Universidad Tecnológica del Uruguay (UTEC)

Universitat Oberta de Catalunya (UOC)

Especialización en Ciberseguridad

PLAN de ESTUDIOS

2024

Índice de contenidos

I – DENOMINACIÓN, JUSTIFICACIÓN Y OBJETIVOS

1.1. Denominación:

Especialización en Ciberseguridad

1.2. Justificación:

Internet se ha convertido en un medio de información básico tanto para nuestras vidas personales como profesionales. Por la red circulan enormes 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. Por lo tanto, se vuelve necesario contar con los conocimientos y habilidades avanzados necesarios para proteger a las organizaciones y las personas de los ataques cibernéticos.

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.

Según (ISC)², la mayor asociación sin fines de lucro de profesionales certificados en ciberseguridad del mundo, en el último año se agravó la escasez de profesionales en ese campo. Su estudio *Cybersecurity Workforce Study* de 2022, revela que, si bien la mano de obra mundial se encuentra en su nivel más alto (4,7 millones de profesionales), aún se necesitan otros 3,4 millones más.

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

En este contexto es clave la formación en ciberseguridad para que profesionales adquieran conocimientos avanzados, se especialicen, obtengan experiencia práctica y se mantengan al día con el panorama de ciberseguridad en evolución. Este posgrado proporciona amplios conocimientos sobre la ciberseguridad en redes informáticas y sistemas corporativos. 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.

En el 2023 la UTEC firma un convenio marco con la Universitat Oberta de Catalunya (UOC) a través del cual ambas universidades se comprometen a trabajar en conjunto para avanzar la calidad educativa de sus programas, así como para implementar un modelo de formación centrado en el estudiante, digital, dinámico y flexible, colaborativo y en constante evolución al ritmo de la sociedad y los avances tecnológicos.

En este sentido y visto el avance de la UOC en temas de ciberseguridad (su desarrollo de dos programas de Posgrado y una Maestría en esa materia), se toma como base de la Especialización los cursos dictados a través de la plataforma de la UOC mediante su Posgrado de Ciberseguridad en Redes y Sistemas, y se complementa con talleres específicos de UTEC y AGESIC para enriquecer el programa y darle la necesaria relevancia para los estudiantes uruguayos y de la región.

1.3. Objetivos de la especialización en ciberseguridad:

1.3.1- Objetivo general

El posgrado tiene como objetivo proporcionar una formación técnica y especializada en el ámbito de la seguridad en redes y sistemas.

La enseñanza combina la adquisición de una base teórica sólida de conocimientos con una formación práctica y basada en el estudio de casos reales. Tras completar la especialización, el estudiante será 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 prevención de ataques.

1.3.2- Objetivos específicos

- Conocer las técnicas de explotación de vulnerabilidades de una red y los puntos débiles de un sistema.
- Identificar, evaluar y gestionar los principales riesgos de un dominio informático, tanto tecnológicos como procedentes de la ingeniería social.
- Implementar técnicas y contramedidas básicas de seguridad para la prevención de ataques derivados de la ingeniería social.
- Desarrollar y gestionar redes de comunicaciones en contextos residenciales, empresariales o institucionales, responsabilizándose de la seguridad del sistema y de la protección de los datos de los usuarios.
- Diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, la detección y la disuasión de ataques.

II – PERFIL DE EGRESO

En relación con las 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.
- Establecer políticas de control de accesos e identidades y manejar servicios de gestión de claves criptográficas.
- 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.

En relación con las competencias transversales, los egresados serán capaces de:

- Autorregular su aprendizaje, habilidad particularmente importante para poder activar las estrategias necesarias para alcanzar los objetivos establecidos en la resolución de problemas concretos.
- Trabajar en equipo.
- Comunicarse efectivamente, tanto en forma oral como escrita.
- Pensar en forma crítica para plantear soluciones a diferentes tipos de problemas y encontrar alternativas de resolución para distintas situaciones de la vida real.
- Pensar creativamente y con una mentalidad resolutiva y emprendedora.

III – REQUISITOS DE INGRESO, DURACIÓN, REQUISITOS DE EGRESO

3.1. Requisitos de Ingreso:

Dirigido especialmente a ingenieros, licenciados o graduados en el área de las Tecnologías de la Información y de las Comunicaciones.

Específicamente, podrán ingresar a la Especialización en Ciberseguridad quienes cuenten con título de grado de una carrera de 4 años o más de duración y:

- 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.
- Conocimientos básicos de seguridad en redes y criptografía.

