Grand Master

Alta Dirección de Ciberseguridad



tech universidad tecnológica



tech universidad tecnológica

Grand Master

Alta Dirección de Ciberseguridad

Modalidad: **Online**
Duración: **2 años**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **3.000 h.**
Acceso web: **www.techtitute.com/informatica/grand-master/grand-master-alta-direccion-ciberseguridad**

Índice

01 Presentación — pág. 4

02 Objetivos — pág. 8

03 Competencias — pág. 16

04 Dirección del curso — pág. 20

05 Estructura y contenido — pág. 28

06 Metodología — pág. 48

07 Titulación — pág. 56

01

Presentación

En el mundo actual, la ciberseguridad es un elemento fundamental para individuos y empresas, que están más expuestas que nunca a ataques. Esto se debe al continuo desarrollo de nuevas tecnologías y al proceso de digitalización, que ha producido transformaciones en todo tipo de compañías, agilizando numerosas actividades pero, también, provocando la aparición de nuevas vulnerabilidades. Por esa razón, uno de los perfiles más buscados en la actualidad es el del director de ciberseguridad, una figura en auge que dispone de numerosas oportunidades profesionales. Este programa ahonda en esta figura, y prepara al informático para abordar, de forma eficaz y completa, todos los retos actuales en este ámbito, donde se requieren, además, habilidades directivas y una perspectiva empresarial. Además, la titulación se desarrolla en un formato 100% online, por lo que es perfecta para compaginarla con el trabajo, permitiendo al profesional estudiar cuando lo desee.





Este programa te preparará para afrontar todos los retos del presente y del futuro en el ámbito de la ciberseguridad, permitiéndote especializarte en la dirección en esta importante área de la informática"

Procesos bancarios, compras por internet, comunicaciones internas en diferentes organizaciones, trámites administrativos... En la actualidad, la digitalización ha transformado la forma en que individuos y empresas operan a diario. Ha agilizado numerosas actividades, ha permitido que no sea necesario realizar determinados desplazamientos, mejorando la calidad de vida de la población y ahorrando costes a las compañías. Sin embargo, esas ventajas han traído, de forma colateral, otras desventajas en materia de ciberseguridad.

Muchas de las tecnologías y herramientas digitales que se emplean en la actualidad están en continuo desarrollo, por lo que están expuestas a ataques. Al haberse generalizado el uso de aplicaciones y dispositivos digitales, un fallo en ellos es crítico, ya que puede afectar al desarrollo de la organización, no sólo en cuanto a comercialización y ventas, sino en su propio funcionamiento interno, que también depende de estas utilidades.

Por esa razón, las empresas necesitan expertos en ciberseguridad que puedan dar respuesta a los diferentes problemas que pueden surgir en este ámbito. Uno de los perfiles más buscados es el de Director de Ciberseguridad, un cargo que conlleva una visión global de esta área, y para el que este Grand Master prepara de forma completa. Así, este programa supone una gran oportunidad para el informático, puesto que le acercará todas las novedades en este ámbito, preparándole, al mismo tiempo, para afrontar decisiones de carácter directivo, que necesitan de los mejores conocimientos y de habilidades de liderazgo.

Todo ello, a partir de una metodología de aprendizaje en línea que se adaptará a las circunstancias profesionales del alumno, mientras es acompañado por un cuadro docente de gran prestigio en esta área de la informática. Asimismo, tendrá a su disposición la mejor tecnología educativa y los recursos didácticos más novedosos: resúmenes interactivos, vídeos, clases magistrales, análisis de casos o lecturas complementarias.

Este **Grand Master en Alta Dirección de Ciberseguridad** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en informática y ciberseguridad
- 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 ciberseguridad
- 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

Con este Grand Master podrás profundizar en la seguridad en el IoT, en el cloud computing, el blockchain y aprenderás a hacer auditorías de alto nivel a todo tipo de empresas y organizaciones”

La dirección de ciberseguridad es un perfil profesional en auge y este programa te ofrece la opción, a partir de la metodología online de TECH, de acceder a las mejores oportunidades en este ámbito”

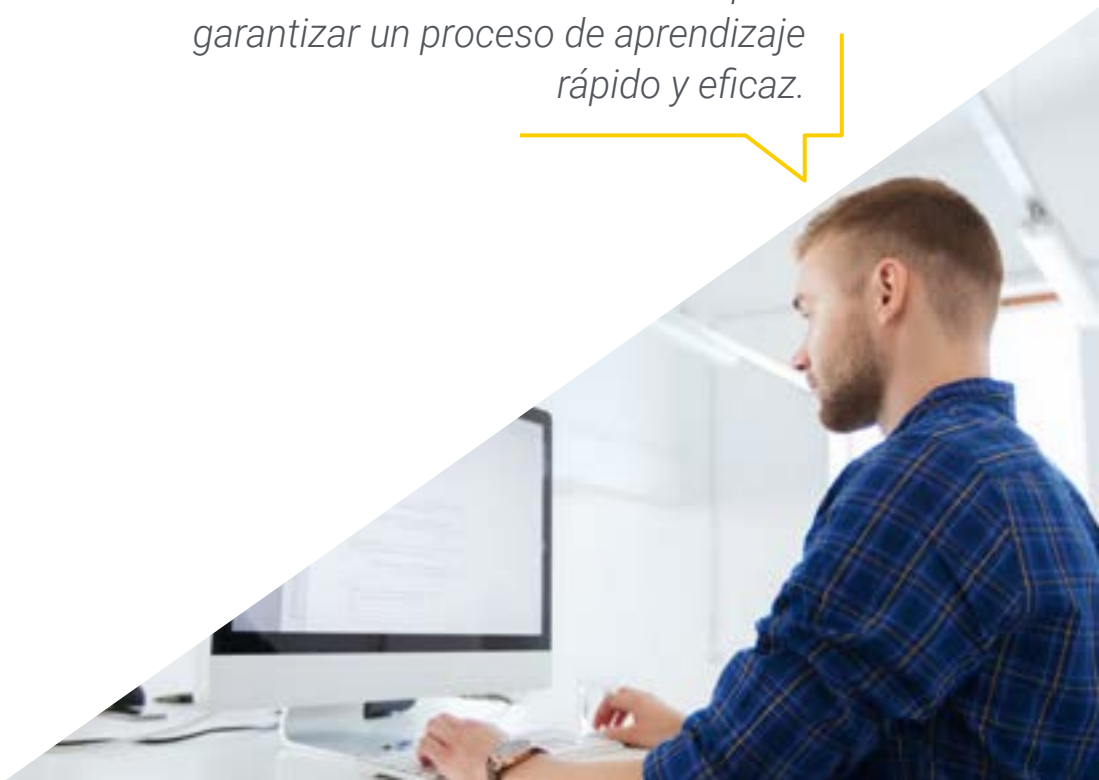
Disfrutarás del acompañamiento de un cuadro docente de gran prestigio, quienes se asegurarán de que obtienes todas las claves en el ámbito de la dirección de ciberseguridad.

Tendrás a tu disposición los recursos didácticos más novedosos para garantizar un proceso de aprendizaje rápido y eficaz.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la ciberseguridad 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

Objetivos

El objetivo principal de este Grand Máster es convertir al informático en un gran especialista en este ámbito, permitiéndole acceder a las mejores oportunidades profesionales. Y, para ello, no sólo abundará en las todas las novedades en el ámbito de la ciberseguridad, sino que le proporcionará las mejores herramientas para obtener una perspectiva global de las necesidades empresariales en este ámbito. Así, podrá trabajar dirigiendo la seguridad de compañías de todo tiempo, al conocer los mejores métodos para proceder en cada caso.





Este Grand Master te ayudará a conseguir el progreso profesional que buscas, gracias a sus contenidos amplios y actualizados, y a su prestigioso profesorado compuesto por expertos en ciberseguridad en activo"

Objetivos generales

- Analizar el rol del analista en ciberseguridad
- Profundizar en la ingeniería social y sus métodos
- Examinar las metodologías OSINT, HUMINT, OWASP, PTEC. OSSTM, OWISAM
- Realizar un análisis de riesgo y conocer las métricas de riesgo
- Determinar el adecuado uso de anonimato y uso de redes como TOR, I2P y Freenet
- Compilar las normativas vigentes en materia de ciberseguridad
- Generar conocimiento especializado para realizar una Auditoría de Seguridad
- Desarrollar políticas de uso apropiadas
- Examinar los sistemas de detección y prevención de las amenazas más importantes
- Evaluar nuevos sistemas de detección de amenazas, así como su evolución respecto a soluciones más tradicionales
- Analizar las principales plataformas móviles actuales, características y uso de las mismas
- Identificar, analizar y evaluar riesgos de seguridad de las partes del proyecto IoT
- Evaluar la información obtenida y desarrollar mecanismos de prevención y hacking
- Aplicar la Ingeniería Inversa al entorno de la ciberseguridad
- Concretar las pruebas que hay que realizar al software desarrollado
- Recopilar todas las pruebas y datos existentes para llevar a cabo un informe forense
- Presentar debidamente el informe forense
- Analizar el estado actual y futuro de la seguridad informática
- Examinar los riesgos de las nuevas tecnologías emergentes
- Compilar las distintas tecnologías en relación a la seguridad informática
- Generar conocimiento especializado sobre un sistema de información, tipos y aspectos de seguridad que deben ser tenidos en cuenta
- Identificar las vulnerabilidades de un sistema de información
- Desarrollar la normativa legal y tipificación del delito atacando a un sistema de información
- Evaluar los diferentes modelos de arquitectura de seguridad para establecer el modelo más adecuado a la organización
- Identificar los marcos normativos de aplicación y las bases reguladoras de los mismos
- Analizar la estructura organizativa y funcional de un área de seguridad de la información (la oficina del CISO)
- Analizar y desarrollar el concepto de riesgo, incertidumbre dentro del entorno en que vivimos
- Examinar el Modelo de Gestión de Riesgos basado en la Iso 31.000
- Examinar la ciencia de la criptología y la relación con sus ramas: criptografía, criptoanálisis, esteganografía y estegoanálisis
- Analizar los tipos de criptografía según el tipo de algoritmo y según su uso
- Examinar los certificados digitales
- Examinar la Infraestructura de Clave Pública (PKI)
- Desarrollar el concepto de gestión de identidades
- Identificar los métodos de autenticación
- Generar conocimiento especializado sobre el ecosistema de seguridad informática
- Evaluar el conocimiento en término de ciberseguridad
- Identificar los ámbitos de seguridad en *cloud*
- Analizar los servicios y herramientas en cada uno de los ámbitos de seguridad
- Desarrollar las especificaciones de seguridad de cada tecnología LPWAN
- Analizar de forma comparativa la seguridad de las tecnologías LPWAN



Objetivos específicos

- Desarrollar las metodologías usadas en materia de ciberseguridad
- Examinar el ciclo de inteligencia y establecer su aplicación en la ciberinteligencia
- Determinar el papel del analista de inteligencia y los obstáculos de actividad evacuativa
- Analizar las metodologías OSINT, OWISAM, OSSTM, PTES, OWASP
- Establecer las herramientas más comunes para la producción de inteligencia
- Llevar a cabo un análisis de riesgos y conocer las métricas usadas
- Concretar las opciones de anonimato y el uso de redes como TOR, I2P, FreeNet
- Detallar las Normativas vigentes en ciberseguridad
- Concretar las políticas de *backup* de los datos de personales y profesionales
- Valorar las diferentes herramientas para dar soluciones a problemas específicos de seguridad
- Establecer mecanismos para tener un sistema actualizado
- Analizar el equipo para detectar intrusos
- Determinar las reglas de acceso al sistema
- Examinar y clasificar los correos para evitar fraudes
- Generar listas de software permitido
- Analizar las arquitecturas actuales de red para identificar el perímetro que debemos proteger
- Desarrollar las configuraciones concretas de firewall y en Linux para mitigar los ataques más comunes
- Compilar las soluciones más usadas como Snort y Suricata, así como su configuración
- Examinar las diferentes capas adicionales que proporcionan los firewalls de nueva generación y funcionalidades de red en entornos *cloud*
- Determinar las herramientas para la protección de la red y demostrar por qué son fundamentales para una defensa multicapa
- Examinar los distintos vectores de ataque para evitar convertirse en un blanco fácil
- Determinar los principales ataques y tipos de malware a los que se exponen los usuarios de dispositivos móviles
- Analizar los dispositivos más actuales para establecer una mayor seguridad en la configuración
- Concretar los pasos principales para realizar una prueba de penetración tanto en plataformas iOS como en plataformas Android
- Desarrollar conocimiento especializado sobre las diferentes herramientas de protección y seguridad
- Establecer buenas prácticas en programación orientadas a dispositivos móviles
- Analizar las principales arquitecturas de IoT
- Examinar las tecnologías de conectividad
- Desarrollar los protocolos de aplicación principales
- Concretar los diferentes tipos de dispositivos existentes
- Evaluar los niveles de riesgo y vulnerabilidades conocidas
- Desarrollar políticas de uso seguras
- Establecer las condiciones de uso apropiadas para estos dispositivos
- Examinar los métodos de IOSINT
- Recopilar la información disponible en medios públicos
- Escanear redes para obtener información de modo activo
- Desarrollar laboratorios de pruebas

