Deloitte.

CyberSOC Academy

2017 – Enero a Mayo

Certificación profesional de Deloitte como Especialista en Desarrollo Seguro

Este sello profesional, avalado por Deloitte **a nivel mundial**, es emitido por el centro de operaciones de seguridad Deloitte CyberSOC–CERT, que certifica la formación impartida por Deloitte CyberSOC Academy en el ámbito de desarrollo seguro.

Este curso de certificación incluye sesiones presenciales en las siguientes dos áreas de conocimiento:

Desarrollo seguro y operaciones de seguridad en el desarrollo (DevSecOps)

Desarrollo seguro en móviles (iOS y Android)

Deloitte.

CyberSOC Academy

La certificación como Especialista en Desarrollo Seguro incluye **un total de 6 sesiones presenciales** (2 por cada área de conocimiento), en las instalaciones de Deloitte.

Para obtener la certificación, el participante deberá asistir, al menos, al 80 % de las 6 sesiones programadas por certificación.

La certificación se divide en una primera parte que consta de un curso de 4 días de Desarrollo Seguro y Operaciones de Seguridad en el Desarrollo (DevSecOps) y de la segunda parte que consta de un curso de 2 días de Desarrollo Seguro en Móviles.

Calendario de sesiones 2017

Precios			
	Total 4 sesiones DS y DevSecOps	Total 2 sesiones DS Móviles	**Total certificación**
**Early Registration* o por certificación completa	1365 €	685 €	**2.050 €**
PVP	1765 €	885 €	**2.650 €**

* Si la preinscripción se realiza 15 días antes del comienzo del curso o para el total de las seis sesiones que componen la certificación.

Deloitte.

CyberSOC Academy

Objetivo de la certificación

El desarrollo de aplicaciones seguras, sobre todo si éstas van a dar soporte a procesos de negocio o van a estar expuestas a Internet, es el mejor mecanismo de defensa de los activos de una organización ante los ciber-ataques. La exposición masiva de estas aplicaciones vía web desde cualquier punto del planeta, por cualquier persona, multiplica las posibilidades de que las vulnerabilidades de estos aplicativos sean explotadas interrumpiendo nuestros servicios (ataques por denegación de servicio) o afectando a la integridad y confidencialidad de los datos, que pueden ser extraídos o manipulados, dando lugar a todo tipo de problemas y sanciones por incumplimientos normativos o legales.

El curso expone al alumno a diferentes lenguajes de programación y entornos de desarrollo. El temario engloba un análisis en profundidad de los riesgos presentes en cada uno de los diferentes entornos, así como las mejores prácticas seguidas por los desarrolladores más expertos para el desarrollo de aplicaciones seguras y estables. Adicionalmente, el programa abarca técnicas específicas para la identificación de vulnerabilidades en código fuente y para la ejecución continuada de acciones que minen una aplicación inicialmente comprometida.

DS Y DevSecOps
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. Programación segura en C, C++
9. SecDevOps

DS en Móviles
1. Programación seguro en iOS
2. Programación segura en Android

Más información y preinscripciones
Para más información sobre esta y sucesivas convocatorias, así como del resto de certificaciones profesionales, visita **https://cybersocacademy.deloitte.es/** Las preinscripciones se llevarán a cabo a través del *email*: **deloittecybersocacademy@deloitte.com** hasta 5 días laborables antes del comienzo del curso. Por favor, adjunta los siguientes datos del participante: nombre y apellidos, *email*, empresa, cargo y CIF.

Deloitte.

CyberSOC Academy

2017 – Enero a junio

Certificación profesional de Deloitte como Especialista en *Computer Incident Response* (CIR)

Este sello profesional, avalado por Deloitte **a nivel mundial**, es emitido por el centro de operaciones de seguridad Deloitte CyberSOC–CERT, que certifica la formación impartida por Deloitte CyberSOC Academy en el ámbito de la respuesta ante incidentes de seguridad.

Este curso de certificación incluye sesiones presenciales en las siguientes tres áreas de conocimiento:

Hacking Ético

Análisis de Malware

Respuesta ante Incidentes de Seguridad (CIR)

Deloitte.

CyberSOC Academy

La certificación como especialista en *Computer Incident Response* incluye **un total de 6 sesiones presenciales** (2 por cada área de conocimiento), en las instalaciones de Deloitte.

