocer los mecanismos de defensa ante esos riesgos y amenazas
-

- Conocer y adquirir los hábitos y buenas prácticas para la protección de activos de información digital.

### **Perfil profesional del egresado**

Una vez cursado el curso y obtenida la certificación el alumno tendrá los conocimientos y competencias necesarios para la protección de activos digitales mediante el manejo y gestión de amenazas.

### **ESTRUCTURA DEL CURSO**

#### **Duración**

La Certificación Internacional en Ciberseguridad y protección de datos personales tiene una duración de 40 horas académicas contenidas en un solo curso

#### **Título que otorga**

Certificado Internacional en Ciberseguridad para Protección de datos personales

#### **Registro Oficial**

No requiere registro oficial ya que se trata de estudios de 4to nivel o educación no formal.

#### **Entrega de Diploma**

Una vez finalizado el curso y el certificado en aproximadamente tres meses se estaría recibiendo el Diploma de cada curso y del certificado completo.

#### **Área de conocimiento**

Ingeniería Informática

#### **Nivel y Modalidad (Sincrónica / Asincrónica)**

Online: 100% virtual.

Offline: Descarga los contenidos de los cursos en tu computador para que puedas estudiar sin conexión a internet.

#### **Educación a distancia**

- Los alumnos trabajan de forma independiente y a su vez en continuo intercambio con los Profesores Tutores a través del formato de educación a distancia de Red Ilumno.
  - Estimulación del aprendizaje activo permitiéndole a los estudiantes lograr aprendizajes significativos, contribuyendo a ser partícipes en todo el proceso de enseñanza y de aprendizaje.
  - Contenidos especializados en línea Comunidades de aprendizaje Interacción y comunicación constante entre los estudiantes, los Profesores de primer nivel junto al Director del Programa, brindando una oportunidad significativa de intercambio con los profesionales más destacados.
-

- Tecnología interactiva 2.0 en constante desarrollo e investigación

### **Idiomas del curso**

Contenidos disponibles en español y portugués.

### **Plataforma y Materiales**

Plataforma Ilumno: Una de las plataformas más modernas del mercado, los materiales estarán disponibles de forma digital en la plataforma.

### **Plan de Estudios**

**El plan de estudios consta de los siguientes 11 temas:**

TEMA 1: Conceptos Básicos en Seguridad

TEMA 2: Amenazas en la Red.

- Tipos de Amenazas
- Amenazas más comunes

TEMA 3: Fraude

- Ingeniería Social
- Top 5
- Ejemplos
- Concienciación

TEMA 4: Malware

- Virus/ troyanos/gusanos, etc.
- Spyware/Ransomware/PUPs/Key Loggers, etc.
- Contramedidas

TEMA 5: Phishing

- Descripción
- Ejemplos
- Concienciación

TEMA 6: Hacktivismo.

- Descripción
- Ejemplos
- HOY
- DDoS

TEMA 7: Mercados negros.

- Compra-venta de información
-

- Fases
- Ejemplos
- Organización
- Servicios

#### TEMA 8: Ataques a credenciales

- Demostración práctica del robo de credenciales de usuario
- Almacenamiento de credenciales
- Passwords en Windows
- Credenciales en caché
- Contramedidas

#### TEMA 9: DoS/DDoS

- Características
- Motivación
- Víctimas
- Ejemplos
- Contramedidas

#### TEMA 10: Seguridad física de los equipos

#### TEMA 11: Tendencias observadas en el SOC

- Tendencias en Ciberamenazas
- Tendencias en malware para móviles

#### Plan de Evaluación

- 4 Foros evaluables (el profesor asigna una calificación de acuerdo a la participación del alumno).
- 1 Evaluación Autoevaluable (La plataforma califica automáticamente).

#### Docentes Desarrolladores y tutores

Los tutores son propios de Deloitte, por lo cual están localizados en España, es importante considerarlo por temas de las diferencias horarias para la logística de foros, respuestas e interacción con los tutores. Se recomienda desde el inicio del Programa verificar los horarios de cada actividad.

Los profesionales que han desarrollado los materiales docentes y que serán los tutores encargados de este programa son miembros del equipo de formadores de Deloitte que lo componen consultores del área de Deloitte Cyber Risk Services, analistas de seguridad, expertos en ciberinteligencia y ciberfraude, hackers profesionales, desarrolladores y analistas de código fuente, todos ellos en primera línea de defensa de los sistemas de información y comunicaciones de clientes y Firma.

El equipo de Deloitte está altamente cualificado, con formación y certificaciones de relevancia en el sector de la Seguridad con el siguiente personal acreditado:

- 12 CISSP, Certified Information Systems Security Professionals.
- 93 CISAs, Certified Information Systems Auditor. Único título internacionalmente reconocido en el mundo de la auditoría informática, otorgado, por la Information Systems Audit and Control Association (ISACA).
- 46 CISM, Certified Information Security Manager.
- 17 SAP.
- 85 BS7799 / 27001
- 9 BS25999
- 4 CIA (Certified Internal Auditor)
- 64 ITIL (IT Infrastructure Library)
- 5 CEH (Certified Ethical Hacker)
- 8 CGEIT (Certified in the Governance of Enterprise IT)
- 13 CRISC (Certified in Risk and Information Systems Control)
- 1 CSSLP (Certified Secure Software Lifecycle Professional)
- 2 CDP (Certified Data Privacy Professional)

Las capacidades, conocimientos y experiencia de los profesionales de Deloitte CyberSOC en la gestión de incidentes de seguridad, se encuentran avalados por la adjudicación, hace ya un año, del sello por la Universidad de Carnegie Mellon: CyberSOC-CERT Computer Emergency Response

### **Sistema de evaluación**

- Para finalizar satisfactoriamente este curso, los alumnos deben tener una calificación de 70.00 o más en el curso. Para finalizar de manera exitosa, el alumno deberá leer el material de lectura, interactuar en los debates en línea y realizar las tareas asignadas.
- Toda la participación se supervisará por medios electrónicos.  
En relación con los trabajos atrasados, se podrán aplicar penalizaciones hasta de 5 puntos por cada día de demora a partir de la fecha y el horario de presentación, salvo que se haya acordado previamente lo contrario con el cuerpo docente.

### **ADMISIONES**

#### **Requisitos mínimos de inscripción**

Llenado y entrega de formulario de inscripción de acuerdo a cada universidad. Fotocopia legible de un documento de identificación. Entrega del proceso administrativo realizado o la realización del primer pago

#### **Calendario de Admisiones**

Dos o tres veces al año se realizan admisiones. Se debe solicitar el calendario actualizado por Universidad para verificar las aperturas.

---

### **Valor de la inversión, descuentos y formas de pago**

Esta información depende de la Universidad o país donde se encuentre el interesado, es importante tener en cuenta que cada Universidad cuenta con descuentos y diferentes formas de pago y financiamiento que facilitaran el ingreso al certificado.

### **Cambios de fecha- apertura**

Existe un volumen mínimo de estudiantes para confirmar la fecha de apertura original del programa, es por ello que de no alcanzar ese mínimo el programa puede sufrir cambio de fecha, dicha información se comunicará por medio de los datos suministrados en el momento de la inscripción.



◀ SÉ ▶

---

INTERNACIONAL

---

**ILUMNO** Transforming how  
the world learns