Con este curso se pretende proporcionar el conocimiento fundamental que deben poseer los decisores estratégicos de empresas y organismos públicos en materia de ciberseguridad (Qué es necesario saber y qué no). Al finalizar el curso, el alumno debe ser capaz de elaborar un plan estratégico que garantice de modo integral la seguridad de la información

Dirigido a

Directores de seguridad, personal implicado en la gestión de la Seguridad Pública y FFAA, personal de seguridad privada, jefes de Seguridad y similares.

Precios

La matrícula se paga en un solo pago, y hay dos precios:

1º 1500€ para alumnos en general

2ª 1000€ para socios CEUSS, personal ICFS, y alumnos y antiguos alumnos de ICFS, y actuales alumnos de la UAM.

Inscripción: desde septiembre de 2019 hasta el 16 octubre de 2018

Para más información

cformacion.icfs@uam.es

Instituto de Ciencias Forenses y de la Seguridad
Universidad Autónoma de Madrid
Ciudad Universitaria de Cantoblanco
C/ Francisco Tomás y Valiente, nº 11 (Edificio C, 3er piso)
28049 MADRID (ESPAÑA)
(+34) 91 497 61 35
@ICFS_UAM

www.icfs-uam.es
Instituto.icfs@uam.es

Universidad Autónoma de Madrid

excelencia UAM CSIC

UAM Universidad Autónoma de Madrid UAM

ICFS Instituto de Ciencias Forenses y Seguridad UAM

CURSO DE FORMACION

GESTIÓN DE CIBERSEGURIDAD Y CIBERINTELIGENCIA EN EL ENTORNO EMPRESARIAL* Edición II

100 horas teórico-prácticas

**Curso pendiente de aprobación por la UAM*

FECHAS: del 18 de octubre de 2019 al 27 de marzo de 2020.
HORARIO: Semanas alternas: Viernes de 15:30 a 20:30 y sábados de 9:30 a 14:30
LUGAR: Universidad Autónoma de Madrid.

El precio del curso incluye el derecho a presentarse al examen para obtener la Certificación de Gestión en Ciberseguridad otorgada por la ACC (Agencia de Cibercertificaciones del ICFS/UAM)

ICFS Instituto de Ciencias Forenses y Seguridad ICFS

CNEC CENTRO NACIONAL EXCELENCIA EN CIBERSEGURIDAD

CEUSS Confederación Empresarial de Usuarios de Seguridad y Servicios

FUAM Fundación de la Universidad Autónoma de Madrid

GESTIÓN DE CIBERSEGURIDAD Y CIBERINTELIGENCIA EN EL ENTORNO EMPRESARIAL

Programa del curso

Instituto de Ciencias Forenses y de la Seguridad UAM

CUMPLIMIENTO DE NORMATIVA EN MATERIA DE CIBERSEGURIDAD (10horas). Enrique Ávila. Director CNEC

Principales normativas. Implementación del nuevo GDPR sobre protección de datos de la Unión Europea. La responsabilidad penal de las Personas Jurídicas en Materia de Ciberseguridad. Aproximación a la Ley de Protección de Infraestructuras Críticas y reglamento que la desarrolla. Entorno regulatorio español: Ley de Seguridad Privada y Estrategia Nacional de Ciberseguridad. Reglamento de Evaluación y Certificación de la Seguridad de las TIC. Entorno regulatorio comunitario: Directiva NIS. Responsabilidad penal corporativa e individual: sistemas digitales de control del delito. Nuevas tendencias en materia de Ciberseguridad. *Taller: Análisis de casos*

AMENAZAS CIBERNÉTICAS (10 horas). Álvaro Ortigosa (UAM) y Luis Herrero Pérez (MCCD)

El ciberespacio como factor riesgo para las empresas. Principales amenazas cibernéticas (Ciberespionaje, cibercriminalidad, Hacktivismo, Ciberterrorismo, Guerra Digital). La amenaza del futuro. El eslabón más débil: Usuarios. Fuentes de vulnerabilidad. Vectores de ataque (Ficheros adjuntos, *Phishing*, Ingeniería social) Ataques DDoS. Amenazas Persistentes Avanzadas (APAs). Ataque a la WIFI, Ataque a la infraestructura cableada. Control sobre los puntos de acceso. Troyanos y *keylogger*, descarga de software con malware. *Community Manager* en la empresa (Página web, troyanos, proxys interpuestos, Redes sociales, protección de acceso, política de cambio de contraseñas). La seguridad en otros S.O. Las amenazas en las comunicaciones. Tipos de comunicaciones: telefónicas, videoconferencia, mensajería, chat,... Redes SCADA empresariales. Hacking ético y pentesting. *Taller: Estudio de casos/proyecto.*

LA ARQUITECTURA GENERAL DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN (TIC). (5 horas) Óscar Maqueda (ACCENTURE)

Dentro y fuera del mundo empresarial. Podremos conocer cual es el software, el hardware y las comunicaciones que se emplean en su establecimiento. Cuáles son las principales y habituales vulnerabilidades.

