Máster en Ciberseguridad en colaboración con Telefefónica

Guía Académica Completa

Índice

1. Guía rápida

Descripción

El Máster Telefónica en Ciberseguiridad, nace de la necesidad de impartir formación en seguridad sólida, actualizada y que abarque la realidad de la ciberseguridad real desde sus cimientos.

Al finalizar el master, los alumnos contarán con el potencial suficiente para cubrir algunos de los perfiles más demandados en el campo de la ciberseguridad, de la mano de profesionales que se dedican, en su día a día, a desarrollar las habilidades que van a impartir para desempeñar su trabajo.

Objetivos

Si bien el máster tiene como objetivo cubrir el plano de la seguridad en profundidad (desde las directivas y procedimientos hasta los datos, pasando por las redes perimetrales, hosts, aplicaciones y redes internas...) huye de los planteamientos clásicos para adaptarse a una realidad donde los nuevos paradigmas de arquitecturas en cloud, IoT o técnicas de OSINT son los que realmente vertebran la ciberseguridad demandada en el mercado.

Destinatarios

El Máster, va dirigido a Titulados Superiores, programadores, desarrolladores y arquitectos, enfocados en la seguridad como requisito. Igualmente a Analistas de seguridad e inteligencia, Consultores y gestores de seguridad integral, Pentesters y auditores de seguridad, Administradores en general con foco en la seguridad como elemento clave y a culaquier persona que, con perfil técnico, esté interesado en orientar o reorientar su Carrera profesional sobre el mundo de la Ciberseguridad.

Certificación Universitaria

Máster Profesional, certificado como Título Propio por la Universidad Católica de Murcia. Institución Académica fundada en el año 1996, en Murcia (España).

Campus multidispositivo 24x7

Podrás acceder al Campus Virtual y a todos los contenidos y actividades del Máster estés donde estés.

Además, podrás comunicarte con el equipo tutorial desde la propia plataforma de formación, a través de tu PC de sobremesa, tu tablet o tu smartphone.

Telefónica & ElevenPaths

Con la participación de Telefónica & ElevenPaths, que contribuyen al desarrollo del Máster a través de la elaboración del programa formativo y la coordinación del profesorado, así como con docentes que desempeñan su labor profesional en empresas del Grupo Telefónica.

- Con la colaboracion de Telefonica & ElevenPaths
- Con el Aval Académnico de la Universidad Católica de Murcia (UCAM)
- Servicios Tutoriales, adapatados a cada estudiante
- Prácticas Opcionales, tras procesos de selección, en empresas punteras en Ciberseguridad

2. El Máster

2.1. Presentación

La seguridad en general y la **ciberseguridad** en particular forman ya parte de nuestro lenguaje cotidiano. La privacidad, los ataques, las vulnerabilidades, el malware, el ciberespionaje… son conceptos que se han incorporado a nuestro día a día, no solo desde el punto de vista del ciudadano, sino desde la perspectiva de los gobiernos, organizaciones, dirigentes, ingenieros, estrategas… Internet y las redes están tan integradas en tantas disciplinas, que la seguridad resulta transversal a todas las áreas e imprescindible en la inmensa mayoría de ellas. Desde principios de este siglo con ataques esporádicos y artesanales a usuarios y sistemas, hasta las ciberguerras y espionaje consolidado que actualmente se libra en la Red: la **tendencia a considerar la seguridad como espina dorsal que debe vertebrar todas las comunicaciones entre personas y dispositivos**, es cada vez mayor.

Como reflejo de esta tendencia, **la seguridad informática se ha convertido en una de las profesiones más cotizadas**. De hecho, la última edición del informe '*Los + Buscados*' del Grupo Adecco, afirma que **el ingeniero de seguridad IT será el profesional mejor pagado de 2017**, con sueldos en la horquilla de entre 50.000 y 90.000 euros brutos. ¿Cómo cubrir esta demanda? Aunque siempre ha estado ahí, como área a tener en cuenta, los atacantes y los ataques han ido por delante de los dedicados a proteger datos, redes e infraestructuras. La oferta de formación oficial especializada en el campo de la ciberseguriad ha sido escasa, obsoleta, no estructurada o deficiente en su vertiente más profesional. Hasta ahora, los profesionales de la seguridad más reputados confiesan, en su mayoría, haber sido autodidactas.

Este máster nace de la necesidad de impartir **formación en seguridad sólida, actualizada y que abarque la realidad de la ciberseguridad real desde sus cimientos**.

Al finalizar el master, **los alumnos contarán con el potencial suficiente para cubrir algunos de los perfiles más demandados en el campo de la ciberseguridad**, de la mano de profesionales que se dedican en su día a día a desarrollar las habilidades que van a impartir para desempeñar su trabajo.

Si bien **el máster tiene como objetivo cubrir el típico plano de la seguridad en profundidad (desde las directivas y procedimientos hasta los datos, pasando por las redes perimetrales, hosts, aplicaciones y redes internas…) huyendo de los planteamientos clásicos para adaptarse a una realidad donde los nuevos paradigmas de arquitecturas en cloud, IoT o técnicas de OSINT son los que realmente vertebran la ciberseguridad demandada en el mercado.** También se aleja de los planteamientos enquistados en obviedades obsoletas para ahondar en la vulnerabilidad como piedra angular de la seguridad, atajando los problemas de raíz desde una profunda comprensión y mostrando no solo cómo mitigar los fallos sino además por qué se producen. Esto nos lleva no solo a mostrar una serie de herramientas, sino a plantear los problemas y permitir al alumno encontrar las utilidades más adecuadas para resolver un problema que ya conoce y ha interiorizado. La compresión del problema y las posibilidades de solución se vuelen así mucho más eficaces para construir un futuro profesional.

Mediante una **combinación equilibrada de teoría y práctica** los estudiantes serán capaces de hacerse las preguntas correctas ante un incidente, aplicar las medidas más eficaces y eficientes, entender los fallos más comunes a la hora de diseñar sistemas complejos y comprender por qué y cómo se producen los fallos de seguridad. Además, ahondarán en la **seguridad específica del IoT**, las complejas arquitecturas que realmente se están construyendo en torno a la seguridad en cloud y a aprovechar la información pública en la red para investigar y obtener la mejor información en un océano de datos.