De acuerdo con la Ordenanza de Posgrados Resolución 384/23 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.

3.2. Duración de la Especialización en Ciberseguridad:

La duración estimada de la Especialización en Ciberseguridad es de 1 año lectivo. Se computan 900 horas totales, con una dedicación promedio estimada de 25 horas semanales.

3.3. Requisitos de Egreso para obtención del título:

Obtendrán el título de Especialista en Ciberseguridad otorgado por UTEC, quienes alcancen el total de créditos asociados a la Especialización y cumplan con los requisitos establecidos por UTEC en sus ordenanzas.

Aquellas personas que alcancen la totalidad de créditos, pero no cuenten con título de grado a la fecha de finalización de las actividades de la Especialización, obtendrán un certificado de Diploma en Ciberseguridad.

UTEC será la institución responsable de controlar el cumplimiento de los requisitos de egreso y titulación. El certificado de egreso será emitido y tramitado por UTEC. Los estudiantes recibirán, además, un diploma de la UOC por el programa cursado y aprobado en su plataforma.

IV – PLAN CURRICULAR

El programa está dirigido a profesionales que quieran adquirir responsabilidades relacionadas con la administración de redes y sistemas corporativos. En particular, el perfil de los estudiantes del posgrado es el de ingenieros, graduados y profesionales de las tecnologías de la información y la comunicación (TIC).

La enseñanza combina la adquisición de una base teórica sólida de conocimientos con una formación práctica y basada en el estudio de casos reales.

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

4.1. Créditos, organización y modalidad de cursado:

El plan de estudios se implementa en base a créditos, expresados en horas cronológicas, y de acuerdo con la carga semanal de actividades que deberá asumir un estudiante para lograr los objetivos de aprendizaje definidos en cada unidad. Cada crédito es equivalente a 15 horas cronológicas y están asociados a objetivos de aprendizajes que son evaluables.

La Especialización en Ciberseguridad comprende **un total de 60 créditos** organizados en:

- 55 créditos de cursos virtuales
- 1 crédito de Taller de *Cyber Range* con AGESIC
- 1 crédito de Taller de Normativa Legal con AGESIC
- 3 créditos de Taller de Emprendimientos

De acuerdo con el Reglamento General de Estudios de la UTEC representa 900 horas cronológicas.

UNIDADES CURRICULARES	**HORAS SINCRÓNICAS/ ASINCRÓNICAS**	**HORAS AUTÓNOMAS**	**HORAS CRONOLÓGICAS TOTALES**	**Créditos**
Fundamentos de ciberseguridad	85	80	165	11
Seguridad y *pentesting* de servidores de datos	55	110	165	11
Seguridad y pentesting de sistemas	55	110	165	11
Arquitecturas y protocolos de seguridad	75	90	165	11

Seguridad *en cloud computing*	55	110	165	11
Taller *Cyber Range*	15	0	15	1
Taller Normativa Legal	13	2	15	1
Taller Emprendimientos	32	13	45	3
Subtotal	**385**	**515**	**900**	**60**

Los programas correspondientes a las unidades curriculares de la Especialización en Ciberseguridad se pueden encontrar en el **Anexo**.

4.2. Metodología:

La Especialización en Ciberseguridad es impartida 100% de forma remota, con posibilidad de realizar alguno de los talleres gestionados por UTEC de forma presencial.

En cuanto a los cursos, según lo definido por la UOC, a lo largo de todo el período docente del posgrado se presentan diferentes enfoques metodológicos. Aparte de las dinámicas de grupo, los estudiantes realizan parte del aprendizaje basándose en el estudio y análisis de casos reales y el desarrollo de proyectos prácticos. Se parte de la idea que el aprendizaje que se quiere promover tiene su base en un paradigma de carácter constructivo y aplicado, dónde la construcción de conocimiento es un acto compartido y parte tanto de la experiencia propia como la de los demás y se ve complementada por un marco teórico que permite comprender mejor algunos de los aspectos prácticos.

El entorno virtual de aprendizaje de la UOC está dotado de la información, los recursos y las herramientas que tanto los estudiantes como los profesores necesitarán a lo largo del proceso formativo. Éste no pretende ser simplemente una plataforma tecnológica dónde comunicarse y albergar los contenidos, sino que los recursos y las dinámicas que puedan ofrecerse desde el mismo signifiquen para docentes y discentes una comunidad educativa real con todos los componentes e interacciones necesarias.

