Grand Master

Secure Information Management

tech global university

tech global university

Grand Master
Secure Information Management

- Modalidad: **online**
- Duración: **2 años**
- Titulación: **TECH Global University**
- Acreditación: **120 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: www.techtitute.com/informatica/grand-master/grand-master-secure-information-management

Índice

01

Presentación del programa

En la era digital actual, las actividades de distintos ámbitos se gestionan de manera integral a través de internet. El entretenimiento, el trabajo y la comunicación con amigos y familiares dependen, cada vez más, de herramientas y recursos en línea. Diariamente se transfieren enormes cantidades de información, desde datos simples en conversaciones en redes sociales y aplicaciones de mensajería, hasta información sensible de carácter personal y profesional alojada en plataformas bancarias o empresariales. Este panorama requiere especialistas capaces de manejar y proteger información en diversos contextos, priorizando su seguridad. Es por ello que TECH ha diseñado este programa en Ingeniería de Software, enfocado en formar profesionales con las habilidades necesarias para gestionar y proteger la información de manera eficaz, abordando los retos digitales actuales y contribuyendo a crear entornos tecnológicos más seguros y confiables.

Proteger datos es clave ante amenazas constantes. Tú podrías ser el guardián de esa información valiosa"

Cada segundo, miles de datos son generados, compartidos y almacenados en el entorno digital. Desde realizar pagos en línea y acceder a servicios educativos hasta coordinar actividades empresariales o proteger identidades digitales, la tecnología se ha convertido en un pilar esencial que transforma continuamente la forma en que vivimos y trabajamos. Estas interacciones generan y transfieren cantidades masivas de datos a cada instante, desde información personal hasta archivos sensibles relacionados con empresas e instituciones. Este flujo constante de datos pone de manifiesto la necesidad de un manejo adecuado para garantizar su seguridad y privacidad.

Gestionar y proteger estos datos no es una tarea sencilla, ya que requiere la combinación de conocimientos altamente especializados en áreas como la ciberseguridad y la gestión de información. Estas disciplinas, aunque distintas, deben integrarse para abordar los complejos desafíos del entorno digital actual. En este contexto, el Grand Master en Secure Information Management representa una oportunidad única para ingenieros y profesionales de la informática interesados en adquirir una visión integral que les permita dominar ambas áreas y posicionarse como líderes en un sector en constante crecimiento.

Numerosas empresas e instituciones enfrentan la necesidad de proteger datos críticos y altamente sensibles, pero carecen de expertos que puedan garantizar una administración, conservación y vigilancia efectivas de su información digital. Para responder a esta demanda, TECH ha diseñado un programa que combina los mejores contenidos con un equipo docente de reconocida trayectoria profesional. Este enfoque asegura que los alumnos adquieran las herramientas y conocimientos necesarios para destacar en el mercado laboral y acceder a puestos estratégicos en organizaciones que buscan fortalecer la seguridad de su información.

Este **Grand Master en Secure Information Management** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Secure Information Management
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que están concebidos recogen una información científica 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 en la dirección de Secure Informaction Management
- 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

Adquiere las habilidades necesarias para garantizar la seguridad y gestionar eficazmente los datos en un entorno digital competitivo”

Consolida tus conocimientos teóricos con los numerosos recursos prácticos incluidos en este Grand Master en Secure Information Management"

Descubre la metodología educativa más innovadora diseñada por TECH para garantizar un aprendizaje inmersivo y contextualizado.

Accede a un programa 100% online que te permite estudiar a tu ritmo, en cualquier momento y desde cualquier lugar del mundo.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de las Finanzas, que vierten en este programa 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 un estudio inmersivo programado para entrenarse ante situaciones reales.

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

02

¿Por qué estudiar en TECH?

TECH es la mayor Universidad digital del mundo. Con un impresionante catálogo de más de 14.000 programas universitarios, disponibles en 11 idiomas, se posiciona como líder en empleabilidad, con una tasa de inserción laboral del 99%. Además, cuenta con un enorme claustro de más de 6.000 profesores de máximo prestigio internacional.

Estudia en la mayor universidad digital del mundo y asegura tu éxito profesional. El futuro empieza en TECH”

La mejor universidad online del mundo según FORBES

La prestigiosa revista Forbes, especializada en negocios y finanzas, ha destacado a TECH como «la mejor universidad online del mundo». Así lo han hecho constar recientemente en un artículo de su edición digital en el que se hacen eco del caso de éxito de esta institución, «gracias a la oferta académica que ofrece, la selección de su personal docente, y un método de aprendizaje innovador orientado a formar a los profesionales del futuro».

El mejor claustro docente top internacional

El claustro docente de TECH está integrado por más de 6.000 profesores de máximo prestigio internacional. Catedráticos, investigadores y altos ejecutivos de multinacionales, entre los cuales se destacan Isaiah Covington, entrenador de rendimiento de los Boston Celtics; Magda Romanska, investigadora principal de MetaLAB de Harvard; Ignacio Wistumba, presidente del departamento de patología molecular traslacional del MD Anderson Cancer Center; o D.W Pine, director creativo de la revista TIME, entre otros.

La mayor universidad digital del mundo

TECH es la mayor universidad digital del mundo. Somos la mayor institución educativa, con el mejor y más amplio catálogo educativo digital, cien por cien online y abarcando la gran mayoría de áreas de conocimiento. Ofrecemos el mayor número de titulaciones propias, titulaciones oficiales de posgrado y de grado universitario del mundo. En total, más de 14.000 títulos universitarios, en once idiomas distintos, que nos convierten en la mayor institución educativa del mundo.

Los planes de estudio más completos del panorama universitario

TECH ofrece los planes de estudio más completos del panorama universitario, con temarios que abarcan conceptos fundamentales y, al mismo tiempo, los principales avances científicos en sus áreas científicas específicas. Asimismo, estos programas son actualizados continuamente para garantizar al alumnado la vanguardia académica y las competencias profesionales más demandadas. De esta forma, los títulos de la universidad proporcionan a sus egresados una significativa ventaja para impulsar sus carreras hacia el éxito.

Un método de aprendizaje único

TECH es la primera universidad que emplea el *Relearning* en todas sus titulaciones. Se trata de la mejor metodología de aprendizaje online, acreditada con certificaciones internacionales de calidad docente, dispuestas por agencias educativas de prestigio. Además, este disruptivo modelo académico se complementa con el "Método del Caso", configurando así una estrategia de docencia online única. También en ella se implementan recursos didácticos innovadores entre los que destacan vídeos en detalle, infografías y resúmenes interactivos.

La universidad online oficial de la NBA

TECH es la universidad online oficial de la NBA. Gracias a un acuerdo con la mayor liga de baloncesto, ofrece a sus alumnos programas universitarios exclusivos, así como una gran variedad de recursos educativos centrados en el negocio de la liga y otras áreas de la industria del deporte. Cada programa tiene un currículo de diseño único y cuenta con oradores invitados de excepción: profesionales con una distinguida trayectoria deportiva que ofrecerán su experiencia en los temas más relevantes.

Líderes en empleabilidad

TECH ha conseguido convertirse en la universidad líder en empleabilidad. El 99% de sus alumnos obtienen trabajo en el campo académico que ha estudiado, antes de completar un año luego de finalizar cualquiera de los programas de la universidad. Una cifra similar consigue mejorar su carrera profesional de forma inmediata. Todo ello gracias a una metodología de estudio que basa su eficacia en la adquisición de competencias prácticas, totalmente necesarias para el desarrollo profesional.

Google Partner Premier

El gigante tecnológico norteamericano ha otorgado a TECH la insignia Google Partner Premier. Este galardón, solo al alcance del 3% de las empresas del mundo, pone en valor la experiencia eficaz, flexible y adaptada que esta universidad proporciona al alumno. El reconocimiento no solo acredita el máximo rigor, rendimiento e inversión en las infraestructuras digitales de TECH, sino que también sitúa a esta universidad como una de las compañías tecnológicas más punteras del mundo.

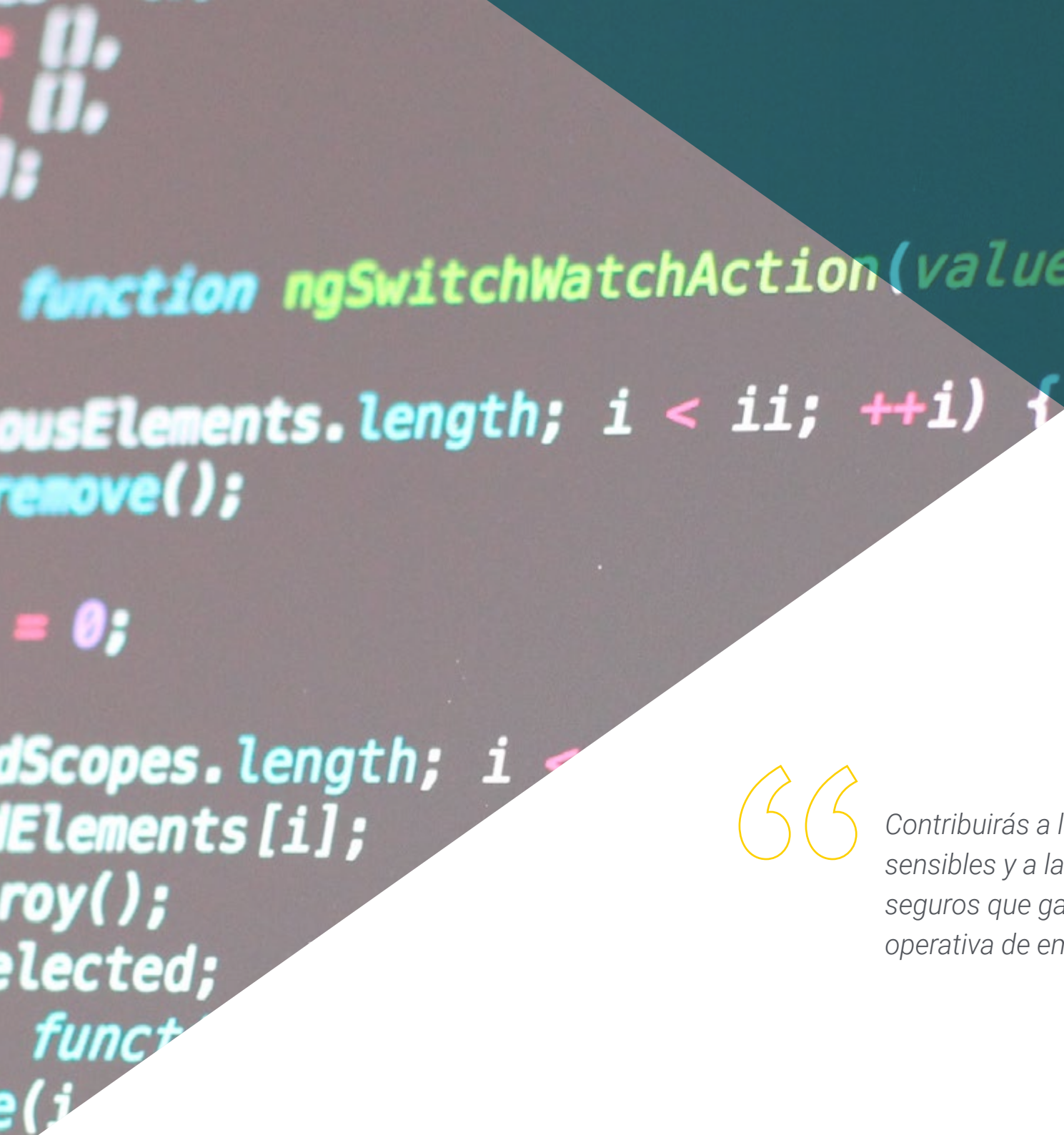
La universidad mejor valorada por sus alumnos

Los alumnos han posicionado a TECH como la universidad mejor valorada del mundo en los principales portales de opinión, destacando su calificación más alta de 4,9 sobre 5, obtenida a partir de más de 1.000 reseñas. Estos resultados consolidan a TECH como la institución universitaria de referencia a nivel internacional, reflejando la excelencia y el impacto positivo de su modelo educativo.