Además de la teoría y las pruebas técnicas diseñadas, **el máster contará con un seminario en directo por cada módulo que consistirá en clases magistrales donde los profesionales más reconocidos del sector ofrecerán una visión particular del temario del módulo basada en la experiencia profesional y la visión de la industria.** Entre otras, contaremos con seminarios sobre la seguridad como negocio, cómo se aborda la vigilancia digital en las grandes empresas, pentesting, gestión de código seguro en la los procesos profesionales de ingeniería del software… todos impartidos por profesionales reconocidos del sector.

2.2. Centro donde se imparte

Campus Internacional el Ciberseguridad [https://www.campusciberseguiridad.com]

2.3. Rama de conocimiento

Informática y Telecomunicaciones

2.4. Modalidad de enseñanza

100% On-line (Posibilidad de realizarlo en Modalidad Semipresencial, en sucesivas ediciones)

2.5. Lengua en la que se imparte

Español

2.6. Duración del Título

1 año, aproximadamente

2.7. Calendario

Del 10 de octubre de 2017 al 30 de junio de 2018.

2.8. Número de plazas ofertadas

60 plazas por edición.

2.9. Número de ECTS del Título

El Máster certificará 60 Créditos ECTS.

2.10. Total de horas en sus diferentes modalidades

El Máster está Certificado con 1.500 horas.

2.11. Destinatarios

Algunos de los destinatarios principales del Máster pueden ser:

- Titulados Superiores, programadores, desarrolladores y arquitectos, enfocados en la seguridad como requisito.
- Analistas de seguridad e inteligencia, Consultores y gestores de seguridad integral, Pentesters y auditores de seguridad, Administradores en general con foco en la seguridad como elemento clave.
- Cualquier persona que, con perfil técnico, esté interesado en orientar o reorientar su carrera profesional sobre el mundo de la Ciberseguridad.

3. Objetivos

Los **objetivos esenciales y las competencias**, que se alcanzarán a lo largo de la impartición del Máster, se pueden resumir en los siguientes:

Objetivos generales:

- Ofrecer una visión realista sobre los diferentes campos de la ciberseguridad actual.
- Comprender la seguridad desde sus cimientos, para construir un discurso completo que abarque desde la vulnerabilidad hasta las políticas y procedimientos.
- Actualizar la información sobre ciberseguridad al verdadero estado del arte del momento actual.
- Incorporar conocimiento demandado actualmente en la industria, como seguridad específica IoT, OSINT y seguridad en Cloud.
- Comprender no solo el punto de vista del atacado, sino del atacante.

Competencias:

- Analizar incidentes de seguridad desde un punto de vista profesional y realista.
- Comprender las amenazas existentes y aplicar las contramedidas más eficaces.
- Dividir eficientemente los activos para poder protegerlos con las herramientas adecuadas y manejando las expectativas correctamente sobre su rendimiento y eficacia.
- Realizar investigaciones online.
- Proteger adecuadamente y entender las características particulares del IoT.
- Comprender los retos del desarrollo seguro, las vulnerabilidades y cómo prevenirlas.
- Comprender los retos del despliegue en arquitecturas seguras, las vulnerabilidades y cómo prevenirlas.

4. Certificación

El Máster cuenta con **Certificación Universitaria**, **Máster Telefónica en Ciberseguridad**, como Título Propio de la Universidad Católica de Murcia (UCAM), con 60 Créditos ECTS, equivalents a 1.500 horas.

5. Calendario y exámenes

Periodo lectivo: del 10 de octubre de 2017 al 30 junio de 2018.

Sistema de evaluación: Sistema de evaluación continua, 100% on-line, compuesta por Cuestionarios de evaluación, Tareas de desarrollo práctico y Actividades colaborativas (en cada uno de los Módulos) y Proyecto Fin de Máster.

Un sistema de evaluación continua asegurará la asimilación del conocimiento a lo largo de todo el periodo formativo y la adquisición de las competencias y destrezas necesarias para desempeñar, una vez superado el Máster, su labor, de forma eficiente, en el sector de la Ciberseguridad.

6. Matrícula

Como requisitos para la matriculación, el alumno debe aportar la siguiente **documentación**;

- Solicitud de Admisión
- Curriculum Vitae
- DNI / NIF / NIE / Pasaporte / Cédula de Identidad
- Fotografía tamaño carnet
- Titulación Académica

7. Profesorado

El **claustro** del **Máster en Ciberseguridad en colaboración con Telefónica**, está formado por los siguientes profesionales:

Jesús Torres es Ingeniero en informática por la Universidad de Granada. Actualmente es Technical lead, en Telefónica Digital España, de importantes proyectos donde el desarrollo de una arquitectura eficiente y segura resulta primordial. En el pasado ha trabajado como Arquitecto Software para Telefónica Digital y también ha ejercido en ElevenPaths como Security Developer para el laboratorio de seguridad. Ahora se encuentra cursando sus estudios de posgrado en Ciencia de Datos.

Julio Gómez Ortega tiene más de 8 años de experiencia como Pentester en varias empresas nacionales e internacionales. Actualmente, trabaja como consultor de seguridad informática en Telefónica, en donde desarrolla servicios de innovación asociados a Threat Intelligence. También, es ponente habitual en diferentes foros de seguridad y co-fundador de HackMeets.

José Rodríguez Pérez es Ingeniero Superior en Telecomunicaciones por la Universidad de Alcalá. José co-lideró la creación de la guía IoT Security Self-Asessment publicada por la GSMA y coordina las actividades de seguridad en grupo de Plataformas y Tecnología del área de IoT en Telefónica. Antes de unirse a la unidad de IoT, trabajó en el desarrollo de software, social media, APIs abiertas para desarrolladores y pagos en Telefónica. Ha representado a Telefónica en varios eventos para desarrolladores e industria (Campus Party México 2012, Green Hackathon Barcelona MWC 2012, HackForGood Valencia 2015, Intel Edison Movilforum Hackathon 2015, Telefónica Todos Incluidos Hackathon 2015).