El Campus Virtual es la plataforma tecnológica que ofrece la UOC para que los participantes del Programa puedan acceder a la información y a los procesos de comunicación propia de éste utilizando la comunicación telemática (mediante Internet) en donde los participantes de todos los programas de posgrado llevan a cabo la mayoría

de las acciones comunicativas. En el Campus Virtual se encuentran los espacios comunes, que se comparten con el resto de los compañeros del curso y con el equipo docente. Estos espacios se distribuyen básicamente en cuatro grandes bloques que concretan la metodología de la UOC:

Planificación	Espacio de acceso al plan docente o guía de aprendizaje así como al calendario semestral donde se encuentra la temporalización prevista de las actividades.
Comunicación (docencia)	Comunicación con el profesor y trabajo cooperativo con los compañeros: la tecnología de este entorno y la metodología propia de la UOC facilitan el trabajo cooperativo.
Recursos	Desde este espacio se facilita el acceso a los materiales didácticos del curso y también a la Biblioteca de la UOC y a otras bibliotecas del mundo, bases de datos, revistas, etc.
Evaluación	Espacio de entrega y registro de las actividades de evaluación continua así como el de consulta de la valoración continua de las actividades de aprendizaje.

Para los talleres organizados por UTEC se utilizarán metodologías participativas, que resaltan el carácter práctico de los aprendizajes y proporcionan herramientas claves para la construcción de las competencias en la materia.

4.3- Sistema de calificaciones y evaluación final:

Cada una de las unidades curriculares cuenta con instancias y actividades de evaluación. De acuerdo con las normas de evaluación y calificación utilizadas en UTEC, la escala de calificaciones va del 1 al 5 y se expresa en rangos correspondientes a los niveles de logro que se detallan a continuación:

CALIFICACIÓN	CONCEPTO	RANGOS
1	Deficiente	1.00 a 1.99
2	Insuficiente	2.00 a 2.99
3	Suficiente	3.00 a 3.99
4	Muy bueno	4.00 a 4.99
5	Excelente	5.00

Para aprobar cada unidad curricular de los distintos módulos de este Plan de Estudios la calificación final deberá ser igual o superior a 3, correspondiente al 60% de logro, a excepción de los tres talleres donde la calificación final será APROBADO o NO APROBADO.

V - NÚMERO DE CUPOS Y COSTO

El cupo máximo de estudiantes es de 30 personas.

Se actualizan anualmente los costos de derechos universitarios que pudieran corresponder, y las becas previstas.

ANEXO

Se presentan a continuación los programas de las unidades curriculares correspondientes a la Especialización en Ciberseguridad.

Fundamentos de ciberseguridad		
PLAN DE ESTUDIOS	Especialización en Ciberseguridad - 2024	
NOMBRE DE LA UNIDAD CURRICULAR	Fundamentos de ciberseguridad	
MODALIDAD	Asincrónica y a distancia	
CARÁCTER	Obligatorio	
CRÉDITOS	11	
CARGA HORARIA TOTAL (en horas)	165 horas totales	
DEDICACIÓN (en horas)	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	85 horas	80 horas
❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**		

- **Presentación de la Unidad Curricular:**

  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.

- **Objetivos de aprendizaje**

  Se espera que los estudiantes puedan:

  - Identificar, examinar y gestionar los principales riesgos de un dominio informático.
  - Evaluar los sistemas de prevención y protección de ataques.
  - Comprender el funcionamiento de los sistemas criptográficos, y validar su implantación en diferentes sistemas.
  - Diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, detección y disuasión de ataques
  - Comprender, configurar, y gestionar herramientas para la administración y protección de redes cableadas e inalámbricas, y la gestión de alertas de seguridad.
  - Conocer y saber desplegar los diferentes sistemas de detección de intrusiones.

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad sólo puede superarse a partir de la evaluación continua (EC), por medio de las pruebas de evaluación continua (PEC), nota que se combina con una nota de prácticas (Pr) para obtener la nota final. La fórmula de acreditación de la unidad es la siguiente: EC + Pr. Para ello es necesario entregar un mínimo de 50% de las PEC y tener una nota mínima para el aprobado (C+ en UOC, 3 en UTEC).

❖ **MODALIDAD y CONTENIDOS**

La unidad se desarrolla alrededor de las siguientes actividades y resultados de aprendizaje:

1) Riesgos, vulnerabilidades y amenazas
- Identificar, examinar y gestionar los principales riesgos de un dominio informático.
- Evaluar los sistemas de prevención y protección de ataques.
- Comprender, configurar, y gestionar herramientas para la administración y protección de redes cableadas e inalámbricas, y la gestión de alertas de seguridad.
- Evaluar los sistemas de prevención y protección de ataques.
- ¿Qué es una nube? ¿Qué tipo de nubes podemos encontrar y como protegerlos?