03

Plan de estudios

Los materiales didácticos que conforman este Grand Master en Secure Information Management han sido elaborados por un equipo de expertos en ciberseguridad y gestión de datos. De esta forma, el plan de estudios profundiza en las principales amenazas digitales y las metodologías más avanzadas para la protección y administración de información. Esto permitirá a los egresados identificar riesgos específicos y desarrollar soluciones eficaces para garantizar la seguridad de los datos en diversos entornos profesionales. Asimismo, el temario aborda las herramientas más innovadoras del sector, impulsando estrategias destinadas a proteger los activos digitales de las organizaciones.



Contribuirás a la protección de datos sensibles y a la creación de sistemas seguros que garanticen la continuidad operativa de empresas e instituciones”

Módulo 1. Analítica del dato en la organización empresarial

1.1. Análisis de negocio
- 1.1.1. Análisis de negocio
- 1.1.2. Estructura del dato
- 1.1.3. Fases y elementos

1.2. Analítica del dato en la empresa
- 1.2.1. Cuadros de mando y Kpi's por departamentos
- 1.2.2. Informes operativos, tácticos y estratégicos
- 1.2.3. Analítica del dato aplicada a cada departamento
  - 1.2.3.1. Marketing y comunicación
  - 1.2.3.2. Comercial
  - 1.2.3.3. Atención al cliente
  - 1.2.3.4. Compras
  - 1.2.3.5. Administración
  - 1.2.3.6. RR.HH.
  - 1.2.3.7. Producción
  - 1.2.3.8. IT

1.3. Marketing y comunicación
- 1.3.1. Kpi's a medir, aplicaciones y beneficios
- 1.3.2. Sistemas de marketing y *data warehouse*
- 1.3.3. Implementación de una estructura de analítica del dato en Marketing
- 1.3.4. Plan de marketing y comunicación
- 1.3.5. Estrategias, predicción y gestión de campañas

1.4. Comercial y ventas
- 1.4.1. Aportaciones de analítica del dato en el área comercial
- 1.4.2. Necesidades del departamento de Ventas
- 1.4.3. Estudios de mercado

1.5. Atención al cliente
- 1.5.1. Fidelización
- 1.5.2. Calidad personal e inteligencia emocional
- 1.5.3. Satisfacción del cliente

1.6. Compras
- 1.6.1. Analítica del dato para estudios de mercado
- 1.6.2. Analítica del dato para estudios de competencia
- 1.6.3. Otras aplicaciones

1.7. Administración
- 1.7.1. Necesidades en el departamento de administración
- 1.7.2. *Data Warehouse* y análisis de riesgo financiero
- 1.7.3. *Data Warehouse* y análisis de riesgo de crédito

1.8. Recursos humanos
- 1.8.1. RR.HH y beneficios de la analítica del dato
- 1.8.2. Herramientas de analítica del dato en el departamento de RR.HH.
- 1.8.3. Aplicación de analítica del dato en los RR.HH.

1.9. Producción
- 1.9.1. Análisis de datos en un departamento de producción
- 1.9.2. Aplicaciones
- 1.9.3. Beneficios

1.10. IT
- 1.10.1. Departamento de IT
- 1.10.2. Analítica del dato y transformación digital
- 1.10.3. Innovación y productividad

Módulo 2. Gestión, manipulación de datos e información para ciencia de datos

2.1. Estadística. Variables, índices y ratios
- 2.1.1. La Estadística
- 2.1.2. Dimensiones estadísticas
- 2.1.3. Variables, índices y ratios

2.2. Tipología del dato
- 2.2.1. Cualitativos
- 2.2.2. Cuantitativos
- 2.2.3. Caracterización y categorías

2.3. Conocimiento de los datos a partir de medidas
- 2.3.1. Medidas de centralización
- 2.3.2. Medidas de dispersión
- 2.3.3. Correlación

2.4. Conocimiento de los datos a partir de gráficos
- 2.4.1. Visualización según el tipo de dato
- 2.4.2. Interpretación de información gráfica
- 2.4.3. Customización de gráficos con R

2.5. Probabilidad
- 2.5.1. Probabilidad
- 2.5.2. Función de probabilidad
- 2.5.3. Distribuciones

2.6. Recolección de datos
- 2.6.1. Metodología de recolección
- 2.6.2. Herramientas de recolección
- 2.6.3. Canales de recolección

2.7. Limpieza del dato
- 2.7.1. Fases de la limpieza de datos
- 2.7.2. Calidad del dato
- 2.7.3. Manipulación de datos (con R)

2.8. Análisis de datos, interpretación y valoración de resultados
- 2.8.1. Medidas estadísticas
- 2.8.2. Índices de relación
- 2.8.3. Minería de datos

2.9. Almacén del dato (*Datawarehouse*)
- 2.9.1. Elementos
- 2.9.2. Diseño

2.10. Disponibilidad del dato
- 2.10.1. Acceso
- 2.10.2. Utilidad
- 2.10.3. Seguridad

Módulo 3. Dispositivos y plataformas IoT como base para la ciencia de datos

3.1. *Internet of Things*
- 3.1.1. Internet del futuro, *Internet of Things*
- 3.1.2. El consorcio de internet industrial

3.2. Arquitectura de referencia
- 3.2.1. La Arquitectura de referencia
- 3.2.2. Capas
- 3.2.3. Componentes

3.3. Sensores y dispositivos IoT
- 3.3.1. Componentes principales
- 3.3.2. Sensores y actuadores

3.4. Comunicaciones y protocolos
- 3.4.1. Protocolos. Modelo OSI
- 3.4.2. Tecnologías de comunicación

3.5. Plataformas *cloud* para IoT e IIoT
- 3.5.1. Plataformas de propósito general
- 3.5.2. Plataformas Industriales
- 3.5.3. Plataformas de código abierto

3.6. Gestión de datos en plataformas IoT
- 3.6.1. Mecanismos de gestión de datos. Datos abiertos
- 3.6.2. Intercambio de datos y visualización

3.7. Seguridad en IoT
- 3.7.1. Requisitos y áreas de seguridad
- 3.7.2. Estrategias de seguridad en IIoT

3.8. Aplicaciones de IoT
- 3.8.1. Ciudades inteligentes
- 3.8.2. Salud y condición física
- 3.8.3. Hogar inteligente
- 3.8.4. Otras aplicaciones

3.9. Aplicaciones de IIoT
- 3.9.1. Fabricación
- 3.9.2. Transporte
- 3.9.3. Energía
- 3.9.4. Agricultura y ganadería
- 3.9.5. Otros sectores

3.10. Industria 4.0.
- 3.10.1. IoRT *(Internet of Robotics Things)*
- 3.10.2. Fabricación aditiva 3D
- 3.10.3. *Big Data Analytics*

Módulo 4. Representación gráfica para análisis de datos

4.1. Análisis exploratorio
- 4.1.1. Representación para análisis de información
- 4.1.2. El valor de la representación gráfica
- 4.1.3. Nuevos paradigmas de la representación gráfica

4.2. Optimización para ciencia de datos
- 4.2.1. La Gama cromática y el diseño
- 4.2.2. La Gestalt en la representación gráfica
- 4.2.3. Errores a evitar y consejos

4.3. Fuentes de datos básicos
- 4.3.1. Para representación de calidad
- 4.3.2. Para representación de cantidad
- 4.3.3. Para representación de tiempo

4.4. Fuentes de datos complejos
- 4.4.1. Archivos, listados y BBDD
- 4.4.2. Datos abiertos
- 4.4.3. Datos de generación continua

4.5. Tipos de gráficas
- 4.5.1. Representaciones básicas
- 4.5.2. Representación de bloques
- 4.5.3. Representación para análisis de dispersión
- 4.5.4. Representaciones circulares
- 4.5.5. Representaciones burbujas
- 4.5.6. Representaciones geográficas

4.6. Tipos de visualización
- 4.6.1. Comparativas y relacional
- 4.6.2. Distribución
- 4.6.3. Jerárquica

4.7. Diseño de informes con representación gráfica
- 4.7.1. Aplicación de gráficas en informes de marketing
- 4.7.2. Aplicación de gráficas en cuadros de mando y Kpi's
- 4.7.3. Aplicación de gráficas en planes estratégicos
- 4.7.4. Otros usos: ciencia, salud, negocio

4.8. Narración gráfica
- 4.8.1. La narración gráfica
- 4.8.2. Evolución
- 4.8.3. Utilidad

4.9. Herramientas orientadas a visualización
- 4.9.1. Herramientas avanzadas
- 4.9.2. Software en línea
- 4.9.3. *Open Source*

4.10. Nuevas tecnologías en la visualización de datos
- 4.10.1. Sistemas para virtualización de la realidad
- 4.10.2. Sistemas para aumento y mejora de la realidad
- 4.10.3. Sistemas inteligentes

Módulo 5. Herramientas de ciencia de datos

5.1. Ciencia de datos
- 5.1.1. La ciencia de datos
- 5.1.2. Herramientas avanzadas para el científico de datos

5.2. Datos, información y conocimiento
- 5.2.1. Datos, información y conocimiento
- 5.2.2. Tipos de datos
- 5.2.3. Fuentes de datos

5.3. De los datos a la información
- 5.3.1. Análisis de datos
- 5.3.2. Tipos de análisis
- 5.3.3. Extracción de Información de un *Dataset*

5.4. Extracción de información mediante visualización
- 5.4.1. La visualización como herramienta de análisis
- 5.4.2. Métodos de visualización
- 5.4.3. Visualización de un conjunto de datos

5.5. Calidad de los datos
- 5.5.1. Datos de calidad
- 5.5.2. Limpieza de datos
- 5.5.3. Preprocesamiento básico de datos

5.6. *Dataset*
- 5.6.1. Enriquecimiento del *dataset*
- 5.6.2. La maldición de la dimensionalidad
- 5.6.3. Modificación de nuestro conjunto de datos

5.7. Desbalanceo
- 5.7.1. Desbalanceo de clases
- 5.7.2. Técnicas de mitigación del desbalanceo
- 5.7.3. Balanceo de un *dataset*

5.8. Modelos no supervisados
- 5.8.1. Modelo no supervisado
- 5.8.2. Métodos
- 5.8.3. Clasificación con modelos no supervisados

5.9. Modelos supervisados
- 5.9.1. Modelo supervisado
- 5.9.2. Métodos
- 5.9.3. Clasificación con modelos supervisados

5.10. Herramientas y buenas prácticas
- 5.10.1. Buenas prácticas para un científico de datos
- 5.10.2. El mejor modelo
- 5.10.3. Herramientas útiles

Módulo 6. Minería de datos. selección, preprocesamiento y transformación

6.1. La inferencia estadística
- 6.1.1. Estadística descriptiva vs. Inferencia estadística
- 6.1.2. Procedimientos paramétricos
- 6.1.3. Procedimientos no paramétricos

6.2. Análisis exploratorio
- 6.2.1. Análisis descriptivo
- 6.2.2. Visualización
- 6.2.3. Preparación de datos

6.3. Preparación de datos
- 6.3.1. Integración y limpieza de datos
- 6.3.2. Normalización de datos
- 6.3.3. Transformando atributos

6.4. Los Valores perdidos
- 6.4.1. Tratamiento de valores perdidos
- 6.4.2. Métodos de imputación de máxima verosimilitud
- 6.4.3. Imputación de valores perdidos usando aprendizaje automático

6.5. El ruido en los datos
- 6.5.1. Clases de ruido y atributos
- 6.5.2. Filtrado de ruido
- 6.5.3. El efecto del ruido

6.6. La maldición de la dimensionalidad
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Reducción de datos multidimensionales