- Analizar las herramientas para el desempeño del *pentesting*
- Catalogar y evaluar las diferentes vulnerabilidades de los sistemas
- Concretar las diferentes metodologías de hacking
- Analizar las fases de un compilador
- Examinar la arquitectura de procesadores x86 y la arquitectura de procesadores ARM
- Determinar los diferentes tipos de análisis
- Aplicar sandboxing en diferentes entornos
- Desarrollar las diferentes técnicas de análisis de malware
- Establecer las herramientas orientadas al análisis de malware
- Establecer los requisitos necesarios para el correcto funcionamiento de una aplicación de forma segura
- Examinar los archivos de Logs para entender los mensajes de error
- Analizar los diferentes eventos y decidir qué mostrar al usuario y qué guardar en los logs
- Generar un Código Sanitizado, fácilmente verificable y de calidad
- Evaluar la documentación adecuada para cada fase del desarrollo
- Concretar el comportamiento del servidor para optimizar el sistema
- Desarrollar Código Modular, reusable y mantenible
- Identificar los diferentes elementos que ponen en evidencia un delito
- Generar conocimiento especializado para obtener los datos de los diferentes medios antes de que se pierdan
- Recuperar los datos que hayan sido borrados intencionadamente
- Analizar los registros y los logs de los sistemas
- Determinar cómo se Duplican los datos para no alterar los originales





- Fundamentar las pruebas para que sean consistentes
- Generar un informe sólido y sin fisuras
- Presentar las conclusiones de forma coherente
- Establecer cómo defender el informe ante la autoridad competente
- Concretar estrategias para que el teletrabajo sea seguro
- Conocer los principios sintácticos del lenguaje gráfico y aplicar sus reglas para describir con claridad y precisión objetos e ideas
- Conocer el origen de las letras y su importancia histórica
- Reconocer, estudiar y aplicar de forma coherente la tipografía a procesos gráficos
- Conocer y aplicar los fundamentos estéticos de la tipografía
- Saber analizar la disposición de los textos en el objeto de diseño
- Ser capaz de realizar trabajos profesionales partiendo de la composición tipográfica
- Evaluar la seguridad de un sistema de información en todos sus componentes y capas
- Identificar los tipos de amenazas de seguridad actuales y su tendencia
- Establecer directrices de seguridad definiendo políticas y planes de seguridad y contingencia
- Analizar estrategias y herramientas para asegurar la integridad y seguridad de los sistemas de información
- Aplicar las técnicas y herramientas específicas para cada tipo de ataque o vulnerabilidad de seguridad
- Proteger la información sensible almacenada en el sistema de información
- Disponer del marco legal y tipificación del delito, completando la visión con la tipificación del delincuente y su víctima

- Alinear el Plan Director de Seguridad con los objetivos estratégicos de la organización
- Establecer un marco continuo de gestión de riesgos como parte integral del Plan Director de Seguridad
- Determinar los indicadores adecuados para el seguimiento de la implantación del SGSI
- Establecer una estrategia de seguridad basada en políticas
- Analizar los objetivos y procedimientos asociados al plan de concienciación de empleados, proveedores y socios
- Identificar, dentro del marco normativo, las normativas, certificaciones y leyes de aplicación en cada organización
- Desarrollar los elementos fundamentales requeridos por la norma ISO 27001:2013
- Implantar un modelo de gestión de privacidad en línea con la regulación europea GDPR/RGPD
- Identificar las diferentes estructuras que puede tener un área de seguridad de la información
- Desarrollar un modelo de seguridad basado en tres líneas de defensa
- Presentar los diferentes comités periódicos y extraordinarios en los que interviene el área de ciberseguridad
- Concretar las herramientas tecnológicas que dan soporte a las principales funciones del equipo de operaciones de seguridad (SOC)
- Evaluar las medidas de control de vulnerabilidades adecuadas a cada escenario
- Desarrollar el marco de trabajo de operaciones de seguridad basado en NIST CSF
- Concretar el alcance de los diferentes tipos de auditorías (Red Team, Pentesting, Bug Bounty, etc.)
- Proponer las actividades a realizar después de un incidente de seguridad
- Configurar un centro de mando de seguridad de la información que englobe a todos los actores relevantes (autoridades, clientes, proveedores, etc.)
- Examinar, con una visión holística, el entorno en el que nos movemos
- Identificar los principales riesgos y oportunidades que pueden afectar a la consecución de nuestros objetivos
- Analizar los riesgos en base a las mejores prácticas a nuestro alcance
- Evaluar el posible impacto de dichos riesgos y oportunidades
- Desarrollar técnicas que nos permitan tratar los riesgos y oportunidades de manera que maximicemos nuestro aporte de valor
- Examinar en profundidad las diferentes técnicas de transferencia de riesgos, así como de valor
- Generar valor desde el diseño de modelos propios para la gestión ágil de riesgos
- Examinar los resultados para proponer mejoras continuas en gestión de proyectos y procesos basados en modelos de gestión impulsados por el riesgo o *risk-driven*
- Innovar y transformar los datos generales en información relevante para la toma de decisiones basadas en el riesgo
- Compilar las operaciones fundamentales (XOR, números grandes, sustitución y transposición) y los diversos componentes (funciones One-Way, Hash, generadores de números aleatorios)
- Analizar las técnicas criptográficas
- Desarrollar los diferentes algoritmos criptográficos
- Demostrar el uso de las firmas digitales y su aplicación en los certificados digitales

- Evaluar los sistemas de manejo de claves y la importancia de la longitud de las claves criptográficas
- Examinar los algoritmos derivación de claves
- Analizar el ciclo de vida de las claves
- Evaluar los modos de cifrado de bloque y de flujo
- Determinar los generadores de números pseudoaleatorios
- Desarrollar casos reales de aplicación de criptografía, como Kerberos, PGP o tarjetas inteligentes
- Examinar asociaciones y organismos relacionados, como ISO, NIST o NCSC
- Determinar los retos en la criptografía de la computación cuántica
- Desarrollar el concepto de identidad digital
- Evaluar el control de acceso físico a la información
- Fundamentar la autenticación biométrica y la autenticación MFA
- Evaluar ataques relacionados con la confidencialidad de la información
- Analizar la federación de identidades
- Establecer el control de acceso a la red
- Desarrollar conocimiento especializado en materia de seguridad física y lógica
- Demostrar el conocimiento en comunicaciones y redes
- Identificar principales ataques maliciosos
- Establecer un marco de desarrollo seguros
- Demostrar conocer las principales normativas de sistemas de gestión de la seguridad de la información
- Fundamentar el funcionamiento de un centro de operaciones en materias de ciberseguridad
- Demostrar la importancia de contar con prácticas en ciberseguridad para catástrofes organizativas
- Identificar riesgos de un despliegue de infraestructura en *cloud* pública
- Definir los requerimientos de seguridad
- Desarrollar un plan de seguridad para un despliegue en *cloud*
- Identificar los servicios *cloud* a desplegar para la ejecución de un plan de seguridad
- Determinar la operativa necesaria para los mecanismos de prevención
- Establecer las Directrices para un sistema de *logging* y monitorización
- Proponer acciones de respuesta ante incidentes
- Presentar la arquitectura simplificada del IoT
- Fundamentar las diferencias entre tecnologías de conectividad generalistas y tecnologías de conectividad para el IoT
- Establecer el concepto del triángulo de hierro de la conectividad del IoT
- Analizar las especificaciones de seguridad de la tecnología LoRaWAN, de la tecnología NB-IoT y de la tecnología WiSUN
- Fundamentar la elección de la tecnología IoT adecuada para cada proyecto
- Presentar los elementos clave de cada fase y Analizar las características del Plan de Continuidad de Negocio (PCN)
- Fundamentar la necesidad de un Plan de Continuidad para el Negocio
- Determinar los mapas de éxito y riesgo de cada fase del Plan de Continuidad de Negocio
- Concretar cómo se establece un Plan de Acción para la implantación
- Evaluar la completitud de un Plan de Continuidad del Negocio (PCN)
- Desarrollar el Plan de Implantación con éxito de un Plan de continuidad para nuestro Negocio

03

Competencias

A lo largo de este Grand Master, el profesional adquirirá una serie de herramientas y competencias que le habilitarán para trabajar en la dirección de ciberseguridad de una gran compañía. Por esa razón, este programa no se centra solo en los aspectos informáticos, sino que presta atención al proceso de digitalización, a las tecnologías emergentes, y cómo estos elementos han afectado a las actividades comunes y diarias de las organizaciones. De esta manera, el alumno egresado habrá podido adaptarse al contexto actual, conociendo las mejores soluciones en materia de seguridad para cada empresa.





Mejora tus habilidades hasta convertirte en el gran especialista de ciberseguridad de tu entorno"

Competencias generales

- Conocer las metodologías usadas en materia de ciberseguridad
- Saber evaluar cada tipo de amenaza para ofrecer una solución óptima en cada caso
- Ser capaz de generar soluciones inteligentes completas para automatizar comportamientos ante incidentes
- Saber cómo evaluar los riesgos asociados a las vulnerabilidades tanto fuera como dentro de la empresa
- Conocer la evolución y el impacto del IoT a lo largo del tiempo
- Ser capaz de demostrar que un sistema es vulnerable, atacarlo con fines preventivos y solventar dichos problemas
- Saber aplicar *sandboxing* en diferentes entornos
- Conocer las directrices que debe seguir un buen desarrollador para cumplir con la Seguridad necesaria
- Aplicar las medidas de seguridad más adecuadas dependiendo de las amenazas
- Determinar la política y plan de seguridad en el sistema de información de una compañía, completando el diseño y puesta en marcha del Plan de Contingencia
- Establecer un programa de auditorías que cubra las necesidades de autoevaluación de la organización en materia de ciberseguridad
- Desarrollar un programa de análisis y control de vulnerabilidades y un plan de respuesta a incidentes de ciberseguridad
- Maximizar las oportunidades que se presenten y eliminar la exposición a todos los posibles riesgos desde el propio diseño
- Compilar los sistemas de gestión de claves
- Evaluar la seguridad de la información de una compañía
- Analizar los sistemas de acceso a la información
- Desarrollar las mejores prácticas en el desarrollo seguro
- Presentar los riesgos que supone a las compañías no tener un entorno de seguridad informática

Este programa te trasladará al futuro de la ciberseguridad”

Competencias específicas

- Saber realizar operaciones de seguridad defensiva
- Tener una percepción profunda y especializada sobre la seguridad informática
- Ostentar conocimiento especializado en el ámbito de la ciberseguridad y ciberinteligencia
- Tener conocimientos profundos sobre aspectos fundamentales como el Ciclo de inteligencia, fuentes de inteligencia, ingeniería social, metodología OSINT, HUMINT, Anonimización, análisis de riesgos, metodologías existentes (OWASP, OWISAM, OSSTM, PTES) y normativas vigentes en materia de ciberseguridad
- Entender la importancia de idear una defensa multicapa, también conocida como "Defense in Depth", que cubra todos los aspectos de una red corporativa donde algunos de los conceptos y sistemas que veremos podrán ser utilizados y aplicados también en un ambiente doméstico
- Saber aplicar procesos de seguridad para smartphones y dispositivos portátiles
- Conocer los medios para realizar el llamado hacking ético y proteger una empresa de un ciberataque
- Ser capaz de investigar un incidente de ciberseguridad
- Conocer las diferentes técnicas de ataque y defensa existentes
- Analizar el rol del Analista en Dirección de Ciberseguridad (Chief Information Security Officer)
- Conocer el funcionamiento de la ingeniería social y sus métodos
- Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI)
- Identificar los elementos claves que conforman un SGSI
- Aplicar la metodología MAGERIT para evolucionar el modelo y llevarlo un paso más allá
- Diseñar nuevas Metodologías de gestión de riesgos propias, basadas en el concepto *agile risk management*
- Identificar, analizar, evaluar y tratar los riesgos a los que se enfrenta el profesional desde una nueva perspectiva empresarial basada en un modelo *risk-driven* o impulsado por el riesgo que permita no sólo sobrevivir en propio entorno, sino impulsar el aporte de valor propio
- Examinar el proceso de diseño de una estrategia de seguridad al desplegar servicios corporativos en *cloud*
- Evaluar las diferencias en las implementaciones concretas de diferentes vendedores de *cloud* pública
- Evaluar las opciones de conectividad IoT para afrontar un proyecto, con especial énfasis en tecnologías LPWAN
- Presentar las especificaciones básicas de las principales tecnologías LPWAN para el IoT

04

Dirección del curso

TECH ha recopilado la información más actualizada del momento en el ámbito de la dirección de sistemas de información para que los informáticos puedan encontrar, en un solo programa, el soporte didáctico necesario para mejorar su capacitación y lograr convertirse en un chief information officer de éxito. Si duda, un Grand Master que marcará un antes y un después en su capacitación y que les dará la oportunidad de aumentar sus opciones de empleabilidad.