2) Criptografía
- Comprender el funcionamiento de los sistemas criptográficos, y validar su implantación en diferentes sistemas.
- Conocer las deficiencias de los sistemas criptográficos.

- Principales herramientas y aplicaciones de la criptografía.

3) Ataques
- ¿Cuál es el camino para hacer un *hacking*?
- Mecanismos y herramientas para hacer un reconocimiento del objetivo.
- Identificación de servicios activos.
- Identificar qué tipo de ataques nos podemos encontrar.
- Cómo mantener el acceso y no revelar la intrusión.
- Mecanismos, funcionamiento, ataques y cracking en el *Wireless*.

4) Medidas de ciberdefensa
- Evaluar los sistemas de prevención y protección de ataques.
- Diseñar soluciones integrales apropiadas en escenarios complejos que combinen las técnicas y contramedidas conocidas para la prevención, protección, detección y disuasión de ataques.
- Conocer y saber desplegar las diferentes soluciones de detección de intrusiones.

Un docente de UTEC brindará acompañamiento semanal sincrónico a los estudiantes en formato de clases de apoyo.

Seguridad y pentesting de servidores de datos		
PLAN DE ESTUDIOS	Especialización en Ciberseguridad 2024	
NOMBRE DE LA UNIDAD CURRICULAR	Seguridad y *pentesting* de servidores de datos	
MODALIDAD	Asincrónico y a distancia	
CARÁCTER	Obligatorio	
CRÉDITOS	11	
CARGA HORARIA TOTAL (en horas)	165 horas totales	
DEDICACIÓN (en horas)	TRABAJO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	55 horas	110 horas
❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**		

- **Presentación de la Unidad Curricular:**

  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.

- **Objetivos de aprendizaje**

  Se espera que los estudiantes puedan:

  - 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.

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad sólo puede superarse a partir de la evaluación continua (EC), por medio de las pruebas de evaluación continua (PEC), nota que se combina con una nota de prácticas (Pr) para obtener la nota final. La fórmula de acreditación de la unidad es la siguiente: EC + Pr. Para ello es necesario entregar un mínimo de 50% de las PEC y tener una nota mínima para el aprobado (C+ en UOC, 3 en UTEC).

❖ **MODALIDAD y CONTENIDOS**

La unidad se desarrolla alrededor de las siguientes actividades y resultados de aprendizaje:

1) Ataques a aplicaciones Web
   - *Cross site scripting (XSS)*
   - *Cross site request forgery*
   - *Clickjacking*
   - *LDAP Injection Injection*
   - *Blind LDAP Injection*
   - *XPath*
   - *Path Disclosure*
   - *Remote Hilo Inclusion*
   - *Local Hilo Inclusion*
   - *Webtrojans*

2) Ataques a BBDD, *SQL injection*
   - En torno a explotación del ataque
   - Herramienta Priamos

- El parámetro vulnerable
- ¿Cómo se atacan este tipo de vulnerabilidades?
- Métodos de automatización
- Herramientas
- Protección contra *Blind SQL Injection*
- Time-Based Blind SQL Injection
- Consultas pesants
- *Remote Hilo Downloading*
- Booleanitzación de datos
- Metodología de trabajo
- *Remote Hilo Downloading en Oráculo Database*
- Identificación mediante funciones
- Objetivos principales para cada base de datos
- IDS Evasion

3) Auditoría y desarrollo seguro
   - OWASP
   - Escáner de vulnerabilidades de caja negra
   - Auditoría de código fuente
   - Herramientas de filtraje: Web *Application Firewalls*

Un docente de UTEC brindará acompañamiento semanal sincrónico a los estudiantes en formato de clases de apoyo.

Seguridad y *pentesting* de sistemas		
PLAN DE ESTUDIOS	Especialización en Ciberseguridad - 2024	
NOMBRE DE LA UNIDAD CURRICULAR	Seguridad y *pentesting* de sistemas	
MODALIDAD	Asincrónico y a distancia	
CARÁCTER	Obligatorio	
CRÉDITOS	11	
CARGA HORARIA TOTAL (en horas)	165 horas totales	
DEDICACIÓN (en horas)	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	55 horas	110 horas
❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**		

- **Presentación de la Unidad Curricular:**

  Esta unidad muestra la manera en que se tienen que instalar y configurar los dos sistemas operativos más mayoritarios. 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.