Carmen Torrano es doctora en Informática por la Universidad Carlos III de Madrid. El doctorado, especializado en seguridad informática e inteligencia artificial, lo desarrolló en el Consejo Superior de Investigaciones Científicas. Actualmente trabaja como investigadora senior en el departamento de innovación de ElevenPaths (Telefónica Digital España). Entre las labores de investigación se encuentran la apertura de líneas que puedan derivar en la introducción de elementos innovadores que mejoren los productos o en la creación de nuevos productos. Además es profesora en la Universidad de Castilla La Mancha. Carmen ha publicado en numerosas conferencias y revistas, y colabora en la difusión de contenidos científico-técnicos.

Marcos Arjona trabaja como Consultor de Innovación e Investigación en ElevenPaths, división global de ciberseguridad de Telefónica. Desde 2011 ha estado ligado a la seguridad y privacidad de la información inicialmente en la Universidad de Málaga y posteriormente en el Centro Andaluz de Tecnologías de la Información y las Comunicaciones donde ha participado y conseguido varios proyectos Europeos relacionados con la ciberseguridad. Ha sido gestor del clúster andaluz de la AEI de Ciberseguridad y en su labor actual es responsable de la evaluación y análisis de soluciones de seguridad que provean tecnologías y servicios de ciberseguridad cuya principal componente sea la innovación.

Javier Espinosa actualmente es Tech Lead en ElevenPaths, la unidad de ciberseguridad de Telefonica donde se incorporó en el año 2013. Anteriormente formó parte de beMee Technologies como responsable de aplicaciones Android y como investigador en prácticas del Grupo de Sistemas Inteligentes de la Universidad Politécnica de Madrid realizando proyectos de web semántica y análisis de sentimientos.

Pablo San Emeterio es Ingeniero Informático y Máster en Auditoría y Seguridad de la Información por la UPM. Llleva trabajando en el mundo de la seguridad más de 8 años, destacando principalmente sus investigaciones sobre la seguridad de las distintas aplicaciones de mensajería instantánea junto con trabajos sobre técnicas de hooking. Esto le ha permitido participar como unos de los ponentes principales en eventos internacionales de renombre tales como Shmoocon (Washington), Black Hat (Amsterdam, Sao Paulo y Las Vegas), Defcon (Las Vegas), así como repetidas ponencias en congresos nacionales de prestigio como Rootedcon, NcN, Navajas Negras, ConectaCON, etc.

Sergio de los Santos es el Director Académico del Programa del Máster en Ciberseguridad en colaboración con Telefónica, durante los años 2016 y 2017 cordinó y diseñó el programa académico. Actualmente es director del área de Innovación y Laboratorio de ElevenPaths en Telefónica Digital España. De 2005 a 2013, ha sido Consultor Técnico en Hispasec, responsable de antifraude, del servicio de alertas de vulnerabilidades y de la publicación sobre seguridad más veterana en español.

Desde el año 2000 ha trabajado como auditor y coordinador técnico, ha escrito un libro sobre la historia de la seguridad, y tres libros más técnicos sobre hacking y seguridad Windows.

Es ingeniero técnico en informática de sistemas por la Universidad de Málaga, donde también ha cursado un Máster en Ingeniería del Software e Inteligencia Artificial. Ha sido galardonado durante 2013 a 2105 con el premio Microsoft MVP Consumer Security e imparte clases del máster de Seguridad TIC en la Universidad de Sevilla, además de galardonado como MVP de seguridad de Microsoft.

David R. Sáez Ávila. Co-Director Académico. Máster en Gestión de Proyectos, en Dirección comercial y Marketing, Liderazgo y Desarrollo de Aplicaciones para Internet.

Es Director del Big Data International Campus y Co-director académico del Campus Internacional en Ciberseguridad.

Tiene más de 16 años dirigiendo proyectos de e-learning para compañías de primer nivel, tanto nacionales como internacionales. Es experto en tecnología educativa, e-learning, nuevas metodologías, producción y gestión de cursos de posgrado y de plataformas de formación. A lo largo de la impartición del Máster, se encargará de introducir a los estudiantes en el uso de la plataforma e-learning y de la dirección académica, dinamización y conducción cada uno de los módulos del Máster, siendo su enlace académico con el campus y con los tutores.

8. Plan de Estudios

A continuación, presentamos el Plan de Estudios del Máster:

MÓDULO 1: CRIPTOGRAFÍA.
100 horas / 4 créditos.

La criptografía ha jugado un papel fundamental en la historia en relación con la protección de secretos y ha evolucionado a lo largo del tiempo, pasando de los sencillos algoritmos iniciales a sistemas mucho más complejos con un fuerte fundamento matemático.

Este módulo va encaminado a que el alumno conozca los diferentes aspectos de la criptografía, haciendo un repaso de los principales algoritmos criptográficos, de los que se analizará su funcionamiento y características, así como su seguridad y puntos débiles que pueden permitir que se realice un criptoanálisis. El repaso de estos algoritmos se inicia con los clásicos y a continuación se estudia la criptografía simétrica, distinguiendo entre la criptografía en flujo y la criptografía en bloque. Se analizarán los algoritmos más importantes así como el estándar de cifrado actual.

Además se analizan las funciones hash, de vital importancia y con multitud de aplicaciones en diferentes ámbitos de la informática. También se trata la criptografía de clave asimétrica, incluyendo el famoso algoritmo RSA. En este apartado se incluye el estudio de la firma digital, certificados digitales e infraestructuras de clave pública (PKI).

Lejos de considerarse algo puramente teórico, la criptografía tiene multitud de aplicaciones prácticas, como pueden ser las criptomonedas. En la última parte del módulo se verán con más profundidad algunas de estas aplicaciones y su importancia en la actualidad.

PROGRAMA DE LA ASIGNATURA:

- Introducción y algoritmos clásicos
- Algoritmos de clave simétrica y funciones hash
- Algoritmos de clave asimétrica
- Certificados digitales y PKI
- Aplicaciones criptográficas

OBJETIVOS GENERALES:

- Conocer los principales algoritmos criptográficos, así como su seguridad, desde los algoritmos clásicos, pasando por los simétricos y finalizando con los algoritmos asimétricos.
- Conocer aplicaciones actuales de la criptografía.