Un completísimo temario que te acercará a los conceptos más novedosos sobre la dirección empresarial y la informática de sistemas para convertirte en un chief information officer de éxito"

Dirección



Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético. Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones. Madrid
- Instructora certificada E-Council. Madrid
- 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*). Universidad de las Islas Baleares
- Ingeniera en Informática. Universidad de Alcalá de Henares. Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies. E-Council. Madrid



D. Olalla Bonal, Martín

- Chief Information Officer en ePETID – Global Animal Health
- *Blockchain technical specialist* en IBM SPGI
- Arquitecto *blockchain*
- Arquitecto de Infraestructura en banca
- Gestión de proyectos y puesta en producción de soluciones
- Técnico en electrónica digital
- Docente: Formación *Hyperledger Fabric* a empresas
- Docente: Formación *Blockchain* orientado a negocio en empresas

Profesores

Dña. Marcos Sbarbaro, Victoria Alicia

- Desarrolladora de Aplicaciones Móviles Android Nativas en B60. UK
- Analista Programadora para la gestión, coordinación y documentación de entorno virtualizado de alarmas de seguridad en cliente
- Analista Programadora de aplicaciones Java para cajeros automáticos en cliente
- Profesional del Desarrollo de Software para aplicación de validación de firma y gestión documental en cliente
- Técnico de Sistemas para la migración de equipos y para la gestión, mantenimiento y formación de dispositivos móviles PDAs en cliente
- Ingeniería Técnica de Informática de Sistemas. Universitat Oberta de Catalunya.
- 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

- Mando intermedio en el MINISDEF. Distintos cometidos y responsabilidades dentro del GOE III, tales como administración y gestión de incidencias de la red interna, realización de programas a medida para diferentes áreas, cursos de formación a los usuarios de la red y al personal del grupo en general
- Técnico electrónico en Factoría Ford sita en Almusafes, Valencia, programaciónde robots, PLC,s, reparación y mantenimiento
- Técnico Electrónico
- Desarrollador de aplicaciones para dispositivos móviles

D. Peralta Alonso, Jon

- Abogado / DPO Altia Consultores SA
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC. Universidad Pública del País Vasco (UPV-EHU)
- Abogado / Asesor jurídico. Arriaga Asociados Asesoramiento Jurídico y Económico, SL
- 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

D. Redondo, Jesús Serrano

- Desarrollador FrontEnd Junior y Técnico de Ciberseguridad Junior
- Desarrollador FrontEnd en Telefónica, Madrid
- Desarrollador de FrontEnd. Best Pro Consulting SL, Madrid
- Instalador de equipos y servicios de Telecomunicaciones. Grupo Zener, Castilla y León
- Instalador de equipos y servicios de Telecomunicaciones. Lican Comunicaciones SL, Castilla y León
- Certificado en Seguridad Informática. CFTIC Getafe, Madrid
- Técnico Superior: Sistemas Telecomunicaciones e Informáticos. IES Trinidad Arroyo, Palencia
- Técnico Superior: Instalaciones Electrotécnicas MT y BT. IES Trinidad Arroyo, Palencia
- Formación en Ingeniería inversa, estenografía, cifrado. Academia Hacker Incibe (Talentos Incibe)

D. Jiménez Ramos, Álvaro

- Analista de seguridad en Capgemini
- Analista de ciberseguridad L1 en Axians
- Analista de ciberseguridad L2 en Axians
- Analista de ciberseguridad en SACYR SA
- 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

Dr. Plaza Merino, Pedro

- Profesional senior de ingeniería de sistemas de I+D en SIEMENS RAIL AUTOMATION SAU, Tres Cantos, España
- Doctor en Tecnologías Industriales por la Universidad Nacional de Educación a Distancia
- Ingeniero Industrial, especialidad Electrónica y Automática, y Electricidad por la Universidad Carlos III de Madrid
- Máster Universitario en Ingeniería Industrial en Electricidad, Electrónica y Control Industrial, intensificación en Electricidad y Electrónica por la Universidad Nacional de Educación a Distancia

D. Moreno Villares, Manuel

- Kyndryl (España y Portugal). Arquitecto de Soluciones
- IBM (España, Portugal, Grecia e Israel). Software Services Manager, Premium Support Manager, IT Program Manager, Cloud & Mobile Client Leader, Rational Software Services Leader
- D&D Grupos Dydes. Director Técnico de Ingeniería del Software y Bases de Datos
- ADD Distribuciones. Grupo ADD (España y Portugal). Director Técnico de Ingeniería del Software y Base de Datos
- Ingeniero Superior Industrial. Especialidad Automática y Electrónica. Universidad Politécnica de Madrid
- Codirector Máster Universitario en Ingeniería de Organización, Dirección de Proyectos y Empresas. Universidad Europea de Madrid

D. Tobal Redondo, Javier

- Responsable de seguridad de la información de la división de medios de pago. Amadeus IT Group
- Jefe de seguridad de la información de FINTONIC, Servicios Financieros
- Gerente del programa de innovación de aplicaciones de HUAWEI
- Ingeniero de servicios y arquitecto en el área de Planificación y arquitectura de servicios
  y seguridad en Amena / Orange España
- Licenciado en Informática por la Universidad de Deusto (Bilbao, España)
- Posgrado en Informática Industrial. Escuela de Ingeniería Industrial. Bilbao

D. Gonzalo Alonso, Félix

- Director general y fundador. Smart REM Solutions
- Socio fundador y responsable de ingeniería de riesgos e Innovación. Dynargy
- Gerente y socio fundador. Risknova (Gabinete pericial especializado en tecnología)
- Licenciado en Ingeniería de Organización Industrial por la Universidad Pontificia de Comillas ICAI
- Graduado en Ingeniería técnica Industrial especialidad Electrónica Industrial por la Universidad Pontificia de Comillas ICAI
- Master en Dirección Aseguradora por ICEA (Instituto para la Colaboración entre Entidades Aseguradoras)

D. Sevillano Izquierdo, Javier

- Global Cyber Security Architect. Vodafone España
- Chief Technology Security Office (CTSO). Vodafone España
- Responsable Seguridad Tecnológica. Bankia
- Responsable Seguridad Tecnológica. Caja Madrid
- Manager Seguridad. Sistema 4B
- SEINCA - Analista senior
- Técnico superior en Informática Empresarial por Instituto Cibernos

D. Entrenas, Alejandro

- Entelgy Innotec
- Innovery España
- Atos Spain
- Licenciado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Córdoba
- Máster en Dirección y Gestión de la Seguridad de la Información en la Universidad Politécnica de Madrid

D. Nogales Ávila, Javier

- Enterprise Cloud and sourcing senior consultant. Quint
- Cloud and Technology Consultant. Indra
- Associate Technology Consultant. Accenture
- Graduado por la Universidad de Jaén y University of Technology and Economics of Budapest (BME)
- Grado en Ingeniería de Organización Industrial

D. Gómez Rodríguez, Antonio

- Ingeniero de soluciones Cloud en Oracle
- Director de Proyectos en Sopra Group
- Director de Proyectos en Everis
- Jefe de Proyectos en Empresa pública de Gestion de Programas Culturales Consejería de Cultura de Andalucía
- Analista de Sistemas de Información. Sopra Group
- Licenciado en Ingeniería Superior de Telecomunicación por la Universidad Politécnica de Cataluña
- Postgrado en Tecnologías y Sistemas de Información, Instituto Catalán de Tecnología
- E-Business Master, Escuela de Negocios La Salle





D. del Valle Arias, Jorge

- Smart Cities Business Growth Manager Spain en Itron Inc.
- Consultor IoT
- Director de División IoT en Diode España
- Sales Manager IoT & Celular en Aicox Soluciones
- Fundador y CEO de Sensor Intelligence
- Director de Operaciones en Codium Networks
- Jefe del Área de Electrónica en Aitemin
- Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid
- Executive MBA por la International Graduate School de La Salle de Madrid

D. Gozalo Fernández, Juan Luis

- Director Blockchain DevOps en Alastria
- Director Desarrollo Aplicación Móvil Tinkerlink en Cronos Telecom
- Director Informática en Banco Santander
- Director Tecnología Gestión de Servicio IT en Barclays Bank España
- Licenciado en Ingeniería Superior Informática por la Universidad Nacional Educación a Distancia (UNED)

05

Estructura y contenido

Este Grand Máster en Alta Dirección de Ciberseguridad está compuesto por 20 módulos, y ha sido diseñado cuidadosamente para acercar al profesional las últimas novedades en este ámbito. Así, podrá conocer los más recientes avances en cuestiones como la seguridad en *smartphones*, la seguridad en el internet de las cosas, en el desarrollo seguro, la criptografía o la seguridad en entornos *cloud computing*. Con este temario, por tanto, el informático habrá accedido a los conocimientos más actualizados y completos, preparándose, de forma rápida, para convertirse en un especialista en ciberseguridad de gran prestigio.





No encontrarás unos contenidos más completos que estos para actualizarte en el ámbito de la ciberseguridad”

Módulo 1. Ciberinteligencia y Ciberseguridad

1.1. Ciberinteligencia
- 1.1.1. Ciberinteligencia
  - 1.1.1.1. La Inteligencia
    - 1.1.1.1.1. Ciclo de Inteligencia
  - 1.1.1.2. Ciberinteligencia
  - 1.1.1.3. Ciberinteligencia y Ciberseguridad
- 1.1.2. El Analista de Inteligencia
  - 1.1.2.1. El rol del Analista de Inteligencia
  - 1.1.2.2. Los sesgos del Analista de Inteligencia en la actividad evaluativa

1.2. Ciberseguridad
- 1.2.1. Las Capas de Seguridad
- 1.2.2. Identificación de las Ciberamenazas
  - 1.2.2.1. Amenazas Externas
  - 1.2.2.2. Amenazas Internas
- 1.2.3. Acciones adversas
  - 1.2.3.1. Ingeniería social
  - 1.2.3.2. Métodos comúnmente usados

1.3. Técnicas y Herramientas de Inteligencias
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Distribuciones de Linux y herramientas
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. Metodologías de evaluación
- 1.4.1. El Análisis de Inteligencia
- 1.4.2. Técnicas de organización de la información adquirida
- 1.4.3. Fiabilidad y credibilidad de las fuentes de información
- 1.4.4. Metodologías de Análisis
- 1.4.5. Presentación de los Resultados de la Inteligencia

1.5. Auditorías y documentación
- 1.5.1. La Auditoria en Seguridad Informática
- 1.5.2. Documentación y permisos para Auditoria
- 1.5.3. Tipos de Auditoría
- 1.5.4. Entregables
  - 1.5.4.1. Informe Técnico
  - 1.5.4.2. Informe Ejecutivo

1.6. Anonimato en la Red
- 1.6.1. Uso de anonimato
- 1.6.2. Técnicas de anonimato (Proxy, VPN)
- 1.6.3. Redes TOR, Freenet e IP2

1.7. Amenazas y tipos de seguridad
- 1.7.1. Tipos de amenazas
- 1.7.2. Seguridad física
- 1.7.3. Seguridad en redes
- 1.7.4. Seguridad lógica
- 1.7.5. Seguridad en aplicaciones web
- 1.7.6. Seguridad en dispositivos móviles