- **Objetivos de aprendizaje**

  Se espera que los estudiantes puedan:

  - Instalar los sistemas operativos *Windows Server* y GNU/Linux y configurarlos de forma segura y robusta.
  - Entender los conceptos de seguridad pasiva y seguridad activa de los sistemas informáticos.
  - Mantener y controlar los sistemas.
  - Integrar diferentes tecnologías y preparar ataques contra los sistemas informáticos para encontrar malas configuraciones.
  - Iniciarse en el uso del *framework Metasploit.*

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad sólo puede superarse a partir de la evaluación continua (EC), por medio de las pruebas de evaluación continua (PEC), nota que se combina con una nota de prácticas (Pr) para obtener la nota final. La fórmula de acreditación de la unidad es la siguiente: EC + Pr. Para ello es necesario entregar un mínimo de 50% de las PEC y tener una nota mínima para el aprobado (C+ en UOC, 3 en UTEC).

❖ **MODALIDAD y CONTENIDOS**

La unidad se desarrolla alrededor de las siguientes actividades y resultados de aprendizaje:

1) Administración de servidores
- Análisis de requerimientos
- Instalación del servidor GNU/Linux
- Instalación del servidor *Windows Server*
- Administración y mantenimiento del servidor GNU/Linux
- Administración y mantenimiento del servidor *Windows Server*

2) Seguridad pasiva
- Elementos redundantes
- Políticas de copias de seguridad
- Sistemas de recuperación en Windows Server
- Planes de contingencia

3) Seguridad activa
- Certificados y sistemas de clave pública y privada
- Certificados en GNU/Linux
- Certificados en *Windows Server*
- IPSEC
- Redes privadas virtuales

- Monitorización de la red
- Herramientas de comprobación

4) Configuración de servicios
   - Servidores de ficheros e impresoras
   - Cortafuegos
   - Servidor de correo
   - Servidor de web y FTP
   - Protección de los puertos

5) Mantenimiento
   - Actualizaciones
   - Monitorización de eventos
   - Automatización de tareas

Un docente de UTEC brindará acompañamiento semanal sincrónico a los estudiantes en formato de clases de apoyo.

Arquitecturas y protocolos de seguridad		
PLAN DE ESTUDIOS	Especialización en Ciberseguridad - 2024	
NOMBRE DE LA UNIDAD CURRICULAR	Arquitecturas y protocolos de seguridad	
MODALIDAD	Asincrónico y a distancia	
CARÁCTER	Obligatorio	
CRÉDITOS	11	
CARGA HORARIA TOTAL (en horas)	165 horas totales	
DEDICACIÓN (en horas)	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	75 horas	90 horas
❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**		

- **Presentación de la Unidad Curricular:**

  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.

- **Objetivos de aprendizaje**

  Se espera que los estudiantes puedan:

  - Comprender el funcionamiento de protocolos básicos de red para securizar sistemas informáticos.
  - Comprender el funcionamiento de protocolos de autenticación y autorización para poder diseñar arquitecturas complejas de control de acceso y sistemas de *Single Sign On*.
  - Comprender los riesgos de seguridad y el funcionamiento de las arquitecturas de microservicios para poder desplegar de forma segura los sistemas estudiados durante el curso en el cloud.

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad sólo puede superarse a partir de la evaluación continua (EC), por medio de las pruebas de evaluación continua (PEC), nota que se combina con una nota de prácticas (Pr) para obtener la nota final. La fórmula de acreditación de la unidad es la siguiente: EC + Pr. Para ello es necesario entregar un mínimo de 50% de las PEC y tener una nota mínima para el aprobado (C+ en UOC, 3 en UTEC).

❖ **MODALIDAD y CONTENIDOS**

La unidad se desarrolla alrededor de las siguientes actividades y resultados de aprendizaje:

1) Introducción a la seguridad en arquitecturas de microservicios basadas en contenedores
   - Virtualización del sistema operativo: *Docker*
   - Seguridad en contenedores

2) Protocolos de autenticación, autorización y control de acceso
   - Técnicas de identificación y autenticación
   - Ciclo de vida de la identidad digital
   - Control de acceso

3) Servicios de directorio
   - Concepto y uso de los directorios
   - Diseño del directorio
   - Implementaciones de servicio de directorio

4) *Single Sign-On* y federación de identidades
   - La federación de identidades
   - Estándares
   - Tecnología para la gestión de identidades

5) Protocolos seguros de red
   - SSH
   - SSL / TLS
   - IPSEC
   - RADIUS
   - EAP (protocolo de autenticación extensible) y 802.1x

Un docente de UTEC brindará acompañamiento semanal sincrónico a los estudiantes en formato de clases de apoyo.

