Experto Universitario

Gestión de Amenazas de Seguridad Informática

tech universidad ULAC

tech universidad ULAC

Experto Universitario
Gestión de Amenazas de Seguridad Informática

- Modalidad: **online**
- Duración: **6 meses**
- Titulación: **TECH Universidad ULAC**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: www.techtitute.com/informatica/experto-universitario/experto-gestion-amenazas-seguridad-informatica

Índice

01

Presentación

Una encuesta del Foro Económico Mundial revela que los ataques de *Ransomware* en empresas aumentaron un 150% en 2021, en comparación con el año anterior. Una amenaza que afecta tanto a grandes compañías, instituciones y pequeñas empresas que operan en la red. Este escenario obliga a una correcta implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta enseñanza 100% online aporta a los profesionales informáticos un conocimiento específico en el campo de la seguridad, que engloba, además, todo su desarrollo bajo la correcta aplicación del marco legal existente. Un equipo docente con amplia experiencia en el sector de la ciberseguridad imparte este programa al que podrán acceder en cualquier momento y lugar desde un dispositivo con conexión a internet.

Transforma cualquier empresa en un entorno seguro, libre de amenazas cibernéticas con este Experto Universitario"

La seguridad en internet se ha convertido en uno de los principales problemas para las grandes compañías y gobiernos que invierten grandes sumas de dinero para impedir el robo de datos e información especialmente sensible. Esta problemática es atendida por profesionales informáticos capaces de detectar y anticiparse a los hackers, aunque para ello, precisan de un conocimiento profundo, no sólo de la técnica, sino también de los conceptos más avanzados y aplicables en un SGSI.

Este Experto Universitario en Gestión de Amenazas de Seguridad Informática facilita que el alumnado profundice en los pilares en los que se basa el SGSI, los documentos y modelos a implementar, además de las normativas y estándares aplicables actualmente. Un equipo docente, con experiencia en el área informática y de derecho orientado a la ciberseguridad, dará las pautas esenciales para gestionar la seguridad en una empresa en aplicación de la normativa ISO/IEC 27.000, la cual establece el marco de buenas prácticas para la seguridad de la información.

Una excelente oportunidad para los profesionales informáticos que deseen progresar en su carrera profesional dando la máxima seguridad a las empresas que soliciten sus servicios. El modelo online de TECH permite compaginar la vida laboral y personal, al facilitar el acceso a todo el temario del plan de estudio desde el primer día, sin horarios y con posibilidad de descargar el contenido para su visualización con un dispositivo con conexión a internet.

Este **Experto Universitario en Gestión de Amenazas de Seguridad Informática** contiene el programa más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en 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

Profundiza en los beneficios de las normas ISO/IEC 27.000 y aplícalos para dar Seguridad Informática"

Avanza en el campo de la Seguridad Informática. Cada día millones de empresas se ven afectadas por ciberataques. Matricúlate en este Experto Universitario”

Planifica y diseña un SGSI sin fisuras para los negocios. Sé el profesional informático en seguridad que están buscando.

Las empresas reclaman profesionales informáticos que sean capaces de proteger sus datos más sensibles. Conviértete en un experto en Seguridad Informática.

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 a los profesionales un aprendizaje situado y contextual, es decir, un entorno simulado que les proporcionará una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante los profesionales deberán tratar de resolver las distintas situaciones de práctica profesional que se les plantee a lo largo del programa académico. Para ello, contará con la ayuda de un novedoso sistema de vídeos interactivos realizados por reconocidos expertos.

02

Objetivos

Este Experto Universitario brinda la oportunidad a los estudiantes de profundizar en los conceptos claves de la seguridad de la información, así como lograr una correcta implementación de un SGSI acorde a los estándares básicos y la normativa existente con el fin de poder alcanzar una especialización que les facilite la progresión en su carrera profesional. Los casos prácticos, que pondrán en situación real a los profesionales informáticos y el sistema *Relearning*, basado en la reiteración de contenido, facilitarán el alcance de dichas metas.

Obtén las claves para implementar un SGSI cumpliendo toda la normativa existente. Logra ser un gran profesional de la seguridad informática”

Objetivos generales

- Profundizar en los conceptos clave de la seguridad de la información
- Desarrollar las medidas necesarias para garantizar buenas prácticas en materia de seguridad de la información
- Desarrollar las diferentes metodologías para la realización de un análisis exhaustivo de amenazas
- Instalar y conocer las distintas herramientas utilizadas en el tratamiento y prevención de incidencias

Implementa las contramedidas de seguridad más efectivas gracias a este Experto Universitario. Haz clic y matricúlate ya"

Objetivos específicos

Módulo 1. Sistema de Gestión de Seguridad de Información (SGSI)

- Analizar las normativas y estándares aplicables en la actualidad a los SGSI
- Desarrollar las fases necesarias para implementar un SGSI en una entidad
- Analizar los procedimientos de gestión de incidentes de seguridad de la información e implantación