1.8. Normativa y *Compliance*
- 1.8.1. RGPD
- 1.8.2. La estrategia nacional de ciberseguridad 2019
- 1.8.3. Familia ISO 27000
- 1.8.4. Marco de ciberseguridad NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativas Cloud
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Análisis de riesgos y métricas
- 1.9.1. Alcance de riesgos
- 1.9.2. Los activos
- 1.9.3. Las amenazas
- 1.9.4. Las vulnerabilidades
- 1.9.5. Evaluación del riesgo
- 1.9.6. Tratamiento del riesgo

1.10. Organismos importantes en materia de ciberseguridad
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR-PROSUR

Módulo 2. Seguridad en *host*

2.1. Copias de seguridad
- 2.1.1. Estrategias para las copias de seguridad
- 2.1.2. Herramientas para Windows
- 2.1.3. Herramientas para Linux
- 2.1.4. Herramientas para MacOS

2.2. Antivirus de usuario
- 2.2.1. Tipos de antivirus
- 2.2.2. Antivirus para Windows
- 2.2.3. Antivirus para Linux
- 2.2.4. Antivirus para MacOS
- 2.2.5. Antivirus para smartphones

2.3. Detectores de intrusos - HIDS
- 2.3.1. Métodos de detección de intrusos
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Firewall local
- 2.4.1. Firewalls para Windows
- 2.4.2. Firewalls para Linux
- 2.4.3. Firewalls para MacOS

2.5. Gestores de contraseñas
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Detectores de *phishing*
- 2.6.1. Detección del phishing de forma manual
- 2.6.2. Herramientas *antiphishing*

2.7. *Spyware*
- 2.7.1. Mecanismos de Evitación
- 2.7.2. Herramientas *antispyware*

2.8. Rastreadores
- 2.8.1. Medidas para proteger el sistema
- 2.8.2. Herramientas anti-rastreadores

2.9. EDR- End point Detection and Response
- 2.9.1. Comportamiento del Sistema EDR
- 2.9.2. Diferencias entre EDR y Antivirus
- 2.9.3. El futuro de los sistemas EDR

2.10. Control sobre la instalación de software
- 2.10.1. Repositorios y tiendas de software
- 2.10.2. Listas de software permitido o prohibido
- 2.10.3. Criterios de actualizaciones
- 2.10.4. Privilegios para instalar software

Módulo 3. Seguridad En Red (Perimetral)

3.1. Sistemas de detección y prevención de amenazas
- 3.1.1. Marco general de los incidentes de seguridad
- 3.1.2. Sistemas de Defensa Actuales: Defense in Depth y SOC
- 3.1.3. Arquitecturas de red Actuales
- 3.1.4. Tipos de herramientas para la detección y prevención de incidentes
  - 3.1.4.1. Sistemas basados en Red
  - 3.1.4.2. Sistemas basados en Host
  - 3.1.4.3. Sistemas centralizados
- 3.1.5. Comunicación y detección de instancias/hosts, contenedores y *serverless*

3.2. Firewall
- 3.2.1. Tipos de Firewalls
- 3.2.2. Ataques y mitigación

3.2.3. Firewalls comunes en kernel Linux
3.2.3.1. UFW
3.2.3.2. Nftables e iptables
3.2.3.3. Firewalld
3.2.4. Sistemas de detección basados en logs del sistema
3.2.4.1. TCP Wrappers
3.2.4.2. BlockHosts y DenyHosts
3.2.4.3. Fai2ban
3.3. Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)
3.3.1. Ataques sobre IDS/IPS
3.3.2. Sistemas de IDS/IPS
3.3.2.1. Snort
3.3.2.2. Suricata
3.4. Firewalls de Siguiente Generación (NGFW)
3.4.1. Diferencias entre NGFW y Firewall tradicional
3.4.2. Capacidades principales
3.4.3. Soluciones comerciales
3.4.4. Firewalls para servicios de Cloud
3.4.4.1. Arquirtectura Cloud VPC
3.4.4.2. Cloud ACLs
3.4.4.3. Security Group
3.5. Proxy
3.5.1. Tipos de Proxy
3.5.2. Uso de Proxy. Ventajas e inconvenientes
3.6. Motores de Antivirus
3.6.1. Contexto general del Malware e IOCs
3.6.2. Problemas de los motores de Antiviru
3.7. Sistemas de Protección de Correo
3.7.1. Antispam
3.7.1.1. Listas blancas y negras
3.7.1.2. Filtros bayesianos
3.7.2. Mail Gateway (MGW)
3.8. SIEM
3.8.1. Componentes y Arquitectura
3.8.2. Reglas de correlación y casos de uso
3.8.3. Retos actuales de los sistemas SIEM
3.9. SOAR
3.9.1. SOAR y SIEM: Enemigos o aliados
3.9.2. El futuro de los sistemas SOAR
3.10. Otros Sistemas basados en Red
3.10.1. WAF
3.10.2. NAC
3.10.3. HoneyPots y HoneyNets
3.10.4. CASB

Módulo 4. Seguridad en *Smartphones*

4.1. El mundo del Dispositivo Móvil
4.1.1. Tipos de Plataformas móviles
4.1.2. Dispositivos Ios
4.1.3. Dispositivos Android
4.2. Gestión de la Seguridad Móvil
4.2.1. Proyecto de Seguridad Móvil OWASP
4.2.1.1. Top 10 Vulnerabilidades
4.2.2. Comunicaciones, Redes y Modos de Conexión
4.3. El Dispositivo Móvil en el entorno Empresarial
4.3.1. Riesgos
4.3.2. Políticas de Seguridad
4.3.3. Monitorización de Dispositivos
4.3.4. Gestión de Dispositivos Móviles (MDM)
4.4. Privacidad del Usuario y Seguridad de los Datos
4.4.1. Estados de la Información
4.4.2. Protección y Confidencialidad de los Datos
4.4.2.1. Permisos
4.4.2.2. Encriptación

4.4.3. Almacenamiento Seguro de los Datos
4.4.3.1. Almacenamiento Seguro en iOS
4.4.3.2. Almacenamiento Seguro en Android
4.4.4. Buenas prácticas en el Desarrollo de Aplicaciones
4.5. Vulnerabilidades y Vectores de Ataque
4.5.1. Vulnerabilidades
4.5.2. Vectores de ataque
4.5.2.1. Malware
4.5.2.2. Exfiltración de datos
4.5.2.3. Manipulación de los datos
4.6. Principales Amenazas
4.6.1. Usuario no forzado
4.6.2. Malware
4.6.2.1. Tipos de Malware
4.6.3. Ingeniería Social
4.6.4. Fuga de Datos
4.6.5. Robo de información
4.6.6. Redes Wi-Fi no seguras
4.6.7. Software desactualizado
4.6.8. Aplicaciones Maliciosas
4.6.9. Contraseñas poco seguras
4.6.10. Configuración débil o inexistente de Seguridad
4.6.11. Acceso Físico
4.6.12. Pérdida o robo del dispositivo
4.6.13. Suplantación de identidad (Integridad)
4.6.14. Criptografía débil o rota
4.6.15. Denegación de Servicio (DoS)
4.7. Principales ataques
4.7.1. Ataques de *phishing*
4.7.2. Ataques relacionados con los modos de comunicación
4.7.3. Ataques de *smishing*
4.7.4. Ataques de *criptojacking*
4.7.5. *Man in The Middle*
4.8. Hacking
4.8.1. *Rooting* y *Jailbreaking*
4.8.2. Anatomía de un Ataque Móvil
4.8.2.1. Propagación de la amenaza
4.8.2.2. Instalación de Malware en el Dispositivo
4.8.2.3. Persistencia
4.8.2.4. Ejecución del *payload* y extracción de la información
4.8.3. Hacking en Dispositivos iOS: mecanismos y herramientas
4.8.4. Hacking en Dispositivos Android: mecanismos y herramientas
4.9. Pruebas de Penetración
4.9.1. iOS PenTesting
4.9.2. Android PenTesting
4.9.3. Herramientas
4.10. Protección y Seguridad
4.10.1. Configuración de Seguridad
4.10.1.1. En Dispositivos iOS
4.10.1.2. En Dispositvos Android
4.10.2. Medidas de Seguridad
4.10.3. Herramientas de protección

Módulo 5. Seguridad en IoT

5.1. Dispositivos
5.1.1. Tipos de Dispositivos
5.1.2. Arquitecturas Estandarizadas
5.1.2.1. ONEM2M
5.1.2.2. IoTWF
5.1.3. Protocolos de Aplicación
5.1.4. Tecnologías de conectividad
5.2. Dispositivos IoT. Áreas de aplicación
5.2.1. *SmartHome*
5.2.2. *SmartCity*
5.2.3. Transportes
5.2.4. Wearables
5.2.5. Sector Salud
5.2.6. IioT

5.3. Protocolos de comunicación
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*
- 5.4.1. Domótica
- 5.4.2. Redes
- 5.4.3. Electrodomésticos
- 5.4.4. Vigilancia y seguridad

5.5. *SmartCity*
- 5.5.1. Iluminación
- 5.5.2. Meteorología
- 5.5.3. Seguridad

5.6. Transportes
- 5.6.1. Localización
- 5.6.2. Realización de pagos y obtención de servicios
- 5.6.3. Conectividad

5.7. *Wearables*
- 5.7.1. Ropa inteligente
- 5.7.2. Joyas inteligentes
- 5.7.3. Relojes inteligentes

5.8. Sector Salud
- 5.8.1. Monitorización de ejercicio/Ritmo Cardiaco
- 5.8.2. Monitorización de pacientes y personas mayores
- 5.8.3. Implantadles
- 5.8.4. Robots Quirúrgicos

5.9. Conectividad
- 5.9.1. Wi-Fi/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Conectividad incorporada

5.10. Securización
- 5.10.1. Redes dedicadas
- 5.10.2. Gestor de Contraseñas
- 5.10.3. Uso de protocolos cifrados
- 5.10.4. Consejos de uso

Módulo 6. Hacking Ético

6.1. Entorno de trabajo
- 6.1.1. Distribuciones Linux
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Sistemas de Virtualización
- 6.1.3. *Sandbox*
- 6.1.4. Despliegue de laboratorios

6.2. Metodologías
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. *Footprinting*
- 6.3.1. Inteligencia de fuentes abiertas (OSINT)
- 6.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 6.3.3. Uso de herramientas pasivas

6.4. Escaneo de Redes
- 6.4.1. Herramientas de escaneo
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Otras herramientas de escaneo
- 6.4.2. Técnicas de Escaneo
- 6.4.3. Técnicas de Evasión de Firewall e IDS
- 6.4.4. *Banner Grabbing*
- 6.4.5. Diagramas de red

6.5. Enumeración
- 6.5.1. Enumeración SMTP
- 6.5.2. Enumeración DNS
- 6.5.3. Enumeración de NetBIOS y Samba
- 6.5.4. Enumeración de LDAP
- 6.5.5. Enumeración de SNMP
- 6.5.6. Otras técnicas de Enumeración

6.6. Análisis de Vulnerabilidades
- 6.6.1. Soluciones de Análisis de Vulnerabilidades
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Sistemas de puntuación de Vulnerabilidades
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Ataques a Redes Inalámbrica
- 6.7.1. Metodología de Hacking en Redes inalámbricas
  - 6.7.1.1. Wi-Fi Discovery
  - 6.7.1.2. Análisis de tráfico
  - 6.7.1.3. Ataques del *aircrack*
    - 6.7.1.3.1. Ataques WEP
    - 6.7.1.3.2. Ataques WPA/WPA2
  - 6.7.1.4. Ataques de *Evil Twin*
  - 6.7.1.5. Ataques a WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Herramientas para la Seguridad Inalámbrica

6.8. Hackeo de servidores webs
- 6.8.1. *Cross site scripting*
- 6.8.2. CSRF
- 6.8.3. Session Hijacking
- 6.8.4. SQLinjection

6.9. Explotación de vulnerabilidades
- 6.9.1. Uso de *exploits* conocidos
- 6.9.2. Uso de *metasploit*
- 6.9.3. Uso de malware
  - 6.9.3.1. Definición y alcance
  - 6.9.3.2. Generación de malware
  - 6.9.3.3. Bypass de soluciones antivirus

6.10. Persistencia
- 6.10.1. Instalación de *rootkits*
- 6.10.2. Uso de ncat
- 6.10.3. Uso de tareas programadas para *backdoors*
- 6.10.4. Creación de usuarios
- 6.10.5. Detección de HIDS