OBJETIVOS ESPECÍFICOS:

- Conocer los principales algoritmos criptográficos clásicos y simétricos, como pueden ser el cifrado César, Vigenère, LSFR, DES, AES.
- Conocer algoritmos asimétricos como RSA y el algoritmo Diffie Hellman.
- Conocer aplicaciones actuales de la criptografía, como pueden ser la red Tor y el bitcoin.

COMPETENCIAS, APTITUDES Y DESTREZAS QUE DEBE ADQUIRIR EL ALUMNO:

- Conocer qué es la criptografía, el criptoanálisis y las diferentes ramas que abarcan.
- Conocer los principales algoritmos criptográficos.
- Conocer la seguridad de los algoritmos criptográficos, así como los puntos débiles que los pueden hacer vulnerables.
- Saber distinguir cuándo es recomendable utilizar cada tipo de algoritmo.
- Conocer algunas de las principales aplicaciones de la criptografía.

MÓDULO 2. SEGURIDAD WEB
6 ECTS / 150 horas

Las tecnologías basadas en la web son las más utilizadas por las empresas de cara a ofrecer sus servicios a través de Internet. Desde las páginas HTML estáticas de los años 80 y 90, la web ha evolucionado hasta el punto de que diferentes empresas comercializan dispositivos hardware que tan sólo disponen de un navegador web, sin más software cliente. Esta evolución del mundo web hace que las aplicaciones sean cada vez más complejas y conlleva más factores que deben ser tenidos en cuenta de cara a asegurar las aplicaciones desde el punto de vista de la seguridad.

Por estos motivos, es importante conocer cuáles son las amenazas más comunes que afectan a las tecnologías web, cómo ser capaces de identificarlas, evitarlas y solucionarlas para mejorar la calidad del software.

PROGRAMA DE LA ASIGNATURA

Este módulo se vertebra en los siguientes puntos principales:

- El protocolo HTTP y tecnologías Web
- Inyecciones de código y SQL
- Vulnerabilidades del lado de cliente
- Control de acceso y lógica de la aplicación
- Fugas de información
- Problemas de configuración y vulnerabilidades del lado del servidor

OBJETIVOS GENERALES:

- Conocer los protocolos y las principales tecnologías basadas en web
- Conocer las principales vulnerabilidades que afectan a las aplicaciones web

OBJETIVOS ESPECÍFICOS:

- Comprender cómo se llevan a cabo la comunicación entre clientes y servidores web
- Conocer los principales vectores de ataques para identificar diferentes tipos de vulnerabilidades
- Comprender la autenticación y los procesos de autorización más comunces en las aplicaciones web

COMPETENCIAS, APTITUDES Y DESTREZAS QUE DEBE ADQUIRIR EL ALUMNO:

- Identificar vulnerabilidades en aplicaciones web en funcionamiento
- Entender a qué se deben cada una de las vulnerabilidades
- Identificar las vulnerabilidades y ser capaz de corregirlas a nivel de código fuente

MÓDULO 3: SEGURIDAD OSINT, INVESTIGACIÓN EN FUENTES ABIERTAS.
150 horas / 6 créditos

La información presente en fuentes abiertas es un componente fundamental para el analista de seguridad. La inteligencia de fuentes abiertas (OSINT) se corresponde con un tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público.

La definición de fuentes abiertas acapara una gran variedad de contenidos disponibles en multitud de soportes (papel, fotográfico, magnético, óptico...) y que se transmite por diversos medios (impreso, sonoro, audiovisual...) y a los que se puede acceder en modo digital o no, pero que ha sido puesto a disposición pública, con independencia de que esté comercializado, se difunda por canales restringidos o sea gratuito. Por este motivo, el hecho de que esta información sea pública no implica necesariamente que se encuentre en un estado aceptable como para ser de utilidad para un analista en ciberseguridad.

En el ámbito del ciberespacio es necesario que el analista conozca cuáles son las herramientas a su disposición para trabajar con la información disponible a través de este tipo de fuentes con el objetivo de conseguir maximizar los recursos a su alcance a la hora de clarificar el origen de cualquier acción que tiene lugar en la red y entender mejor el quién y el porqué de cualquier incidente de seguridad.

PROGRAMA DE LA ASIGNATURA

- Introducción al OSINT en internet.
- Usos avanzados de buscadores.
- Metodologías para la realización de ejercicios de atribución.
- Extracción de metadatos y análisis de ficheros.
- OPSEC y anonimato orientado a las investigaciones en la red.

OBJETIVOS GENERALES

- Entender la estructura de internet y las limitaciones a la hora de obtener información de las distintas fuentes que se presentan.
- Desarrollar métodos de trabajo que les permitan entender el proceso de atribución de una acción que tiene lugar en la red.

OBJETIVOS ESPECÍFICOS

- Adquirir conocimientos avanzados sobre el uso de los buscadores principales y de los mecanismos existentes para indexar información.
- Conocer la información que es posible obtener a partir de los diferentes inputs de información que se le pueden presentar en el transcurso de una investigación.
- Desarrollar una concienciación a la hora de controlar la información que un analista expone sobre sí mismo a la hora de investigar.

COMPETENCIAS, APTITUDES Y DESTREZAS QUE DEBE ADQUIRIR EL ALUMNO

- Ser capaz de realizar búsquedas avanzadas en los principales buscadores genéricos y específicos de la red.
- Conocer la información que se puede extraer de un fichero en función de su naturaleza y de los metadatos que contiene.
- Manejar con soltura las soluciones existentes para prevenir la filtración de información sobre su persona.

MÓDULO 4: VULNERABILIDADES
125 horas / 5 créditos

Una vulnerabilidad es un fallo en el código del software o en su configuración que provoca un comportamiento no esperado o erróneo, que puede llevar a comprometer la seguridad de un equipo informática. Las consecuencias pueden ser desde una denegación de servicio hasta una ejecución arbitraria de código pasando por una elevación de privilegios. Las vulnerabilidades y los fallos de seguridad son la piedra angular que habitualmente sostienen los fundamentos de ataques a todas las escalas.

A lo largo de este módulo iremos profundizando, de forma eminentemente práctica, en comprender las causas de buen parte de los fallos de seguridad que se publican a diario y la forma en la que se pueden aprovechar. Analizaremos sus componentes teóricas y cómo se han ido añadiendo medidas de seguridad en los sistemas operativos que tratan de dificultar la explotación de estos fallos, junto con las técnicas que, a su vez, se pueden utilizar para ser superadas.

