

GRADO EN GESTIÓN GLOBAL DE LA CIBERSEGURIDAD

RESULTADOS DE APRENDIZAJE

CÓDIGO	DENOMINACIÓN
COMP1	Desarrollar la capacidad de ejercer labores como director de ciberseguridad o responsable en la gestión de la ciberseguridad, liderando las actividades objeto de los proyectos relacionados con la sociedad de la información, bien como trabajador autónomo, por cuenta ajena y en sistemas de autoempleo.
COMP2	Desarrollar la capacidad para ejercer como responsable de proyectos en el ámbito de la gestión de la ciberseguridad, responsable en la confección de planes de seguridad y
COMP3	Dominar y desarrollar el ejercicio de responsable en la gestión de la ciberseguridad en un entorno transdisciplinar y global, transmitiendo valores basados en la búsqueda de la verdad y del bien común.
COMP4	Capacidad para definir temas de innovación que puedan contribuir al desarrollo de nuevos paradigmas o métodos de protección, para garantizar la ciberseguridad y exponer de forma adecuada los resultados de la innovación, conforme a los cánones de las disciplinas de la sociedad de la información.
COMP5	Desarrollar, de forma compartida, un proyecto de servicio social concreto.
COMP6	Aplicar de forma autónoma los principios, técnicas y procedimientos básicos de gestión de la ciberseguridad en entornos profesionales reales, identificando riesgos, adoptando medidas de protección y documentando adecuadamente las acciones realizadas.
COMP7	Capacidad para sintetizar e interrelacionar los conocimientos adquiridos a lo largo del grado para aplicarlos en un Trabajo de Fin de Grado.
COMP8	Descubrir, valorar y contrastar con uno mismo diversas respuestas a las preguntas existenciales que caracterizan la vida personal y comunitaria.
COMP9	Participar en la vida universitaria a través de actividades universitarias de cooperación, solidarias, culturales, deportivas y de representación estudiantil.
CON1	Conocer los fundamentos de la organización de empresas en un entorno digital: organización, planificación, control de gestión y estudio de las áreas funcionales, para aplicarlas en el ejercicio cotidiano de la gestión de la ciberseguridad.
CON2	Conocer el ordenamiento jurídico y los marcos regulatorios, organizaciones de referencia, estándares y recomendaciones existentes en el ámbito digital y de la ciberseguridad tanto en España como en el resto del mundo, para ejercer la profesión dentro del marco legal correspondiente.
CON4	Reconocer la antropología implícita en toda acción y ciencia humana y analizarla críticamente para averiguar qué idea del hombre subyace en las diversas teorías y cuáles son sus implicaciones prácticas personales y sociales.

CON5	Adquirir un conocimiento de los fundamentos matemáticos para resolver problemas en el campo de la estadística, programación, bases de datos y criptografía, de cara a analizar datos, desarrollar procesos y gestionar información garantizando su seguridad.
CON6	Conocer los fundamentos y principios en el desarrollo seguro de software, así como los lenguajes básicos de programación en el ámbito de la ciberseguridad.
CON7	Conocer y comprender los fundamentos de las configuraciones, arquitectura, protocolos y sistemas de seguridad utilizados en la transmisión de datos.
CON8	Conocer y comprender la estructura, organización, funcionamiento, administración e interconexión de los sistemas informáticos y su aplicación para la resolución de problemas propios en el ámbito de la seguridad.
CON9	Conocer la gestión y metodología en el análisis de riesgos, amenazas y vulnerabilidades de los sistemas de información y comunicación, así como las técnicas y herramientas propias en el ámbito de la gestión de la ciberseguridad.
HAB1	Diseñar la gestión y puesta en marcha de proyectos de implantación de la seguridad en el marco de los proyectos de ciberseguridad de la sociedad de la información.
HAB2	Dominar la elaboración y establecimiento de planes de recuperación y continuidad de negocio con actitud de liderazgo y trabajo en equipo, en el marco de los proyectos de ciberseguridad de la sociedad de la información.
HAB3	Identificar y utilizar adecuadamente los fundamentos de la seguridad para la defensa (ciberdefensa), así como las principales referencias y organizaciones nacionales e internacionales en la materia.
HAB4	Expresarse con fluidez, eficacia y responsabilidad social ante la toma de decisiones oportunas y requeridas, considerando los cambios del entorno en el desempeño personal y profesional.
HAB5	Saber aplicar la legislación necesaria y manejar especificaciones, reglamentos y normas de obligado cumplimiento.
HAB6	Saber utilizar y conocer las técnicas de diseño, implementación, explotación y gestión de datos en los sistemas de información, para la resolución de problemas propios en el ámbito de la seguridad.
HAB7	Utilizar herramientas y técnicas de cara a valorar vulnerabilidades de los sistemas informáticos y de telecomunicaciones de una organización.
HAB8	Aplicar pensamiento crítico, analítico y reflexivo para comprender y evaluar la realidad social y humana, identificando problemas y formulando juicios fundamentados.

HAB9	Emplear herramientas cuantitativas e informáticas para sintetizar información y tomar decisiones fundamentadas en contextos profesionales y personales.
HAB10	Identificar y formular las preguntas clave relacionadas con las causas y consecuencias de incidentes de ciberseguridad, evaluando su impacto en el entorno organizativo.
HAB11	Proponer respuestas y medidas de actuación ante incidentes de ciberseguridad aplicando principios éticos y códigos deontológicos propios de la profesión.