6.7. De atributos continuos a discretos
- 6.7.1. Datos continuos versus discretos
- 6.7.2. Proceso de discretización

6.8. Los datos
- 6.8.1. Selección de datos
- 6.8.2. Perspectivas y criterios de selección
- 6.8.3. Métodos de selección

6.9. Selección de Instancias
- 6.9.1. Métodos para la selección de instancias
- 6.9.2. Selección de prototipos
- 6.9.3. Métodos avanzados para la selección de instancias

6.10. Preprocesamiento de datos en entornos *Big Data*
- 6.10.1. *Big Data*
- 6.10.2. Preprocesamiento "clásico" versus masivo
- 6.10.3. *Smart Data*

Módulo 7. Predictibilidad y análisis de fenómenos estocásticos

7.1. Series de tiempo
- 7.1.1. Series de tiempo
- 7.1.2. Utilidad y aplicabilidad
- 7.1.3. Casuística relacionada

7.2. La Serie temporal
- 7.2.1. Tendencia Estacionalidad de ST
- 7.2.2. Variaciones típicas
- 7.2.3. Análisis de residuos

7.3. Tipologías
- 7.3.1. Estacionarias
- 7.3.2. No estacionarias
- 7.3.3. Transformaciones y ajustes

7.4. Esquemas para series temporales
- 7.4.1. Esquema (modelo) aditivo
- 7.4.2. Esquema (modelo) multiplicativo
- 7.4.3. Procedimientos para determinar el tipo de modelo

7.5. Métodos básicos de *forecast*
- 7.5.1. Media
- 7.5.2. *Naïve*
- 7.5.3. *Naïve* estacional
- 7.5.4. Comparación de métodos

7.6. Análisis de residuos
- 7.6.1. Autocorrelación
- 7.6.2. ACF de residuos
- 7.6.3. Test de correlación

7.7. Regresión en el contexto de series temporales
- 7.7.1. ANOVA
- 7.7.2. Fundamentos
- 7.7.3. Aplicación práctica

7.8. Modelos predictivos de series temporales
- 7.8.1. ARIMA
- 7.8.2. Suavizado exponencial

7.9. Manipulación y análisis de Series temporales con R
- 7.9.1. Preparación de los datos
- 7.9.2. Identificación de patrones
- 7.9.3. Análisis del modelo
- 7.9.4. Predicción

7.10. Análisis gráficos combinados con R
- 7.10.1. Situaciones habituales
- 7.10.2. Aplicación práctica para resolución de problemas sencillos
- 7.10.3. Aplicación práctica para resolución de problemas avanzados

Módulo 8. Diseño y desarrollo de sistemas inteligentes

8.1. Preprocesamiento de datos
- 8.1.1. Preprocesamiento de datos
- 8.1.2. Transformación de datos
- 8.1.3. Minería de datos

8.2. Aprendizaje Automático
- 8.2.1. Aprendizaje supervisado y no supervisado
- 8.2.2. Aprendizaje por refuerzo
- 8.2.3. Otros paradigmas de aprendizaje

8.3. Algoritmos de clasificación
- 8.3.1. Aprendizaje Automático Inductivo
- 8.3.2. SVM y KNN
- 8.3.3. Métricas y puntuaciones para clasificación

8.4. Algoritmos de Regresión
- 8.4.1. Regresión lineal, regresión logística y modelos no lineales
- 8.4.2. Series temporales
- 8.4.3. Métricas y puntuaciones para regresión

8.5. Algoritmos de Agrupamiento
- 8.5.1. Técnicas de agrupamiento jerárquico
- 8.5.2. Técnicas de agrupamiento particional
- 8.5.3. Métricas y puntuaciones para *clustering*

8.6. Técnicas de reglas de asociación
- 8.6.1. Métodos para la extracción de reglas
- 8.6.2. Métricas y puntuaciones para los algoritmos de reglas de asociación

8.7. Técnicas de clasificación avanzadas. Multiclasificadores
- 8.7.1. Algoritmos de *Bagging*
- 8.7.2. Clasificador *Random Forests*
- 8.7.3. *Boosting* para árboles de decisión

8.8. Modelos gráficos probabilísticos
- 8.8.1. Modelos probabilísticos
- 8.8.2. Redes bayesianas. Propiedades, representación y parametrización
- 8.8.3. Otros modelos gráficos probabilísticos

8.9. Redes Neuronales
- 8.9.1. Aprendizaje automático con redes neuronales artificiales
- 8.9.2. Redes *feedforward*

8.10. Aprendizaje profundo
- 8.10.1. Redes *feedforward* profundas
- 8.10.2. Redes neuronales convolucionales y modelos de secuencia
- 8.10.3. Herramientas para implementar redes neuronales profundas

Módulo 9. Arquitecturas y sistemas para uso intensivo de datos

9.1. Requisitos no funcionales. Pilares de las aplicaciones de datos masivos
- 9.1.1. Fiabilidad
- 9.1.2. Adaptabilidad
- 9.1.3. Mantenibilidad

9.2. Modelos de datos
- 9.2.1. Modelo relacional
- 9.2.2. Modelo documental
- 9.2.3. Modelo de datos tipo grafo

9.3. Bases de datos. Gestión del almacenamiento y recuperación de datos
- 9.3.1. Índices has
- 9.3.2. Almacenamiento estructurado en log
- 9.3.3. Árboles B

9.4. Formatos de codificación de datos
- 9.4.1. Formatos específicos del lenguaje
- 9.4.2. Formatos estandarizados
- 9.4.3. Formatos de codificación binarios
- 9.4.4. Flujo de datos entre procesos

9.5. Replicación
- 9.5.1. Objetivos de la replicación
- 9.5.2. Modelos de replicación
- 9.5.3. Problemas con la replicación

9.6. Transacciones distribuidas
- 9.6.1. Transacción
- 9.6.2. Protocolos para transacciones distribuidas
- 9.6.3. Transacciones serializables

9.7. Particionado
- 9.7.1. Formas de particionado
- 9.7.2. Interacción de índice secundarios y particionado
- 9.7.3. Rebalanceo de particiones

9.8. Procesamiento de datos *offline*
- 9.8.1. Procesamiento por lotes
- 9.8.2. Sistemas de ficheros distribuidos
- 9.8.3. *MapReduce*

9.9. Procesamiento de datos en tiempo real
- 9.9.1. Tipos de *broker* de mensajes
- 9.9.2. Representación de bases de datos como flujos de datos
- 9.9.3. Procesamiento de flujos de datos

9.10. Aplicaciones prácticas en la empresa
- 9.10.1. Consistencia en lecturas
- 9.10.2. Enfoque holístico de datos
- 9.10.3. Escalado de un servicio distribuido

Módulo 10. Aplicación práctica de la ciencia de datos en sectores de actividad empresarial

10.1. Sector sanitario
- 10.1.1. Implicaciones de la IA y la analítica de datos en el sector sanitario
- 10.1.2. Oportunidades y desafíos

10.2. Riesgos y tendencias en sector sanitario
- 10.2.1. Uso en el sector sanitario
- 10.2.2. Riesgos potenciales relacionados con el uso de IA

10.3. Servicios financieros
- 10.3.1. Implicaciones de la IA y la analítica de datos en el sector de los servicios financiero
- 10.3.2. Uso en los servicios financieros
- 10.3.3. Riesgos potenciales relacionados con el uso de IA

10.4. Retail
- 10.4.1. Implicaciones de la IA y la analítica de datos en el sector del retail
- 10.4.2. Uso en el retail
- 10.4.3. Riesgos potenciales relacionados con el uso de IA

10.5. Industria 4.0.
- 10.5.1. Implicaciones de la IA y la analítica de datos en la Industria 4.0.
- 10.5.2. Uso en la Industria 4.0.

10.6. Riesgos y tendencias en Industria 4.0.
- 10.6.1. Riesgos potenciales relacionados con el uso de IA

10.7. Administración pública
- 10.7.1. Implicaciones de la IA y la analítica de datos en la administración pública
- 10.7.2. Uso en la administración pública
- 10.7.3. Riesgos potenciales relacionados con el uso de IA

10.8. Educación
- 10.8.1. Implicaciones de la IA y la analítica de datos en la educación
- 10.8.2. Riesgos potenciales relacionados con el uso de IA

10.9. Silvicultura y agricultura
- 10.9.1. Implicaciones de la IA y la analítica de datos en la silvicultura y agricultura
- 10.9.2. Uso en silvicultura y agricultura
- 10.9.3. Riesgos potenciales relacionados con el uso de IA

10.10. Recursos humanos
- 10.10.1. Implicaciones de la IA y la analítica de datos en la gestión de recursos humanos
- 10.10.2. Aplicaciones prácticas en el mundo empresarial
- 10.10.3. Riesgos potenciales relacionados con el uso de IA

Módulo 11. Ciberinteligencia y ciberseguridad

11.1. Ciberinteligencia
- 11.1.1. Ciberinteligencia
  - 11.1.1.1. La inteligencia
    - 11.1.1.1.1. Ciclo de inteligencia
  - 11.1.1.2. Ciberinteligencia
  - 11.1.1.3. Ciberinteligencia y ciberseguridad
- 11.1.2. El Analista de Inteligencia
  - 11.1.2.1. El rol del analista de inteligencia
  - 11.1.2.2. Los sesgos del analista de inteligencia en la actividad evaluativa

11.2. Ciberseguridad
- 11.2.1. Las capas de seguridad
- 11.2.2. Identificación de las ciberamenazas
  - 11.2.2.1. Amenazas externas
  - 11.2.2.2. Amenazas internas
- 11.2.3. Acciones adversas
  - 11.2.3.1. Ingeniería social
  - 11.2.3.2. Métodos comúnmente usados

11.3. Técnicas y herramientas de inteligencias
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Distribuciones de Linux y herramientas
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Metodologías de evaluación
- 11.4.1. El análisis de inteligencia
- 11.4.2. Técnicas de organización de la información adquirida
- 11.4.3. Fiabilidad y credibilidad de las fuentes de información
- 11.4.4. Metodologías de análisis
- 11.4.5. Presentación de los resultados de la inteligencia

11.5. Auditorías y documentación
- 11.5.1. La auditoría en seguridad informática
- 11.5.2. Documentación y permisos para auditoria
- 11.5.3. Tipos de auditoría
- 11.5.4. Entregables
  - 11.5.4.1. Informe técnico
  - 11.5.4.2. Informe ejecutivo

11.6. Anonimato en la red
- 11.6.1. Uso de anonimato
- 11.6.2. Técnicas de anonimato (Proxy, VPN)
- 11.6.3. Redes TOR, Freenet e IP2

11.7. Amenazas y tipos de seguridad
- 11.7.1. Tipos de amenazas
- 11.7.2. Seguridad física
- 11.7.3. Seguridad en redes
- 11.7.4. Seguridad lógica
- 11.7.5. Seguridad en aplicaciones web
- 11.7.6. Seguridad en dispositivos móviles

11.8. Normativa y *compliance*
- 11.8.1. RGPD
- 11.8.2. La estrategia nacional de ciberseguridad 2019
- 11.8.3. Familia ISO 27000
- 11.8.4. Marco de ciberseguridad NIST
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Normativas *cloud*
- 11.8.8. SOX
- 11.8.9. PCI

11.9. Análisis de riesgos y métricas
- 11.9.1. Alcance de riesgos
- 11.9.2. Los activos
- 11.9.3. Las amenazas
- 11.9.4. Las vulnerabilidades
- 11.9.5. Evaluación del riesgo
- 11.9.6. Tratamiento del riesgo

11.10. Organismos importantes en materia de ciberseguridad
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Módulo 12. Seguridad en host

12.1. Copias de seguridad
- 12.1.1. Estrategias para las copias de seguridad
- 12.1.2. Herramientas para Windows
- 12.1.3. Herramientas para Linux
- 12.1.4. Herramientas para MacOS

12.2. Antivirus de usuario
- 12.2.1. Tipos de antivirus
- 12.2.2. Antivirus para Windows
- 12.2.3. Antivirus para Linux
- 12.2.4. Antivirus para MacOS
- 12.2.5. Antivirus para smartphones

