

# Curso Universitario

## Gestión de Incidencias de Seguridad Informáticas



## Curso Universitario Gestión de Incidencias de Seguridad Informáticas

- » Modalidad: **online**
- » Duración: **6 semanas**
- » Titulación: **TECH Universidad Tecnológica**
- » Acreditación: **6 ECTS**
- » Horario: **a tu ritmo**
- » Exámenes: **online**

Acceso web: [www.techtitute.com/informatica/curso-universitario/gestion-incidencias-seguridad-informaticas](http://www.techtitute.com/informatica/curso-universitario/gestion-incidencias-seguridad-informaticas)

# Índice

01

Presentación

---

*pág. 4*

02

Objetivos

---

*pág. 8*

03

Dirección del curso

---

*pág. 12*

04

Estructura y contenido

---

*pág. 16*

05

Metodología de estudio

---

*pág. 20*

06

Titulación

---

*pág. 30*

# 01

# Presentación

Una correcta gestión de incidencias en la seguridad informática permite conocer a las empresas y organismos afectados cómo se ha producido el ataque, quién, responder ante ella y prevenir para que no vuelve a suceder. Una labor que desempeña el profesional de la informática a través del análisis forense informático. En esta enseñanza el alumnado, guiado por profesionales expertos en materia de seguridad cibernética, profundizará en un área que requiere constantemente de personal con conocimiento actualizado. La modalidad 100% de este programa permite además acceder a todo el temario a cualquier hora del día y con tan solo un dispositivo con conexión a internet.





“

*Perfecciona tus conocimientos materia de Ciberseguridad y prospera en tu carrera profesional. Matricúlate ahora”*

La política de implementación práctica de todos los dispositivos tecnológicos permite detectar y responder ante las incidencias de seguridad informática. Esta es una de las principales armas que posee las empresas para evitar sufrir ataques cibernéticos, la otra es contar en sus equipos con profesionales informáticos capaces de realizar un trabajo excelente que les garantice una gestión que dé seguridad a todos sus sistemas.

Esta enseñanza aporta al estudiante toda la información necesaria para responder ante incidentes y detectar su nivel de importancia. La gestión es amplia abarca operaciones que permiten la detección de los mismos a través de sistemas IDS/IPS y su posterior tratamiento en SIEM, notificarlo y escalado al departamento correspondiente. Un análisis exhaustivo que será posible gracias conocimiento aportado en esta titulación por un equipo de profesionales expertos en esta rama de la informática.

La modalidad 100% de esta enseñanza, que ofrece TECH, facilita al alumnado el aprendizaje al poder compatibilizar sus responsabilidades personales con una enseñanza que le permitirá avanzar en su carrera profesional. Así, el alumnado únicamente necesita de un dispositivo con conexión a internet para poder acceder a todo el temario, que además podrá descargarse desde el primer día.

Este **Curso Universitario en Gestión de Incidencias de Seguridad Informáticas** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- ♦ El desarrollo de casos prácticos presentados por expertos en políticas de seguridad informática
- ♦ Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información técnica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- ♦ Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- ♦ Su especial hincapié en metodologías innovadoras
- ♦ Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- ♦ La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet



*Conviértete en un profesional de la seguridad informática. Gestiona cualquier incidente con resultados óptimos. Matricúlate”*

“

*Aprende cómo trabajan los organismos CERT en la detección de incidencias y supérate. Inscríbete ya”*

El programa incluye, en su cuadro docente, a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el profesional deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.

*Domina con este Curso Universitario la normas ISO y las normativas de seguridad aplicadas a los diferentes sectores. Haz clic y matricúlate.*

*Este Curso Universitario 100% online te concede total libertad para acceder a él sin horarios fijos y con un dispositivo con acceso a internet.*

# 02 Objetivos

A la finalización de este Curso Universitario, el profesional de la informática habrá adquirido un exhaustivo conocimiento en la gestión de incidencias de seguridad informática. El alumnado será capaz de analizar las distintas fases implicadas en la detección y resolución de incidencias, realizar un correcto análisis forense informático, así como aplicar la normativa legal y normas ISO vigentes. El equipo docente especializado en esta área será el encargado de acompañar al alumnado para que alcance todas sus metas y progrese en su carrera profesional.