Módulo 2. Aspectos organizativos en Política de Seguridad de la Información

- Implementar un SGSI en la empresa
- Determinar qué departamentos debe abarcar la implementación del sistema de gestión de seguridad
- Implementar contramedidas de seguridad necesaria en la operativa

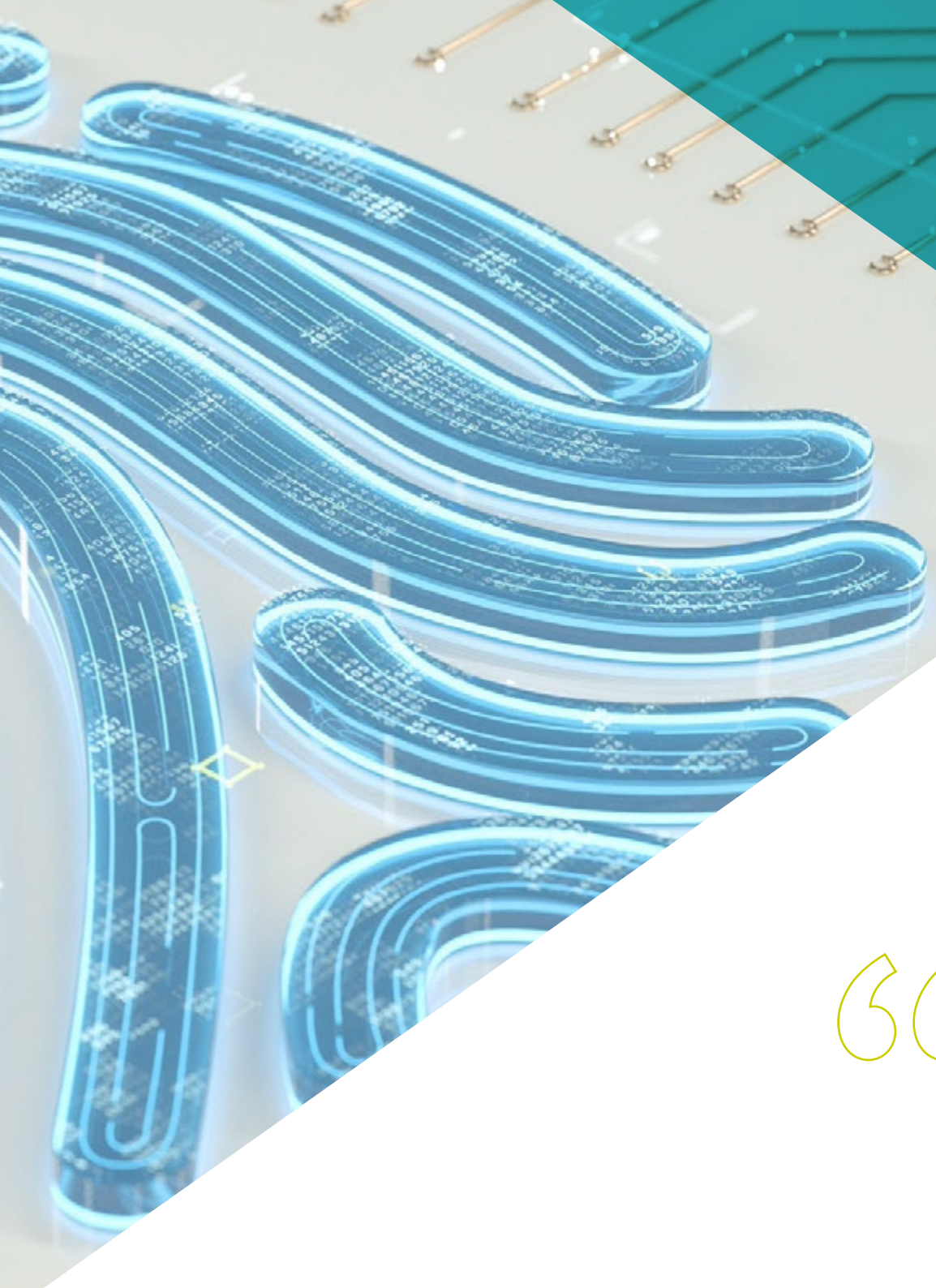
Módulo 3. Políticas de Seguridad para el Análisis de Amenazas en Sistemas Informáticos

- Analizar el significado de amenazas
- Determinar las fases de una gestión preventiva de amenazas
- Comparar las distintas metodologías de gestión de amenazas

03

Dirección del curso

Los profesionales que conforman el cuerpo docente de este Experto Universitario poseen una titulación académica de gran nivel y una amplia experiencia en el sector de la Ciberseguridad. Es precisamente su participación en proyectos de seguridad informática, lo que ayudará al alumnado a conocer la realidad en el sector tecnológico, los principales problemas que se detectan en los protocolos de actuación, así como su corrección para dar garantías y tranquilidad a las empresas. En este recorrido de seis meses de duración, el profesorado acompañará al alumnado en una enseñanza de calidad, que mejorará sus capacidades durante todo el aprendizaje.