12.3. Detectores de intrusos - HIDS
- 12.3.1. Métodos de detección de intrusos
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. *Firewall* local
- 12.4.1. *Firewalls* para Windows
- 12.4.2. *Firewalls* para Linux
- 12.4.3. *Firewalls* para MacOS

12.5. Gestores de contraseñas
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *StickyPassword*
- 12.5.5. *RoboForm*

12.6. Detectores de *phishing*
- 12.6.1. Detección del *phishing* de forma manual
- 12.6.2. Herramientas *antiphishing*

12.7. *Spyware*
- 12.7.1. Mecanismos de evitación
- 12.7.2. Herramientas *antispyware*

12.8. Rastreadores
- 12.8.1. Medidas para proteger el sistema
- 12.8.2. Herramientas antirastreadores

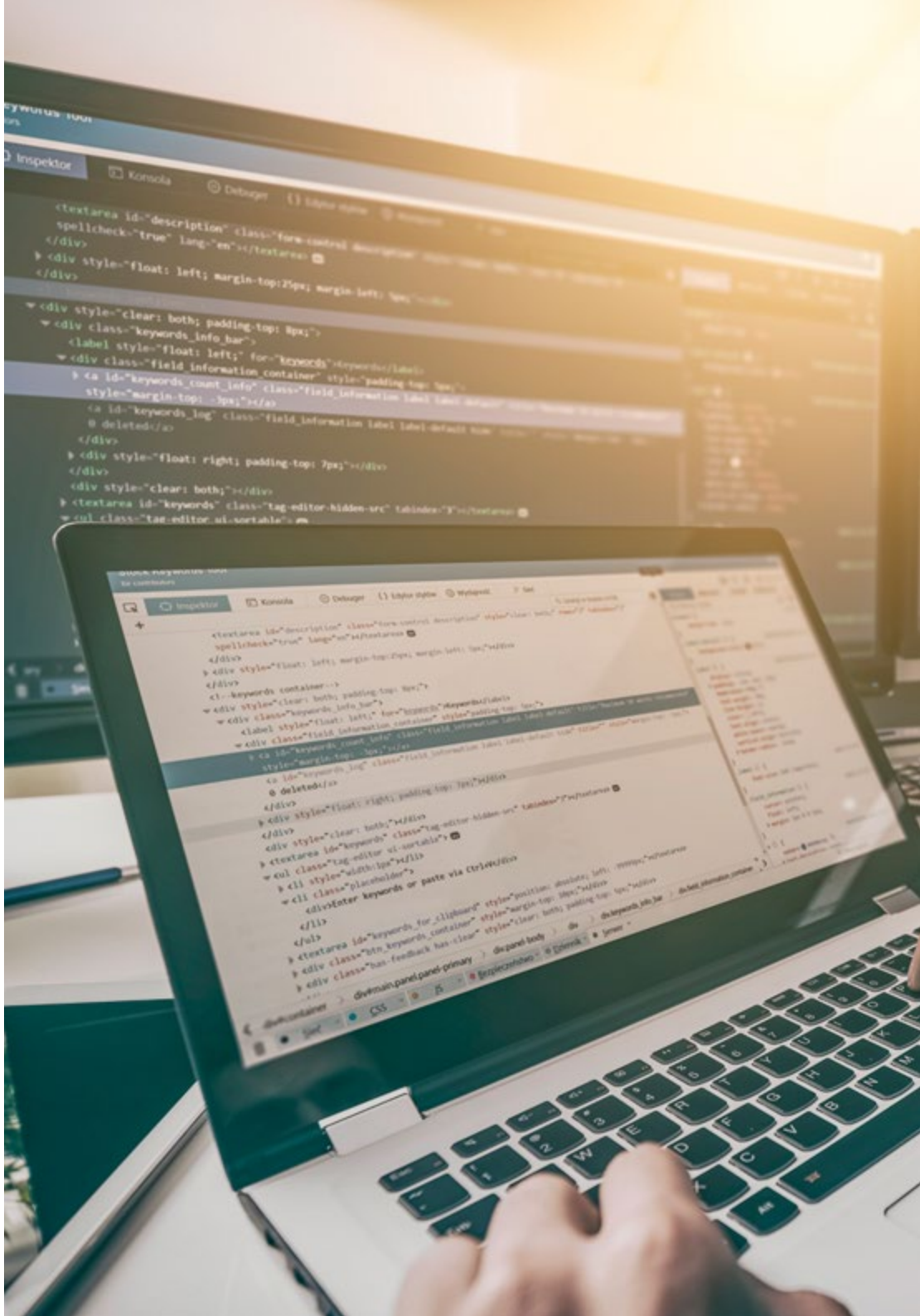
12.9. EDR- *End Point Detection and Response*
- 12.9.1. Comportamiento del sistema EDR
- 12.9.2. Diferencias entre EDR y antivirus
- 12.9.3. El futuro de los sistemas EDR

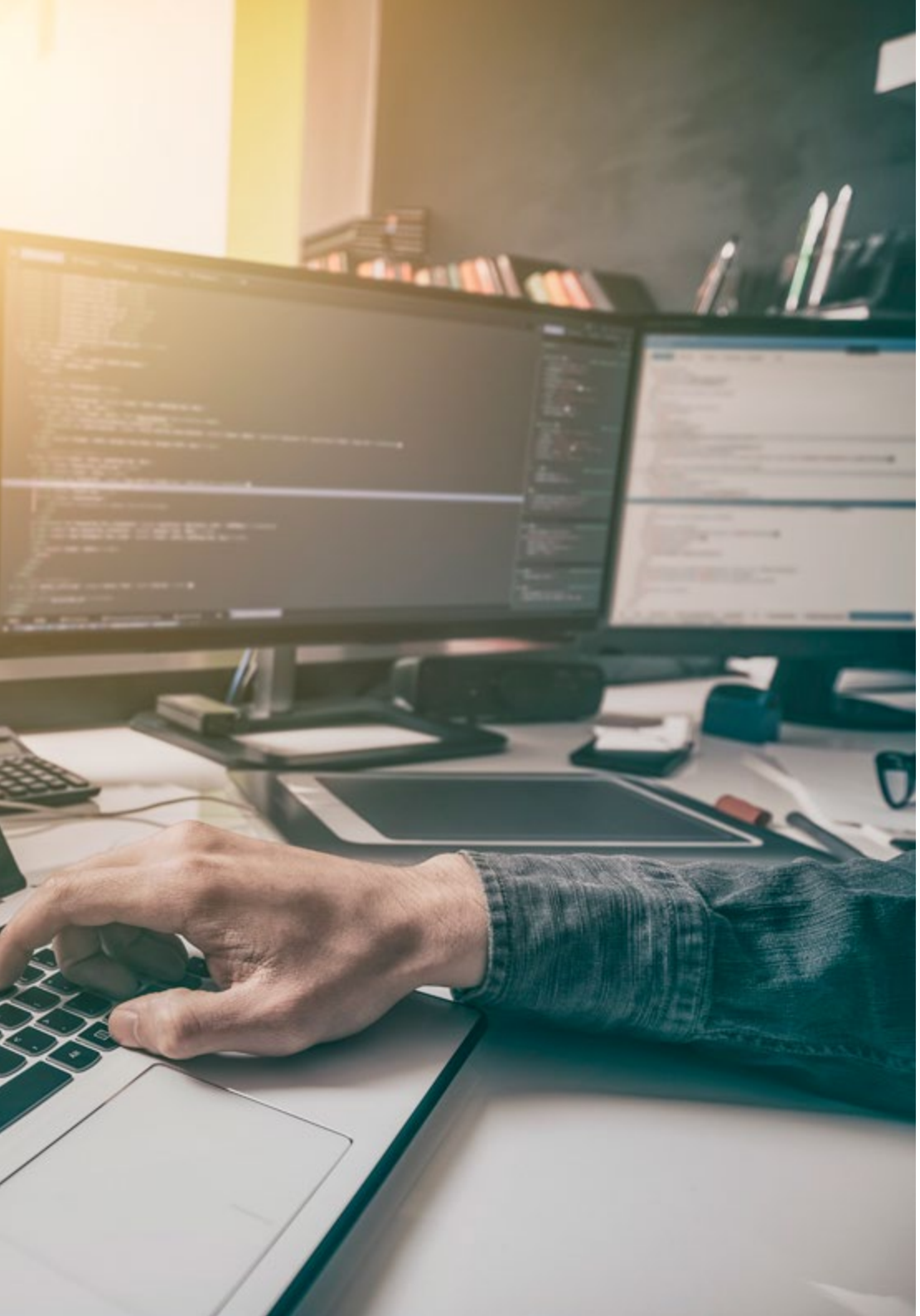
12.10. Control sobre la instalación de software
- 12.10.1. Repositorios y tiendas de software
- 12.10.2. Listas de software permitido o prohibido
- 12.10.3. Criterios de actualizaciones
- 12.10.4. Privilegios para instalar software

Módulo 13. Seguridad en red (Perimetral)

13.1. Sistemas de detección y prevención de amenazas
- 13.1.1. Marco general de los incidentes de seguridad
- 13.1.2. Sistemas de defensa actuales: *Defense in Depth* y SOC
- 13.1.3. Arquitecturas de red actuales
- 13.1.4. Tipos de herramientas para la detección y prevención de incidentes
  - 13.1.4.1. Sistemas basados en red
  - 13.1.4.2. Sistemas basados en host
  - 13.1.4.3. Sistemas centralizados
- 13.1.5. Comunicación y detección de instancias/*hosts*, contenedores y *serverless*

13.2. *Firewall*
- 13.2.1. Tipos de *firewalls*
- 13.2.2. Ataques y mitigación
- 13.2.3. *Firewalls* comunes en kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables e iptables
  - 13.2.3.3. *Firewalld*
- 13.2.4. Sistemas de detección basados en logs del sistema
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* y *DenyHosts*
  - 13.2.4.3. Fai2ban





13.3. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 13.3.1. Ataques sobre IDS/IPS
- 13.3.2. Sistemas de IDS/IPS
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Firewalls* de siguiente generación (NGFW)
- 13.4.1. Diferencias entre NGFW y Firewall tradicional
- 13.4.2. Capacidades principales
- 13.4.3. Soluciones comerciales
- 13.4.4. Firewalls para servicios de *Cloud*
  - 13.4.4.1. Arquitectura *Cloud* VPC
  - 13.4.4.2. *Cloud* ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Tipos de Proxy
- 13.5.2. Uso de Proxy. Ventajas e inconvenientes

13.6. Motores de antivirus
- 13.6.1. Contexto general del *Malware* e IOCs
- 13.6.2. Problemas de los motores de antivirus

13.7. Sistemas de protección de correo
- 13.7.1. Antispam
  - 13.7.1.1. Listas blancas y negras
  - 13.7.1.2. Filtros bayesianos
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Componentes y arquitectura
- 13.8.2. Reglas de correlación y casos de uso
- 13.8.3. Retos actuales de los sistemas SIEM

13.9. SOAR
- 13.9.1. SOAR y SIEM: enemigos o aliados
- 13.9.2. El futuro de los sistemas SOAR

13.10. Otros sistemas basados en red
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots y HoneyNets
- 13.10.4. CASB

Módulo 14. Seguridad en smartphones

14.1. El mundo del dispositivo móvil
- 14.1.1. Tipos de plataformas móviles
- 14.1.2. Dispositivos iOS
- 14.1.3. Dispositivos Android

14.2. Gestión de la Seguridad Móvil
- 14.2.1. Proyecto de Seguridad Móvil OWASP
  - 14.2.1.1. Top 10 Vulnerabilidades
- 14.2.2. Comunicaciones, redes y modos de conexión

14.3. El dispositivo móvil en el entorno empresarial
- 14.3.1. Riesgos
- 14.3.2. Políticas de seguridad
- 14.3.3. Monitorización de dispositivos
- 14.3.4. Gestión de dispositivos móviles (MDM)