Módulo 7. Ingeniería Inversa

7.1. Compiladores
- 7.1.1. Tipos de Códigos
- 7.1.2. Fases de un compilador
- 7.1.3. Tabla de símbolos
- 7.1.4. Gestor de errores
- 7.1.5. Compilador GCC

7.2. Tipos de Análisis en compiladores
- 7.2.1. Análisis léxico
  - 7.2.1.1. Terminología
  - 7.2.1.2. Componentes léxicos
  - 7.2.1.3. Analizador léxico LEX
- 7.2.2. Análisis sintáctico
  - 7.2.2.1. Gramáticas libres de contexto
  - 7.2.2.2. Tipos de análisis sintácticos
    - 7.2.2.2.1. Análisis descendente
    - 7.2.2.2.2. Análisis ascendente
  - 7.2.2.3. Árboles sintácticos y derivaciones
  - 7.2.2.4. Tipos de analizadores sintácticos
    - 7.2.2.4.1. Analizadores LR (*Left To Right*)
    - 7.2.2.4.2. Analizadores LALR

7.2.3. Análisis semántico
7.2.3.1. Gramáticas de atributos
7.2.3.2. S-Atribuidas
7.2.3.3. L-Atribuidas
7.3. Estructuras de Datos en Ensamblador
7.3.1. Variables
7.3.2. Arrays
7.3.3. Punteros
7.3.4. Estructuras
7.3.5. Objetos
7.4. Estructuras de Código en Ensamblador
7.4.1. Estructuras de selección
7.4.1.1. *If, else if, Else*
7.4.1.2. Switch
7.4.2. Estructuras de iteración
7.4.2.1. For
7.4.2.2. While
7.4.2.3. Uso del break
7.4.3. Funciones
7.5. Arquitectura Hardware x86
7.5.1. Arquitectura de procesadores x86
7.5.2. Estructuras de datos en x86
7.5.3. Estructuras de código en x86
7.5.3. Estructuras de código en x86
7.6. Arquitectura Hardware ARM
7.6.1. Arquitectura de procesadores ARM
7.6.2. Estructuras de datos en ARM
7.6.3. Estructuras de código en ARM
7.7. Análisis de código estático
7.7.1. Desensambladores
7.7.2. IDA
7.7.3. Reconstructores de código
7.8. Análisis de código dinámico
7.8.1. Análisis del comportamiento
7.8.1.1. Comunicaciones
7.8.1.2. Monitorización
7.8.2. Depuradores de código en Linux
7.8.3. Depuradores de código en Windows
7.9. *Sandbox*
7.9.1. Arquitectura de un *sandbox*
7.9.2. Evasión de un *sandbox*
7.9.3. Técnicas de detección
7.9.4. Técnicas de evasión
7.9.5. Contramedidas
7.9.6. *Sandbox* en Linux
7.9.7. *Sandbox* en Windows
7.9.8. *Sandox* en MacOS
7.9.9. *Sandbox* en Android
7.10. Análisis de Malware
7.10.1. Métodos de análisis de Malware
7.10.2. Técnicas de ofuscación de Malware
7.10.2.1. Ofuscación de ejecutables
7.10.2.2. Restricción de entornos de ejecución
7.10.3. Herramientas de análisis de Malware

Módulo 8. Desarrollo Seguro

8.1. Desarrollo Seguro
8.1.1. Calidad, funcionalidad y seguridad
8.1.2. Confidencialidad, integridad y disponibilidad
8.1.3. Ciclo de vida del desarrollo de software
8.2. Fase de Requerimientos
8.2.1. Control de la autenticación
8.2.2. Control de roles y privilegios
8.2.3. Requerimientos orientados al riesgo
8.2.4. Aprobación de privilegios

8.3. Fases de Análisis y Diseño
- 8.3.1. Acceso a componentes y administración del sistema
- 8.3.2. Pistas de auditoría
- 8.3.3. Gestión de sesiones
- 8.3.4. Datos históricos
- 8.3.5. Manejo apropiado de errores
- 8.3.6. Separación de funciones

8.4. Fase de Implementación y Codificación
- 8.4.1. Aseguramiento del ambiente de desarrollo
- 8.4.2. Elaboración de la documentación técnica
- 8.4.3. Codificación segura
- 8.4.4. Seguridad en las comunicaciones

8.5. Buenas prácticas de Codificación Segura
- 8.5.1. Validación de datos de entrada
- 8.5.2. Codificación de los datos de salida
- 8.5.3. Estilo de programación
- 8.5.4. Manejo de registro de cambios
- 8.5.5. Prácticas criptográficas
- 8.5.6. Gestión de errores y logs
- 8.5.7. Gestión de archivos
- 8.5.8. Gestión de. Memoria
- 8.5.9. Estandarización y reutilización de funciones de seguridad

8.6. Preparación del servidor y *hardening*
- 8.6.1. Gestión de usuarios, grupos y roles en el servidor
- 8.6.2. Instalación de software
- 8.6.3. *Hardening* del servidor
- 8.6.4. Configuración robusta del entorno de la aplicación

8.7. Preparación de la BBDD y *hardening*
- 8.7.1. Optimización del motor de BBDD
- 8.7.2. Creación del usuario propio para la aplicación
- 8.7.3. Asignación de los privilegios precisos para el usuario
- 8.7.4. *Hardening* de la BBDD

8.8. Fase de pruebas
- 8.8.1. Control de calidad en controles de seguridad
- 8.8.2. Inspección del código por fases
- 8.8.3. Comprobación de la gestión de las configuraciones
- 8.8.4. Pruebas de caja negra

8.9. Preparación del Paso a producción
- 8.9.1. Realizar el control de cambios
- 8.9.2. Realizar procedimiento de paso a producción
- 8.9.3. Realizar procedimiento de *rollback*
- 8.9.4. Pruebas en fase de preproducción

8.10. Fase de mantenimiento
- 8.10.1. Aseguramiento basado en riesgos
- 8.10.2. Pruebas de mantenimiento de seguridad de caja blanca
- 8.10.3. Pruebas de mantenimiento de seguridad de caja negra

Módulo 9. Análisis Forense

9.1. Adquisición de datos y duplicación
- 9.1.1. Adquisición de datos volátiles
  - 9.1.1.1. Información del sistema
  - 9.1.1.2. Información de la red
  - 9.1.1.3. Orden de volatilidad
- 9.1.2. Adquisición de datos estáticos
  - 9.1.2.1. Creación de una imagen duplicada
  - 9.1.2.2. Preparación de un documento para la cadena de custodia
- 9.1.3. Métodos de validación de los datos adquiridos
  - 9.1.3.1. Métodos para Linux
  - 9.1.3.2. Métodos para Windows

9.2. Evaluación y derrota de técnicas anti-forenses
- 9.2.1. Objetivos de las técnicas anti-forenses
- 9.2.2. Borrado de datos
  - 9.2.2.1. Borrado de datos y ficheros
  - 9.2.2.2. Recuperación de archivos
  - 9.2.2.3. Recuperación de particiones borradas

9.2.3. Protección por contraseña
9.2.4. Esteganografía
9.2.5. Borrado seguro de dispositivos
9.2.6. Encriptación
9.3. Análisis Forense del sistema operativo
9.3.1. Análisis Forense de Windows
9.3.2. Análisis Forense de Linux
9.3.3. Análisis Forense de Mac
9.4. Análisis Forense de la red
9.4.1. Análisis de los logs
9.4.2. Correlación de datos
9.4.3. Investigación de la red
9.4.4. Pasos a seguir en el análisis forense de la red
9.5. Análisis Forense Web
9.5.1. Investigación de los ataques webs
9.5.2. Detección de ataques
9.5.3. Localización de direcciones IPs
9.6. Análisis Forense de Bases de Datos
9.6.1. Análisis Forense en MSSQL
9.6.2. Análisis Forense en MySQL
9.6.3. Análisis Forense en PostgreSQL
9.6.4. Análisis Forense en MongoDB
9.7. Análisis Forense en Cloud
9.7.1. Tipos de Crímenes en Cloud
9.7.1.1. Cloud como Sujeto
9.7.1.2. Cloud como Objeto
9.7.1.3. Cloud como Herramienta
9.7.2. Retos del Análisis Forense en Cloud
9.7.3. Investigación de los servicios de Almacenamiento el Cloud
9.7.4. Herramientas de Análisis Forense para Cloud
9.8. Investigación de crímenes de Correo Electrónico
9.8.1. Sistemas de correo
9.8.1.1. Clientes de Correo
9.8.1.2. Servidor de Correo
9.8.1.3. Servidor SMTP
9.8.1.4. Servidor POP3
9.8.1.5. Servidor IMAP4
9.8.2. Crímenes de correo
9.8.3. Mensaje de Correo
9.8.3.1. Cabeceras Estándar
9.8.3.2. Cabeceras Extendidas
9.8.4. Pasos para la investigación de estos crímenes
9.8.5. Herramientas Forenses para Correo Electrónico
9.9. Análisis Forense de Móviles
9.9.1. Redes Celulares
9.9.1.1. Tipos de redes
9.9.1.2. Contenidos del CDR
9.9.2. *Subscriber Identity Module* (SIM)
9.9.3. Adquisición lógica
9.9.4. Adquisición física
9.9.5. Adquisición del sistema de ficheros
9.10. Redacción y presentación de Informes Forenses
9.10.1. Aspectos importantes de un Informe Forense
9.10.2. Clasificación y tipos de informes
9.10.3. Guía para escribir un informe
9.10.4. Presentación del informe
9.10.4.1. Preparación previa para testificar
9.10.4.2. Deposición
9.10.4.3. Trato con los medios

Módulo 10. Retos Actuales y Futuros en Seguridad Informática

10.1. Tecnología *Blockchain*
- 10.1.1. Ámbitos de aplicación
- 10.1.2. Garantía de confidencialidad
- 10.1.3. Garantía de no-repudio

10.2. Dinero Digital
- 10.2.1. Bitcoins
- 10.2.2. Critpomonedas
- 10.2.3. Minería de criptomonedas
- 10.2.4. Estafas piramidales
- 10.2.5. Otros potenciales delitos y problemas

10.3. *Deepfake*
- 10.3.1. Impacto en los medios
- 10.3.2. Peligros para la sociedad
- 10.3.3. Mecanismos de detección

10.4. El futuro de la inteligencia artificial
- 10.4.1. Inteligencia artificial y computación cognitiva
- 10.4.2. Usos para simplificar el servicio a clientes

10.5. Privacidad digital
- 10.5.1. Valor de los datos en la red
- 10.5.2. Uso de los datos en la red
- 10.5.3. Gestión de la privacidad e identidad digital

10.6. Ciberconflictos, cibercriminales y ciberataques
- 10.6.1. Impacto de la ciberseguridad en conflictos internacionales
- 10.6.2. Consecuencias de ciberataques en la población general
- 10.6.3. Tipos de cibercriminales. Medidas de Protección

10.7. Teletrabajo
- 10.7.1. Revolución del teletrabajo durante y post Covid19
- 10.7.2. Cuellos de botella en el acceso
- 10.7.3. Variación de la superficie de ataque
- 10.7.4. Necesidades de los trabajadores

10.8. Tecnologías *wireless* emergentes
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Ondas milimétricas
- 10.8.4. Tendencia en "*Get Smart*" en vez de "*Get more*"

10.9. Direccionamiento futuro en redes
- 10.9.1. Problemas actuales con el direccionamiento IP
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Ventajas de IPv4+ sobre IPv4
- 10.9.5. Ventajas de IPv6 sobre IPv4

10.10. El reto de la concienciación de la Formación temprana y continua de la población
- 10.10.1. Estrategias actuales de los gobiernos
- 10.10.2. Resistencia de la Población al aprendizaje
- 10.10.3. Planes de formación que deben adoptar las empresas

Módulo 11. Seguridad en el diseño y desarrollo de sistemas

11.1. Sistemas de Información
- 11.1.1. Dominios de un sistema de información
- 11.1.2. Componentes de un sistema de información
- 11.1.3. Actividades de un sistema de información
- 11.1.4. Ciclo de vida de un sistema de información
- 11.1.5. Recursos de un sistema de información

11.2. Sistemas de información. Tipología
- 11.2.1. Tipos de sistemas de información
  - 11.2.1.1. Empresarial
  - 11.2.1.2. Estratégicos
  - 11.2.1.3. Según el ámbito de la aplicación
  - 11.2.1.4. Específicos
- 11.2.2. Sistemas de Información. Ejemplos reales
- 11.2.3. Evolución de los sistemas de información: Etapas
- 11.2.4. Metodologías de los sistemas de información