Expertos en Ciberseguridad y protección de datos te aportarán su valiosa experiencia en este Experto 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 Techonologies. E-Council

Profesores

D. Oropesiano Carrizosa, Francisco

- Ingeniero informático
- Técnico en Microinformática, Redes y Seguridad en Cas-Training
- Desarrollador de servicios web, CMS, e-Commerce, UI y UX en Fersa Reparaciones
- Gestor de servicios web, contenidos, correo y DNS en Oropesia Web & Network
- Diseñador gráfico y de aplicaciones web en Xarxa Sakai Projectes
- Diplomado en Informática de Sistemas por la Universidad de Alcalá de Henares
- Master en DevOps: Docker and Kubernetes por Cyber Business Center
- Técnico de Redes y Seguridad Informática por la Universidad de las Islas Baleares
- Experto en Diseño Gráfico por la Universidad Politécnica de Madrid

D. Ortega López, Florencio

- Consultor de seguridad (Gestión de Identidades) en SIA Group
- Consultor de TIC y Seguridad como profesional independiente
- Profesor formador en sector TI
- Graduado en Ingeniería Técnica Industrial por la Universidad de Alcalá de Henares
- Máster para el Profesorado por la UNIR
- MBA en Gestión y Dirección de Empresas por IDE-CESEM
- Máster en Dirección y Gestión de Tecnología de la Información por IDE-CESEM
- Certified Information Security Management (CISM) por la ISACA

D. Peralta Alonso, Jon

- Consultor senior - Protección de Datos y Ciberseguridad. Altia
- Abogado / Asesor jurídico. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Asesor jurídico / Pasante. Despacho de profesional: Oscar Padura
- Grado en Derecho. Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos. EIS Innovative School
- Máster Universitario en Abogacía. Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil. Universidad Internacional Isabel I de Castilla
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC

04

Estructura y contenido

El temario de este Experto Universitario ha sido elaborado con un amplio contenido multimedia y lecturas esenciales que aportarán un conocimiento profundo sobre los sistemas de gestión de seguridad de información. En el desarrollo de este programa se darán las principales claves en Ciberseguridad y de forma progresiva se adentrará en los aspectos organizativos de la empresa para mejorar la protección de sus datos, hasta llegar al análisis de las amenazas en sistemas informáticos a los que debe hacer frente los profesionales.

Un plan de estudios que te dará las pautas para poner en marcha políticas de seguridad efectivas en cualquier empresa”

Módulo 1. Sistema de gestión de seguridad de información (SGSI)

1.1. Seguridad de la información. Aspectos clave
- 1.1.1. Seguridad de la información
  - 1.1.1.1. Confidencialidad
  - 1.1.1.2. Integridad
  - 1.1.1.3. Disponibilidad
  - 1.1.1.4. Medidas de seguridad de la Información