14.4. Privacidad del usuario y seguridad de los datos
- 14.4.1. Estados de la información
- 14.4.2. Protección y confidencialidad de los datos
  - 14.4.2.1. Permisos
  - 14.4.2.2. Encriptación
- 14.4.3. Almacenamiento seguro de los datos
  - 14.4.3.1. Almacenamiento seguro en iOS
  - 14.4.3.2. Almacenamiento seguro en Android
- 14.4.4. Buenas prácticas en el desarrollo de aplicaciones

14.5. Vulnerabilidades y vectores de ataque
- 14.5.1. Vulnerabilidades
- 14.5.2. Vectores de ataque
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Exfiltración de datos
  - 14.5.2.3. Manipulación de los datos

14.6. Principales amenazas
- 14.6.1. Usuario no forzado
- 14.6.2. *Malware*
  - 14.6.2.1. Tipos de *Malware*
- 14.6.3. Ingeniería social
- 14.6.4. Fuga de datos
- 14.6.5. Robo de información
- 14.6.6. Redes *Wi-Fi* no seguras
- 14.6.7. Software desactualizado
- 14.6.8. Aplicaciones maliciosas
- 14.6.9. Contraseñas poco seguras
- 14.6.10. Configuración débil o inexistente de seguridad
- 14.6.11. Acceso físico
- 14.6.12. Pérdida o robo del dispositivo
- 14.6.13. Suplantación de identidad (Integridad)
- 14.6.14. Criptografía débil o rota
- 14.6.15. Denegación de Servicio (DoS)

14.7. Principales ataques
- 14.7.1. Ataques de *phishing*
- 14.7.2. Ataques relacionados con los modos de comunicación
- 14.7.3. Ataques de *Smishing*
- 14.7.4. Ataques de *Criptojacking*
- 14.7.5. *Man in The Middle*

14.8. *Hacking*
- 14.8.1. *Rooting y Jailbreaking*
- 14.8.2. Anatomía de un ataque móvil
  - 14.8.2.1. Propagación de la amenaza
  - 14.8.2.2. Instalación de *malware* en el dispositivo
  - 14.8.2.3. Persistencia
  - 14.8.2.4. Ejecución del *Payload* y extracción de la información
- 14.8.3. *Hacking* en dispositivos iOS: mecanismos y herramientas
- 14.8.4. *Hacking* en dispositivos Android: mecanismos y herramientas

14.9. Pruebas de penetración
- 14.9.1. *iOS PenTesting*
- 14.9.2. *Android PenTesting*
- 14.9.3. Herramientas

14.10. Protección y seguridad
- 14.10.1. Configuración de seguridad
  - 14.10.1.1. En dispositivos iOS
  - 14.10.1.2. En dispositvos Android
- 14.10.2. Medidas de seguridad
- 14.10.3. Herramientas de protección

Módulo 15. Seguridad en IoT

15.1. Dispositivos
- 15.1.1. Tipos de dispositivos
- 15.1.2. Arquitecturas estandarizadas
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Protocolos de aplicación
- 15.1.4. Tecnologías de conectividad

15.2. Dispositivos IoT. Áreas de aplicación
- 15.2.1. *SmartHome*
- 15.2.2. *SmartCity*
- 15.2.3. Transportes
- 15.2.4. *Wearables*
- 15.2.5. Sector salud
- 15.2.6. IioT

15.3. Protocolos de comunicación
- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. *SmartHome*
- 15.4.1. Domótica
- 15.4.2. Redes
- 15.4.3. Electrodomésticos
- 15.4.4. Vigilancia y seguridad

15.5. *SmartCity*
- 15.5.1. Iluminación
- 15.5.2. Meteorología
- 15.5.3. Seguridad

15.6. Transportes
- 15.6.1. Localización
- 15.6.2. Realización de pagos y obtención de servicios
- 15.6.3. Conectividad

15.7. *Wearables*
- 15.7.1. Ropa inteligente
- 15.7.2. Joyas inteligentes
- 15.7.3. Relojes inteligentes

15.8. Sector salud
- 15.8.1. Monitorización de ejercicio/ritmo cardiaco
- 15.8.2. Monitorización de pacientes y personas mayores
- 15.8.3. Implantables
- 15.8.4. Robots quirúrgicos

15.9. Conectividad
- 15.9.1. *Wi-Fi/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Conectividad incorporada

15.10. Securización
- 15.10.1. Redes dedicadas
- 15.10.2. Gestor de contraseñas
- 15.10.3. Uso de protocolos cifrados
- 15.10.4. Consejos de uso

Módulo 16. *Hacking* ético

16.1. Entorno de trabajo
- 16.1.1. Distribuciones Linux
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Sistemas de virtualización
- 16.1.3. *Sandbox*
- 16.1.4. Despliegue de laboratorios

16.2. Metodologías
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. Inteligencia de fuentes abiertas (OSINT)
- 16.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 16.3.3. Uso de herramientas pasivas

16.4. Escaneo de redes
- 16.4.1. Herramientas de escaneo
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Otras herramientas de escaneo
- 16.4.2. Técnicas de escaneo
- 16.4.3. Técnicas de evasión de *Firewall* e IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Diagramas de red

16.5. Enumeración
- 16.5.1. Enumeración SMTP
- 16.5.2. Enumeración DNS
- 16.5.3. Enumeración de NetBIOS y Samba
- 16.5.4. Enumeración de LDAP
- 16.5.5. Enumeración de SNMP
- 16.5.6. Otras técnicas de enumeración

16.6. Análisis de vulnerabilidades
- 16.6.1. Soluciones de análisis de vulnerabilidades
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Sistemas de puntuación de vulnerabilidades
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Ataques a redes *inalámbricas*
- 16.7.1. Metodología de *hacking* en redes inalámbricas
  - 16.7.1.1. Wi-Fi Discovery
  - 16.7.1.2. Análisis de tráfico
  - 16.7.1.3. Ataques del *aircrack*
    - 16.7.1.3.1. Ataques WEP
    - 16.7.1.3.2. Ataques WPA/WPA2
  - 16.7.1.4. Ataques de *Evil Twin*
  - 16.7.1.5. Ataques a WPS
  - 16.7.1.6. *Jamming*
- 16.7.2. Herramientas para la seguridad inalámbrica

16.8. Hackeo de servidores webs
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQLinjection*

16.9. Explotación de vulnerabilidades
- 16.9.1. Uso de *exploits* conocidos
- 16.9.2. Uso de *metasploit*
- 16.9.3. Uso de *malware*
  - 16.9.3.1. Definición y alcance
  - 16.9.3.2. Generación de *malware*
  - 16.9.3.3. Bypass de soluciones antivirus

16.10. Persistencia
- 16.10.1. Instalación de rootkits
- 16.10.2. Uso de ncat
- 16.10.3. Uso de tareas programadas para backdoors
- 16.10.4. Creación de usuarios
- 16.10.5. Detección de HIDS

Módulo 17. Ingeniería inversa

17.1. Compiladores
- 17.1.1. Tipos de códigos
- 17.1.2. Fases de un compilador
- 17.1.3. Tabla de símbolos
- 17.1.4. Gestor de errores
- 17.1.5. Compilador GCC

17.2. Tipos de análisis en compiladores
- 17.2.1. Análisis léxico
  - 17.2.1.1. Terminología
  - 17.2.1.2. Componentes léxicos
  - 17.2.1.3. Analizador léxico LEX
- 17.2.2. Análisis sintáctico
  - 17.2.2.1. Gramáticas libres de contexto
  - 17.2.2.2. Tipos de análisis sintácticos
    - 17.2.2.2.1. Análisis descendente
    - 17.2.2.2.2. Análisis ascendente
  - 17.2.2.3. Árboles sintácticos y derivaciones
  - 17.2.2.4. Tipos de analizadores sintácticos
    - 17.2.2.4.1. Analizadores LR (*Left To Right*)
    - 17.2.2.4.2. Analizadores LALR
- 17.2.3. Análisis semántico
  - 17.2.3.1. Gramáticas de atributos
  - 17.2.3.2. S-Atribuidas
  - 17.2.3.3. L-Atribuidas

17.3. Estructuras de datos en ensamblador
- 17.3.1. Variables
- 17.3.2. Arrays
- 17.3.3. Punteros
- 17.3.4. Estructuras
- 17.3.5. Objetos

17.4. Estructuras de código en ensamblador
- 17.4.1. Estructuras de selección
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Estructuras de iteración
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Uso del break
- 17.4.3. Funciones

17.5. Arquitectura Hardware x86
- 17.5.1. Arquitectura de procesadores x86
- 17.5.2. Estructuras de datos en x86
- 17.5.3. Estructuras de código en x86

17.6. Arquitectura Hardware ARM
- 17.6.1. Arquitectura de procesadores ARM
- 17.6.2. Estructuras de datos en ARM
- 17.6.3. Estructuras de código en ARM

17.7. Análisis de código estático
- 17.7.1. Desensambladores
- 17.7.2. IDA
- 17.7.3. Reconstructores de código

17.8. Análisis de código dinámico
- 17.8.1. Análisis del comportamiento
  - 17.8.1.1. Comunicaciones
  - 17.8.1.2. Monitorización
- 17.8.2. Depuradores de código en Linux
- 17.8.3. Depuradores de código en Windows

17.9. *Sandbox*
- 17.9.1. Arquitectura de un *Sandbox*
- 17.9.2. Evasión de un *Sandbox*
- 17.9.3. Técnicas de detección
- 17.9.4. Técnicas de evasión
- 17.9.5. Contramedidas
- 17.9.6. *Sandbox* en Linux
- 17.9.7. *Sandbox* en Windows
- 17.9.8. *Sandbox* en MacOS
- 17.9.9. *Sandbox* en Android

17.10. Análisis de malware
- 17.10.1. Métodos de análisis de *malware*
- 17.10.2. Técnicas de ofuscación de *malware*
  - 17.10.2.1. Ofuscación de ejecutables
  - 17.10.2.2. Restricción de entornos de ejecución
- 17.10.3. Herramientas de análisis de *malware*

Módulo 18. Desarrollo seguro

18.1. Desarrollo seguro
- 18.1.1. Calidad, funcionalidad y seguridad
- 18.1.2. Confidencialidad, integridad y disponibilidad
- 18.1.3. Ciclo de vida del desarrollo de software

18.2. Fase de Requerimientos
- 18.2.1. Control de la autenticación
- 18.2.2. Control de roles y privilegios
- 18.2.3. Requerimientos orientados al riesgo
- 18.2.4. Aprobación de privilegios

18.3. Fases de análisis y diseño
- 18.3.1. Acceso a componentes y administración del sistema
- 18.3.2. Pistas de auditoría
- 18.3.3. Gestión de sesiones
- 18.3.4. Datos históricos
- 18.3.5. Manejo apropiado de errores
- 18.3.6. Separación de funciones

18.4. Fase de Implementación y codificación
- 18.4.1. Aseguramiento del ambiente de desarrollo
- 18.4.2. Elaboración de la documentación técnica
- 18.4.3. Codificación segura
- 18.4.4. Seguridad en las comunicaciones

18.5. Buenas prácticas de codificación segura
- 18.5.1. Validación de datos de entrada
- 18.5.2. Codificación de los datos de salida
- 18.5.3. Estilo de programación
- 18.5.4. Manejo de registro de cambios
- 18.5.5. Prácticas criptográficas
- 18.5.6. Gestión de errores y logs
- 18.5.7. Gestión de archivos
- 18.5.8. Gestión de memoria
- 18.5.9. Estandarización y reutilización de funciones de seguridad

18.6. Preparación del servidor y *Hardening*
- 18.6.1. Gestión de usuarios, grupos y roles en el servidor
- 18.6.2. Instalación de software
- 18.6.3. *Hardening* del servidor
- 18.6.4. Configuración robusta del entorno de la aplicación

18.7. Preparación de la BBDD y *Hardening*
- 18.7.1. Optimización del motor de BBDD
- 18.7.2. Creación del usuario propio para la aplicación
- 18.7.3. Asignación de los privilegios precisos para el usuario
- 18.7.4. *Hardening* de la BBDD

