_MCS
master de ciberseguridad en la práctica

ESCUELA INTERNACIONAL DE GERENCIA eig

Deloitte.

_MCS

Grandes preocupaciones, grandes oprtunidades.

> Ciberseguridad

4ª preocupación mundial.

> Necesidad de profesionales expertos en este ámbito.

Cada vez más, un mayor número de dispositivos están conectados alnternet; el crecimiento es vertiginoso y los beneficios son muchospero también tiene su parte negativa.

Organizaciones criminales están beneficiándose del "BOOM" tecnológico y del desconocimiento de los usuarios par extorsionar, robar y perjudicar a la reputación de individuos y empresas, con el objetivo de obtener un beneficio económico.

La Economía Digital y el desarrollo de las actividades en internet han abierto nuevas oportunidades de negocio y en consecuencia oportunidades de empleo con alto valor añadido.Y desde esta necesidad procuramos la mejor formación para los alumnos, en función de las demandas actuales y futuras de profesionales formados para los retos que surgen.

Ahora, en colaboración con Deloitte, ofrecemos el Master de Ciberseguridad en la práctica, contribuyendo a la creación de talento para el desempeño profesional en esta materia. Así formamos expertos en la seguridad de las tecnologías y capacita para realizar auditoría de seguridad, analizar los hechos y la información de seguridad recopiladas, aplicar la ingeniería inversa, así como llevar a cabo un correcto análisis forense.

La creciente preocupación por la ciberseguridad es un hecho constatado: representa la 4ª preocupación a nivel mundial. En 2014 el número de empresas que han invertido en protegerse de amenazas cibernéticas ha aumentado un 33%. Solo en España se necesitan 20.000 profesionales (600.000 en la Unión Europea), puestos que no se cubren por falta de formación y especialización en la materia..

Sergi Gil López

Director del Máster en Ciberseguridad
EIG - Deloitte CyberSOC

Manager- E.R.S. IT - Departamento de Riesgos Tecnológicos de Deloitte

Hoy en día, el cibercrimen es el negocio principal más lucrativo de las mafias internacionales por encima de la venta de armas y del tráfico de drogas, considerado uno de los principales problemas a nivel mundial. Los delitos informáticos asociados al cibercrimen son una de las principales amenazas y preocupaciones para la sociedad, la Administración Pública, la empresa privada y el entorno privado de las personas, convirtiéndose en un claro objetivo de la delincuencia que buscan lucrarse a cambio de la información robada o manipulada conseguida fraudulentamente en el ciberespacio.

Se estima que la demanda de empleo a nivel mundial para cubrir este amenaza está muy por encima de las posibilidades actuales de profesionales especializados, es por ello que la formación en todos los ámbitos, en la gestión personal, en el área empresarial y en desarrollo técnico avanzado, se convierte en una pieza indispensable para asegurar el progreso futuro.

El equipo de **Deloitte CyberSOC (Cyber Security Operations Center)** está formado por más de 120 profesionales que prestan servicios en más de 18 países y dispone de competencias avanzadas en la detección, tratamiento y análisis de ciberamenazas. Deloitte CyberSOC proporciona servicios a medida en las áreas de: inteligencia aplicada a la Ciberseguridad, evaluación de vulnerabilidades, mejora en la madurez del SOC interno y proporcionar servicios gestionado de seguridad en formato externalizado, 24x7 desde el CyberSOC de Deloitte.

El equipo de CyberSOC incluye los profesionales más cualificados de consultoría cibernetica, así como especialistas en diferentes reputated Cybertopics y expertos en tecnología de seguridad, con gran experiencia en productos de mayor adopción en la industria de TI.

La relación con distintos fabricantes de seguridad, combinada con la especialización técnica y los servicios proporcionados por el CyberSOC, permiten ofrecer la información y formación más completa y personalizada de las amenazas que aplican a cada organización. Siendo capaz de superar la visión estática convencional sobre riesgos y proporcionar una perspectiva dinámica e inteligente del escenario de Ciberamenazas.