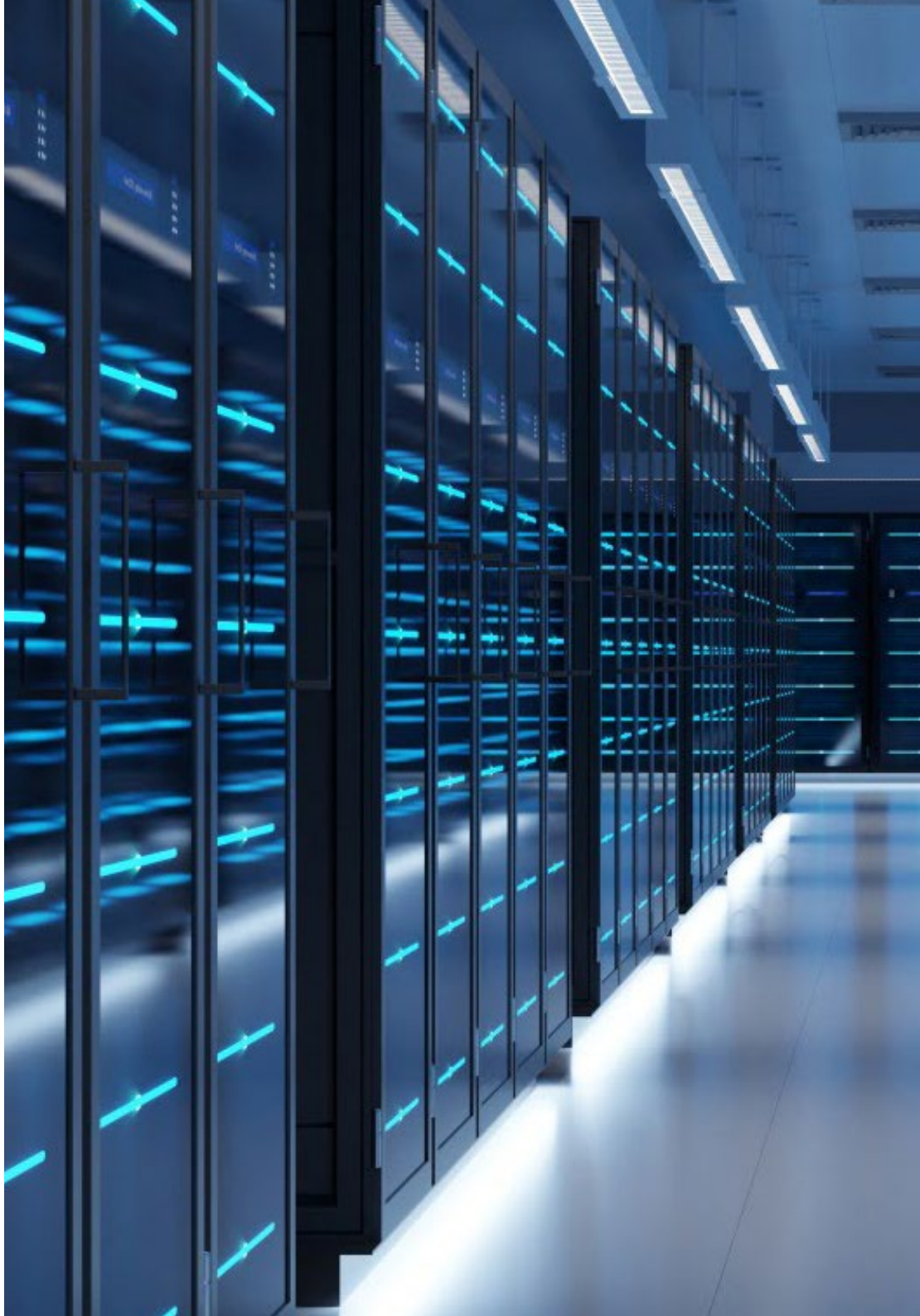
1.2. Sistema de gestión de la seguridad de la información
- 1.2.1. Modelos de gestión de seguridad de la información
- 1.2.2. Documentos para implantar un SGSI
- 1.2.3. Niveles y controles de un SGSI

1.3. Normas y estándares internacionales
- 1.3.1. Estándares internacionales en la seguridad de la información
- 1.3.2. Origen y evolución del estándar
- 1.3.3. Estándares Internacionales Gestión de la Seguridad de la Información
- 1.3.4. Otras normas de referencia

1.4. Normas ISO/IEC 27.000
- 1.4.1. Objeto y ámbito de aplicación
- 1.4.2. Estructura de la norma
- 1.4.3. Certificación
- 1.4.4. Fases de acreditación
- 1.4.5. Beneficios normas ISO/IEC 27.000

1.5. Diseño e implantación de un Sistema General de Seguridad de Información
- 1.5.1. Fases de implantación de un sistema General de Seguridad de la Información
- 1.5.2. Plan de continuidad de negocio

1.6. Fase I: diagnóstico
- 1.6.1. Diagnóstico preliminar
- 1.6.2. Identificación del nivel de estratificación
- 1.6.3. Nivel de cumplimiento de estándares/normas



1.7. Fase II: preparación
- 1.7.1. Contexto de la organización
- 1.7.2. Análisis de normativas de seguridad aplicables
- 1.7.3. Alcance del Sistema General de Seguridad de Información
- 1.7.4. Política del Sistema General de Seguridad de Información
- 1.7.5. Objetivos del Sistema General de Seguridad de Información

1.8. Fase III: planificación
- 1.8.1. Clasificación de activos
- 1.8.2. Valoración de riesgos
- 1.8.3. Identificación de amenazas y riesgos

1.9. Fase IV: implantación y seguimiento
- 1.9.1. Análisis de resultados
- 1.9.2. Asignación de responsabilidades
- 1.9.3. Temporalización del plan de acción
- 1.9.4. Seguimiento y auditorias

1.10. Políticas de seguridad en la gestión de incidentes
- 1.10.1. Fases
- 1.10.2. Categorización de incidentes
- 1.10.3. Procedimientos y gestión de incidentes

Módulo 2. Aspectos organizativos en Política de Seguridad de la Información

2.1. Organización interna
- 2.1.1. Asignación de responsabilidades
- 2.1.2. Segregación de tareas
- 2.1.3. Contactos con autoridades
- 2.1.4. Seguridad de la información en gestión de proyectos

2.2. Gestión de activos
- 2.2.1. Responsabilidad sobre los activos
- 2.2.2. Clasificación de la información
- 2.2.3. Manejo de los soportes de almacenamiento

2.3. Políticas de seguridad en los procesos de negocio
- 2.3.1. Análisis de los procesos de negocio vulnerables
- 2.3.2. Análisis de impacto de negocio
- 2.3.3. Clasificación procesos respecto al impacto de negocio