11.3. Seguridad de los sistemas de información. Implicaciones legales
- 11.3.1. Acceso a datos
- 11.3.2. Amenazas de seguridad: Vulnerabilidades
- 11.3.3. Implicaciones legales: Delitos
- 11.3.4. Procedimientos de mantenimiento de un sistema de información

11.4. Seguridad de un sistema de información. Protocolos de seguridad
- 11.4.1. Seguridad de un sistema de información
  - 11.4.1.1. Integridad
  - 11.4.1.2. Confidencialidad
  - 11.4.1.3. Disponibilidad
  - 11.4.1.4. Autenticación
- 11.4.2. Servicios de seguridad
- 11.4.3. Protocolos de seguridad de la información. Tipología
- 11.4.4. Sensibilidad de un sistema de información

11.5. Seguridad en un sistema de información. Medidas y sistemas de control de acceso
- 11.5.1. Medidas de seguridad
- 11.5.2. Tipo de medidas de seguridad
  - 11.5.2.1. Prevención
  - 11.5.2.2. Detección
  - 11.5.2.3. Corrección
- 11.5.3. Sistemas de control de acceso. Tipología
- 11.5.4. Criptografía

11.6. Seguridad en redes e internet
- 11.6.1. Firewalls
- 11.6.2. Identificación digital
- 11.6.3. Virus y gusanos
- 11.6.4. Hacking
- 11.6.5. Ejemplos y casos reales

11.7. Delitos informáticos
- 11.7.1. Delito informático
- 11.7.2. Delitos informáticos. Tipología
- 11.7.3. Delito Informático. Ataque. Tipologías
- 11.7.4. El caso de la realidad virtual
- 11.7.5. Perfiles de delincuentes y víctimas. Tipificación del delito
- 11.7.6. Delitos informáticos. Ejemplos y casos reales

11.8. Plan de seguridad en un sistema de información
- 11.8.1. Plan de seguridad. Objetivos
- 11.8.2. Plan de seguridad. Planificación
- 11.8.3. Plan de riesgos. Análisis
- 11.8.4. Política de seguridad. Implementación en la organización
- 11.8.5. Plan de seguridad. Implementación en la organización
- 11.8.6. Procedimientos de seguridad. Tipos
- 11.8.7. Planes de seguridad. Ejemplos

11.9. Plan de contingencia
- 11.9.1. Plan de contingencia. Funciones
- 11.9.2. Plan de emergencia: Elementos y objetivos
- 11.9.3. Plan de contingencia en la organización. Implementación
- 11.9.4. Planes de contingencia. Ejemplos

11.10. Gobierno de la seguridad de sistemas de información
- 11.10.1. Normativa legal
- 11.10.2. Estándares
- 11.10.3. Certificaciones
- 11.10.4. Tecnologías

Módulo 12. Arquitecturas y modelos de seguridad de la información

12.1. Arquitectura de seguridad de la información
- 12.1.1. SGSI / PDS
- 12.1.2. Alineación estratégica
- 12.1.3. Gestión del riesgo
- 12.1.4. Medición del desempeño

12.2. Modelos de seguridad de la información
- 12.2.1. Basados en políticas de seguridad
- 12.2.2. Basados en herramientas de protección
- 12.2.3. Basados en equipos de trabajo

12.3. Modelo de seguridad. Componentes clave
- 12.3.1. Identificación de riesgos
- 12.3.2. Definición de controles
- 12.3.3. Evaluación continua de niveles de riesgo
- 12.3.4. Plan de concienciación de empleados, proveedores, socios, etc.

12.4. Proceso de gestión de riesgos
- 12.4.1. Identificación de activos
- 12.4.2. Identificación de amenazas
- 12.4.3. Evaluación de riesgos
- 12.4.4. Priorización de controles
- 12.4.5. Reevaluación y riesgo residual

12.5. Procesos de negocio y seguridad de la información
- 12.5.1. Procesos de negocio
- 12.5.2. Evaluación de riesgos basados en parámetros de negocio
- 12.5.3. Análisis de impacto al negocio
- 12.5.4. Las operaciones de negocio y la seguridad de la información

12.6. Proceso de mejora continua
- 12.6.1. El ciclo de Deming
  - 12.6.1.1. Planificar
  - 12.6.1.2. Hacer
  - 12.6.1.3. Verificar
  - 12.6.1.4. Actuar

12.7. Arquitecturas de seguridad
- 12.7.1. Selección y homogeneización de tecnologías
- 12.7.2. Gestión de identidades. Autenticación
- 12.7.3. Gestión de accesos. Autorización
- 12.7.4. Seguridad de infraestructura de red
- 12.7.5. Tecnologías y soluciones de cifrado
- 12.7.6. Seguridad de equipos terminales (EDR)

12.8. El marco normativo
- 12.8.1. Normativas sectoriales
- 12.8.2. Certificaciones
- 12.8.3. Legislaciones

12.9. La norma ISO 27001
- 12.9.1. Implementación
- 12.9.2. Certificación
- 12.9.3. Auditorías y tests de intrusión
- 12.9.4. Gestión continua del riesgo
- 12.9.5. Clasificación de la información

12.10. Legislación sobre privacidad. RGPD (GDPR)
- 12.10.1. Alcance del reglamento general de protección de datos (RGPD)
- 12.10.2. Datos personales
- 12.10.3. Roles en el tratamiento de datos personales
- 12.10.4. Derechos ARCO
- 12.10.5. El DPO. Funciones

Módulo 13. Gestión de la seguridad IT

13.1. Gestión de la seguridad
- 13.1.1. Operaciones de seguridad
- 13.1.2. Aspecto legal y regulatorio
- 13.1.3. Habilitación del negocio
- 13.1.4. Gestión de riesgos
- 13.1.5. Gestión de identidades y accesos

13.2. Estructura del área de seguridad. La oficina del CISO
- 13.2.1. Estructura organizativa. Posición del CISO en la estructura
- 13.2.2. Las líneas de defensa
- 13.2.3. Organigrama de la oficina del CISO
- 13.2.4. Gestión presupuestaria

13.3. Gobierno de seguridad
- 13.3.1. Comité de seguridad
- 13.3.2. Comité de seguimiento de riesgos
- 13.3.3. Comité de auditoría
- 13.3.4. Comité de crisis

13.4. Gobierno de seguridad. Funciones
- 13.4.1. Políticas y normas
- 13.4.2. Plan director de seguridad
- 13.4.3. Cuadros de mando
- 13.4.4. Concienciación y formación
- 13.4.5. Seguridad en la cadena de suministro

13.5. Operaciones de seguridad
- 13.5.1. Gestión de identidades y accesos
- 13.5.2. Configuración de reglas de seguridad de red. Firewalls
- 13.5.3. Gestión de plataformas IDS/IPS
- 13.5.4. Análisis de vulnerabilidades

13.6. Marco de trabajo de ciberseguridad. NIST CSF
- 13.6.1. Metodología NIST
  - 13.6.1.1. Identificar
  - 13.6.1.2. Proteger
  - 13.6.1.3. Detectar
  - 13.6.1.4. Responder
  - 13.6.1.5. Recuperar

13.7. Centro de operaciones de seguridad (SOC). Funciones
- 13.7.1. Protección. *Red Team, pentesting, threat intelligence*
- 13.7.2. Detección. SIEM, *user behavior analytics, fraud prevention*
- 13.7.3. Respuesta

13.8. Auditorías de seguridad
- 13.8.1. Test de intrusión
- 13.8.2. Ejercicios de *red team*
- 13.8.3. Auditorías de código fuente. Desarrollo seguro
- 13.8.4. Seguridad de componentes (*software supply chain*)
- 13.8.5. Análisis forense

13.9. Respuesta a incidentes
- 13.9.1. Preparación
- 13.9.2. Detección, análisis y notificación
- 13.9.3. Contención, erradicación y recuperación
- 13.9.4. Actividad post incidente
  - 13.9.4.1. Retención de evidencias
  - 13.9.4.2. Análisis forense
  - 13.9.4.3. Gestión de brechas
- 13.9.5. Guías oficiales de gestión de ciberincidentes

13.10. Gestión de vulnerabilidades
- 13.10.1. Análisis de vulnerabilidades
- 13.10.2. Valoración de vulnerabilidad
- 13.10.3. Bastionado de sistemas
- 13.10.4. Vulnerabilidades de día 0. Zero-day

Módulo 14. Análisis de riesgos y entorno de seguridad IT

14.1. Análisis del entorno
- 14.1.1. Análisis de la situación coyuntural
  - 14.1.1.1. Entornos VUCA
    - 14.1.1.1.1. Volátil
    - 14.1.1.1.2. Incierto
    - 14.1.1.1.3. Complejo
    - 14.1.1.1.4. Ambiguo
  - 14.1.1.2. Entornos BANI
    - 14.1.1.2.1. Quebradizo
    - 14.1.1.2.2. Ansioso
    - 14.1.1.2.3. No lineal
    - 14.1.1.2.4. Incomprensible
- 14.1.2. Análisis del entorno general. PESTEL
  - 14.1.2.1. Político
  - 14.1.2.2. Económico
  - 14.1.2.3. Social
  - 14.1.2.4. Tecnológico
  - 14.1.2.5. Ecológico/Ambiental
  - 14.1.2.6. Legal
- 14.1.3. Análisis de la situación interna. DAFO
  - 14.1.3.1. Objetivos
  - 14.1.3.2. Amenazas
  - 14.1.3.3. Oportunidades
  - 14.1.3.4. Fortalezas

14.2. Riesgo e incertidumbre
- 14.2.1. Riesgo
- 14.2.2. Gerencia de riesgos
- 14.2.3. Estándares de gestión de riesgos

14.3. Directrices para la gestión de riesgos ISO 31.000:2018
- 14.3.1. Objeto
- 14.3.2. Principios
- 14.3.3. Marco de referencia
- 14.3.4. Proceso

14.4. Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT)
- 14.4.1. Metodología MAGERIT
  - 14.4.1.1. Objetivos
  - 14.4.1.2. Método
  - 14.4.1.3. Elementos
  - 14.4.1.4. Técnicas
  - 14.4.1.5. Herramientas disponibles (PILAR)

14.5. Transferencia del riesgo cibernético
- 14.5.1. Transferencia de riesgos
- 14.5.2. Riesgos cibernéticos. Tipología
- 14.5.3. Seguros de ciber riesgos

14.6. Metodologías ágiles para la gestión de riesgos
- 14.6.1. Metodologías ágiles
- 14.6.2. Scrum para la gestión del riesgo
- 14.6.3. *Agile risk management*

14.7. Tecnologías para la gestión del riesgo
- 14.7.1. Inteligencia artificial aplicada a la gestión de riesgos
- 14.7.2. *Blockchain* y criptografía. Métodos de preservación del valor
- 14.7.3. Computación cuántica. Oportunidad o amenaza

14.8. Elaboración de mapas de riesgos IT basados en metodologías ágiles
- 14.8.1. Representación de la probabilidad y el impacto en entornos ágiles
- 14.8.2. El riesgo como amenaza del valor
- 14.8.3. Re-evolución en la gestión de proyectos y procesos ágiles basados en KRIs

14.9. *Risk driven* en la gestión de riesgos
- 14.9.1. *Risk driven*
- 14.9.2. *Risk driven* en la gestión de riesgos
- 14.9.3. Elaboración de un modelo de gestión empresarial impulsado por el riesgo

14.10. Innovación y transformación digital en la gestión de riesgos IT
- 14.10.1. La gestión de riesgos ágiles como fuente de innovación empresarial
- 14.10.2. Transformación de datos en información útil para la toma de decisiones
- 14.10.3. Visión holística de la empresa a través del riesgo

Módulo 15. Criptografía en IT

15.1. Criptografía
- 15.1.1. Criptografía
- 15.1.2. Fundamentos matemáticos

15.2. Criptología
- 15.2.1. Criptología
- 15.2.2. Criptoanálisis
- 15.2.3. Esteganografía y estegoanálisis

15.3. Protocolos criptográficos
- 15.3.1. Bloques básicos
- 15.3.2. Protocolos básicos
- 15.3.3. Protocolos intermedios
- 15.3.4. Protocolos avanzados
- 15.3.5. Protocolos exotéricos