_MCS

El master en la práctica

> Creación de talento para el desempeño profesional en materia de ciberseguridad.

El Máster en Ciberseguridad cuenta con la colaboración y participación de Deloitte y su CyberSOC-CERT Academy, que aportan su conocimiento, experiencia y especialización en áreas de elevada cualificación técnica en el ámbito de la Ciberseguridad.

> Objetivos.

El objetivo del Máster es formar a los futuros profesionales del mundo de la ciberseguridad. Recorriendo las temáticas más relevantes en el área, los estudiantes obtendrán un conocimiento amplio y riguroso en disciplinas tales como ciberinteligencia, análisis de malware, auditorías técnicas de sistemas y redes (hacking ético), análisis forense y gestión de incidentes de seguridad, desarrollo seguro de aplicaciones web y la monitorización y correlación de eventos de seguridad (por medio de tecnologías SIEM).

> Adquirir las capacidades necesarias para obtener, mantener y procesar evidencias digitales utilizando procedimientos y herramientas específicas.

> Instruir a los alumnos en el desarrollo de técnicas y en el uso de herramientas que exploten al máximo sus habilidades y conocimientos para la realización de pruebas de intrusión a sistemas y redes.

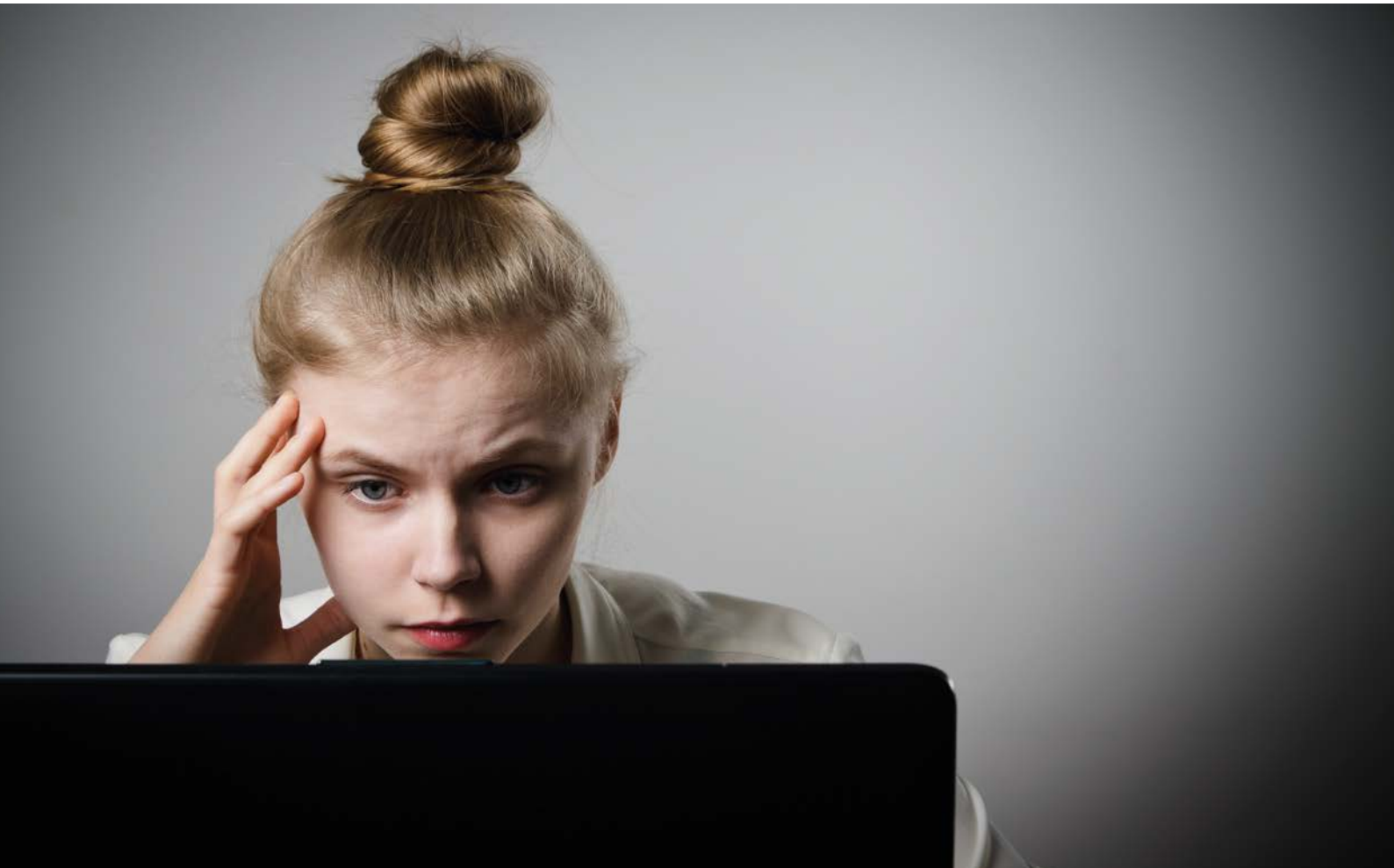
> Dar una visión general e introductoria al mundo de la ciberseguridad, explicando los ataques más relevantes y cómo mitigarlos.