Seguridad en Cloud Computing		
PLAN DE ESTUDIOS	Especialización en Ciberseguridad - 2024	
NOMBRE DE LA UNIDAD CURRICULAR	Seguridad *en cloud computing*	
MODALIDAD	Asincrónico y a distancia	
CARÁCTER	Obligatorio	
CRÉDITOS	11	
CARGA HORARIA TOTAL (en horas)	165 horas totales	
DEDICACIÓN (en horas)	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	55 horas	110 horas
❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**		

- **Presentación de la Unidad Curricular:**

El *Cloud Computing* (o computación a la nube, servicios a la nube, informática en la nube, nube de cómputo o nube de conceptos) 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 (tecnologías de la información y la comunicación) 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.

Las actividades del cibercrimen se desarrollan por organizaciones internacionales que tienen como objetivo perjudicar individuos, empresas y entidades gubernamentales. Por este motivo las organizaciones necesitan tratar la seguridad en el cloud de una manera estructurada. Cuando una organización decide confiar sus datos sensibles, como la información de sus clientes, debe controlar en todo momento:

1. La localización de la información.
2. El proveedor y el modelo de servicio.
3. Los niveles de servicio respecto a la integridad y la disponibilidad de los datos.

- **Objetivos de aprendizaje**
    - Analizar y gestionar los riesgos de seguridad en el *cloud*.
    - Establecer políticas de control de accesos e identidades.
    - Manejar servicios de gestión de claves criptográficas.
    - 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.

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad sólo puede superarse a partir de la evaluación continua (EC). La nota final de evaluación continua se convierte en la nota final de la unidad. La fórmula de acreditación de la asignatura es la siguiente: EC y se debe obtener una nota mínima para el aprobado (C+ en UOC, 3 en UTEC).

❖ **MODALIDAD y CONTENIDOS**

Los contenidos del curso que se trabajarán en esta asignatura son:

1) El *Cloud Computing*: Un nuevo paradigma de servicios

Módulo 1 - Fundamentos y plataformas de *cloud computing*
Módulo 2 - Introducción a la seguridad en *cloud computing*

2) Gestión de riesgos en *Cloud Computing*: Un modelo, por defecto, distribuido

Módulo 3 - Gestión del riesgo en cloud computing
Módulo 4 - Seguridad en entornos IaaS públicos

3) Gobierno de las aplicaciones *Cloud* y modelos DevSecOps

Módulo 5 - Seguridad de aplicaciones en la nube: gestión de la identidad digital
Módulo 6 - Fundamentos de DevSecOps

4) Aspectos legales de *Cloud Computing*: Una visión global

Módulo 7 - Cumplimiento legal

Un docente de UTEC brindará acompañamiento semanal sincrónico a los estudiantes en formato de clases de apoyo.

Taller de Emprendimientos		
PLAN DE ESTUDIOS	Especialización en Ciberseguridad - 2024	
NOMBRE DE LA UNIDAD CURRICULAR	Taller de Emprendimientos	
MODALIDAD	Sincrónico y a distancia	
CARÁCTER	Obligatorio	
CRÉDITOS	3	
CARGA HORARIA TOTAL (en horas)	45 horas totales	
DEDICACIÓN (en horas)	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	32 horas	13 horas
❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**		

- **Presentación de la Unidad Curricular:**

  Este taller proporciona una serie de 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 el estudiante sea capaz de comprender el funcionamiento del proceso de innovación, identificar oportunidades y atraer clientes, segmentar el mercado y generar valor. Además, será capaz de 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.

- **Objetivos de aprendizaje**
  - Conocer el proceso de innovación e identificar oportunidades
  - Poder realizar una segmentación de mercado y una propuesta de valor de un nuevo emprendimiento/innovación
  - Identificar los problemas organizativos y legales asociados con la creación de una empresa

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad se evaluará mediante la participación en las instancias sincrónicas, con una asistencia mínima del 80% de las horas efectivamente dictadas, y un entregable final. La nota final será de Aprobado/No Aprobado.

❖ **MODALIDAD y CONTENIDOS**

El taller se realizará durante 4 días, 8 horas cada día de forma sincrónica. Y se complementa con trabajo autónomo preparatorio para cada instancia además de un entregable final.