También estudiaremos los criterios que se utilizan en la evaluación de las vulnerabilidades y cuáles son los motivos por los que una vulnerabilidad se puede considerar más o menos grave.

PROGRAMA DE LA ASIGNATURA

- Vulnerabilidades, exploits y payloads.
- Detección y análisis.
- Protecciones genéricas frente a vulnerabilidades
- Bastionado de Windows frente a vulnerabilidades.

OBJETIVOS GENERALES

- Entender los principales tipos de vulnerabilidades y cuáles son los criterios de la seguridad de la información a los que afecta.
- Ser capaces de detectar vulnerabilidades en un software y cómo poder explotarlas.
- Conocer el tipo de protecciones que suelen implementar los sistemas operativos para dificultar la explotación de las vulnerabilidades.

OBJETIVOS ESPECÍFICOS

- Comprender qué es una vulnerabilidad, un exploit y un payload.
- Programar un exploit y configurar diferentes payloads.
- Detectar vulnerabilidades y explotarlas.
- Configurar protecciones de sistemas operativos.

MÓDULO 5: SEGURIDAD EN REDES CORPORATIVAS
125 horas / 5 créditos

Las redes empresariales son la infraestructura a través de la que se comparten los mayores secretos de las empresas. Están formadas por diferentes equipos que comparten información organizada y disponible en multitud de protocolos de red que circulan por las redes. Aunque buena parte de la infraestructura necesaria para el desarrollo de las compañías se encuentra hoy en día desplazada en la nube, la red interna de comunicación siempre mantiene conectadas los servicios básicos que permiten interconectar a los usuarios de una compañía entre sí. Por tanto, su seguridad sigue siendo fundamental a pesar del cada vez mayor consumo de datos online.

Conocer cómo funcionan los protocolos utilizados así como identificar los diferentes sistemas que se comunican a lo largo de una red es básico para entender su seguridad, detectar sus puntos débiles y aplicar las medidas de prevención adecuadas.

En este módulo se estudian los principales protocolos que se pueden encontrar en una red empresarial para, en una segunda fase, aprender a realizar un análisis minucioso la misma que permita identificar las mayores deficiencias desde el punto de vista de la seguridad.

PROGRAMA DE LA ASIGNATURA:

Este módulo se vertebra en los siguientes puntos principales:

- Protocolos seguros en la LAN.
- Reconocimiento de red.
- Vulnerabilidades y ataques en red.

OBJETIVOS GENERALES:

- Conocer los protocolos más comunes que conforman las redes empresariales.
- Identificar deficiencias en la red como entidad que puedan afectar a la su seguridad.

OBJETIVOS ESPECÍFICOS:

- Aprender las fortalezas y deficiencias de los principales protocolos usados principalmente en redes corporativas.
- Conocer las vulnerabilidades y fallos de configuración más comunes en las redes empresariales.
- Ser capaz de proponer recomendaciones para evitar fallos comunes de seguridad

COMPETENCIAS, APTITUDES Y DESTREZAS QUE DEBE ADQUIRIR EL ALUMNO:

- Ser capaz de decidir qué protocolos usar y cuáles evitar
- Aprender a realizar un reconocimiento de red para identificar sistemas y servicios accesibles en una red.
- Aprender a detectar y explotar vulnerabilidades en diferentes sistemas.

MÓDULO 6: SEGURIDAD EN ARQUITECTURAS BASADAS EN LINUX
150 horas / 6 créditos

Los diferentes métodos de construir sistemas en la red han evolucionado en los últimos años. Desde por ejemplo un clásico sistema LAMP (Linux, Apache, MySQL y PHP) hasta las arquitecturas más modernas y complejas que poco tienen que ver con la web pero que procesan gran cantidad de información. En todos ellos es posible encontrar problemas de seguridad específicos que es necesario conocer no solo a nivel global de arquitectura, sino a nivel particular de cada máquina que compone finalmente todo el sistema en su conjunto.

Este módulo aborda la seguridad desde el punto de vista de las arquitecturas más recientes que podemos encontrar como sustento de la mayoría de servicios que gestionan los volúmenes de información típicos de hoy. En él, desde el punto de vista del defensor, se describen algunas de las medidas que podemos utilizar para proteger estos sistemas habitualmente basados en Linux, manteniendo un enfoque práctico con un objetivo de ser realmente útil en el mundo real.

La asignatura se divide en cuatro secciones que van avanzando desde arquitecturas de un solo nodo hasta las basadas en cloud, donde es posible escalar hasta los miles de nodos. Se analiza cómo se establece la seguridad de este tipo de entornos, sistemas y conexiones para que el servicio no solo sea eficiente sino que se mantenga a salvo de los ataques típicos e inherentes a cada arquitectura.

Finalmente se realizarán algunos análisis de arquitecturas de soluciones típicas reales y trataremos de resaltar los principales problemas que podremos encontrarnos en ellas.

PROGRAMA DE LA ASIGNATURA

- Seguridad en instancias locales.
- Seguridad en granjas de servidores.
- Seguridad en proveedores cloud.
- Análisis de arquitecturas típicas.

OBJETIVOS GENERALES

- Dotar al alumno de la habilidad suficiente para ser capaz de reconocer debilidades en sistemas locales y arquitecturas cotidianas.
- Conocer algunas de las herramientas o mecanismos disponibles para los diferentes actores que participan en el diseño, desarrollo y mantenimiento de una arquitectura segura: Arquitecto Software, Arquitecto de seguridad, equipo de operaciones, devops, IT, vigilancia, etc.
- Trasladar al alumno la importancia de tener la seguridad presente desde las fases de diseño hasta la puesta en funcionamiento de cualquier sistema y la necesidad de introducir (por defecto) mecanismos de protección frente a intrusiones y su detección.

OBJETIVOS ESPECÍFICOS

- Conocer en profundidad las medidas de protección que nos presta el kernel de Linux y cuales son algunas de las herramientas típicas que podemos usar para aumentar este nivel de seguridad.
- Conocer cómo aplican las medidas anteriores y cómo se trasladan a granjas de servidores y servicios en cloud.
- Tratar de describir los patrones de los ataques que podemos sufrir en este tipo de arquitecturas de forma que podamos anticiparnos a ellos.
- Estudiar las principales vías que tenemos para detectar cuándo un sistema está siendo atacado o ya ha sido vulnerado.

