UTEC Universidad Tecnológica | uruguay global | UOC Universitat Oberta de Catalunya | agesic

ESPECIALIZACIÓN EN
Ciberseguridad

especializacion.ciberseguridad@utec.edu.uy

utec.edu.uy

¿POR QUÉ ESTUDIAR ESTA ESPECIALIZACIÓN?

La demanda de profesionales de ciberseguridad está creciendo rápidamente. Las organizaciones de diversas industrias necesitan expertos calificados que puedan salvaguardar sus activos digitales y defenderse contra las ciberamenazas.

La Especialización en Ciberseguridad de UTEC, en colaboración con la Universitat Oberta de Catalunya (UOC) y Agesic, proporciona amplios conocimientos sobre la ciberseguridad en redes informáticas y sistemas corporativos.

La enseñanza combina la adquisición de una base teórica sólida de conocimientos con una formación práctica y basada en el estudio de casos reales. Se estudian los problemas y las soluciones empleadas para resolver el cibercrimen, se examinan en profundidad los riesgos de ciberseguridad en las redes fijas e inalámbricas, y se analizan los mecanismos de protección particulares de cada sistema operativo.

Modalidad | Online
Idioma | Español

Duración | 11 meses
Inicio | 25 de setiembre de 2024
Dedicación semanal | 25 hs aprox.

¿PARA QUÉ ESTUDIAR CIBERSEGURIDAD?

Internet se ha convertido en un medio de información básico tanto para nuestras vidas personales como profesionales. Por la red circulan grandes volúmenes de datos privados y confidenciales (datos financieros, médicos, industriales, etc.) vulnerables a todo tipo de ataques. Las medidas de seguridad son imprescindibles para proteger los sistemas de usos indebidos y abusivos, y los habilita para ofrecer servicios robustos y de calidad.

El campo de la ciberseguridad se está volviendo cada vez más crítico a medida que la tecnología sigue avanzando y las ciberamenazas aumentan. En este contexto es clave la formación en ciberseguridad para que profesionales adquieran conocimientos avanzados, se especialicen, adquieran experiencia práctica y se mantengan al día en un escenario en constante evolución, logrando así proteger a las organizaciones y las personas de los ataques cibernéticos.

Según el Banco Interamericano de Desarrollo, Uruguay necesita 600 especialistas en ciberseguridad (BID, 2019).

Se espera que al terminar esta formación, el estudiante sea capaz de diseñar e implementar estrategias que puedan garantizar la seguridad de los recursos informáticos de una empresa, a través de políticas de prevención, protección y detección de ataques.

REQUISITOS DE INGRESO

El programa está especialmente dirigido a ingenieros, licenciados o graduados en el área de las **Tecnologías de la Información y de las Comunicaciones.**

- Conocimientos de **redes**, de **sistemas operativos**, y de **administración de redes** y **sistemas operativos**.
- Conocimientos medios de **programación**: competencias para entender pequeños scripts, o programar partes de una aplicación.
- Conocimientos básicos de **sistemas distribuidos**.
- **Título de grado** de una carrera de 4 años o más de duración. Requiere **apostilla a presentar de forma obligatoria** (antes del 31 de diciembre de 2024) que incorpore código de verificación electrónica.
- En caso de no contar con título de grado se requiere, además de los conocimientos explicitados, experiencia profesional comprobable de al menos 2 años en el ámbito TIC, con carta de certificación de la empresa donde se desarrollaron las tareas.

* Accedé a la información ampliada en el documento "Requisitos de acceso legal Diploma de Especialización de Ciberseguridad de redes y sistemas de la UOC" adjunto en el mail informativo y disponible también en la web en la sección "Requisitos de ingreso".

¿QUÉ NECESITAS PARA POSTULAR?

Completar el formulario en la página web, adjuntando:

- CV
- Carta de motivación
- Documento de identidad escaneado (frente y dorso)
- Título de grado escaneado (bajo condición de apostilla a presentar durante 2024).

Solo en el caso de no contar con título de grado, se debe adjuntar:

- CV
- Carta de motivación
- Documento de identidad escaneado (frente y dorso)
- Fórmula 69A o Constancia de Egreso de UTU
- Autoinforme completo
- Carta de certificación de la empresa

Luego de completado el formulario, desde la oficina de coordinación académica **te contactaremos para agendar una entrevista**, que es excluyente para el proceso de admisión.

PLAN DE ESTUDIOS

La Especialización está conformada por cinco cursos de conceptualización teórico-práctica pertenecientes al Posgrado de Ciberseguridad en Redes y Sistemas de la UOC, y se complementa con tres talleres organizados por UTEC.