18.8. Fase de pruebas
- 18.8.1. Control de calidad en controles de seguridad
- 18.8.2. Inspección del código por fases
- 18.8.3. Comprobación de la gestión de las configuraciones
- 18.8.4. Pruebas de caja negra

18.9. Preparación del paso a producción
- 18.9.1. Realizar el control de cambios
- 18.9.2. Realizar procedimiento de paso a producción
- 18.9.3. Realizar procedimiento de *rollback*
- 18.9.4. Pruebas en fase de preproducción

18.10. Fase de mantenimiento
- 18.10.1. Aseguramiento basado en riesgos
- 18.10.2. Pruebas de mantenimiento de seguridad de caja blanca
- 18.10.3. Pruebas de mantenimiento de seguridad de caja negra

Módulo 19. Análisis forense

19.1. Adquisición de datos y duplicación
- 19.1.1. Adquisición de datos volátiles
  - 19.1.1.1. Información del sistema
  - 19.1.1.2. Información de la red
  - 19.1.1.3. Orden de volatilidad
- 19.1.2. Adquisición de datos estáticos
  - 19.1.2.1. Creación de una imagen duplicada
  - 19.1.2.2. Preparación de un documento para la cadena de custodia
- 19.1.3. Métodos de validación de los datos adquiridos
  - 19.1.3.1. Métodos para Linux
  - 19.1.3.2. Métodos para Windows

19.2. Evaluación y derrota de técnicas antiforenses
- 19.2.1. Objetivos de las técnicas antiforenses
- 19.2.2. Borrado de datos
  - 19.2.2.1. Borrado de datos y ficheros
  - 19.2.2.2. Recuperación de archivos
  - 19.2.2.3. Recuperación de particiones borradas
- 19.2.3. Protección por contraseña
- 19.2.4. Esteganografía
- 19.2.5. Borrado seguro de dispositivos
- 19.2.6. Encriptación

19.3. Análisis Forense del sistema operativo
- 19.3.1. Análisis forense de Windows
- 19.3.2. Análisis forense de Linux
- 19.3.3. Análisis forense de Mac

19.4. Análisis Forense de la red
- 19.4.1. Análisis de los logs
- 19.4.2. Correlación de datos
- 19.4.3. Investigación de la red
- 19.4.4. Pasos a seguir en el análisis forense de la red

19.5. Análisis forense Web
- 19.5.1. Investigación de los ataques webs
- 19.5.2. Detección de ataques
- 19.5.3. Localización de direcciones IPs

19.6. Análisis forense de bases de datos
- 19.6.1. Análisis forense en MSSQL
- 19.6.2. Análisis forense en MySQL
- 19.6.3. Análisis forense en PostgreSQL
- 19.6.4. Análisis forense en MongoDB

19.7. Análisis forense en *cloud*
- 19.7.1. Tipos de crímenes en *cloud*
  - 19.7.1.1. *Cloud* como sujeto
  - 19.7.1.2. *Cloud* como objeto
  - 19.7.1.3. *Cloud* como herramienta
- 19.7.2. Retos del análisis forense en *cloud*
- 19.7.3. Investigación de los servicios de almacenamiento el *cloud*
- 19.7.4. Herramientas de análisis forense para *cloud*

19.8. Investigación de crímenes de correo electrónico
- 19.8.1. Sistemas de correo
  - 19.8.1.1. Clientes de correo
  - 19.8.1.2. Servidor de correo
  - 19.8.1.3. Servidor SMTP
  - 19.8.1.4. Servidor POP3
  - 19.8.1.5. Servidor IMAP4
- 19.8.2. Crímenes de correo
- 19.8.3. Mensaje de correo
  - 19.8.3.1. Cabeceras estándar
  - 19.8.3.2. Cabeceras extendidas
- 19.8.4. Pasos para la investigación de estos crímenes
- 19.8.5. Herramientas forenses para correo electrónico

19.9. Análisis forense de móviles
- 19.9.1. Redes celulares
  - 19.9.1.1. Tipos de redes
  - 19.9.1.2. Contenidos del CDR
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Adquisición lógica
- 19.9.4. Adquisición física
- 19.9.5. Adquisición del sistema de ficheros

19.10. Redacción y presentación de Informes forenses
- 19.10.1. Aspectos importantes de un Informe forense
- 19.10.2. Clasificación y tipos de informes
- 19.10.3. Guía para escribir un informe
- 19.10.4. Presentación del informe
  - 19.10.4.1. Preparación previa para testificar
  - 19.10.4.2. Deposición
  - 19.10.4.3. Trato con los medios

Módulo 20. Retos actuales y futuros en seguridad informática

20.1. Tecnología *blockchain*
- 20.1.1. Ámbitos de aplicación
- 20.1.2. Garantía de confidencialidad
- 20.1.3. Garantía de no-repudio

20.2. Dinero digital
- 20.2.1. Bitcoins
- 20.2.2. Critpomonedas
- 20.2.3. Minería de criptomonedas
- 20.2.4. Estafas piramidales
- 20.2.5. Otros potenciales delitos y problemas

20.3. *Deepfake*
- 20.3.1. Impacto en los medios
- 20.3.2. Peligros para la sociedad
- 20.3.3. Mecanismos de detección

20.4. El futuro de la inteligencia artificial
- 20.4.1. Inteligencia artificial y computación cognitiva
- 20.4.2. Usos para simplificar el servicio a clientes

20.5. Privacidad digital
- 20.5.1. Valor de los datos en la red
- 20.5.2. Uso de los datos en la red
- 20.5.3. Gestión de la privacidad e identidad digital

20.6. Ciberconflictos, cibercriminales y ciberataques
- 20.6.1. Impacto de la ciberseguridad en conflictos internacionales
- 20.6.2. Consecuencias de ciberataques en la población general
- 20.6.3. Tipos de cibercriminales. Medidas de protección

20.7. Teletrabajo
- 20.7.1. Revolución del teletrabajo durante y post Covid19
- 20.7.2. Cuellos de botella en el acceso
- 20.7.3. Variación de la superficie de ataque
- 20.7.4. Necesidades de los trabajadores

20.8. Tecnologías *wireless* emergentes
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Ondas milimétricas
- 20.8.4. Tendencia en *Get Smart* en vez de *Get more*

20.9. Direccionamiento futuro en redes
- 20.9.1. Problemas actuales con el direccionamiento IP
- 20.9.2. IPv6
- 20.9.3. IPv4+
- 20.9.4. Ventajas de IPv4+ sobre IPv4
- 20.9.5. Ventajas de IPv6 sobre IPv4

20.10. El reto de la concienciación de la formación temprana y continua de la población
- 20.10.1. Estrategias actuales de los gobiernos
- 20.10.2. Resistencia de la población al aprendizaje
- 20.10.3. Planes de formación que deben adoptar las empresas

Aprenderás a través de casos reales diseñados en entornos simulados de aprendizaje que reflejan los desafíos actuales en la gestión de datos y ciberseguridad”

04

Objetivos docentes

El objetivo principal del Grand Master en Secure Information Management es proporcionar a los alumnos conocimientos de excelencia en dos áreas fundamentales y complementarias de la informática y las ingenierías: la gestión de datos en entornos digitales y la ciberseguridad. Este programa combina ambas disciplinas para capacitar a profesionales en la implementación de soluciones avanzadas, permitiéndoles afrontar desafíos laborales con las herramientas necesarias para administrar y proteger información sensible en sus organizaciones.

Transforma tu carrera profesional con este Grand Master innovador, diseñado para marcar un antes y un después en tu especialización en gestión de datos y ciberseguridad"

Objetivos generales

- Desarrolla conocimientos avanzados en analítica de datos y ciberseguridad para optimizar procesos empresariales con herramientas y técnicas innovadora
- Implementa estrategias de seguridad efectivas para prevenir amenazas digitales en sistemas, redes y dispositivos móviles
- Resuelve desafíos en ciberseguridad mediante auditorías, ingeniería inversa y análisis forense basado en pruebas
- Anticipa tendencias tecnológicas aplicando soluciones disruptivas que protejan activos digitales y sistemas avanzados

Lidera la gestión de datos y ciberseguridad en el entorno digital con este programa de especialización"

Objetivos específicos

Módulo 1. Analítica del dato en la organización empresarial

- Desarrollar competencias en la utilización de técnicas de análisis de datos
- Generar información valiosa que impulse la toma de decisiones estratégicas en las organizaciones empresariales, mejorando la eficiencia y la competitividad

Módulo 2. Gestión, manipulación de datos e información para Ciencia de Datos

- Capacitar en la gestión y manipulación eficiente de grandes volúmenes de datos
- Aplicar metodologías y herramientas para estructurar, limpiar y transformar datos en información útil para proyectos de ciencia de datos

Módulo 3. Dispositivos y plataformas IoT como base para la Ciencia de Datos

- Proporcionar los conocimientos necesarios sobre las plataformas y dispositivos de Internet de las Cosas y su integración en la ciencia de datos
- Ahonda en la captura, procesamiento y análisis de datos en tiempo real

Módulo 4. Representación gráfica para análisis de datos

- Representar gráficamente los datos mediante herramientas y técnicas avanzadas de visualización
- Facilitar la comprensión de patrones, tendencias y relaciones dentro de grandes conjuntos de datos

Módulo 5. Herramientas de ciencia de datos

- Capacitar en el uso de herramientas y software específicos de ciencia de datos, como Python
- Ahondar en la recolección, análisis y presentación de datos en diversos contextos profesionales

Módulo 6. Minería de datos. Selección, preprocesamiento y transformación

- Proporcionar los conocimientos y habilidades necesarios para aplicar técnicas de minería de datos
- Analizar la selección, el preprocesamiento y la transformación de datos para extraer patrones y tendencias significativas

Módulo 7. Predictibilidad y análisis de fenómenos estocásticos

- Desarrollar competencias en la modelización y análisis de fenómenos estocásticos
- Utilizar métodos estadísticos avanzados para predecir comportamientos y tendencias en entornos inciertos y dinámicos

Módulo 8. Diseño y desarrollo de sistemas inteligentes

- Capacitar en el diseño y desarrollo de sistemas inteligentes, integrando técnicas de aprendizaje automático e inteligencia artificial
- Crear soluciones automáticas que resuelvan problemas complejos de manera eficiente

Módulo 9. Arquitecturas y sistemas para uso intensivo de datos

- Brindar conocimientos sobre la creación de arquitecturas de sistemas capaces de procesar grandes volúmenes de datos de manera eficiente
- Utilizar tecnologías avanzadas como bases de datos distribuidas y procesamiento paralelo

Módulo 10. Aplicación práctica de la ciencia de datos en sectores de actividad empresarial

- Desarrollar la capacidad de aplicar prácticas de ciencia de datos en diversos sectores empresariales
- Integrar los conocimientos adquiridos para mejorar la toma de decisiones, la optimización de procesos y la innovación en la empresa

Módulo 11. Ciberinteligencia y ciberseguridad
- Proporcionar los conocimientos y habilidades necesarios para aplicar técnicas de ciberinteligencia y ciberseguridad
- Proteger los sistemas y redes empresariales frente a amenazas cibernéticas y asegurando la integridad de los datos

Módulo 12. Seguridad en Host
- Capacitar en la implementación de medidas de seguridad en sistemas host
- Asegurar la protección de servidores y aplicaciones críticas mediante el uso de herramientas y buenas prácticas de seguridad informática

Módulo 13. Seguridad en red (perimetral)
- Brindar conocimientos sobre la protección de redes y sistemas informáticos a nivel perimetral
- Manejar cortafuegos, VPNs y otras herramientas para garantizar la seguridad en la infraestructura de red de la empresa

Módulo 14. Seguridad en smartphones
- Desarrollar competencias para asegurar la seguridad en dispositivos móviles
- Comprender las vulnerabilidades comunes y aplicando medidas preventivas para proteger la información y las aplicaciones en smartphone