15.4. Técnicas criptográficas
- 15.4.1. Longitud de claves
- 15.4.2. Manejo de claves
- 15.4.3. Tipos de algoritmos
- 15.4.4. Funciones resumen. *Hash*
- 15.4.5. Generadores de números pseudoaleatorios
- 15.4.6. Uso de algoritmos

15.5. Criptografía simétrica
- 15.5.1. Cifrados de bloque
- 15.5.2. DES (*Data Encryption Standard*)
- 15.5.3. Algoritmo RC4
- 15.5.4. AES (*Advanced Encryption Standard*)
- 15.5.5. Combinación de cifrados de bloques
- 15.5.6. Derivación de claves

15.6. Criptografía asimétrica
- 15.6.1. Diffie-Hellman
- 15.6.2. DSA (*Digital Signature Algorithm*)
- 15.6.3. RSA (*Rivest, Shamir y Adleman*)
- 15.6.4. Curva elíptica
- 15.6.5. Criptografía asimétrica. Tipología

15.7. Certificados digitales
- 15.7.1. Firma digital
- 15.7.2. Certificados X509
- 15.7.3. Infraestructura de clave pública (PKI)

15.8. Implementaciones
- 15.8.1. Kerberos
- 15.8.2. IBM CCA
- 15.8.3. *Pretty Good Privacy* (PGP)
- 15.8.4. ISO *Authentication Framework*
- 15.8.5. SSL y TLS
- 15.8.6. Tarjetas inteligentes en medios de pago (EMV)
- 15.8.7. Protocolos de telefonía móvil
- 15.8.8. *Blockchain*

15.9. Esteganografía
- 15.9.1. Esteganografía
- 15.9.2. Estegoanálisis
- 15.9.3. Aplicaciones y usos

15.10. Criptografía cuántica
- 15.10.1. Algoritmos cuánticos
- 15.10.2. Protección de algoritmos frente a computación cuántica
- 15.10.3. Distribución de claves cuántica

Módulo 16. Gestión de identidad y accesos en seguridad IT

16.1. Gestión de identidad y accesos (IAM)
- 16.1.1. Identidad digital
- 16.1.2. Gestión de identidad
- 16.1.3. Federación de identidades

16.2. Control de acceso físico
- 16.2.1. Sistemas de protección
- 16.2.2. Seguridad de las áreas
- 16.2.3. Instalaciones de recuperación

16.3. Control de acceso lógico
- 16.3.1. Autenticación: Tipología
- 16.3.2. Protocolos de autenticación
- 16.3.3. Ataques de autenticación

16.4. Control de acceso lógico. Autenticación MFA
- 16.4.1. Control de acceso lógico. Autenticación MFA
- 16.4.2. Contraseñas. Importancia
- 16.4.3. Ataques de autenticación

16.5. Control de acceso lógico. Autenticación biométrica
- 16.5.1. Control de Acceso Lógico. Autenticación biométrica
  - 16.5.1.1. Autenticación biométrica. Requisitos
- 16.5.2. Funcionamiento
- 16.5.3. Modelos y técnicas

16.6. Sistemas de gestión de autenticación
- 16.6.1. *Single sign on*
- 16.6.2. Kerberos
- 16.6.3. Sistemas AAA

16.7. Sistemas de gestión de autenticación: Sistemas AAA
- 16.7.1. TACACS
- 16.7.2. RADIUS
- 16.7.3. DIAMETER

16.8. Servicios de control de acceso
- 16.8.1. FW - Cortafuegos
- 16.8.2. VPN - Redes Privadas Virtuales
- 16.8.3. IDS - Sistema de Detección de Intrusiones

16.9. Sistemas de control de acceso a la red
- 16.9.1. NAC
- 16.9.2. Arquitectura y elementos
- 16.9.3. Funcionamiento y estandarización

16.10. Acceso a redes inalámbricas
- 16.10.1. Tipos de redes inalámbricas
- 16.10.2. Seguridad en redes inalámbricas
- 16.10.3. Ataques en redes inalámbricas

Módulo 17. Seguridad en comunicaciones y operación software

17.1. Seguridad informática en comunicaciones y operación software
- 17.1.1. Seguridad informática
- 17.1.2. Ciberseguridad
- 17.1.3. Seguridad en la nube

17.2. Seguridad informática en comunicaciones y operación software. Tipología
- 17.2.1. Seguridad física
- 17.2.2. Seguridad lógica

17.3. Seguridad en comunicaciones
- 17.3.1. Principales elementos
- 17.3.2. Seguridad de redes
- 17.3.3. Mejores prácticas

17.4. Ciberinteligencia
- 17.4.1. Ingeniería social
- 17.4.2. *Deep web*
- 17.4.3. *Phishing*
- 17.4.4. *Malware*

17.5. Desarrollo seguro en comunicaciones y operación software
- 17.5.1. Desarrollo seguro. Protocolo HTTP
- 17.5.2. Desarrollo seguro. Ciclo de vida
- 17.5.3. Desarrollo seguro. Seguridad PHP
- 17.5.4. Desarrollo seguro. Seguridad NET
- 17.5.5. Desarrollo seguro. Mejores prácticas

17.6. Sistemas de gestión de la seguridad de la información en comunicaciones y operación software
- 17.6.1. GDPR
- 17.6.2. ISO 27021
- 17.6.3. ISO 27017/18

17.7. Tecnologías SIEM
- 17.7.1. Tecnologías SIEM
- 17.7.2. Operativa de SOC
- 17.7.3. SIEM *vendors*

17.8. El rol de la seguridad en las organizaciones
- 17.8.1. Roles en las organizaciones
- 17.8.2. Rol de los especialistas IoT en las compañías
- 17.8.3. Certificaciones reconocidas en el mercado

17.9. Análisis forense
- 17.9.1. Análisis forense
- 17.9.2. Análisis forense. Metodología
- 17.9.3. Análisis forense. Herramientas e implantación

17.10. La ciberseguridad en la actualidad
- 17.10.1. Principales ataques informáticos
- 17.10.2. Previsiones de empleabilidad
- 17.10.3. Retos

Módulo 18. Seguridad en entornos *cloud*

18.1. Seguridad en entornos *cloud computing*
- 18.1.1. Seguridad en entornos *cloud computing*
- 18.1.2. Seguridad en entornos *cloud computing*. Amenazas y riesgos seguridad
- 18.1.3. Seguridad en entornos *cloud computing*. Aspectos clave de seguridad

18.2. Tipos de infraestructura *cloud*
- 18.2.1. Público
- 18.2.2. Privado
- 18.2.3. Híbrido

18.3. Modelo de gestión compartida
- 18.3.1. Elementos de seguridad gestionados por proveedor
- 18.3.2. Elementos gestionados por cliente
- 18.3.3. Definición de la estrategia para seguridad

18.4. Mecanismos de prevención
- 18.4.1. Sistemas de gestión de autenticación
- 18.4.2. Sistema de gestión de autorización: Políticas de acceso
- 18.4.3. Sistemas de gestión de claves

18.5. Securización de sistemas
- 18.5.1. Securización de los sistemas de almacenamiento
- 18.5.2. Protección de los sistemas de base de datos
- 18.5.3. Securización de datos en tránsito

18.6. Protección de infraestructura
- 18.6.1. Diseño e implementación de red segura
- 18.6.2. Seguridad en recursos de computación
- 18.6.3. Herramientas y recursos para protección de infraestructura

18.7. Detección de las amenazas y ataques
- 18.7.1. Sistemas de auditoría, *logging* y monitorización
- 18.7.2. Sistemas de eventos y alarmas
- 18.7.3. Sistemas SIEM

18.8. Respuesta ante incidentes
- 18.8.1. Plan de respuesta a incidentes
- 18.8.2. La continuidad de negocio
- 18.8.3. Análisis forense y remediación de incidentes de la misma naturaleza

18.9. Seguridad en *clouds* públicos
- 18.9.1. AWS (Amazon Web Services)
- 18.9.2. Microsoft Azure
- 18.9.3. Google GCP
- 18.9.4. Oracle Cloud

18.10. Normativa y cumplimiento
- 18.10.1. Cumplimiento de normativas de seguridad
- 18.10.2. Gestión de riesgos
- 18.10.3. Personas y proceso en las organizaciones

Módulo 19. Seguridad en comunicaciones de dispositivos Iot

19.1. De la telemetría al IoT
- 19.1.1. Telemetría
- 19.1.2. Conectividad M2M
- 19.1.3. Democratización de la telemetría

19.2. Modelos de referencia IoT
- 19.2.1. Modelo de referencia IoT
- 19.2.2. Arquitectura simplificada IoT

19.3. Vulnerabilidades de seguridad del IoT
- 19.3.1. Dispositivos IoT
- 19.3.2. Dispositivos IoT. Casuística de uso
- 19.3.3. Dispositivos IoT. Vulnerabilidades

19.4. Conectividad del IoT
- 19.4.1. Redes PAN, LAN, WAN
- 19.4.2. Tecnologías inalámbricas no IoT
- 19.4.3. Tecnologías inalámbricas LPWAN

19.5. Tecnologías LPWAN
- 19.5.1. El triángulo de hierro de las redes LPWAN
- 19.5.2. Bandas de frecuencia libres vs. Bandas licenciadas
- 19.5.3. Opciones de tecnologías LPWAN

19.6. Tecnología LoRaWAN
- 19.6.1. Tecnología LoRaWAN
- 19.6.2. Casos de uso LoRaWAN. Ecosistema
- 19.6.3. Seguridad en LoRaWAN

19.7. Tecnología Sigfox
- 19.7.1. Tecnología Sigfox
- 19.7.2. Casos de uso Sigfox. Ecosistema
- 19.7.3. Seguridad en Sigfox

19.8. Tecnología Celular IoT
- 19.8.1. Tecnología Celular IoT (NB-IoT y LTE-M)
- 19.8.2. Casos de uso Celular IoT. Ecosistema
- 19.8.3. Seguridad en Celular IoT

19.9. Tecnología WiSUN
- 19.9.1. Tecnología WiSUN
- 19.9.2. Casos de uso WiSUN. Ecosistema
- 19.9.3. Seguridad en WiSUN

19.10. Otras tecnologías IoT
- 19.10.1. Otras tecnologías IoT
- 19.10.2. Casos de uso y ecosistema de otras tecnologías IoT
- 19.10.3. Seguridad en otras tecnologías IoT

Módulo 20. Plan de continuidad del negocio asociado a la seguridad

20.1. Plan de continuidad de negocio
- 20.1.1. Los planes de continuidad de negocio (PCN)
- 20.1.2. Plan de continuidad de negocio (PCN). Aspectos clave
- 20.1.3. Plan de continuidad de negocio (PCN) para la valoración de la empresa

20.2. Métricas en un plan de continuidad de negocio (PCN)
- 20.2.1. *Recovery time objective* (RTO) y *recovery point objective* (RPO)
- 20.2.2. Tiempo máximo tolerable (MTD)
- 20.2.3. Niveles mínimos de recuperación (ROL)
- 20.2.4. Punto de recuperación objetivo (RPO)

20.3. Proyectos de continuidad. Tipología
- 20.3.1. Plan de continuidad de negocio (PCN)
- 20.3.2. Plan de continuidad de TIC (PCTIC)
- 20.3.3. Plan de recuperación ante desastres (PRD)

20.4. Gestión de riesgos asociada al PCN
- 20.4.1. Análisis de impacto sobre el negocio
- 20.4.2. Beneficios de la implantación de un PCN
- 20.4.3. Mentalidad basada en riesgos

20.5. Ciclo de vida de un plan de continuidad de negocio
- 20.5.1. Fase 1: análisis de la organización
- 20.5.2. Fase 2: determinación de la estrategia de continuidad
- 20.5.3. Fase 3: respuesta a la contingencia
- 20.5.4. Fase 4: prueba, mantenimiento y revisión

20.6. Fase del análisis de la organización de un PCN
- 20.6.1. Identificación de procesos en el alcance del PCN
- 20.6.2. Identificación de áreas críticas del negocio
- 20.6.3. Identificación de dependencias entre áreas y procesos
- 20.6.4. Determinación del MTD adecuado
- 20.6.5. Entregables. Creación de un plan

20.7. Fase de determinación de la estrategia de continuidad en un PCN
- 20.7.1. Roles en la fase de determinación de la estrategia
- 20.7.2. Tareas de la fase de determinación de la estrategia
- 20.7.3. Entregables

20.8. Fase de respuesta a la contingencia en un PCN
- 20.8.1. Roles en la fase de respuesta
- 20.8.2. Tareas en esta fase
- 20.8.3. Entregables

20.9. Fase de pruebas, mantenimiento y revisión de un PCN
- 20.9.1. Roles en la fase de pruebas, mantenimiento y revisión
- 20.9.2. Tareas en la fase de pruebas, mantenimiento y revisión
- 20.9.3. Entregables

20.10. Normas ISO asociadas a los planes de continuidad de negocio (PCN)
- 20.10.1. ISO 22301:2019
- 20.10.2. ISO 22313:2020
- 20.10.3. Otras normas ISO e internacionales relacionadas

Podrás profundizar en cuestiones como el plan de continuidad del negocio asociado a la seguridad o la gestión de identidad y accesos en seguridad IT”

06

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"

En TECH empleamos el Método del Caso

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"



Somos la primera universidad online en español que combina los case studies de Harvard Business School con un sistema de aprendizaje 100% online basado en la reiteración.