COMPETENCIAS, APTITUDES Y DESTREZAS QUE DEBE ADQUIRIR EL ALUMNO.

- Capacidad para diseñar y aplicar las medidas de seguridad necesarias para sistemas que corren sobre arquitecturas Linux.
- Capacidad de automatizar estas medidas y hacerlas escalables cuando el número de nodos hace inmanejable un control manual.
- Adquirir la destreza suficiente para empezar a reconocer problemas de seguridad en este tipo de arquitecturas.

MÓDULO 7: MALWARE Y CÓDIGOS MALICIOSOS
125 horas / 5 créditos

Una de las principales amenazas que sufren empresas y particulares en relación con la seguridad de la información son los programas o códigos maliciosos, también conocidos como malware. Programas que se introducen en los ordenadores y dispositivos móviles alterando su funcionamiento normal, principalmente por motivos económicos. Para hacernos una idea de la dimensión de este problema basta con ver la cifra de malware que se creó en 2016: 600 millones de muestras según McAfee. Esto son 19 muestras de malware al segundo. Se suele pensar que los creadores de malware son personas con una alta cualificación y un alto nivel de sofisticación, pero no siempre es así.

En este módulo empezaremos abordando la definición de código malicioso y la descripción de los distintos tipos que existen desde un punto de vista actual. Se continuará exponiendo las distintas técnicas que existen para analizar malware que permitirán poder extraer indicadores de compromiso (IOCs) que ayuden a determinar la presencia de malware en una red o en un equipo. Por último, en este módulo nos centraremos en las distintas soluciones de seguridad existentes en el mercado que permiten combatir estas amenazas.

PROGRAMA DE LA ASIGNATURA

- Malware y tipologías.
- Protección, análisis y detección.
- Análisis estático y dinámico.
- Técnicas de evasión de análisis.

OBJETIVOS GENERALES

- Comprender qué es el malware y las distintas tipologías de códigos maliciosos.
- Ser capaces de analizar un malware básico, pudiendo determinar su comportamiento, objetivos e indicadores que nos permitan detectar infecciones en otros equipos.
- Conocer las distintas soluciones que existen en el mercado para poder realizar este tipo de tareas y que ayudan a defenderse del malware.

OBJETIVOS ESPECÍFICOS

- Conocer los distintos formatos de ficheros y lenguajes en los que podemos encontrar código malicioso.
- Conocer técnicas y herramientas que nos permitan llevar a cabo un análisis estático y el análisis dinámico de malware.
- Conocer técnicas de evasión de que implementan los códigos maliciosos para dificultar su análisis.
- Mucho malware utiliza criptografía para ocultar partes maliciosas y comunicaciones con el exterior. Abordaremos algunos de los algoritmos utilizados más frecuentemente.
- Conocer los elementos y herramientas necesarias para configurar un laboratorio de análisis de malware.

MÓDULO 8: DESARROLLO SEGURO Y GESTIÓN DE IDENTIDAD
150 horas / 6 créditos

En este módulo dirigido fundamentalmente a desarrolladores, ingenieros de software, o programadores esporádicos, se pretende introducir al alumno en el ciclo de vida del desarrollo seguro de software y la importancia de implantar estos procesos desde las primeras fases del diseño de los componentes y las aplicaciones.

Además se prestará especial importancia al tratamiento de la identidad digital, explorando los diversos esquemas de autenticación y autorización, así como exponer las necesidades de los sistemas de autenticación de permitir autenticaciones basadas en múltiples factores. En este contexto de identidad digital también se expondrán las necesidades de las aplicaciones y sistemas para hacer una correcta gestión de la identidad analizando e implementando soluciones que las contemplen.

Por último, se tratará la gestión del código fuente y las aplicaciones para permitir la gestión de diferentes componentes software a lo largo del tiempo facilitando su mantenimiento e intentando minimizar su exposición ante amenazas y vulnerabilidades.

PROGRAMA DE LA ASIGNATURA

- SDLC y desarrollo seguro.
- Gestión de identidad y autenticación.
- Esquemas de autenticación.
- Modelado de amenazas.
- Gestión y mantenimiento seguro del código fuente.

OBJETIVOS GENERALES

- Conocer y entender los procesos de desarrollo de software seguro y su ciclo de vida, analizando sus distintas fases y como implantar dichos procesos en proyectos de ingeniería de software.
- Conocer diversos procesos de autenticación y autorización así como abordar la gestión de la identidad digital desde el punto de vista de aplicaciones software.
- Conocer procesos y metodologías que permitan la mantenibilidad del código en proyectos software desde el punto de vista de la seguridad. Identificando amenazas y vulnerabilidades.

OBJETIVOS ESPECÍFICOS

- Conocer las distintas fases de un S-SDLC estableciendo requisitos de diseño, implementando soluciones y realizando pruebas y validaciones.
- Conocer diversos esquemas de autenticación y verificación en dos pasos para la realización de una autenticación fuerte.
- Aprender a identificar y modelar amenazas de un sistema software asi como aplicar las contramedidas necesarias para mitigarlas.

COMPETENCIAS

- Aprender a diseñar y evaluar sistemas y soluciones software bajo el prisma de la seguridad desde las primeras fases del diseño.
- Analizar componentes software para identificar posibles deficiencias y debilidades así como a aplicar las medidas adecuadas para evitarlas.
- Entender las diferentes técnicas de autenticación, cómo realizar una autenticación de forma segura y cómo llevar un control de acceso autorizado.

MÓDULO 9: SEGURIDAD IOT.
150 horas / 6 créditos.

El objetivo del módulo es proporcionar una visión general de la seguridad en IoT, conociendo sus principales retos y particularidades, qué medidas se pueden tomar para asegurar un despliegue IoT y cuáles son las mejores prácticas de seguridad en la industria.