2.4. Políticas de seguridad ligada a los Recursos Humanos
- 2.4.1. Antes de contratación
- 2.4.2. Durante la contratación
- 2.4.3. Cese o cambio de puesto de trabajo

2.5. Políticas de seguridad en dirección
- 2.5.1. Directrices de la dirección en seguridad de la información
- 2.5.2. BIA- analizando el impacto
- 2.5.3. Plan de recuperación como política de seguridad

2.6. Adquisición y mantenimientos de los sistemas de información
- 2.6.1. Requisitos de seguridad de los sistemas de información
- 2.6.2. Seguridad en los datos de desarrollo y soporte
- 2.6.3. Datos de prueba

2.7. Seguridad con suministradores
- 2.7.1. Seguridad informática con suministradores
- 2.7.2. Gestión de la prestación del servicio con garantía
- 2.7.3. Seguridad en la cadena de suministro

2.8. Seguridad operativa
- 2.8.1. Responsabilidades en la operación
- 2.8.2. Protección contra código malicioso
- 2.8.3. Copias de seguridad
- 2.8.4. Registros de actividad y supervisión

2.9. Gestión de la seguridad y normativas
- 2.9.1. Cumplimiento de los requisitos legales
- 2.9.2. Revisiones en la seguridad de la información

2.10. Seguridad en la gestión para la continuidad de negocio
- 2.10.1. Continuidad de la seguridad de la información
- 2.10.2. Redundancias

Módulo 3. Políticas de Seguridad para el Análisis de Amenazas en Sistemas Informáticos

3.1. La gestión de amenazas en las políticas de seguridad
- 3.1.1. La gestión del riesgo
- 3.1.2. El riesgo en seguridad
- 3.1.3. Metodologías en la gestión de amenazas
- 3.1.4. Puesta en marcha de metodologías

3.2. Fases de la gestión de amenazas
- 3.2.1. Identificación
- 3.2.2. Análisis
- 3.2.3. Localización
- 3.2.4. Medidas de salvaguarda

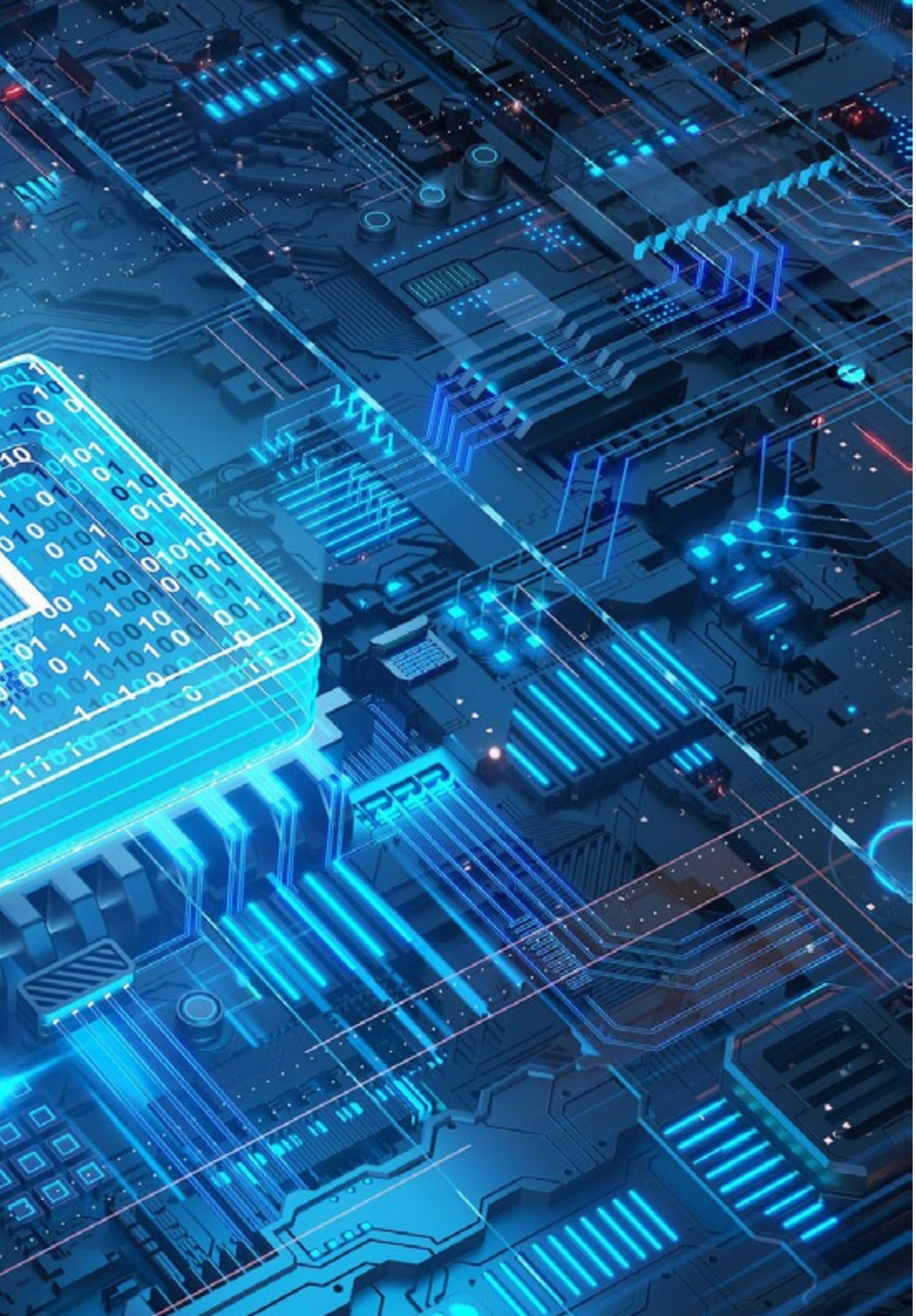
3.3. Sistemas de auditoria para localización de amenazas
- 3.3.1. Clasificación y flujo de información
- 3.3.2. Análisis de los procesos vulnerables