> Presentar el mundo de la ingeniería inversa y el análisis de código malicioso, asumiendo los procesos para entender el funcionamiento de los ficheros que trabajan a bajo nivel en sistemas y redes.

> Asimilar los conocimientos suficientes para gestionar y establecerunas políticas claras de seguridad para el componente móvil de un sistema de información.

> Conocer los fundamentos de la monitorización y correlación de eventos de seguridad, mediante el estudio, la elaboración e interpretación de informes reales.

> Formar desarrolladores en programación segura y mejorar las habilidades de los auditores de seguridad en el análisis y evaluación del código fuente de las aplicaciones.



ESCUELA INTERNACIONAL DE GERENCIA eig

Dirigido a

> **Licenciados** en informática o telecomunicaciones que deseen enfocar su carrera profesional en la seguridad informática.

> **Profesionales junior** que estén ya trabajando en departamentos TIC que requieran de un nivel de especialización mayor.

> **Profesionales responsables de TIC** con experiencia en la ingeniería de sistemas o programación y que desee dar un cambio a su carrera profesional manteniendose dentro del mundo de la informática.

> **En general,** apasionados por esta actividad con experiencia.

Calendario

> de osctubre de 2016 a octubre de 2017

> **horario:** viernes tarde (16,30h a 21:30h) y sábado mañana (de 9h a 14h)