“

*Perfecciona tus conocimientos en un campo que requiere de profesionales que sepan gestionar eficazmente cualquier ataque informático”*



## Objetivos generales

- Desarrollar conocimiento especializado sobre cómo gestionar incidencias causadas por eventos de seguridad informática
- Determinar el funcionamiento de un equipo de tratamiento de incidencias en materia de seguridad
- Analizar las distintas fases de una gestión de eventos de seguridad informática
- Instalar y conocer las distintas herramientas utilizadas en el tratamiento y prevención de incidencias
- Examinar los protocolos estandarizados para el tratamiento de incidencias de seguridad



*Domina todas las fases necesarias para el tratamiento de incidencias provocadas por fallos de seguridad. Matricúlate ahora*





## Objetivos específicos

---

- ♦ Analizar la importancia de un tratamiento correcto en materia de incidencias de seguridad
- ♦ Determinar las fases necesarias para el tratamiento de las incidencias provocadas por fallos de seguridad informática
- ♦ Implementar las distintas herramientas de prevención de incidencias
- ♦ Determinar qué es un equipo de tratamiento preventivo y reactivo de incidencias de seguridad
- ♦ Valorar la necesidad de un Análisis Forense informático para el estudio en profundidad de las incidencias registradas
- ♦ Implementar CCN-STIC 817 e Implementar ISO 27035

# 03

## Dirección del curso

Este Curso Universitario cuenta con un equipo docente experto en el ámbito de la seguridad informática en entidades públicas y privadas, lo que proporciona al alumnado una enseñanza muy próxima a la realidad del sector de la informática. Asimismo, la alta cualificación de la profesional que imparte esta titulación supone un respaldo de calidad en el aprendizaje que adquiera el estudiante durante las seis semanas de duración de esta titulación. La cercanía del docente permitirá al profesional avanzar y conseguir sus objetivos.



“

*Un cuerpo docente con experiencia en el sector público y privado guiarán al alumnado en este Curso Universitario”*

## Dirección



### Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones de Madrid
- Instructora certificada E-Council
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formadora acreditada experta por la CAM de los siguientes certificados de profesionalidad: Seguridad Informática (IFCT0190), Gestión de Redes de Voz y datos (IFCM0310), Administración de Redes departamentales (IFCT0410), Gestión de Alarmas en redes de telecomunicaciones (IFCM0410), Operador de Redes de voz y datos (IFCM0110), y Administración de servicios de internet (IFCT0509)
- Colaboradora externa CSO/SSA (*Chief Security Officer/Senior Security Architect*) en la Universidad de las Islas Baleares
- Ingeniera en Informática por la Universidad de Alcalá de Henares de Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Technologies. E-Council



## Profesores

### D. Solana Villarias, Fabián

- ◆ Consultor de Tecnologías de la Información
- ◆ Creador y Administrador de servicios de encuestas en Investigación, Planificación y Desarrollo SA
- ◆ Especialista en Mantenimiento de Mercados Financieros y Sistemas Informáticos en Iberia Financial Software
- ◆ Desarrollador Web y Especialista en Accesibilidad en Indra
- ◆ Licenciado en Ingeniería Superior de Sistemas por la Universidad de Gales/CESINE
- ◆ Diplomado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Gales/ CESINE

“

*Una experiencia de capacitación  
única, clave y decisiva para impulsar  
tu desarrollo profesional”*

# 04

## Estructura y contenido

El plan de estudio de este Curso Universitario desgana cada uno de los puntos críticos para la aplicación de políticas de seguridad de la información en las empresas. Así el temario, confeccionado por profesionales del sector, versará sobre la gestión de incidencias, los sistemas de detección y prevención de intrusos, las herramientas empleadas y la normativa a aplicar en el sector público y privado. Los video resúmenes y lecturas adicionales facilitarán al alumnado la cimentación de conocimientos en una enseñanza que le proporciona una especialización en un área con amplias salidas laborales.