3.4. Clasificación del riesgo
- 3.4.1. Tipos de riesgo
- 3.4.2. Calculo de la probabilidad de amenaza
- 3.4.3. Riesgo residual

3.5. Tratamiento del riesgo
- 3.5.1. Implementación de medidas de salvaguarda
- 3.5.2. Transferir o asumir

3.6. Control de riesgo
- 3.6.1. Proceso continuo de gestión de riesgo
- 3.6.2. Implementación de métricas de seguridad
- 3.6.3. Modelo estratégico de métricas en seguridad de la información

3.7. Metodologías prácticas para el análisis y control de amenazas
- 3.7.1. Catálogo de amenazas
- 3.7.2. Catálogo de medidas de control
- 3.7.3. Catálogo de salvaguardas



3.8. Norma ISO 27005
- 3.8.1. Identificación del riesgo
- 3.8.2. Análisis del riesgo
- 3.8.3. Evaluación del riesgo

3.9. Matriz de riesgo, impacto y amenazas
- 3.9.1. Datos, sistemas y personal
- 3.9.2. Probabilidad de amenaza
- 3.9.3. Magnitud del daño

3.10. Diseño de fases y procesos en el análisis de amenazas
- 3.10.1. Identificación elementos críticos de la organización
- 3.10.2. Determinación de amenazas e impactos
- 3.10.3. Análisis del impacto y riesgo
- 3.10.4. Metodologías

Los casos prácticos de este Experto Universitario te pondrán en situaciones reales de ataques cibernéticos. Los conocimientos adquiridos te ayudarán a afrontarlos"

05

Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.

Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine.***

Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización"

Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo"

Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.

El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.

Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y profesional más vigente.

> *Nuestro programa te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"*

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomasen decisiones y emitiesen juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