Desde hace décadas se han conectado dispositivos a Internet. Sin embargo, en los últimos años se ha producido una consolidación tecnológica y un incremento en el número, variedad y posibilidades de los dispositivos conectados que permite predecir que en los próximos años el IoT será masivo y se extenderá a diversos segmentos de nuestra vida diaria (automoción, salud, hogar, smart cities o industria).

El incremento del número de dispositivos aumenta también la superficie de ataque y esto hace que la preocupación por la seguridad IoT sea creciente en la industria. De hecho, han surgido diferentes iniciativas (OWASP, GSMA IoT Security, Online Trust Alliance, Cloud Security Alliance...) con el objetivo de recopilar las mejores prácticas en Seguridad IoT. Sin embargo, la adopción de estas mejores prácticas por parte de proveedores de soluciones conectadas es todavía incipiente. Es necesario considerar tanto el riesgo de que los dispositivos IoT sean atacados con el objetivo de afectar a su operativa (como por ejemplo tomar el control remoto de un Jeep Grand Cherokee), como en el caso en el que se usen para lanzar ataques distribuidos de denegación de servicio como por ejemplo los ataque de final de 2016 con la red Mirai que impidieron el acceso a sistemas tan robustos como los de Twitter y Facebook.

El objetivo de esta asignatura es proporcionar una visión general de la seguridad en IoT, mencionando su principales retos y particularidades, qué medidas se pueden tomar para asegurar un despliegue IoT y qué recomienda la industria.

PROGRAMA DE LA ASIGNATURA

- Introducción: modelo de referencia IoT, Principios de la seguridad IoT, incidentes populares y redes de botnets
- Retos de seguridad IoT: limitación de recursos en el dispositivo, identidad y autenticación, operación y mantenimiento
- Seguridad aplicada: medidas en las diferentes capas del modelo de referencia IoT, conocimiento de las medidas en Amazon Web Services y Azure IoT.
- Frameworks de seguridad: GMSA Security Guidelines & Self Assessment, OWASP IoT, Online Trust Alliance, Cloud Security Alliance e Industrial Internet Consortium

OBJETIVOS GENERALES

- Conocer la arquitectura típica de una solución IoT.
- Estudiar el modelo de referencia clásico de una solución IoT y las diferentes tecnologías que se emplean en la industria incluyendo: dispositivos, redes, gestión de conectividad y dispositivo, habilitadores de aplicación, aplicación y Big Data.
- Conocer las principales recomendaciones de seguridad aplicables a IoT.
- Identificar las medidas de seguridad que aplican a las diferentes capas tecnológicas. Cómo asegurar de forma física los dispositivos, gestionar su identidad y autenticación mediantes certificados, cómo asegurar la conectividad y qué medidas implementar en la plataforma IoT de recolección de datos.

OBJETIVOS ESPECÍFICOS

- Conocer las principales amenazas en cada uno de los niveles tecnológicos
- Análisis de los principales incidentes de seguridad IoT, conocer los riesgos asociados a cada capa y las decisiones de diseño aceptadas en la industria en función del tipo de solución y aplicación a asegurar.
- Conocer los frameworks de seguridad de la industria.
- Estudio de las principales recomendaciones de la industria y su aplicación en los diferentes negocios. En particular conocer: GMSA Security Guidelines & Self Assessment, OWASP IoT, Online Trust Alliance, Cloud Security Alliance e Industrial Internet Consortium.
- Conocer las medidas ofrecidas por las principales plataformas IoT del mercado
- Conocer las principales medidas y herramientas de seguridad que ofrecen las plataformas IoT de referencia en el mercado: Azure IoT y Amazon Web Services IoT. Estudiar cómo se realiza la provisión de identidad en los dispositivos, qué alternativas de identificación se ofrecen y cuáles son las configuraciones recomendadas.

COMPETENCIAS, APTITUDES Y DESTREZAS QUE DEBE ADQUIRIR EL ALUMNO

- Identificación de los diferentes componentes y caracterización de la superficie de ataque de una solución IoT.
- Conocimiento de los riesgos de seguridad IoT y las mejores prácticas en la industria para mitigarlos en función del tipo de aplicación.
- Diseño de solución de seguridad para un despliegue IoT que emplee Amazon Web Services IoT o Azure IoT.

MÓDULO 10: GESTIÓN Y REGULACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 75 horas / 3 créditos.

La Seguridad de la información es un paradigma muy amplio que abarca todos los aspectos de la protección y salvaguarda de la información. Esta disciplina incluye desde las medidas organizativas, definición de políticas de seguridad, adecuaciones físicas y lógicas de las infraestructuras y técnicas preventivas... hasta los detalles más técnicos de la ciberseguridad. Pero este enfoque holístico tiene el eslabón más débil y problemático en el individuo. Ya sea un usuario final o un empleado, su labor en la cadena es clave para que el conjunto de medidas de seguridad instauradas pueda funcionar adecuadamente. Para ello la seguridad de la información promueve no solo el conocimiento de los pilares básicos de la seguridad, sino también debe fomentar una cultura de sensibilización y concienciación que inyecte en los usuarios una conducta de buenas prácticas de la seguridad de la información.

Por tanto, la seguridad de la información debe abordar las necesidades que afectarán a los usuarios y por ende a las empresas desde los propios pilares organizativos, propiciando la adopción de una adecuada normativa regulada y de un Sistema de Gestión de la Seguridad de la Información. Sin olvidar el conocimiento y cumplimiento del marco legal que rige en definitiva todo tratamiento de la información y que permite formalizar cuáles son las garantías que nos amparan respecto a la seguridad y sobretodo la privacidad del individuo.

PROGRAMA DE LA ASIGNATURA:

- Principios y buenas prácticas de la Seguridad de la Información.
- Gestión de riesgos de seguridad. Tipos de amenazas y vulnerabilidades.
- Normativas, regulaciones y legislación.
- Sistemas de Gestión de la Seguridad de la Información.

OBJETIVOS GENERALES:

- Abordar los fundamentos de la seguridad de la información. El alumno obtendrá una visión amplia de la necesidad de la seguridad de la información relativa a los riesgos de seguridad y amenazas existentes.
- Normativa y legislación. Es fundamentar conocer la legislación y regulación existente a nivel estatal e internacional de cara a la provisión o consumo de servicios online. Así como conocer los derechos que nos amparan en caso de que la privacidad de los usuarios se haya visto comprometida.
- Conocer los sistemas de gestión de la seguridad de la información (SGSI).
- Las organizaciones cada vez más dependen de una correcta gestión de sus activos de información, lo que se traduce en una adecuada organización y estructura de los procesos internos que así lo permitan.