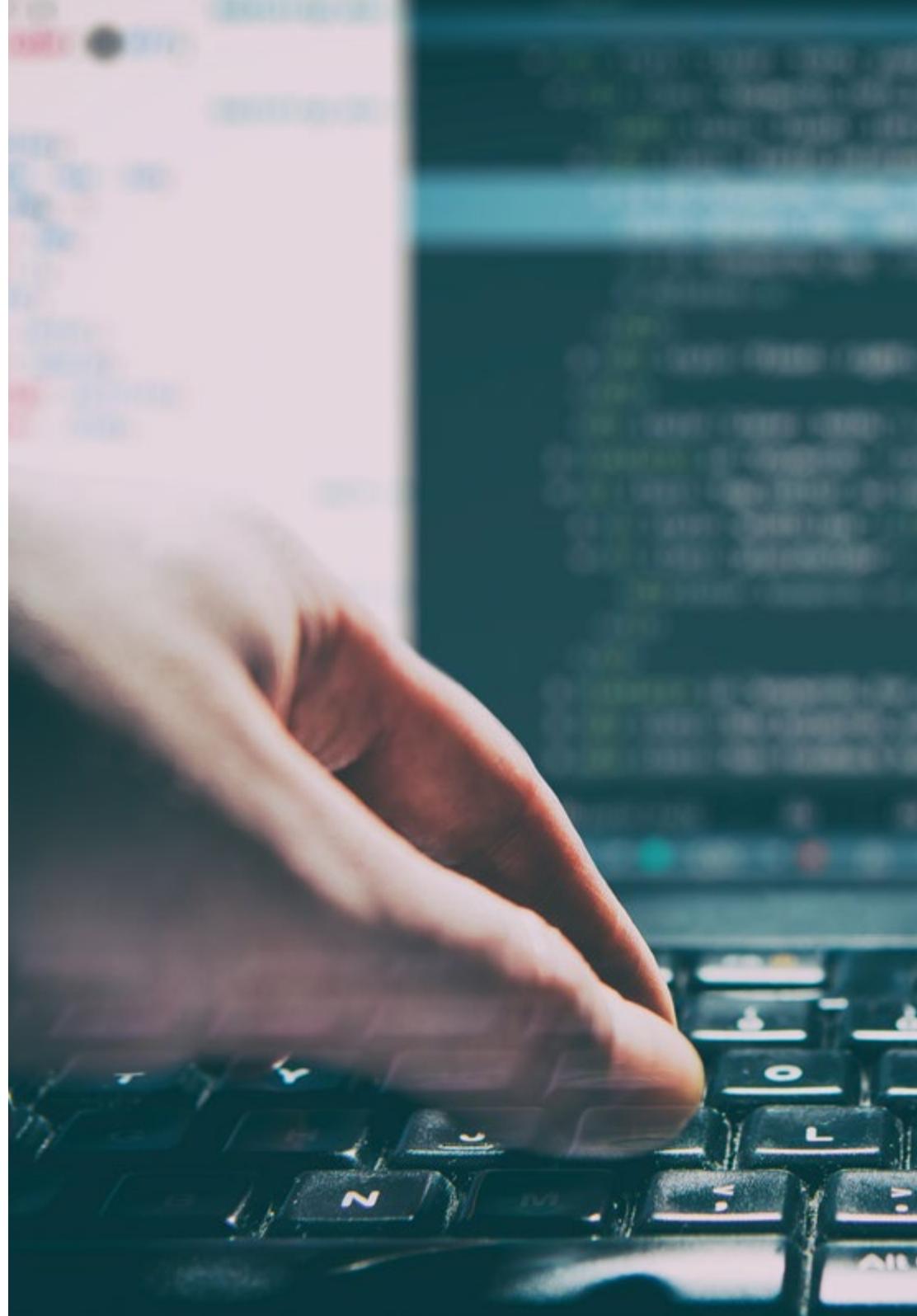


“

*Un temario con contenido actualizado y disponible al completo desde el inicio de este Curso Universitario. Aprende a tu ritmo”*

