

**COMPETENCIAS DE LAS ASIGNATURAS DEL MÁSTER EN SEGURIDAD INFORMÁTICA
(CIBERSEGURIDAD)****AUDITORÍA Y ANÁLISIS DE RIESGOS**

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CE1 Conocer el procedimiento de realización de una autoría informática

CE2 Aplicar una metodología para el análisis y evaluación de riesgos y utilizar las herramientas para su gestión.

LEGISLACIÓN Y NORMATIVA APLICADA A LA SEGURIDAD INFORMÁTICA

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CE3 Conocer y comprender el marco legal vigente europeo y español relativo a la privacidad y seguridad de la información, tanto en el ámbito privado como en el de la administración pública para satisfacer las exigencias profesionales.

CE4 Conocer las normas y estándares de referencia y certificación relacionados con seguridad de la información.

PRÁCTICAS EN ANÁLISIS FORENSE

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CE5 Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales

PRÁCTICAS EN HACKING ÉTICO

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CE12 Detectar vulnerabilidades en los distintos elementos de un sistema informático.

CE13 Conocer y aplicar técnicas y herramientas para la realización de pruebas de penetración.

INGENIERÍA INVERSA Y ARQUITECTURAS SEGURAS

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CE10 Conocer, detectar y evaluar las vulnerabilidades de bajo nivel que afectan a los sistemas informáticos, así como analizar amenazas a partir de la reconstrucción de código.

CE11 Comprender el funcionamiento y las aplicaciones de los dispositivos de seguridad TPM.

DESARROLLO DE APLICACIONES SEGURAS

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CE8 Aplicar técnicas para auditar y mejorar la seguridad de una aplicación.

CE9 Diseñar aplicaciones incorporando el criterio de seguridad dentro del propio proceso de desarrollo.

CE10 Conocer, detectar y evaluar las vulnerabilidades de bajo nivel que afectan a los sistemas informáticos, así como analizar amenazas a partir de la reconstrucción de código.

INTELIGENCIA ARTIFICIAL APLICADA A LA SEGURIDAD

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CE14 Conocer las principales técnicas y herramientas de IA y sus aplicaciones en problemas de seguridad.

CE15 Desarrollar modelos para la resolución de problemas de seguridad con algoritmos de IA.

CRIPTOGRAFÍA APLICADA Y SEGURIDAD EN SOFTWARE DE SISTEMAS

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CE6 Aplicar los mecanismos de cifrado, esteganografía y firma digital para garantizar la confidencialidad, integridad y autenticidad de los datos en un sistema, así como el acceso y seguridad en las comunicaciones.

CE7 Implantar medidas que garanticen la seguridad de los datos en el software de sistemas.

SEGURIDAD EN REDES

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CE6 Aplicar los mecanismos de cifrado, esteganografía y firma digital para garantizar la confidencialidad, integridad y autenticidad de los datos en un sistema, así como el acceso y seguridad en las comunicaciones.

CE18 Describir las amenazas de seguridad de las infraestructuras de redes modernas y aplicar técnicas para comprobar redes y mitigar dichas amenazas.

MONITORIZACIÓN Y SEGURIDAD INALÁMBRICA

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CE6 Aplicar los mecanismos de cifrado, esteganografía y firma digital para garantizar la confidencialidad, integridad y autenticidad de los datos en un sistema, así como el acceso y seguridad en las comunicaciones.

CE19 Conocer los sistemas de detección y prevención de intrusiones en redes cableadas e inalámbricas. Discernir, seleccionar y usar el sistema de monitorización adecuado de acuerdo a la legislación vigente.

CE20 Diseñar, desplegar y configurar redes inalámbricas seguras mediante la aplicación de políticas de seguridad apropiadas.

SEGURIDAD EN SISTEMAS e INFRAESTRUCTURAS CRÍTICAS

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CT2 Expresarse de forma oral y escrita en lengua inglesa

CE16 Diseñar mecanismos de prevención de amenazas a la seguridad, así como de detección y respuesta a las incidencias de seguridad en los sistemas críticos.

CE17 Analizar las particularidades de los sistemas críticos y sus esquemas de autenticación y acceso según el ámbito de aplicación.

SEGURIDAD EN SISTEMAS DISTRIBUIDOS

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CT1 Trabajar en equipos y con equipos (del mismo ámbito interdisciplinares) y desarrollar actitudes de participación colaboración como miembro activo de la comunidad.

CT2 Expresarse de forma oral y escrita en lengua inglesa

CE21 Capacidad de desarrollar arquitecturas, plataformas y sistemas distribuidos seguros.

TRABAJO FIN DE MÁSTER

CB6 Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

CB8 Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

CG2 Concebir, diseñar, poner en práctica y mantener un sistema global de ciberseguridad en un contexto definido.

CG3 Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la ciberseguridad.

CG4 Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

CG5 Planificar, gestionar, organizar e implantar medidas de seguridad en la operación y gestión de los sistemas.

CE22 Presentar y defender públicamente un proyecto integral de ciberseguridad de naturaleza profesional.