Salidas Profesionales

> Analista de seguridad

> Experto en ciberinteligencia y ciberfraude

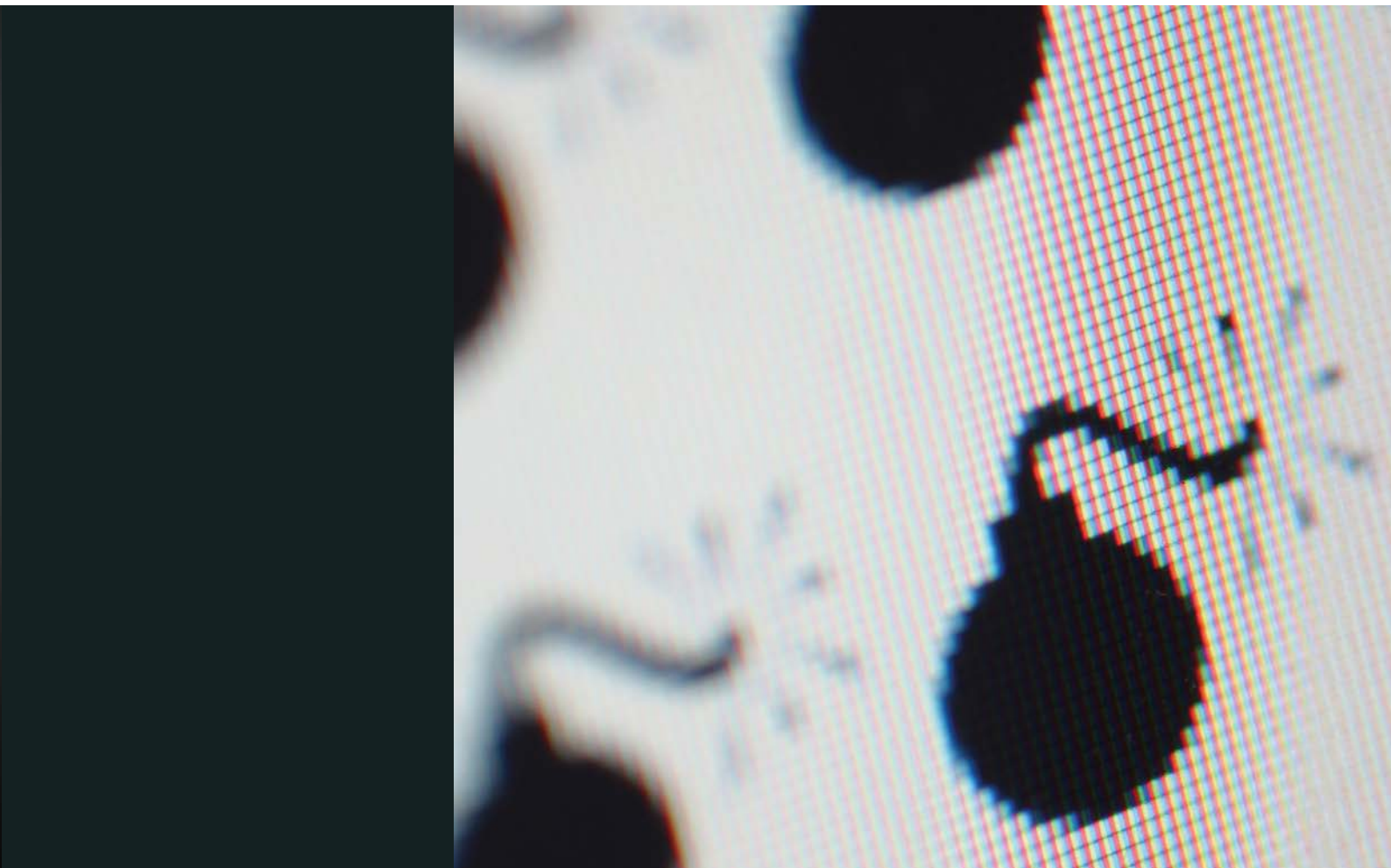
> Desarrolladores y analistas de código fuente

> Consultor en ciberseguridad

> Hacker ético

> Analista forense

> Analista de malware



_MCS

Programa

MCS. Comité de expertos

MCS está diseñado por un comité de expertos compuesto por doctores y profesionales en activo de una empresa líder en el ámbito de la seguridad como es Deloitte. Su experiencia avala la idoneidad de los estudios y las competencias que se adquieren, ya sea para la incorporación al mundo laboral o para la mejora profesional en el sector.

Este equipo de expertos, además de participar en el comité de diseño de programas formativos, colabora en la tutorización e impartición de las sesiones de máster.

DFC-101 Análisis Forense

1. Introducción a la ciencia forense
2. Leyes y ciencia forense
3. Proceso de investigación
4. Laboratorio forense
5. Adquisición de evidencias
6. Recolección de evidencias volátiles en Microsoft Windows
7. Análisis forense con TSK y Autopsy
8. Análisis forense con Rekall Forensics
9. Discos duros y sistemas de ficheros (FAT y NTFS)
10. Análisis forense en sistemas Microsoft Windows
11. Análisis forense de la memoria RAM
12. Análisis forense en sistemas GNU/Linux
13. Análisis de ficheros
14. Análisis de correos electrónicos
15. Análisis de perfiles de navegación web