## Módulo 1. Políticas de gestión de incidencias de seguridad

- 1.1. Políticas de gestión de incidencias de seguridad de la información y mejoras
  - 1.1.1. Gestión de incidencias
  - 1.1.2. Responsabilidades y procedimientos
  - 1.1.3. Notificación de eventos
- 1.2. Sistemas de detección y prevención de intrusiones (IDS/IPS)
  - 1.2.1. Datos de funcionamiento del sistema
  - 1.2.2. Tipos de sistemas de detección de intrusos
  - 1.2.3. Criterios para la ubicación de los IDS/IPS
- 1.3. Respuesta ante incidentes de seguridad
  - 1.3.1. Procedimiento de recolección de información
  - 1.3.2. Proceso de verificación de intrusión
  - 1.3.3. Organismos CERT
- 1.4. Proceso de notificación y gestión de intentos de intrusión
  - 1.4.1. Responsabilidades en el proceso de notificación
  - 1.4.2. Clasificación de los incidentes
  - 1.4.3. Proceso de resolución y recuperación
- 1.5. Análisis forense como política de seguridad
  - 1.5.1. Evidencias volátiles y no volátiles
  - 1.5.2. Análisis y recogida de evidencias electrónicas
    - 1.5.2.1. Análisis de evidencias electrónicas
    - 1.5.2.2. Recogida de evidencias electrónicas
- 1.6. Herramientas de Sistemas de detección y prevención de intrusiones (IDS/IPS)
  - 1.6.1. Snort
  - 1.6.2. Suricata
  - 1.6.3. Solar-Winds
- 1.7. Herramientas centralizadoras de eventos
  - 1.7.1. SIM
  - 1.7.2. SEM
  - 1.7.3. SIEM



- 1.8. Guía de seguridad CCN-STIC 817
  - 1.8.1. Gestión de ciberincidentes
  - 1.8.2. Métricas e Indicadores
- 1.9. NIST SP800-61
  - 1.9.1. Capacidad de respuesta antes incidentes de seguridad informática
  - 1.9.2. Manejo de un incidente
  - 1.9.3. Coordinación e información compartida
- 1.10. Norma ISO 27035
  - 1.10.1. Norma ISO 27035. Principios de la gestión de incidentes
  - 1.10.2. Guías para la elaboración de un plan para la gestión de incidentes
  - 1.10.3. Guías de operaciones en la respuesta a incidentes

“*Un plan de estudios pensado para ti. Sin horarios fijos, ni presencialidad. Distribuye la carga lectiva acorde a tus necesidades. Inscríbete ya”*

# 05

## Metodología de estudio

TECH es la primera universidad en el mundo que combina la metodología de los **case studies** con el **Relearning**, un sistema de aprendizaje 100% online basado en la reiteración dirigida.

Esta disruptiva estrategia pedagógica ha sido concebida para ofrecer a los profesionales la oportunidad de actualizar conocimientos y desarrollar competencias de un modo intensivo y riguroso. Un modelo de aprendizaje que coloca al estudiante en el centro del proceso académico y le otorga todo el protagonismo, adaptándose a sus necesidades y dejando de lado las metodologías más convencionales.

*Excelencia.  
Flexibilidad.  
Vanguardia.*



“

*TECH te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera”*

## El alumno: la prioridad de todos los programas de TECH

En la metodología de estudios de TECH el alumno es el protagonista absoluto. Las herramientas pedagógicas de cada programa han sido seleccionadas teniendo en cuenta las demandas de tiempo, disponibilidad y rigor académico que, a día de hoy, no solo exigen los estudiantes sino los puestos más competitivos del mercado.