Módulo 15. Seguridad en IoT
- Proporcionar los conocimientos necesarios para implementar soluciones de seguridad en dispositivos IoT
- Proteger redes y sistemas que interconectan dispositivos y garantizando la confidencialidad e integridad de los datos generados

Módulo 16. Hacking ético
- Capacitar en las prácticas de hacking ético, enseñando a realizar pruebas de penetración controladas
- Identificar vulnerabilidades en los sistemas informáticos para mejorar la seguridad antes de que puedan ser explotadas por atacantes

Módulo 17. Ingeniería inversa
- Brindar conocimientos sobre técnicas de ingeniería inversa, permitiendo analizar y comprender el funcionamiento de software y hardware
- Detectar fallos de seguridad o mejorar la funcionalidad de los sistemas existentes

Módulo 18. Desarrollo seguro
- Capacitar en el desarrollo de software seguro, enseñando buenas prácticas de codificación y seguridad durante el ciclo de vida del software
- Ser capaz de prevenir vulnerabilidades y proteger los sistemas informáticos contra ataques

Módulo 19. Análisis forense
- Desarrollar las habilidades necesarias para llevar a cabo investigaciones forenses digitales
- Utilizar herramientas y técnicas avanzadas para recuperar, analizar y preservar pruebas electrónicas en incidentes de seguridad informática

Módulo 20. Retos actuales y futuros en seguridad informática
- Explorar los desafíos actuales y futuros en el campo de la seguridad informática, analizando las amenazas emergentes y las nuevas tecnologías de protección
- Ahondar en las estrategias para mitigar los riesgos en un entorno tecnológico en constante cambio

05

Salidas profesionales

Tras finalizar este Grand Master en Secure Information Management, los profesionales habrán adquirido una comprensión sólida de las estrategias más avanzadas en ciberseguridad y gestión de datos digitales. Los egresados estarán preparados para diseñar e implementar soluciones que garanticen la protección de la información sensible y optimicen los procesos de análisis y toma de decisiones en entornos empresariales. De esta forma, mejorarán sus perspectivas laborales y asumirán roles especializados como analistas de ciberseguridad, consultores de inteligencia o gestores de datos críticos.

Garantizarás la seguridad de los activos digitales y serás clave en la transformación digital de las organizaciones”

Perfil del egresado

El egresado del Grand Master en Secure Information Management será un profesional altamente capacitado para gestionar y proteger información en entornos digitales. Poseerá un conocimiento avanzado en áreas como ciberseguridad, inteligencia digital y análisis de datos, además de habilidades prácticas en el diseño e implementación de estrategias de defensa ante amenazas. Su perfil combina un entendimiento técnico profundo con competencias estratégicas que le permitirán liderar proyectos en sectores empresariales clave.

Te convertirás en un líder en la protección de datos y la ciberseguridad, colaborando con empresas para afrontar los retos del entorno digital.

- **Gestión de la seguridad:** Desarrollar la capacidad de identificar riesgos, implementar estrategias de defensa multicapa y garantizar la confidencialidad, integridad y disponibilidad de los datos
- **Análisis crítico y resolución de problemas:** Aplicarás técnicas avanzadas para evaluar sistemas, detectar vulnerabilidades y diseñar soluciones adaptadas a diferentes entornos tecnológicos
- **Competencia técnica y digital:** Manejarás herramientas avanzadas de análisis de datos, ciberseguridad y sistemas de inteligencia, permitiéndote liderar proyectos de innovación tecnológica
- **Pensamiento estratégico:** Diseñarás políticas de seguridad y estrategias empresariales que respondan a las demandas actuales y futuras del entorno digital
- **Colaboración interdisciplinaria:** Trabajarás con equipos multidisciplinarios para abordar desafíos complejos y garantizar la seguridad en redes, plataformas IoT y dispositivos móviles

Después de realizar el Grand Master, podrás desempeñar tus conocimientos y habilidades en los siguientes cargos:

1. **Director de Ciberseguridad:** Líder encargado de coordinar equipos y diseñar estrategias para proteger activos digitales en grandes organizaciones
2. **Analista de Datos:** Diseñador de análisis predictivos y sistemas de visualización para optimizar la toma de decisiones
3. **Consultor en Inteligencia Digital:** Asesor especializado en ofrecer soluciones avanzadas basadas en inteligencia y análisis de riesgos
4. **Especialista en IoT y Seguridad:** Diseñador de medidas de protección para dispositivos conectados y entornos industriales
5. **Hacker Ético:** Evaluador de vulnerabilidades que corrige fallos en sistemas empresariales para prevenir ciberataques
6. **Auditor de Seguridad:** Inspector que realiza auditorías y análisis forenses para garantizar el cumplimiento normativo
7. **Gestor de Datos Empresariales:** Administrador responsable de diseñar y gestionar sistemas de almacenamiento y análisis para mejorar la eficiencia operativa

Completa este programa y destaca como especialista en las áreas más demandadas del entorno digital"

06

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.

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 según el índice global score, 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.

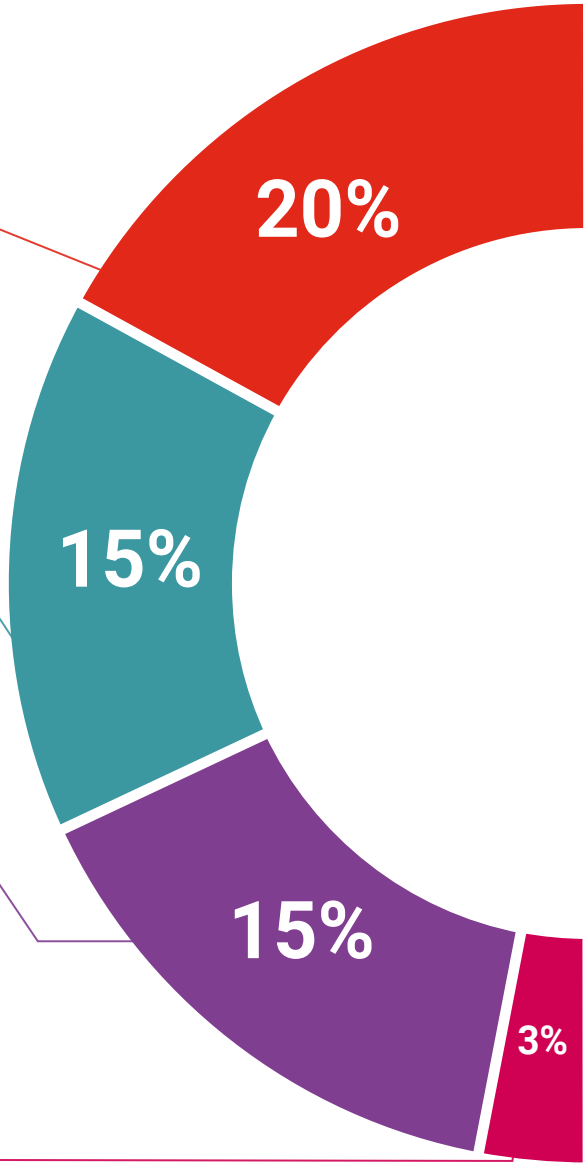
Resúmenes interactivos

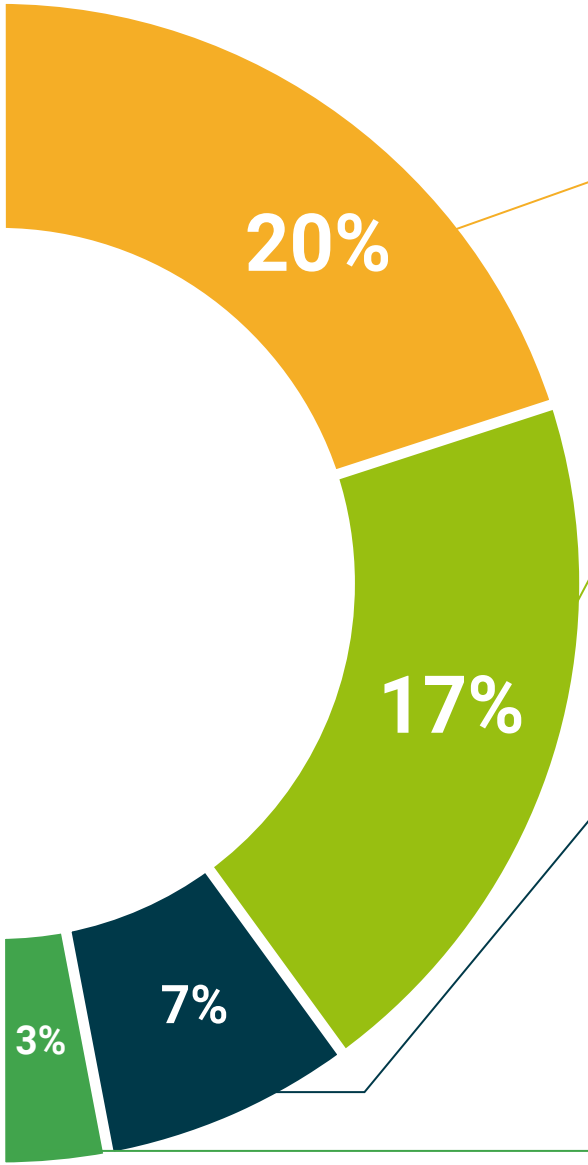
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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.

07

Cuadro docente

Esta titulación está impartida por destacados profesionales en ciberseguridad y gestión digital de datos. Su experiencia asegura que los alumnos reciban contenidos completos y actualizados, aplicables directamente en sus carreras. Así, los docentes de este Grand Master en Secure Information Management comparten sus conocimientos, formando especialistas altamente cualificados y demandados por grandes compañías a nivel internacional.

Triunfa de la mano de los mejores y adquiere los conocimientos y competencias clave para liderar en la gestión de datos y ciberseguridad en el entorno digital"

Director Invitado Internacional

El Doctor Frederic Lemieux es reconocido a nivel internacional como experto innovador y líder inspirador en los campos de la **Inteligencia**, **Seguridad Nacional, Seguridad Interna, Ciberseguridad** y **Tecnologías Disruptivas.** Y es que su constante dedicación y relevantes aportaciones en Investigación y Educación, le posicionan como una figura clave en la promoción de la seguridad y el entendimiento de las tecnologías emergentes en la actualidad. Durante su trayectoria profesional, ha conceptualizado y dirigido programas académicos de vanguardia en diversas instituciones de renombre, como la **Universidad de Montreal**, la **Universidad George Washington** y la **Universidad de Georgetown**.

A lo largo de su extenso bagaje, ha publicado múltiples libros de gran relevancia, todos ellos relacionados con la **inteligencia criminal, la labor policial, las amenazas cibernéticas y la seguridad internacional.** Asimismo, ha contribuido de manera significativa al campo de la Ciberseguridad con la publicación de numerosos artículos en revistas académicas, las cuales examinan el control del crimen durante desastres importantes, la lucha contra el terrorismo, las agencias de inteligencia y la cooperación policial. Además, ha sido panelista y ponente principal en diversas conferencias nacionales e internacionales, consolidándose como un referente en el ámbito académico y profesional.