Relearning Methodology

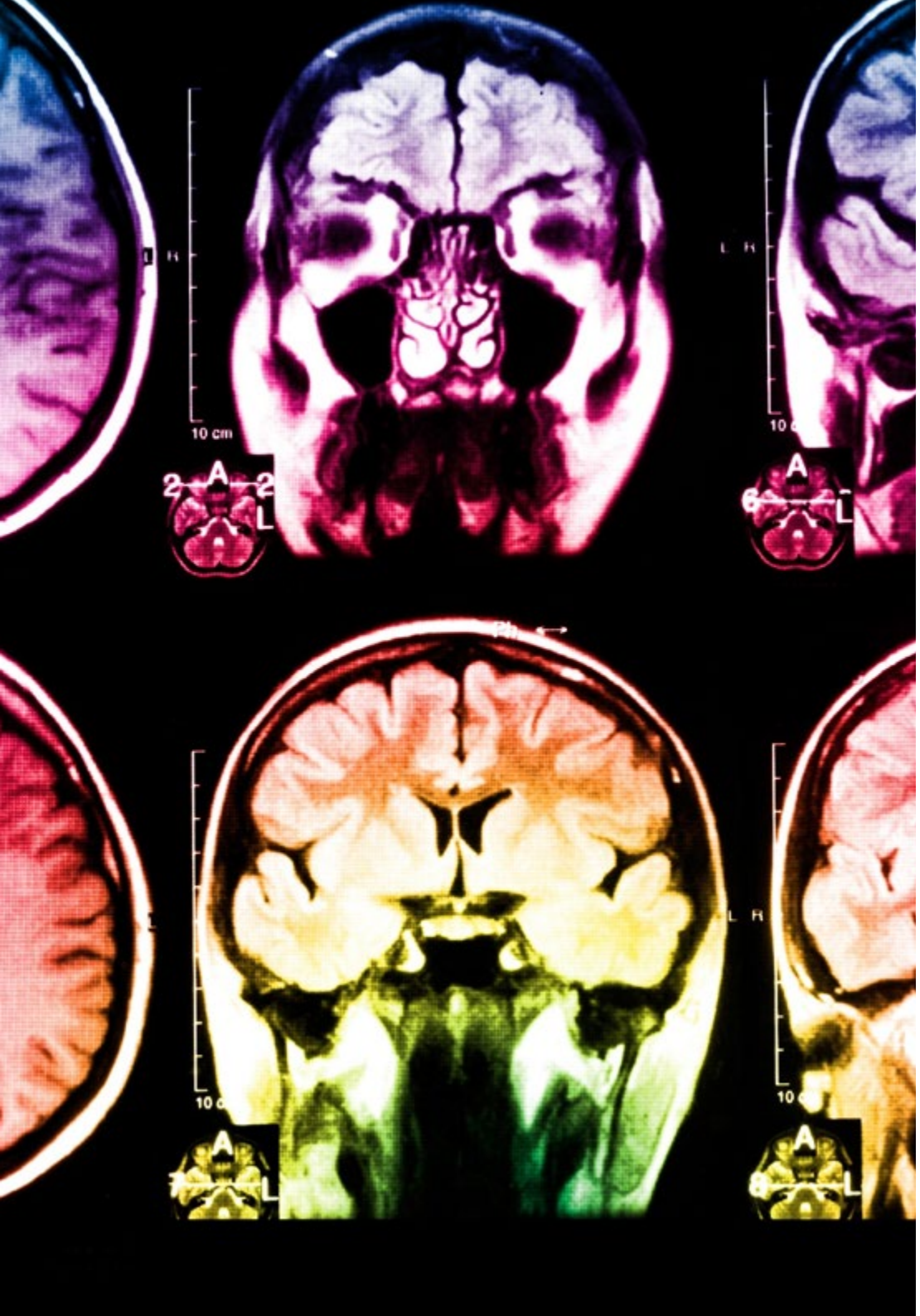
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

En 2019 obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra universidad es la única en habla hispana licenciada para emplear este exitoso método. En 2019, conseguimos mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos…) con respecto a los indicadores de la mejor universidad online en español.



En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, se combinan cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

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

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.

Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:

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, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.

Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

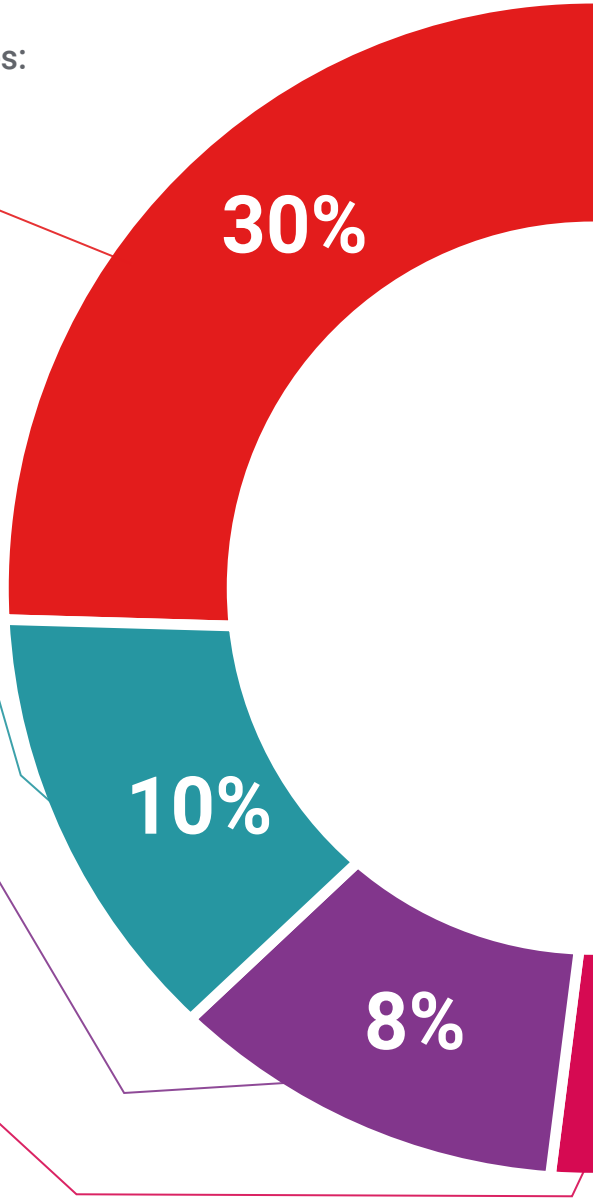
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