Con el modelo educativo asincrónico de TECH, es el alumno quien elige el tiempo que destina al estudio, cómo decide establecer sus rutinas y todo ello desde la comodidad del dispositivo electrónico de su preferencia. El alumno no tendrá que asistir a clases en vivo, a las que muchas veces no podrá acudir. Las actividades de aprendizaje las realizará cuando le venga bien. Siempre podrá decidir cuándo y desde dónde estudiar.

“

*En TECH NO tendrás clases en directo  
(a las que luego nunca puedes asistir)”*



### Los planes de estudios más exhaustivos a nivel internacional

TECH se caracteriza por ofrecer los itinerarios académicos más completos del entorno universitario. Esta exhaustividad se logra a través de la creación de temarios que no solo abarcan los conocimientos esenciales, sino también las innovaciones más recientes en cada área.

Al estar en constante actualización, estos programas permiten que los estudiantes se mantengan al día con los cambios del mercado y adquieran las habilidades más valoradas por los empleadores. De esta manera, quienes finalizan sus estudios en TECH reciben una preparación integral que les proporciona una ventaja competitiva notable para avanzar en sus carreras.

Y además, podrán hacerlo desde cualquier dispositivo, pc, tableta o smartphone.

“

*El modelo de TECH es asincrónico, de modo que te permite estudiar con tu pc, tableta o tu smartphone donde quieras, cuando quieras y durante el tiempo que quieras”*

## Case studies o Método del caso

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, su función era también presentarles situaciones complejas reales. Así, podían tomar decisiones y emitir juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Con este modelo de enseñanza es el propio alumno quien va construyendo su competencia profesional a través de estrategias como el *Learning by doing* o el *Design Thinking*, utilizadas por otras instituciones de renombre como Yale o Stanford.

Este método, orientado a la acción, será aplicado a lo largo de todo el itinerario académico que el alumno emprenda junto a TECH. De ese modo se enfrentará a múltiples situaciones reales y deberá integrar conocimientos, investigar, argumentar y defender sus ideas y decisiones. Todo ello con la premisa de responder al cuestionamiento de cómo actuaría al posicionarse frente a eventos específicos de complejidad en su labor cotidiana.



## Método Relearning

En TECH los *case studies* son potenciados con el mejor método de enseñanza 100% online: el *Relearning*.

Este método rompe con las técnicas tradicionales de enseñanza para poner al alumno en el centro de la ecuación, proveyéndole del mejor contenido en diferentes formatos. De esta forma, consigue repasar y reiterar los conceptos clave de cada materia y aprender a aplicarlos en un entorno real.

En esta misma línea, y de acuerdo a múltiples investigaciones científicas, la reiteración es la mejor manera de aprender. Por eso, TECH ofrece entre 8 y 16 repeticiones de cada concepto clave dentro de una misma lección, presentada de una manera diferente, con el objetivo de asegurar que el conocimiento sea completamente afianzado durante el proceso de estudio.

*El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu especialización, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.*



## Un Campus Virtual 100% online con los mejores recursos didácticos

Para aplicar su metodología de forma eficaz, TECH se centra en proveer a los egresados de materiales didácticos en diferentes formatos: textos, vídeos interactivos, ilustraciones y mapas de conocimiento, entre otros. Todos ellos, diseñados por profesores cualificados que centran el trabajo en combinar casos reales con la resolución de situaciones complejas mediante simulación, el estudio de contextos aplicados a cada carrera profesional y el aprendizaje basado en la reiteración, a través de audios, presentaciones, animaciones, imágenes, etc.

Y es que las últimas evidencias científicas en el ámbito de las Neurociencias apuntan a la importancia de tener en cuenta el lugar y el contexto donde se accede a los contenidos antes de iniciar un nuevo aprendizaje. Poder ajustar esas variables de una manera personalizada favorece que las personas puedan recordar y almacenar en el hipocampo los conocimientos para retenerlos a largo plazo. Se trata de un modelo denominado *Neurocognitive context-dependent e-learning* que es aplicado de manera consciente en esta titulación universitaria.

Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica, chat y videoconferencia).