DRC-101 Ingeniería Inversa

1. Arquitectura de Computadores (x86-32, x86-64, ARM)
2. Lenguajes de programación, compilación, enlazado, depuración y primer reversing
3. Introducción al lenguaje ensamblador
4. Lenguaje ensamblador
5. Formatos binarios
6. Cargadores dinámicos
7. Análisis estático
8. Análisis dinámico
9. Análisis de binarios protegidos
10. Análisis de shellcodes

SIEM-101 Tecnologías SIEM

1. Introducción a la monitorización y correlación
2. Logging
3. Eventos de seguridad
4. Ciclo de vida de un evento
5. Configuración
6. Reporting
7. Fabricantes

DCS-101 Desarrollo Seguro

1. Introducción
2. Conoce a tu enemigo
3. Conceptos básicos y generales del desarrollo seguro
4. Programación segura en e-commerce
5. Programación segura en JAVA y JSP
6. Programación segura en .NET
7. Programación segura en PHP
8. Desarrollo seguro en C y CPP
9. Programación segura en el lado del cliente
10. Programación segura en servicios web
11. Programación segura en móviles
12. Auditoría de seguridad para aplicaciones con BugScout

DCH-101 Hacking Ético

1.- Introducción a la Seguridad
2.- Footprinting
3.- Fingerprinting
4.- Seguridad en redes
5.- Vulnerabilidades
6.- Metaesploit
7.- Ataques a credenciales
8.- Malware
9.- Seguridad física de los equipos
10.- Seguridad en aplicaciones web

TFM Prácticas

Trabajo fin de master

Pieza clave: Profesores profesionales de Deloitte

Los profesionales del Centro de Operaciones en Ciberseguridad de Deloitte España (Deloitte CyberSOC-CERT) son la pieza clave y el factor diferenciador de este máster con respecto a otros cursos similares. Este equipo de profesionales ha diseñado y configurado este máster.

El equipo de formadores lo componen consultores del área de Deloitte Cyber Risk Services, analistas de seguridad, expertos en ciberinteligencia y ciberfraude, hackers profesionales, desarrolladores y analistas de código fuente.

Deloitte CyberSOC-CERT Academy asegura el proceso de formación

PLAN DE CALIDAD Y SEGURIDAD.

Certificación ISO 27001
El compromiso con la seguridad de la información de nuestros clientes.
Proteger la información que gestionamos de nuestros clientes es una de nuestras principales preocupaciones. Como tal, las medidas de seguridad implantadas en el laboratorio están destinadas a gestionar adecuadamente esta información con las medidas de seguridad pertinentes.
Como prueba de ello, el CyberSOC y los Laboratorios de seguridad de Deloitte en Madrid y Barcelona han implantado un Sistema de Gestión de la Seguridad que ha sido certificado bajo la ISO/IEC 27001:2005.

Certificación continuidad negocio ISO 22301
CyberSOC ha sido certificado en la norma ISO22301, el estándar de continuidad de negocio.
Este certificado prueba la seguridad de las instalaciones del CyberSOC y la existencia de un plan para garantizar la prestación de servicios sin interrupción en 24x7 en caso de desastre.

CERT de la Universidad Carnegie-Mellon
CyberSOC-CERT es miembro de la red CERT de la Universidad Carnegie-Mellon
Las capacidades del CyberSOC han sido certificadas.
Deloitte es la única Big4 con este reconocimiento.

Deloitte.

CyberSOC, ganador del Global CEO Challenge
El proyecto más innovador de la firma a nivel mundial.
Contemplando todas las facetas de las innovación.

ESCUELA INTERNACIONAL DE GERENCIA eig

BUSINESS SCHOOL

C/ Eduardo Molina Fajardo, 38
18014 Granada, T. +34 958 222 914
F. +34 958 159 438 **esgerencia.com**

infórmate
Tel.: 958 222 914
E-mail: info@esgerencia.com

twitter.com/eiggranada
youtube.com/eiggranada
facebook.com/eiggranada