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

Este programa intensivo de Informática de TECH Universidad Tecnológica te prepara para afrontar todos los retos en esta área, tanto en el ámbito nacional como internacional. Tenemos el compromiso de favorecer el crecimiento personal y profesional, la mejor forma de caminar hacia el éxito, por eso, en TECH Universidad Tecnológica utilizarás los *case studies* de Harvard, con la cual tenemos un acuerdo estratégico, que nos permite acercar a nuestros alumnos los materiales de la mejor universidad del mundo.

> *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

Nuestra universidad es la primera en el mundo que combina los *case studies* de Harvard University con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

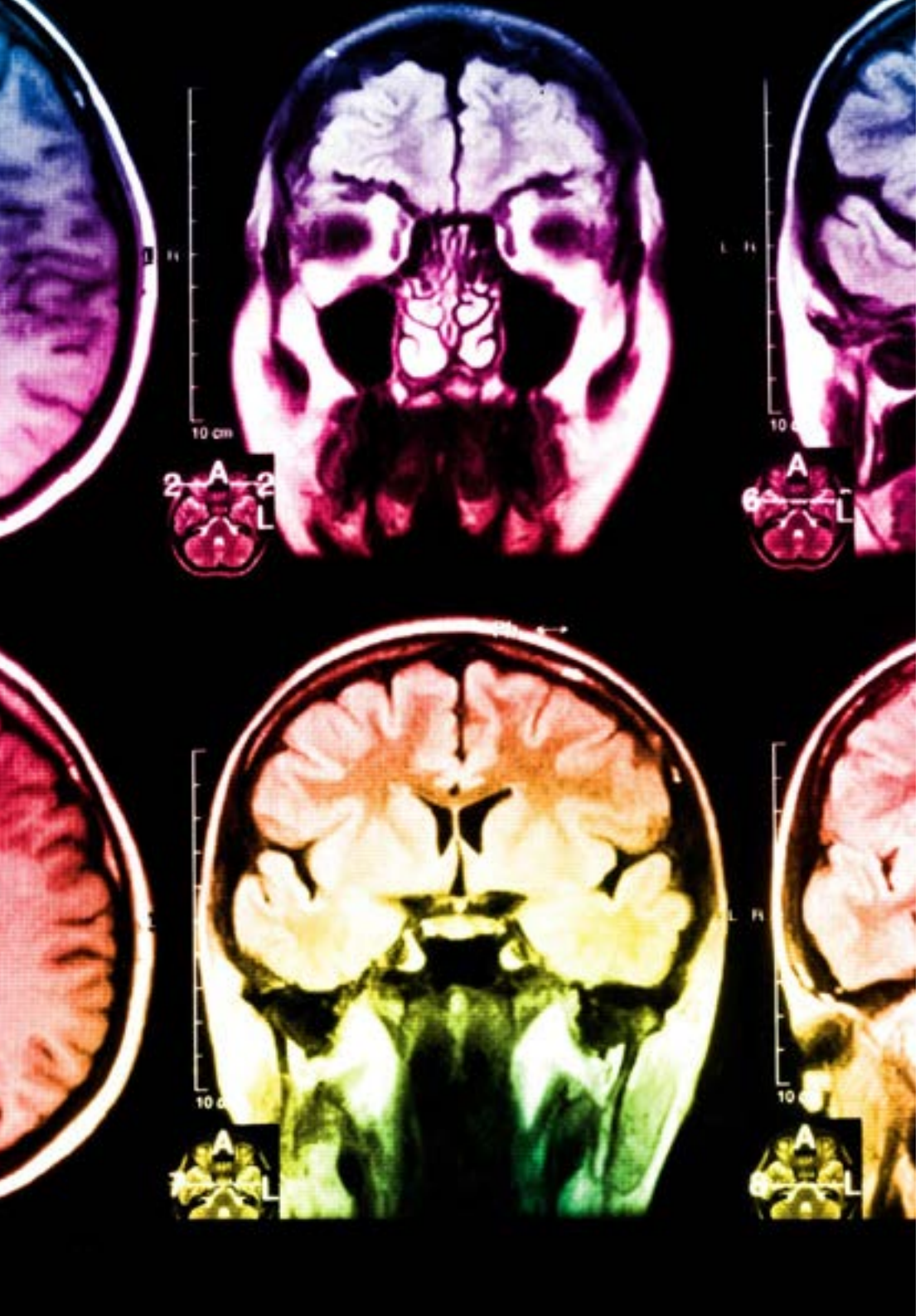
Potenciamos los *case studies* de Harvard con el mejor método de enseñanza 100% online: el Relearning.

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.

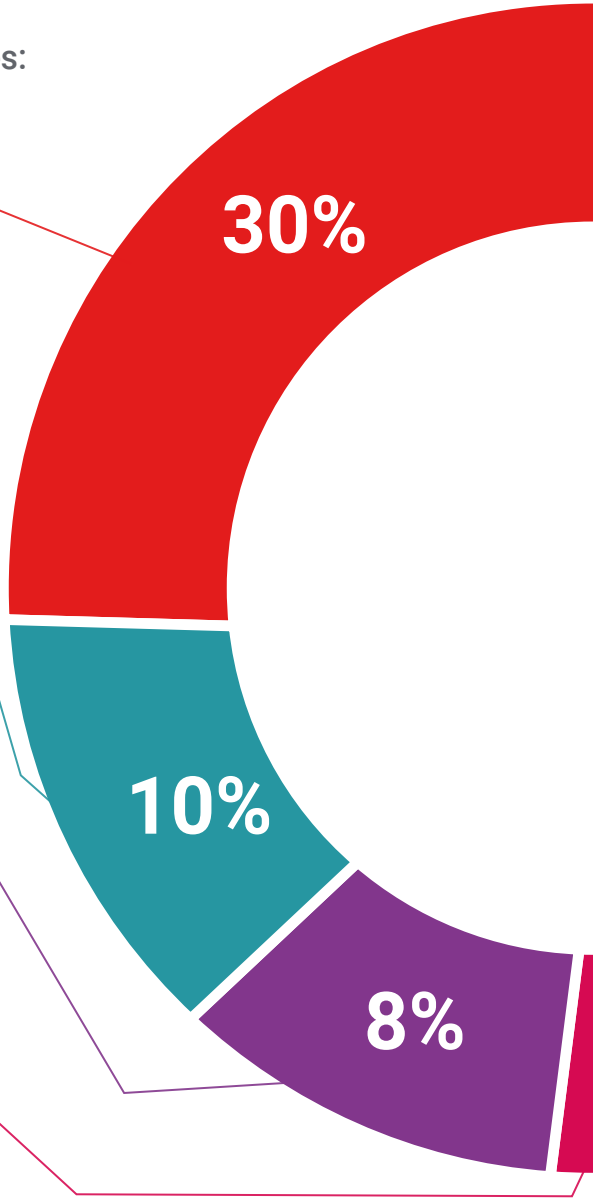
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

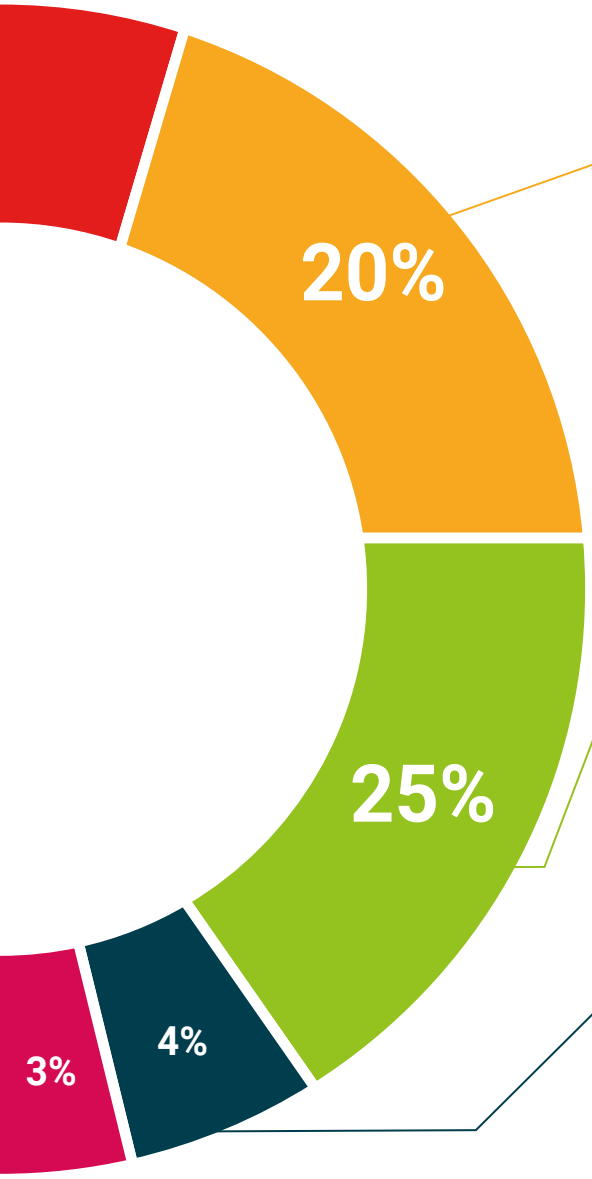
Prácticas de habilidades y competencias

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 cases studies de la materia que se emplean en Harvard. 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.

07

Titulación

El Grand Master en Alta Dirección de Ciberseguridad garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Grand Master expedido por TECH Universidad Tecnológica.





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

Este **Grand Master en Alta Dirección de Ciberseguridad** contiene el programa más completo y actualizado del mercado.

Tras la superación de la evaluación, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Grand Master** emitido por **TECH Universidad Tecnológica**.

El título expedido por **TECH Universidad Tecnológica** expresará la calificación que haya obtenido en el Grand Master, y reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

Título: **Grand Master en Alta Dirección de Ciberseguridad**

Nº Horas Oficiales: **3.000**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

GRAND MASTER

en

Alta Dirección de Ciberseguridad

Se trata de un título propio de esta Universidad con una duración de 3.000 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

Este título propio se deberá acompañar siempre del título universitario habilitante expedido por la autoridad competente para ejercer profesionalmente en cada país. código único TECH: AFWOR23S techtitute.com/titulos


Grand Master en Alta Dirección de Ciberseguridad

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Ciberinteligencia y ciberseguridad	150	OB
1º	Seguridad en host	150	OB
1º	Seguridad en red (perimetral)	150	OB
1º	Seguridad en smartphones	150	OB
1º	Seguridad en IoT	150	OB
1º	Hacking ético	150	OB
1º	Ingeniería inversa	150	OB
1º	Desarrollo seguro	150	OB
1º	Análisis forense	150	OB
1º	Retos Actuales y Futuros en Seguridad Informática	150	OB

Curso	Materia	Horas	Carácter
2º	Seguridad en el diseño y desarrollo de sistemas	150	OB
2º	Arquitecturas y modelos de seguridad de la información	150	OB
2º	Gestión de la seguridad IT	150	OB
2º	Análisis de riesgos y entorno de seguridad IT	150	OB
2º	Criptografía en IT	150	OB
2º	Gestión de identidad y accesos en seguridad IT	150	OB
2º	Seguridad en comunicaciones y operación software	150	OB
2º	Seguridad en entornos cloud	150	OB
2º	Seguridad en comunicaciones de dispositivos Iot	150	OB
2º	Plan de continuidad del negocio asociado a la seguridad	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech universidad tecnológica

Grand Master

Alta Dirección de Ciberseguridad

Modalidad: **Online**

Duración: **2 años**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **3.000 h.**

Grand Master
Alta Dirección de Ciberseguridad



tech universidad tecnológica