Asimismo, este completísimo Campus Virtual permitirá que el alumnado de TECH organice sus horarios de estudio de acuerdo con su disponibilidad personal o sus obligaciones laborales. De esa manera tendrá un control global de los contenidos académicos y sus herramientas didácticas, puestas en función de su acelerada actualización profesional.



*La modalidad de estudios online de este programa te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios”*

### La eficacia del método se justifica con cuatro logros fundamentales:

1. Los alumnos que siguen este método no solo consiguen la asimilación de conceptos, sino un desarrollo de su capacidad mental, mediante ejercicios de evaluación de situaciones reales y aplicación de conocimientos.
2. El aprendizaje se concreta de una manera sólida en capacidades prácticas que permiten al alumno una mejor integración en el mundo real.
3. Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.
4. La sensación de eficiencia del esfuerzo invertido se convierte en un estímulo muy importante para el alumnado, que se traduce en un interés mayor en los aprendizajes y un incremento del tiempo dedicado a trabajar en el curso.

## La metodología universitaria mejor valorada por sus alumnos

Los resultados de este innovador modelo académico son constatables en los niveles de satisfacción global de los egresados de TECH.

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos en la plataforma de reseñas Trustpilot, obteniendo un 4,9 de 5.

*Accede a los contenidos de estudio desde cualquier dispositivo con conexión a Internet (ordenador, tablet, smartphone) gracias a que TECH está al día de la vanguardia tecnológica y pedagógica.*

*Podrás aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, esto es, Learning from an expert.*



Así, en este programa estarán disponibles los mejores materiales educativos, preparados a conciencia:



#### Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual que creará nuestra manera de trabajo online, con las técnicas más novedosas que nos permiten ofrecerte una gran calidad, en cada una de las piezas que pondremos a tu servicio.



#### Prácticas de habilidades y competencias

Realizarás actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.



#### Resúmenes interactivos

Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

Este sistema exclusivo educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".



#### Lecturas complementarias

Artículos recientes, documentos de consenso, guías internacionales... En nuestra biblioteca virtual tendrás acceso a todo lo que necesitas para completar tu capacitación.





#### Case Studies

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.



#### Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.



#### Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos. El denominado *Learning from an expert* afianza el conocimiento y el recuerdo, y genera seguridad en nuestras futuras decisiones difíciles.



#### Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.



06

# Titulación

El Curso Universitario en Gestión de Incidencias de Seguridad Informáticas garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Curso Universitario expedido por TECH Universidad Tecnológica.



“

*Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites”*

Este programa te permitirá obtener el título de **Curso Universitario en Gestión de Incidencias de Seguridad Informáticas** emitido por TECH Universidad Tecnológica.

TECH Universidad Tecnológica, es una Universidad española oficial, que forma parte del Espacio Europeo de Educación Superior (EEES). Con un enfoque centrado en la excelencia académica y la calidad universitaria a través de la tecnología.

Este título propio contribuye de forma relevante al desarrollo de la educación continua y actualización del profesional, garantizándole la adquisición de las competencias en su área de conocimiento y aportándole un alto valor curricular universitario a su formación. Es 100% válido en todas las Oposiciones, Carrera Profesional y Bolsas de Trabajo de cualquier Comunidad Autónoma española.

Además, el riguroso sistema de garantía de calidad de TECH asegura que cada título otorgado cumpla con los más altos estándares académicos, brindándole al egresado la confianza y la credibilidad que necesita para destacarse en su carrera profesional.

Título: **Curso Universitario en Gestión de Incidencias de Seguridad Informáticas**

Modalidad: **online**

Duración: **6 semanas**

Acreditación: **6 ECTS**





## Curso Universitario Gestión de Incidencias de Seguridad Informáticas

- » Modalidad: online
- » Duración: 6 semanas
- » Titulación: TECH Universidad Tecnológica
- » Acreditación: 6 ECTS
- » Horario: a tu ritmo
- » Exámenes: online

# Curso Universitario

## Gestión de Incidencias de Seguridad Informáticas