OBJETIVOS ESPECÍFICOS:

- Estudiar los conceptos básicos de Integridad, Confidencialidad, Disponibilidad y Autenticación. Asimilar dichos conceptos y los riesgos de seguridad asociados a cada uno de ellos en distintos entornos de la seguridad tales como la identificación del usuario, el almacenamiento o el control de acceso a datos.
- Conocer las directivas, regulaciones y el marco legal nacional e internacional respecto a la seguridad de la información. Analizar la normativa ISO 27002 y la ITIL v3 relativa a las recomendaciones de las mejores prácticas en seguridad. Además, se ahondará en las características de leyes como la LSSI, LOPD, LPI o la GPRD, así como políticas y regulaciones como el Esquema Nacional de Seguridad.
- Acercarse a la norma ISO 27001 de los SGSI así como el Plan Director de Seguridad. Se estudiarán las normas ISO 27001 y asociadas como las ISO 27004 e ISO 27005 que permiten establecer los un SGSI en una organización, así como de su correcta consultoría e implantación a través de un Plan Director de Seguridad.

COMPETENCIAS, APTITUDES Y DESTREZAS:

- Conocer y distinguir las propiedades de seguridad fundamentales.
- Aprender y enmarcar las distintas leyes que regulan la seguridad de la información.
- Entender la importancia de la implantación y asimilación de los SGSI, así como obtener capacidades de auditoría y consultoría.

MÓDULO 11: PROYECTO FIN DE MÁSTER
200 horas / 8 créditos

A lo largo de este módulo, el estudiante llevará a cabo la realización, presentación y defensa de un Proyecto fin de Máster en el que, de una forma guiada, deberá aplicar los conocimientos adquiridos a lo largo de los módulos del máster y demostrar que ha adquirido las competencias y destrezas necesarias para trabajar en el ámbito de la Ciberseguiridad.

El trabajo se revisará "a pares", tanto por un tutor como por un compañero. De esta forma, los estudiantes conocerán, de primera mano, dos ámbitos de estudio, el suyo propio y el de un compañero, duplicando el impacto pedagógico de la realización de este proyecto.

PROGRAMA DE LA ASIGNATURA:

Este módulo consta de los siguientes apartados:

- Introducción a la realización de Proyectos de Big Data
- Pautas esenciales para la organización del proyecto
- Realización del Proyecto Fin de Máster
- Presentación

A lo largo del proceso de estudio y realización del proyecto fin de Máster, el estudiante, estará acompañado por un tutor/mentor que le irá guiando en el proceso.

OBJETIVOS GENERALES:

- Aplicar los conocimientos adquiridos a través de los módulos estudiados al o largo del Máster.

OBJETIVOS ESPECÍFICOS

- Seleccionar la temática o campo de aplicación sobre el que se va realizar el proyecto.
- Realizar un estudio previo a la implementación del proyecto.
- Desarrollar un proyecto de Big Data siguiendo las indicaciones del mentor.
- Realizar una presentación ejecutiva del proyecto.

COMPETENCIAS, APTITUDES Y DESTREZAS:

- Ser capaz de articular, de forma completa, un proyecto de Big Data.
- Ejecutar, de forma eficiente, dicho proyecto.
- Comunicar de forma clara y expositiva, el trabajo realizado.

9. Modalidad

El master se impartirá en **Modalidad 100% on-line**.

A través del estudio de los contenidos de los distintos módulos, la participación en dinámicas colaborativas, la realización de tareas y la elaboración del proyecto final, los estudiantes contarán con una experiencia de formación inmersiva.

Los participantes, a través del aula virtual podrán:

- Consultar y descargar los materiales de estudio.
- Visualizar los contenidos audiovisuales en la sección multimedia.
- Realizar los cuestionarios de evaluación continua.
- Consultar y enviar las tareas propuestas en cada uno de los módulos.
- Acceder a las distintas correcciones y a los correspondientes feedbacks que los tutores realicen sobre las tareas enviadas.
- Espacio de acceso, seguimiento, entrega y retroalimentación del Proyecto Fin de Máster.
- Participar en las actividades colaborativas propuestas, tanto de tipo abierto como de tipo pedagógico.
- Acceder a las herramientas de tutorización, tanto síncronas como asíncronas.
- Consultar su libro de calificaciones y sus informes de seguimiento.
- Biblioteca especializada de materiales complementarios.

9.1. Seminarios On-line

Además, como apuntábamos en la descripción, **el estudiante podrá asisitir a un seminario en directo por cada módulo. Estos seminariols se impartiran a modo de clases magistrales donde los profesionales más reconocidos del sector ofrecerán una visión particular del temario del módulo basada en la experiencia profesional y la visión de la industria.** Entre otras, contaremos con seminarios sobre la seguridad como negocio, cómo se aborda la vigilancia digital en las grandes empresas, pentesting, gestión de código seguro en la los procesos profesionales de ingeniería del software... todos impartidos por profesionales reconocidos de la industria.

10. Metodología

La metodología de impartición de los distintos módulos del Máster se sustenta sobre la base al "*Learning by doing*", combinando la exposición y estudio de contenidos teóricos, enfocada a la realización de tareas prácticas del mundo real, en este caso, trabajando, de primera mano, todos aquellos aspectos esenciales del mundo de la Ciberseguridad, estudiados a lo largo de los distintos módulos del Máster.

A lo largo de la impartición, tanto por medio de los tutores como de la Dirección Académica, se fomentan la interacción, la participación y la colaboración de los estudiantes, tanto con el equipo docente como con sus propios compañeros, favoreciendo un planteamiento socio-constructivista del aprendizaje.

11. Más Información e Inscripciones

Más información:

- Portal: https://www.campusciberseguridad.com
- Teléfono: +34 983 390 716
- E-mail: info@campusciberseguridad.com

Reserva de plaza e inscripciones:

- https://campusciberseguridad.com/master-en-ciberseguridad-en-colaboracion-con-telefonica/informacion-e-inscripciones