FUNDAMENTOS DE CIBERSEGURIDAD	En esta unidad se asientan y ordenan las bases de la ciberseguridad haciendo un repaso de los riesgos, vulnerabilidades y amenazas a los que están expuestos los sistemas informáticos, identificando y analizando los sistemas de prevención, protección y detección de ataques que se pueden utilizar hoy en día, y estudiando los algoritmos criptográficos que son la base de muchos mecanismos de seguridad. Se trata de una unidad inicial y de nivelación, que da una visión global de la ciberseguridad, pero que a la vez refuerza mucho la visión práctica y de análisis crítico de las tecnologías de seguridad y privacidad de los sistemas de información y comunicación. La unidad se estructura alrededor de unas actividades que tienen un componente teórico y práctico, permitiendo de este modo que el estudiante comprenda mejor los problemas reales que surgen en la implementación y despliegue de sistemas de seguridad.
SEGURIDAD Y PENTESTING DE SERVIDORES DE DATOS	En esta unidad se verán ejemplos de algunos de los métodos más habituales para atacar formularios de aplicativos web que interactúan con alguna base de datos. Se harán ataques a las Bases de datos, así como a los aplicativos que hacen las consultas. Adicionalmente, se van a analizar algunas de las bases de datos más utilizadas en la actualidad y los principales conceptos que se tienen que considerar para fortificar adecuadamente los diferentes tipos de bases de datos.
SEGURIDAD Y PENTESTING DE SISTEMAS	Esta unidad muestra la manera en que se tienen que instalar y configurar los dos sistemas operativos más mayoritarios: Windows Server y GNU/Linux. Mediante máquinas virtuales se configurarán los servidores y se realizará un ataque informático a un sistema real. Se tendrá que documentar exhaustivamente todo el procedimiento para llegar a hacerse con el control de las máquinas.

ARQUITECTURAS Y PROTOCOLOS DE SEGURIDAD	Los sistemas informáticos complejos requieren del uso de servicios y protocolos de seguridad para protegerlos, tanto localmente como en línea, y también para ofrecer nuevas funcionalidades que mejoren la interacción con el sistema por parte de los usuarios y su gestión por parte de los administradores. Por un lado, se estudian protocolos básicos que permiten establecer conexiones de forma segura (e.g. SSH, WPA). Por otro lado, se estudian conceptos relacionados con la identidad digital, protocolos de autenticación, autorización, control de acceso, y arquitecturas de Single Sign On. Además, teniendo en cuenta que muchos sistemas informáticos se despliegan en una arquitectura cloud, se verán los principales riesgos de seguridad a tener en cuenta para desplegar los servicios de seguridad estudiados en este tipo de arquitectura.
SEGURIDAD EN CLOUD COMPUTING	El Cloud Computing es una propuesta tecnológica adoptada, hoy en día, por la sociedad en general como forma de interacción entre proveedores de servicios, gestores, empresas/administración y usuarios finales para la prestación de servicios y utilización de recursos en el ámbito de las TIC y sustentado por un modelo de negocio viable económicamente. El modelo de servicio de tecnologías de información basada en la nube y el constante aumento de las amenazas informáticas implican un cambio en el concepto de seguridad informática en las organizaciones, especialmente en la importancia estratégica que tiene la seguridad en escenarios de Cloud Computing. Hoy en día, nos encontramos involucrados en una transformación de paradigmas donde las Tecnologías de la Información y Comunicación (TIC) actúan como motor de la transformación digital, y los modelos en la nube son la tónica general.

TALLER DE SIMULACIÓN CON CYBER RANGE

El Cyber Range es una plataforma que permite simular entornos operativos reales para la formación y el entrenamiento individual o colectivo de profesionales. En este taller, llevado adelante por Agesic, los estudiantes participarán de ejercicios de simulación prácticos donde pondrán en práctica los conocimientos adquiridos a lo largo del programa.

