Competencias del título - Maestría en Ciberseguridad

Competencias generales:

- CG1. Capacidad para integrarse en equipos de trabajo multidisciplinares de manera eficaz y cooperativa.
- CG2. Aprender a aplicar a entornos nuevos o poco conocidos, dentro de contextos más amplios (o multidisciplinares), los conceptos, principios, teorías o modelos relacionados con su área de estudio.
- CG3. Elaborar adecuadamente y con cierta originalidad composiciones escritas o argumentos motivados, de redactar planes, proyectos de trabajo o artículos científicos o de formular hipótesis razonables.
- CG4. Emitir juicios en función de criterios, de normas externas o de reflexiones personales.
- CG5. Presentar públicamente ideas, procedimientos o informes de investigación, de transmitir emociones o de asesorar a personas y a organizaciones.

Competencias específicas:

- CE1. Conocer los conceptos de gestión integrada de la seguridad que permitan su evaluación, así como, la organización del mando y respuesta rápida.
- CE2. Comprender los principios por los que se rige el gobierno de la Tecnología de la Información y las Comunicaciones, y ser capaces de analizar las Políticas de la Seguridad de una organización.
- CE3. Conocer las normas y estándares más relevantes, y los criterios y mecanismos de evaluación y certificación de la seguridad vigentes en la actualidad
- CE4. Ser capaces de aplicar una metodología para el análisis y evaluación de riesgos, así como saber utilizar las herramientas para su gestión.
- CE5. Identificar la combinación de controles técnicos, humanos y de procedimiento para ayudar a eliminar o reducir los riesgos de seguridad hasta un nivel manejable.
- CE6. Saber aplicar las técnicas criptográficas actuales y su empleo en el ámbito de la seguridad electrónica.
- CE7. Ser capaces de diseñas una infraestructura de clave pública (PKI) y saber aplicar las tecnologías de certificación y su uso corporativo. También conocerá cuáles son los principales prestadores de servicios de certificación españoles, así como la normativa vigente.

- CE8. Analizar las técnicas de control y administración de usuarios empleando sistemas de autenticación robusta y sistemas para la provisión de identidades.

- CE9. Ser capaces de configurar y gestionar los sistemas operativos para implantar medidas de seguridad, así como los principios de diseño y desarrollo de aplicaciones informáticas seguras y de seguridad en las bases de datos.

- CE10. Ser capaces de supervisar las medidas de protección que se emplean contra virus y otros tipos de software malicioso.

- CE11. Evaluar las técnicas de prevención de accesos no autorizados, daños e interferencias utilizadas en los centros de procesos de datos en la actualidad.

- CE12. Identificar las distintas amenazas y ser capaces de evaluar las medidas de salvaguarda correspondientes.

- CE13. Conocer los conceptos básicos relativos a la seguridad de las personas y ser capaces de planificar políticas de seguridad que las incluyan.

- CE14. Conocer los conceptos avanzados de seguridad en las comunicaciones, aplicados a los casos de controles de seguridad en la red, protección del perímetro de la red y será capaz de discriminar entre las distintas tecnologías VLAN/SSL/SSH/IPSEC.

- CE15. Ser capaces de planificar, organizar, gestionar e implantar las medidas de seguridad en la operación y gestión de los sistemas.

- CE16. Conocer los conceptos básicos de los principales procesos y respuesta ante incidentes y su aplicación a casos reales.

- CE17. Ser capaces de hacer un análisis forense sobre un sistema.

- CE18. Comprender y aplicar el marco legislativo vigente.

- CE19. Ser capaces de aplicar los conocimientos teóricos a través prácticas profesionales para analizar, proponer soluciones e implantarlas en situaciones reales empresariales.

- CE20. Conocer los métodos de trabajo de las empresas consultoras de seguridad y aprender a escribir informes y procedimientos sobre las tareas básicas relacionadas con la seguridad de la organización.

- CE21. Ser capaz de desarrollar una actividad científica dentro del campo de la investigación en áreas relacionadas con la Seguridad TIC.

- CE22. Integrar el conocimiento de las diferentes áreas y disciplinas estudiadas y las reflexiones sobre la propia práctica como medio para la mejora continua.

- CE23. Capacidad para la dirección técnica y la dirección de proyectos en el ámbito de la Seguridad de las Tecnologías de la Información y las Comunicaciones.