RIESGO INTERNO: LAS FUGAS DE INFORMACIÓN. (5 horas). Óscar Maqueda. (ACCENTURE)

Riesgos ligados a la fuga de información de origen humano. La protección del patrimonio informacional de las empresas. Políticas de difusión, need to know, clasificación de la información. La labor del cio-ciso- c´suite frente a depredadores externos de información. Política BYOD

LA AMENAZA INTERNA: INSIDERS. (5 horas). José María Blanco (PROSEGUR)

¿Qué es un *insider*? Tipos de *insiders* (malicioso, negligente, bien intencionado). ¿Cómo piensa un *Insider*? Consecuencias: daños económicos y reputacionales. Fenómeno *Insider*. Motivaciones. Buenas Prácticas en la Organización: Detección del Síndrome de Burnout, formación y concienciación; normativa y régimen sancionador, SANS Institute: Insider Threat Mitigation. Fraude, detección de insiders, indicadores conductuales de insiders. Gestión de identidades y accesos: esquemas de autenticación de identidad (varios factores, firma digital, identificación biométrica, protocolo Kerberos...) y gestión corporativa de las mismas.

INGENIERÍA SOCIAL E INFLUENCIA. (5 horas). Javier Horcajo (UAM)

¿Qué es la ingeniería social? Ingeniería social como forma de Inteligencia y contrainteligencia. Principios de Ingeniería Social. Ingeniería social como método de influencia para el cambio y el posicionamiento. Métodos y estratégicas de ingeniería social. Prevención de acciones de ingeniería social y contramedidas. Ventajas y riesgos. *Taller: Estudio de casos/proyecto.*

COMUNICACIÓN DIGITAL Y REDES SOCIALES. (15 horas). Casimiro Nevado (Policía Nacional) y Álvaro Ortigosa

Análisis de redes sociales: Quién es quién. Vigilancia digital: quiénes y cómo hablan de ti, vigilancia de competidores, detección temprana de oportunidades y amenazas y seguimiento de mercado. Difusión de información: ¡Hazlo viral! Big Data y el mundo real. Detección y gestión de rumores, ataques a la marca, ataques a la persona con fines de desestabilización. Gestión de crisis online: establecimiento de cortafuegos de propagación por canal, por mensaje, por grupo de interés. El impacto de la Reputación en el Mercado de Valores. Gestión de la E-Reputación como solución proactiva. CIBERINTELIGENCIA APLICADA A LA CIBERSEGURIDAD: vigilancia digital. *Taller: Estudio de casos/proyecto.*

CIBERINVESTIGACIONES (5 horas]. Carlos Navarro (INCIDE)

Trataremos las ciberinvestigaciones: tipologías, planificación de las ciberinvestigaciones. Análisis forense en las ciberinvestigaciones. *Taller: caso de ciberinvestigación.*

GUERRAS DE INFORMACIÓN. Intoxicación, Desinformación Influencia y Manipulación a gran escala. (10 horas). Luis Fernando Hernández (Guardia Civil).

Información y Desinformación en la era del Ciberespacio. Finalidad y métodos. Información y Desinformación en la guerra económica y comercial. El softpower de los estados. La cultura subversiva como modelo para el análisis de procedimientos en estrategias ofensivas. Guerra de información: Modo ofensivo (Doxxing). Modo defensivo. Forma radical: Psyops, etc. ContraInfluencia: Métodos y procedimientos. La protección de la comunicación: Criptografía y criptoanálisis. Esteganografía y estegoanálisis. CIBERINTELIGENCIA APLICADA A LA CIBERSEGURIDAD: contrainteligencia y vigilancia digital, "hacktivismo", "Deep web"... *Taller: Estudio de casos/proyecto.*

GESTION DE CRISIS Y COMUNICACIÓN. (10 horas). Fernando Romero (PROSEGUR).

Auditoría de riesgos. Cartografía de actores. Procedimientos de vigilancia. Esquema de alerta. Construcción de argumentarios. Gestión de medios. Selección de medios de comunicación. La crisis como oportunidad. Construcción del mensaje. GESTIÓN DE CRISIS EN CIBERSEGURIDAD: CSIRT/CERT. Funcionamiento de los SOC en ciberseguridad. Estrategias y coordinación de la defensa, continuidad del negocio, planes de contingencia, planes de recuperación ante desastres. *Taller: Estudio de casos/proyecto*. Simulacro de una gestión de crisis cibernética

PLANIFICACION DE LA CIBERSEGURIDAD. (15 horas). Luis Fernando Hernández (Guardia Civil)

Desarrollando la Política de Ciberseguridad Empresarial: Planes de contingencia y planes de seguridad de la información. Medidas básicas de ciberdefensa. Respaldo de la información (plan de *backups*) Protección de virus y control de software. Control de Redes. Protección física de acceso a redes. Web 3.0 y SaaS. La clave: Formación y Certificación. Planes de formación y actualización del conocimiento. Políticas y planes de Certificación. Obligaciones de los prestadores de servicios de certificación (certificados electrónicos). Encriptación: la encriptación como método de defensa de los activos intangibles, soluciones básicas y viables de utilización. Análisis de Riesgos Cibernéticos. Elementos de Riesgo. Análisis de impacto a la empresa. La repercusión económica de los ciberataques. Certificación: ISOs 27000, 27002, 22301, 22313, 31000, 27005 o 38500. Taller: Elaboración del plan de ciberseguridad.

CONCIENCIACIÓN EN CIBERSEGURIDAD (CERTIFICACIÓN) (5 horas) Álvaro Ortigosa (UAM)

Se explicara el temario necesario para poder realizar el examen de certificación de Gestión en Ciberseguridad de la ACC.