La unidad se desarrolla alrededor de las siguientes actividades y resultados de aprendizaje:

1) Personas y proyectos en un contexto global
- *Mindset* emprendedor. Tipologías. Dinámicas de la relación entre socios.
- Propósito personal. Exploración de herramientas como ikigai y círculo dorado.
- Propósito aplicado al proyecto personal.
- Lienzo de negocio actualizado con base al modelo de triple impacto: económico, social y ambiental.
- Personas jurídicas para emprender desde Uruguay. Comparativa. Límites. Acuerdos entre socios para aumentar eficiencias en la operativa. Situación *local-holding.*
- Reconocimiento de actores de apoyo, roles, instrumentos y alcances en Uruguay.
- Ecosistema de apoyo emprendedor regional. Estado y perspectivas.

2) *Human Centered Design y User Research*
- *Double diamond* como marco para guiar soluciones con impacto.
- Definición del problema/objetivo a trabajar.
- Conocimiento de la persona usuaria y su contexto.
- Técnicas básicas del UX *Research* (entrevistas, observación, *user diary*).
- Mapa de *stakeholder* para conocer el universo de personas involucradas.
- Análisis de datos de investigación: creación de *insights,* definición de perfiles de usuarios (*User* Personas) y viaje del usuario (*User Journey*).

3) Relato. *Marketing* y Analítica de comportamiento con datos

- Relatos y contenidos.
- *Marketing* basado en Datos.
- Herramienta de analítica de comportamiento en ambientes online.
- Funnel de conversión.
- *Mailing marketing*. Estado de los Canales en *Social Media.* Uso en campañas. SEM y SEO.
- Ciencia para la gestión de negocios. Metodología de crecimiento basada en experimentos.

4) Lienzo de negocios y próximos pasos

- Avance con el *Business* Canvas con mirada de impactos.
- Indicadores claves de rendimiento.
- Estructura financiera del proyecto. Conceptos claves. Trabajo práctico a partir de las herramientas online autogestionadas Validador Económico Financiero
- Experto® y Termómetro Inversor® creación y propiedad de la Fundación da Vinci.
- Fuentes de financiamiento local y regional. *Investment Readiness.*
- *Mapping* avanzado de *stakeholder.* Identificación de cómo generar valor
- compartido.

Taller de Simulación con Cyber Range		
PLAN DE ESTUDIOS	Especialización en Ciberseguridad - 2024	
NOMBRE DE LA UNIDAD CURRICULAR	Taller de Simulación con *Cyber Range*	
MODALIDAD	Sincrónico y a distancia	
CARÁCTER	Obligatorio	
CRÉDITOS	1	
CARGA HORARIA TOTAL (en horas)	15 horas totales	
DEDICACIÓN (en horas)	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	15 horas	0 horas
❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**		

- **Presentación de la Unidad Curricular:**

  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.

- **Objetivos de aprendizaje**
  - Resolver problemas de simulación reales, habilitando la experimentación, el testeo y la validación de conceptos

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad se evaluará mediante la participación en las instancias sincrónicas, con una asistencia mínima del 80% de las horas efectivamente dictadas. La nota final será de Aprobado/No Aprobado.

❖ **MODALIDAD y CONTENIDOS**

El taller consta de ejercicios de simulación realizados en línea, con la supervisión de un facilitador de AGESIC Se realizarán 6 simulaciones, distribuidas en 5 jornadas.

La unidad se desarrolla alrededor de las siguientes actividades y resultados de aprendizaje:

1) Escenario: *WordPress Blue Bad Plugin*
- Dificultad: Bajo
- Conocimientos previos: *Wordpress, MySQL logs, Network logs, Firewall.*

En este escenario, se piratea un blog corporativo a través de un *plugin* instalado y vulnerable, que está siendo utilizado como pilar para filtrar al exterior datos sensibles de pago de una base de datos que es parte de la red interna. Los estudiantes tratarán de rastrear el origen del ataque al investigar los registros del firewall a la base de datos, identificar el *plugin* vulnerable como el vector del ataque, detectar qué clase de información se filtró, remediar la vulnerabilidad y mitigar el ataque.

2) Escenario: *SQL Injection*
- Dificultad: Medio
- Conocimientos previos: *MS-SQL Server, IIS Server logs, Firewall,* SIEM.