El Doctor Lemieux ha desempeñado roles editoriales y evaluativos en diferentes organizaciones académicas, privadas y gubernamentales, reflejando su influencia y compromiso con la excelencia en su campo de especialización. De esta forma, su prestigiosa carrera académica lo ha llevado a desempeñarse como Profesor de Prácticas y Director de Facultad de los programas MPS en **Inteligencia Aplicada, Gestión de Riesgos en Ciberseguridad, Gestión Tecnológica y Gestión de Tecnologías de la Información**, en la **Universidad de Georgetown.**

Dr. Lemieux, Frederic

- Director del Máster en Cybersecurity Risk Management en Georgetown, Washington, Estados Unidos
- Director del Máster en Technology Management en la Universidad de Georgetown
- Director del Máster en Applied Intelligence en la Universidad de Georgetown
- Profesor de Prácticas en la Universidad de Georgetown
- Doctor en Criminología por la School of Criminology en la Universidad de Montreal
- Licenciado en Sociología y Minor Degree en Psicología por la Universidad de Laval
- Miembro de: New Program Roundtable Committee, Universidad de Georgetown

Gracias a TECH podrás aprender con los mejores profesionales del mundo"

Dirección

Dr. Peralta Martín-Palomino, Arturo

- CEO y CTO en Prometeus Global Solutions
- CTO en Korporate Technologies
- CTO en AI Shepherds GmbH
- Consultor y Asesor Estratégico Empresarial en Alliance Medical
- Director de Diseño y Desarrollo en DocPath
- Doctor en Ingeniería Informática por la Universidad de Castilla-La Mancha
- Doctor en Economía, Empresas y Finanzas por la Universidad Camilo José Cela
- Doctor en Psicología por la Universidad de Castilla-La Mancha
- Máster en Executive MBA por la Universidad Isabel I
- Máster en Dirección Comercial y Marketing por la Universidad Isabel I
- Máster Experto en Big Data por Formación Hadoop
- Máster en Tecnologías Informáticas Avanzadas por la Universidad de Castilla-La Mancha
- Miembro de Grupo de Investigación SMILE

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. Montoro Montarroso, Andrés

- Investigador en el grupo SMILe de la Universidad de Castilla-La Mancha
- Investigador en la Universidad de Granada
- Científico de Datos en Prometeus Global Solutions
- Vicepresidente y Software Developer en CireBits
- Doctorado en Tecnologías Informáticas Avanzadas por la Universidad de Castilla-La Mancha
- Graduado en Ingeniería Informática por la Universidad de Castilla-La Mancha
- Máster en Ciencia de Datos e Ingeniería de Computadores por la Universidad de Granada
- Profesor invitado en la asignatura de Sistemas Basados en el Conocimiento de la Escuela Superior de Informática de Ciudad Real, impartiendo la conferencia: *Técnicas Avanzadas de Inteligencia Artificial: Búsqueda y análisis de potenciales radicales en Medios Sociales*
- Profesor invitado en la asignatura de Minería de Datos de la Escuela Superior de Informática de Ciudad Real, impartiendo la conferencia: *Aplicaciones del Procesamiento de Lenguaje Natural: Lógica borrosa al análisis de mensajes en redes sociales*
- Ponente en el Seminario sobre Prevención de la Corrupción en Administraciones Públicas e Inteligencia Artificial de la Facultad de Ciencias Jurídicas y Sociales de Toledo, impartiendo la conferencia: *Técnicas de Inteligencia Artificial*
- Ponente en el primer Seminario Internacional de Derecho Administrativo e Inteligencia Artificial (DAIA). Organizada por el Centro de Estudios Europeos Luis Ortega Álvarez y el Institut de Recerca TransJus. Conferencia titulada *Análisis de Sentimientos para la prevención de mensajes de odio en las redes sociales*

D. Peris Morillo, Luis Javier

- Senior Technical Lead y Delivery Lead Support en HCL Technologies
- Redactor técnico en Baeldung
- Agile Coach y director de Operaciones en Mirai Advisory
- Desarrollador, Team Lead, Scrum Master, Agile Coach y Product Manager en DocPath
- Tecnólogo en ARCO
- Graduado en Ingeniería Superior en Informática por la Universidad de Castilla-La Mancha
- Posgraduado en Gestión de proyectos por la CEOE

Dña. Fernández Meléndez, Galina

- Especialista en Big Data
- Analista de Datos en Aresi Gestión de Fincas
- Analista de Datos en ADN Mobile Solution
- Licenciada en Administración de Empresas por la Universidad Bicentenaria de Aragua. Caracas, Venezuela
- Diplomada en Planificación y Finanzas Públicas por la Escuela Venezolana de Planificación
- Máster en Análisis de Datos e Inteligencia de Negocio por la Universidad de Oviedo
- MBA en Administración y Dirección de Empresas por la Escuela de Negocios Europea de Barcelona
- Máster en Big Data y Business Intelligence por la Escuela de Negocios Europea de Barcelona

Dña. Pedrajas Perabá, María Elena

- New Technologies and Digital Transformation Consultant en Management Solutions
- Investigadora en el Departamento de Informática y Análisis Numérico en la Universidad de Córdoba
- Investigadora en el Centro Singular de Investigación en Tecnologías Inteligentes en Santiago de Compostela
- Licenciada en Ingeniería Informática por la Universidad de Córdoba
- Máster en Ciencia de Datos e Ingeniería de Computadores por la Universidad de Granada
- Máster en Consultoría de Negocio por la Universidad Pontificia Comillas

Dña. Martínez Cerrato, Yésica

- Responsable de Capacitaciones Técnicas en Securitas Seguridad España
- Especialista en Educación, Negocios y Marketing
- *Product Manager* en Seguridad Electrónica en Securitas Seguridad España
- Analista de Inteligencia Empresarial en Ricopia Technologies
- Técnico Informático y Responsable de Aulas informáticas OTEC en la Universidad de Alcalá de Henares
- Colaboradora en la Asociación ASALUMA
- Grado en Ingeniería Electrónica de Comunicaciones en la Escuela Politécnica Superior, Universidad de Alcalá de Henares

D. Fondón Alcalde, Rubén

- Analista EMEA de Amazon Web Services
- Analista de Negocio en Gestión del Valor del Cliente en Vodafone España
- Jefe de Integración de Servicios en Entelgy para Telefónica Global Solutions
- Administrador de Cuentas en Línea de Servidores Clónicos en EDM Electronics
- Gerente de Implementación de Servicios Internacionales en Vodafone Global Enterprise
- Consultor de Soluciones para España y Portugal en Telvent Global Services
- Analista de Negocios para el sur de Europa en Vodafone Global Enterprise
- Ingeniero de Telecomunicaciones por la Universidad Europea de Madrid
- Máster en Big Data y Analytics por la Universidad Internacional de Valencia

D. Díaz Díaz-Chirón, Tobías

- Investigador en el laboratorio ArCO de la Universidad de Castilla-La Mancha
- Consultor en Blue Telecom
- Freelance dedicado principalmente al sector de las telecomunicaciones, especializado en redes 4G/5G
- OpenStack: deploy and administration
- Ingeniero Superior en Informática por la Universidad de Castilla-La Mancha
- Especialización en Arquitectura y redes de computadores
- Profesor asociado en la Universidad de Castilla-La Mancha
- Ponente en curso del Sepecam sobre administración de redes

D. Tato Sánchez, Rafael

- Director Técnico en Indra Sistemas SA
- Ingeniero de Sistemas en ENA TRÁFICO SAU
- Máster en Industria 4.0. por la Universidad en Internet
- Máster en Ingeniería Industrial por la Universidad Europea
- Grado en Ingeniería en Electrónica Industrial y Automática por la Universidad Europea
- Ingeniero Técnico Industrial por la Universidad Politécnica de Madrid

Dña. Marcos Sbarbaro, Victoria Alicia

- Desarrolladora de Aplicaciones Móviles Android Nativas en B60. UK
- Analista Programadora para la Gestión, Coordinación y Documentación del Entorno Virtualizado de Alarmas de Seguridad
- Analista Programadora de Aplicaciones Java para cajeros automáticos
- Profesional del Desarrollo de *Software* para Aplicación de Validación de Firma y Gestión Documental
- Técnico de Sistemas para la Migración de Equipos y para la Gestión, Mantenimiento y Formación de Dispositivos Móviles PDA
- Ingeniero Técnico de Informática de Sistemas por la Universidad Oberta de Cataluña
- Máster en Seguridad Informática y Hacking Ético Oficial de EC- Council y CompTIA por la Escuela Profesional de Nuevas Tecnologías CICE

D. Catalá Barba, José Francisco

- Técnico Electrónico Experto en Ciberseguridad
- Desarrollador de Aplicaciones para Dispositivos Móviles
- Técnico Electrónico en Mando Intermedio en el Ministerio de la Defensa de España
- Técnico Electrónico en Factoría Ford Sita en Valencia

D. Armero Fernández, Rafael

- Business Intelligence Consultant en SDG Group
- Digital Engineer en MI-GSO
- Logistic Engineer en Torrecid SA
- Quality Intern en INDRA
- Graduado en Ingeniería Aeroespacial por la Universidad Politécnica de Valencia
- Máster en Professional Development 4.0 por la Universidad de Alcalá

D. Peralta Alonso, Jon

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

D. Redondo, Jesús Serrano

- Desarrollador Web y Técnico en Ciberseguridad
- Desarrollador Web en Roams, Palencia
- Desarrollador FrontEnd en Telefónica, Madrid
- Desarrollador FrontEnd en Best Pro Consulting SL, Madrid
- Instalador de Equipos y Servicio de Telecomunicaciones en Grupo Zener, Castilla y León
- Instalador de Equipos y Servicios de Telecomunicaciones en Lican Comunicaciones SL, Castilla y León
- Certificado en Seguridad Informática por CFTIC Getafe, Madrid
- Técnico Superior en Sistemas Telecomunicaciones e Informáticos por IES Trinidad Arroyo, Palencia
- Técnico Superior en Instalaciones Electrotécnicas MT y BT por IES Trinidad Arroyo, Palencia
- Formación en Ingeniería Inversa, Estenografía y Cifrado por la Academia Hacker Incibe

D. Jiménez Ramos, Álvaro

- Analista de Ciberseguridad
- Analista de Seguridad Sénior en The Workshop
- Analista de Ciberseguridad L1 en Axians
- Analista de Ciberseguridad L2 en Axians
- Analista de Ciberseguridad en SACYR S.A.
- Grado en Ingeniería Telemática por la Universidad Politécnica de Madrid
- Máster de Ciberseguridad y Hacking Ético por CICE
- Curso Superior de Ciberseguridad por Deusto Formación

Aprovecha la oportunidad para conocer los últimos avances en esta materia para aplicarla a tu práctica diaria"

08
Titulación

El Grand Master en Secure Information Management garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Grand Master expedido por TECH Global University.

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

Este programa te permitirá obtener el título propio de **Grand Master en Secure Information Management** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra (***boletín oficial***). Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio. El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

Título: **Grand Master en Secure Information Management**

Modalidad: **online**

Duración: **2 años**

Acreditación: **120 ECTS**


tech global university

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

Grand Master en Secure Information Management

Se trata de un título propio de 3.600 horas de duración equivalente a 120 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


Grand Master en Secure Information Management

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	Analítica del dato en la organización empresarial	6	OB
1º	Gestión, Manipulación de datos e información para Ciencia de Datos	6	OB
1º	Dispositivos y plataformas IoT como base para la Ciencia de Datos	6	OB
1º	Representación gráfica para análisis de datos	6	OB
1º	Herramientas de ciencia de datos	6	OB
1º	Minería de Datos. Selección, preprocesamiento y transformación	6	OB
1º	Predictibilidad y análisis de fenómenos estocásticos	6	OB
1º	Diseño y desarrollo de sistemas inteligentes	6	OB
1º	Arquitecturas y sistemas para uso intensivo de datos	6	OB

Curso	Materia	ECTS	Carácter
2º	Aplicación práctica de la ciencia de datos en sectores de actividad empresarial	6	OB
2º	Ciberinteligencia Y Ciberseguridad	6	OB
2º	Seguridad en host	6	OB
2º	Seguridad en red (perimetral)	6	OB
2º	Seguridad en smartphones	6	OB
2º	Seguridad en IoT	6	OB
2º	Hacking ético	6	OB
2º	Ingeniería inversa	6	OB
2º	Desarrollo seguro	6	OB
2º	Análisis forense	6	OB
2º	Retos actuales y futuros en seguridad informática	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

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

tech global university

Grand Master
Secure Information Management

- Modalidad: **online**
- Duración: **2 años**
- Titulación: **TECH Global University**
- Acreditación: **120 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Grand Master

Secure Information Management

tech global university