PROGRAMA DE ESTUDIOS:

CIBERSEGURIDAD

Programa de Ciberseguridad

Conocimientos y competencias

- **Conocimientos básicos**: Desarrollar una sólida comprensión de los conceptos y principios básicos de la ciberseguridad.
- **Competencia técnica**: Adquirir experiencia práctica con herramientas y técnicas esenciales de ciberseguridad.
- **Capacidad de resolución de problemas**: Mejorar la capacidad de analizar y resolver retos complejos de ciberseguridad.
- **Gestión de riesgos**: Aprender a identificar y mitigar los riesgos de seguridad en diversos contextos organizativos.
- **Comunicación y colaboración**: Desarrollar habilidades de comunicación eficaces para transmitir cuestiones de ciberseguridad y colaborar con equipos diversos.

Detalles del curso

1. Introducción a la ciberseguridad y a la seguridad de redes (40 horas), Básico

El curso "Introducción a la ciberseguridad y la seguridad de las redes" está diseñado para proporcionar a los estudiantes una comprensión básica de los principios y prácticas que sustentan la seguridad de los sistemas y redes de información. A lo largo de este curso, los participantes explorarán el vasto panorama de la ciberseguridad, aprendiendo a identificar, analizar y mitigar las amenazas y vulnerabilidades digitales. El plan de estudios está estructurado para ofrecer una visión completa de los fundamentos de la ciberseguridad, incluidos los mecanismos de los ciberataques, la aplicación de protocolos de seguridad sólidos y el desarrollo de estrategias eficaces para proteger los datos y la infraestructura de red.

En este curso se hace especial hincapié en el aprendizaje práctico, en el que los estudiantes realizarán ejercicios prácticos y sesiones de laboratorio utilizando herramientas y tecnologías estándar del sector. Una característica distintiva del curso es su alineación con las normas y prácticas actuales de la industria, asegurando que el contenido sea a la vez relevante y actualizado. Los estudiantes conocerán las últimas tendencias en ciberseguridad, como la seguridad en la nube, la seguridad del Internet de las Cosas (IoT) y la aplicación de la inteligencia artificial en la ciberdefensa. Este plan de estudios está diseñado para preparar a los estudiantes para la naturaleza cambiante de las amenazas cibernéticas y los continuos avances en la tecnología que dan forma al panorama de la ciberseguridad. Además, el curso hace especial hincapié en las consideraciones éticas y los marcos jurídicos que rigen la ciberseguridad. A través de debates sobre hacking ético, leyes de privacidad y normativas de cumplimiento, los estudiantes aprenderán la importancia de la integridad profesional y la responsabilidad legal en el campo de la ciberseguridad.

Temas: Comprensión de las ciberamenazas y los ataques, Criptografía, Fundamentos de la seguridad de redes, Políticas y normas de seguridad, Gestión de identidades y accesos, Seguridad web y de aplicaciones, Seguridad inalámbrica, Hacking ético y pruebas de penetración, Respuesta a incidentes y recuperación tras desastres.

2. Seguridad de los datos (40 horas, Intermedio)

Con un énfasis en las habilidades prácticas y la comprensión de los fundamentos teóricos, el plan de estudios abarca una amplia gama de temas, desde técnicas de cifrado y mecanismos de control de acceso hasta marcos legales y consideraciones éticas. A través de atractivas sesiones de laboratorio y proyectos integrales, los alumnos utilizarán herramientas y tecnologías estándar de la industria para implementar

soluciones criptográficas, configurar redes seguras y evaluar las vulnerabilidades de los datos.

El curso adopta un enfoque interdisciplinario, integrando las dimensiones jurídica, normativa y ética de la seguridad de datos. Los debates sobre las leyes de protección de datos, los requisitos de cumplimiento y los dilemas éticos enriquecen el plan de estudios técnico, proporcionando una visión holística de la seguridad de los datos. Las conferencias invitadas de profesionales del sector y el análisis de violaciones de datos de gran repercusión aportan al aula una visión del mundo real, mejorando la experiencia de aprendizaje y exponiendo a los estudiantes a los retos prácticos y a los procesos de toma de decisiones en este campo.

