



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 | 27 de setiembre de 2023

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*.

* De acuerdo con la Ordenanza de Educación Continua de UTEC podrán acceder también a esta formación personas que no cuenten con título de grado, previa evaluación de que su formación y experiencia laboral sean suficientes para el aprovechamiento del Plan, aprobados por parte de la Coordinación Académica. En estos casos el programa prevé la obtención de un certificado de Diploma en Ciberseguridad.



¿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 (o constancia de egreso de la educación media (fórmula 69A) en caso de no disponer de título).

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 cuatro cursos de conceptualización teórico-práctica y un proyecto final de aplicación profesional y de desarrollo individual, 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.

PROYECTO FINAL

El Proyecto Final tiene como objetivo que el estudiante realice un trabajo individual en el que se apliquen e integren los conocimientos adquiridos a lo largo del posgrado. El estudiante hará la implantación de un sistema, un desarrollo de una aplicación, o un análisis de seguridad de un sistema basado en las tecnologías de la información y de las comunicaciones.

Es un trabajo eminentemente práctico y vinculado al ejercicio profesional de la Seguridad Informática, aunque en algunos casos puede ser, o incluir, un trabajo de investigación.

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 Agestic, 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

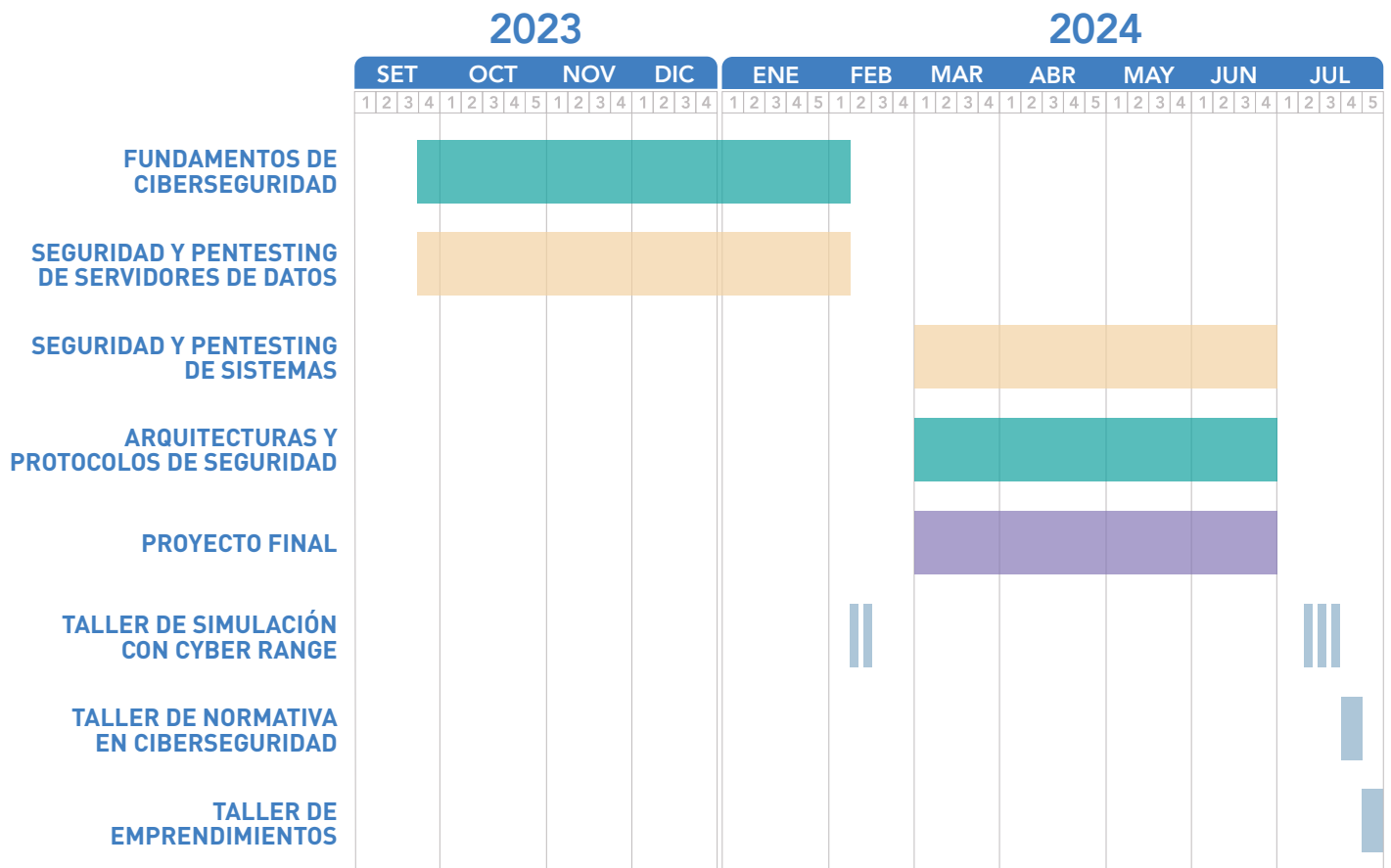
Este taller, llevado adelante por Agestic, proporciona conocimientos básicos acerca de la normativa vigente en Uruguay sobre ciberseguridad, para conocer las leyes y decretos que deben seguirse para proteger la información y los sistemas digitales y comprender las obligaciones y responsabilidades legales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