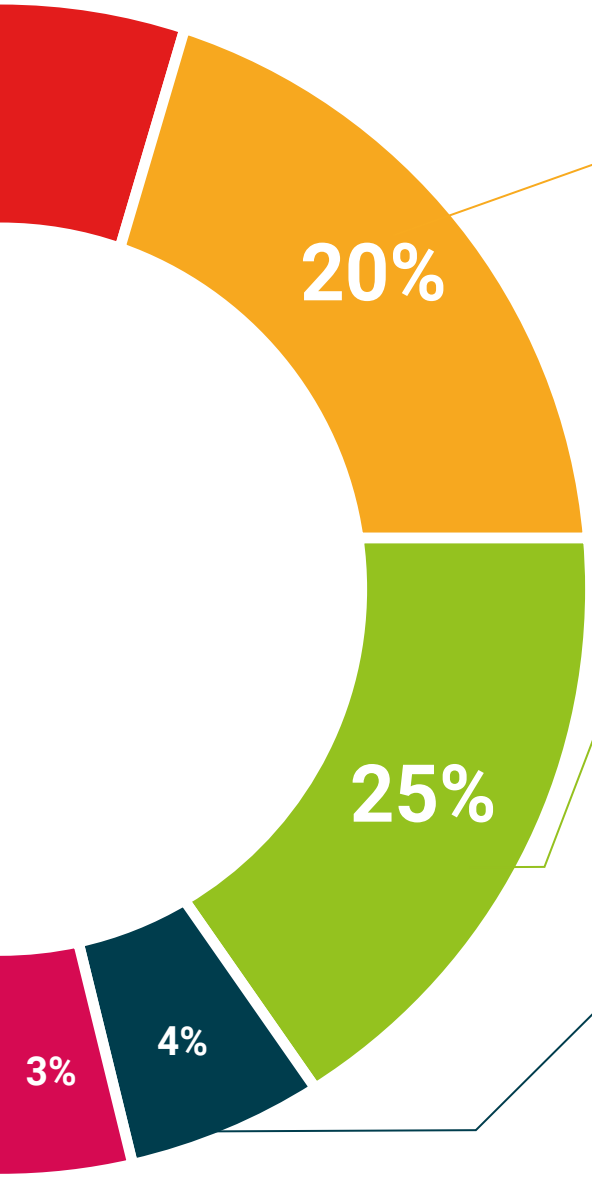
Prácticas de habilidades y competencias

Realizarán 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.

Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





Case studies

Completarán una selección de los mejores casos de estudio elegidos expresamente para esta titulación. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

Testing & Retesting

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.

06

Titulación

El Experto Universitario en Gestión de Amenazas de Seguridad Informática garantiza, además de la capacitación más rigurosa y actualizada, el acceso a dos diplomas de Experto Universitario, uno expedido por TECH Global University y otro expedido por la Universidad Latinoamericana y del Caribe.

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

El programa del **Experto Universitario en Gestión de Amenazas de Seguridad Informática** es el más completo del panorama académico actual. A su egreso, el estudiante recibirá un diploma universitario emitido por TECH Global University, y otro por la Universidad Latinoamericana y del Caribe.

Estos títulos de formación permanente y actualización profesional de TECH Global University y Universidad Latinoamericana y del Caribe garantizan la adquisición de competencias en el área de conocimiento, otorgando un alto valor curricular al estudiante que supere las evaluaciones y acredite el programa tras cursarlo en su totalidad.

Este doble reconocimiento, de dos destacadas instituciones universitarias, suponen una doble recompensa a una formación integral y de calidad, asegurando que el estudiante obtenga una certificación reconocida tanto a nivel nacional como internacional. Este mérito académico le posicionará como un profesional altamente capacitado y preparado para enfrentar los retos y demandas en su área profesional.

Título: **Experto Universitario en Gestión de Amenazas de Seguridad Informática**

Modalidad: **online**

Duración: **6 meses**

Acreditación: **18 ECTS**


UNIVERSIDAD
LATINOAMERICANA Y DEL CARIBE

ULAC

La Vida Integral

CERTIFICA A:

_____

Identificación: _____

Por haber superado con éxito y obtenido el título de:

EXPERTO UNIVERSITARIO EN GESTIÓN DE AMENAZAS DE SEGURIDAD INFORMÁTICA

En la ciudad de Caracas a los 04 días del mes de diciembre de 2023

Dr. Elmo Bell-Smythe
Rector de la ULAC

Rafa Aramayo
CEO de La Vida Integral

Verifique la validez y autenticidad de este Certificado escaneando el código QR


tech global university

D/Dña _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

Experto Universitario en Gestión de Amenazas de Seguridad Informática

Se trata de un título propio de 450 horas de duración equivalente a 18 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH Universidad ULAC realizará las gestiones oportunas para su obtención, con un coste adicional.

tech universidad ULAC

Experto Universitario
Gestión de Amenazas de Seguridad Informática

- Modalidad: **online**
- Duración: **6 meses**
- Titulación: **TECH Universidad ULAC**
- Acreditación: **18 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Experto Universitario
Gestión de Amenazas de Seguridad Informática

tech universidad ULAC