Temas: Criptografía, Control de Acceso, Privacidad de Datos, Almacenamiento Seguro de Datos, Transmisión Segura de Datos, Gestión de Riesgos y Seguridad de Datos.

3. Seguridad de redes y en la nube (40 horas, Intermedio)

Este curso ofrece una exploración exhaustiva de las teorías fundamentales y las estrategias prácticas necesarias para proteger los modernos sistemas en red y los servicios basados en la nube. Al profundizar en los entresijos de la seguridad de las redes, los modelos de seguridad en la nube y las últimas tecnologías de ciberseguridad, los estudiantes están preparados para navegar y mitigar los complejos desafíos de seguridad a los que se enfrentan las organizaciones de hoy en día.

Un elemento central del curso es el análisis en profundidad de las técnicas criptográficas, los protocolos de seguridad y los principios en los que se basan las arquitecturas de red seguras. Los alumnos abordarán temas como el cifrado, la autenticación y el diseño de políticas de seguridad, y adquirirán una sólida comprensión de cómo se aplican estos elementos para proteger la información y garantizar la privacidad.

Al abordar los desafíos únicos de la computación en nube, el curso cubre conceptos esenciales de seguridad en la nube, incluida la gestión de identidades y accesos (IAM), la protección de datos en la nube y el cumplimiento de las normas reglamentarias. Los estudiantes explorarán varios modelos de servicios en la nube (IaaS, PaaS, SaaS) y estrategias de despliegue (público, privado, híbrido), aprendiendo a diseñar y evaluar las medidas de seguridad que se alinean con las necesidades específicas de los entornos basados en la nube.

La experiencia práctica constituye la espina dorsal del enfoque de aprendizaje, con sesiones de laboratorio y ejercicios que simulan escenarios de seguridad del mundo real. Mediante el uso de herramientas y software de seguridad actuales, los estudiantes realizarán evaluaciones de vulnerabilidad, participarán en la detección y respuesta a amenazas y aplicarán políticas de seguridad en entornos prácticos.

Temas: Fundamentos de la computación en nube, amenazas y vulnerabilidades, medidas de protección, seguridad en la nube, políticas de seguridad y cumplimiento de la normativa

4. Ciberseguridad avanzada (40 horas, Intermedio)

En el núcleo de este curso se encuentra un fuerte énfasis en el aprendizaje práctico, asegurando que los estudiantes no sólo comprendan los conceptos avanzados, sino que también los apliquen en escenarios del mundo real. Los laboratorios y las tareas basadas en proyectos simulan auténticos retos de ciberseguridad, ofreciendo a los estudiantes la oportunidad de utilizar las herramientas y técnicas más avanzadas. Desde la realización de sofisticadas pruebas de penetración hasta el análisis y la mitigación de vulnerabilidades, los participantes desarrollarán un conjunto de habilidades prácticas muy valoradas en el campo de la ciberseguridad.

El curso profundiza en áreas críticas como la inteligencia artificial (IA) en la ciberseguridad, la seguridad de blockchain, el Internet de las Cosas (IoT) y la seguridad de la computación en la nube. Al examinar estos temas de vanguardia, los estudiantes obtendrán información sobre las futuras direcciones de la ciberseguridad y aprenderán a anticipar y contrarrestar nuevas amenazas y vulnerabilidades.

Las consideraciones éticas, los marcos legales y las implicaciones sociales de las prácticas de ciberseguridad forman parte integral del curso. A través de debates, estudios de casos y análisis de incidentes de la vida real, los estudiantes explorarán los límites éticos de la piratería informática, la importancia de la privacidad y las ramificaciones legales de las acciones de ciberseguridad.

Temas: Repaso a los fundamentos de la ciberseguridad, seguridad avanzada de redes, hacking ético y pruebas de penetración, respuesta a incidentes dna forense digital, amenazas emergentes y tendencias futuras.