En este escenario, un atacante se dirige directamente a la organización. Una serie de fallas de seguridad en la implementación del ambiente le permite al atacante utilizar servicios accesibles desde el exterior a fin de lograr el acceso a los sistemas internos, extraer información privilegiada e interferir con los procesos comerciales.
Con este ataque los estudiantes comprueban cómo un atacante con experiencia puede usar varias configuraciones erradas “sencillas” y encadenarlas para lograr un impacto crítico sobre el negocio.

3) Escenario: *Web Defacement*
- Dificultad: Medio
- Conocimientos previos: Linux *logs management*, Apache, *Firewall*, SIEM.

Este escenario demuestra uno de los ataques más frecuentes al web cuyo objetivo no es dañar activos o robar información sino dañar principalmente la reputación de la organización

o enviar un mensaje psicológico. El atacante infiltra el servidor web en internet de la organización y lo mutila para mostrar su mensaje.
Ejemplos recientes incluyen los ataques de Anonymous a los sitios web de los gobiernos de Brasil y Singapur.

4) Escenario: Apache *Shutdown*
- Dificultad: Medio
- Conocimientos previos: Linux *logs management*, Apache, *Firewall,* SIEM.

Este escenario simula un ataque sobre los servicios de la organización de acceso público. El ataque interrumpe la operación del servicio y utiliza métodos básicos para fortalecer la presencia del atacante en el sistema. En este escenario, los estudiantes se enfrentan a la interrupción de componentes críticos del negocio y necesitan actuar con rapidez para mantener todo el tiempo de actividad que sea posible y mitigar el ataque. También son testigos de niveles básicos de otras partes de la cadena de ataque como la persistencia y la gestión.

5) Escenario: *Trojan Data Leak*
- Dificultad: Alta
- Conocimientos previos: Linux *logs management*, Apache, HTML / Java, SIEM, Linux *Forensics.*

Spear-phishing, una de las maneras más conocidas y utilizadas de infiltración de una organización aprovecha la debilidad del factor humano a través de la ingeniería social. Los estudiantes sufren de primera mano toda la cadena de eventos del ataque de una *spearphishing* exitosa que incluye la intrusión y la filtración al exterior de información sensible.

6) Escenario: *DB Dump via FTP Exploit*
- Dificultad: Alta
- Conocimientos previos: *Linux logs management, FTP server, MSSQL Server, Firewall, SIEM.*

Este escenario demuestra a un atacante sofisticado que usa métodos múltiples para pivotear dentro del sistema. El atacante sortea múltiples mecanismos de seguridad que le permiten llegar a segmentos de la red que, de otro modo, jamás habría podido alcanzar. El vector de entrada es una laptop conectada al segmento de usuarios, emulando un empleado canalla, una estación de trabajo infectada o un “visitante” que logra acceso a un puerto en la pared dentro de las instalaciones de la compañía.

Taller de Normativa en Ciberseguridad	
PLAN DE ESTUDIOS	Especialización en Ciberseguridad - 2024
NOMBRE DE LA UNIDAD CURRICULAR	Taller de Normativa en Ciberseguridad
MODALIDAD	Sincrónico y a distancia
CARÁCTER	Obligatorio
CRÉDITOS	1

CARGA HORARIA TOTAL (en horas)	15 horas totales	
DEDICACIÓN (en horas)	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	13 horas	2 horas

❖ **DESCRIPCIÓN DE LA UNIDAD CURRICULAR**

- **Presentación de la Unidad Curricular:**

  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.

- **Objetivos de aprendizaje**
  - Comprender las leyes y regulaciones específicas relacionadas con la seguridad cibernética
  - Analizar cómo la normativa vigente influye en la implementación de medidas de seguridad, el manejo de incidentes y la protección de datos sensibles

❖ **CRITERIOS DE EVALUACIÓN**

Esta unidad se evaluará mediante la participación en las instancias sincrónicas, con una asistencia mínima del 80% de las horas efectivamente dictadas. La nota final será de Aprobado/No Aprobado.

❖ **MODALIDAD y CONTENIDOS**

El taller se realizará durante 3 días, de forma sincrónica, con expertos de AGESIC, Y se complementa con trabajo autónomo preparatorio para cada instancia.

La unidad se desarrolla alrededor de las siguientes actividades y resultados de aprendizaje:

1) Descripción del ecosistema de ciberseguridad
   - Marco normativo: leyes y decretos

2) Aspectos técnicos de implementación
   - Identidad digital y firma electrónica

3) Protección de Datos Personales
   - Marco normativo y seguridad desde el diseño