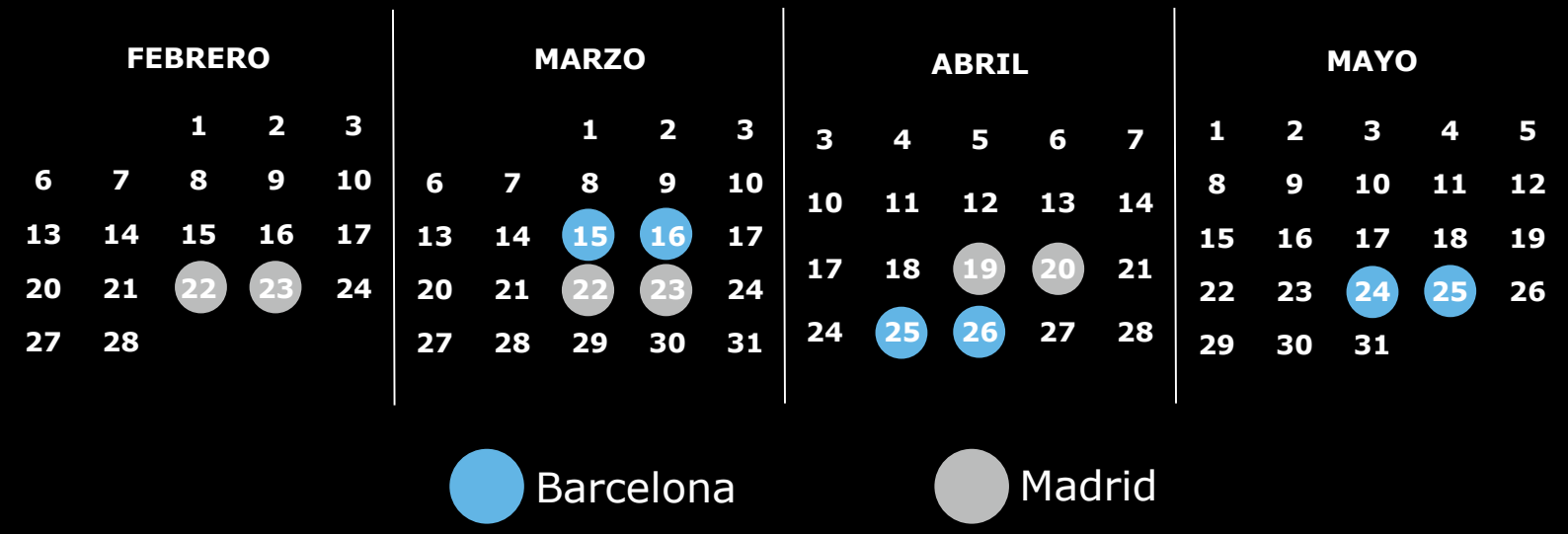
Para obtener la certificación, el participante deberá asistir, al menos, al 80 % de las 6 sesiones programadas por certificación.

Las sesiones se deberán de cursar según el orden establecido para poder obtener la certificación:

1. Hacking Ético
2. CIR
3. Malware

Dicho esto, la inscripción a sesiones independientes también esta permitido.

Calendario de sesiones 2017



Precios				
	Total 2 sesiones Hacking	Total 2 sesiones CIR	Total 2 sesiones Malware	**Total certificación**
**Early Registration* o por certificación completa	500 €	700 €	850 €	**2.050 €**
PVP	700 €	900 €	1.050 €	**2.650 €**

* Si la preinscripción se realiza 30 días antes del comienzo del curso o para el total de las seis sesiones que componen la certificación.

Deloitte.

CyberSOC Academy

Objetivo de la certificación

El objetivo de esta certificación es cubrir de manera integral y práctica la gestión de incidentes de seguridad, desde el punto de vista del conocimiento de cómo los incidentes y las intrusiones pueden suceder (2 sesiones en análisis de vulnerabilidades y tests de penetración), desde el punto de vista de la gestión del incidente o de la intrusión (2 sesiones en respuesta ante incidentes) y del análisis del malware que acompaña al incidente en gran número de casos (2 sesiones de análisis de malware).

Desde un punto de vista neutral con respecto a fabricantes y tecnologías, esta certificación enseña a identificar vulnerabilidades en redes, sistemas y aplicaciones, establecer los riesgos asociados a cada vulnerabilidad y definir las acciones correctivas que sean necesarias. El participante aprenderá la metodología que dicta la normativa internacional en las actuaciones ante incidentes de seguridad y se cubrirán, desde un punto de vista práctico, las principales actividades de un equipo CIR (Computer Incident Response) en la fase de investigación en caliente de un incidente. Por último, se conocerán de manera práctica las bases del análisis de malware y las herramientas más comunes.

HACKING
1. Vulnerabilidades
2. Metasploit
3. Ataques a credenciales

CIR
1. Normativa, fases de actuación
2. Reconocimiento, adquisición, triage.
3. Remediación, indicadores de compromiso (opensource).

ANÁLISIS DE MALWARE
1. Análisis estático
2. Análisis dinámico
3. APTs

Más información y preinscripciones

Para más información sobre esta y sucesivas convocatorias, así como del resto de certificaciones profesionales, visita **https://cybersocacademy.deloitte.es/**

Las preinscripciones se llevarán a cabo a través del *email*:

deloittecybersocacademy@deloitte.com

hasta 5 días laborables antes del comienzo del curso. Por favor, adjunta los siguientes datos del participante: nombre y apellidos, *email*, empresa, cargo y CIF.