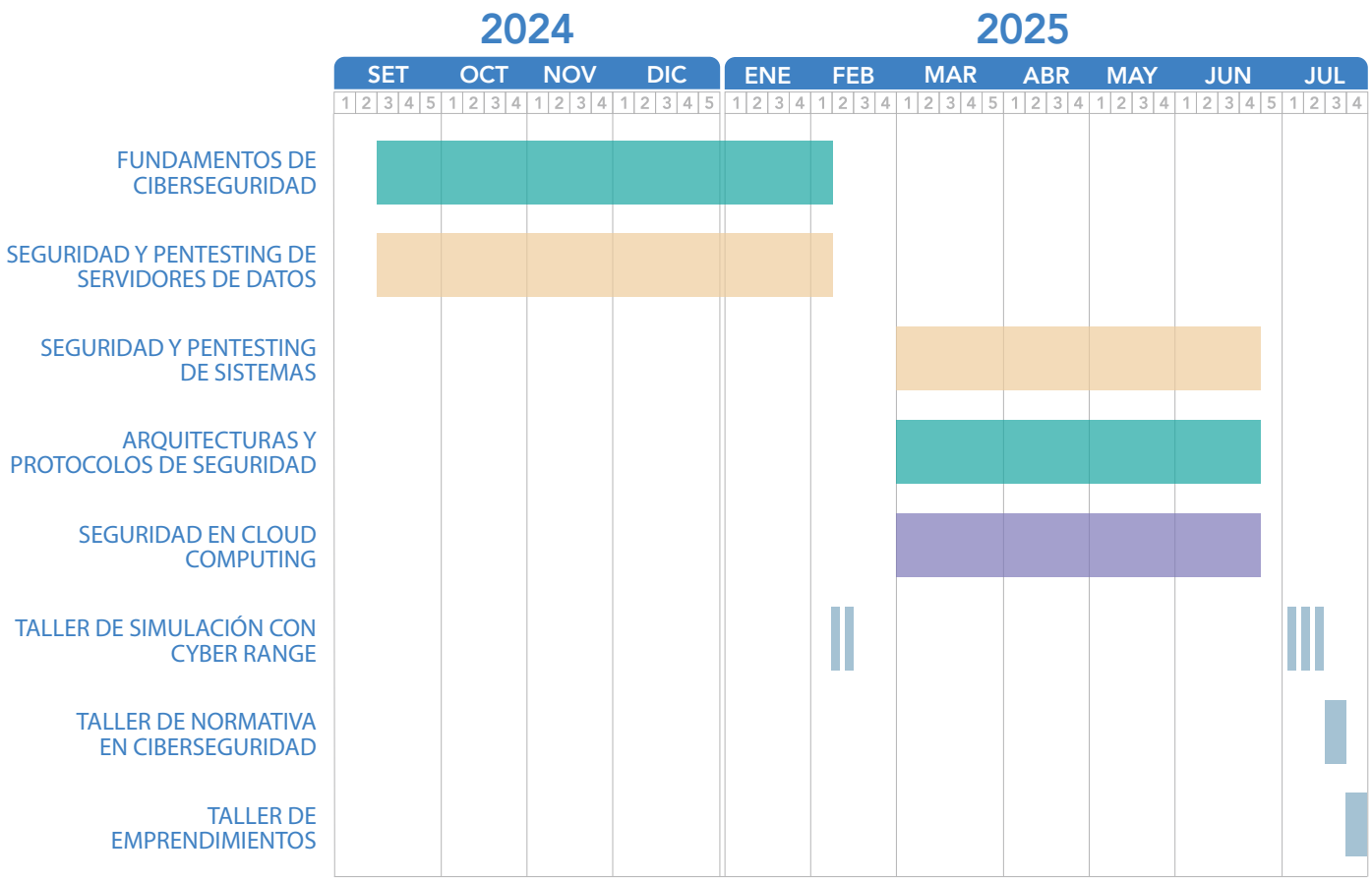
TALLER DE NORMATIVA EN CIBERSEGURIDAD

Este taller, llevado adelante por Agesic, proporciona conocimientos básicos acerca de la normativa vigente en Uruguay sobre ciberseguridad, para conocer las leyes y decretos que deben seguirse para proteger la información y los sistemas digitales y comprender las obligaciones y responsabilidades legales relacionadas con la protección de datos y privacidad.

TALLER DE EMPRENDIMIENTOS

Aprenderás estrategias útiles para incorporar exitosamente la innovación impulsada por tecnología, tanto en empresas ya existentes como en nuevos emprendimientos. Se espera que al completar la actividad puedas comprender el funcionamiento del proceso de innovación, identificar oportunidades y atraer clientes, segmentar el mercado y generar valor, así como mapear los pasos prácticos de los problemas organizativos y legales asociados con la creación de una empresa, insertarse en el ecosistema y apropiarse del valor generado.

CALENDARIO



Este calendario puede sufrir modificaciones.

PERFIL DE EGRESO

Desde un punto de vista relacionado a competencias técnicas, los egresados de la Especialización en Ciberseguridad serán capaces de:

- Analizar y aplicar las técnicas básicas de prevención, protección y detección de ataques a un sistema informático.
- Analizar y gestionar los riesgos de seguridad en el cloud.
- Implantar estrategias de detección de vulnerabilidades y gestión de incidentes en el cloud.
- Conocer los aspectos legales vinculados a la protección de datos en el cloud.
- Establecer acuerdos con proveedores de cloud para asegurar el cumplimiento normativo y la protección de datos.
- Evaluar y tomar las decisiones más adecuadas en cuanto a la selección y uso de herramientas y tecnologías del mercado en el ámbito de la ciberseguridad y la privacidad.
- Identificar, examinar y evaluar los principales riesgos de un dominio informático y diseñar estrategias para gestionarlos.
- Analizar la implementación y despliegue de soluciones criptográficas para validar su funcionamiento.
- Conocer las herramientas y los métodos de pentesting en los servidores de datos.

- Fortalecer los diferentes tipos de bases de datos, para asegurar la integridad, la disponibilidad y la confidencialidad de la información almacenada.
- Formular y desarrollar soluciones integrales e innovadoras en el ámbito de la ciberseguridad y privacidad, teniendo en cuenta las dinámicas de transformación y las tendencias tecnológicas.
- Realizar una configuración segura y robusta de un servidor GNU/Linux o Windows.
- Utilizar herramientas para la administración y la protección de redes cableadas e inalámbricas y la gestión de alertas de seguridad.
- Mantener y controlar los sistemas informáticos, preparando ataques para encontrar malas configuraciones.

CONTACTO

especializacion.ciberseguridad@utec.edu.uy

https://utec.edu.uy/

@uruguayglobal

uruguayglobal

Programa de internacionalización de habilidades digitales avanzadas