

---

**UNIVERSIDAD TECNOLÓGICA  
CONSEJO DIRECTIVO CENTRAL PROVISORIO**

---

RESOLUCIÓN N°	
---------------	--

576	/24
-----	-----

**Referencia: Ajuste del Plan de Estudios de la  
ESPECIALIZACIÓN EN CIBERSEGURIDAD**

Montevideo, 26 de noviembre de 2024.

**VISTO:** La propuesta elevada por la Dirección de Educación para la aprobación de un ajuste en el Plan de Estudios de la Especialización en Ciberseguridad, Plan 2024.

**RESULTANDO:**

- I. que actualmente se está impartiendo el Plan de Estudios 2023 de la Especialización en Ciberseguridad el cual se enmarca en el Programa Uruguay Global en conjunto con la Universitat Oberta de Catalunya (UOC) y que se seguirá impartiendo para la cohorte 2023;
- II. que es necesario actualizar el Plan de Estudios 2023 motivado por ajustes realizados desde la UOC en el “Posgrado de Ciberseguridad en Redes y Sistemas” sobre el cual se articula la Especialización en Ciberseguridad, aprobando el Plan 2024 por Resolución de este Consejo N° 256/24.
- III. que desde la Dirección de Uruguay Global se ha resuelto mantener los contenidos de la especialización que hasta el momento estaban asociados a la participación de AGESIC, incorporando alianzas con el Departamento de Innovación y Emprendimientos de UTEC y docentes invitados bajo la responsabilidad del equipo de la Especialización.
- IV. que el Área de Diseño y Desarrollo Curricular y la Asesoría Jurídica de la Dirección de Educación informan favorablemente sobre la propuesta de ajuste y se confirma que reglamentariamente se adecua a la Ordenanza de Educación Continua vigente.

**CONSIDERANDO:**

- I. El Convenio Marco firmado entre UTEC y la UOC el 25 de enero de 2023, así como el Convenio Específico de setiembre del mismo año.
- II. La Ordenanza de Posgrados vigente, aprobada por Resolución N° 384/23 del 17 de julio de 2023.
- III. El primer Plan de Estudios 2023 de la Especialización en Ciberseguridad, aprobado por este Consejo por Resolución N° 387/23.

IV. El Plan de Estudios vigente 2024 de la Especialización en Ciberseguridad, aprobado por este Consejo por Resolución N° 256/24.

**ATENTO:** a lo precedentemente expuesto y a la atribución conferida por el artículo 16, literal F) de la Ley 19.043.

**EL CONSEJO DIRECTIVO CENTRAL PROVISORIO DE LA UNIVERSIDAD  
TECNOLÓGICA RESUELVE:**

**1º.** Aprobar el ajuste del Plan de Estudios de la Especialización en Ciberseguridad a impartirse a partir de la cohorte 2024, el que se adjunta a la presente Resolución y la integra.

**2º.** Aprobar la expedición del Título de Especialista en Ciberseguridad a quienes cumplan con los requisitos establecidos, anexando la descripción de «en colaboración con la UOC», en cumplimiento del Convenio Específico.

**3º.** Comuníquese y publíquese a todos los efectos.

DocuSigned by:  
  
3616680A4368455...  
**Andrés D. Gil**  
Consejero  
Universidad Tecnológica

DocuSigned by:  
  
B12B3FE1158A46B...  
**Graciela Do Mato**  
Consejera  
Universidad Tecnológica

Signed by:  
  
5D779240B0CB4EE...  
**Rodolfo Silveira**  
Consejero  
Universidad Tecnológica

**Universidad Tecnológica del Uruguay (UTEC)**

**Universitat Oberta de Catalunya (UOC)**

**Especialización en Ciberseguridad**

**PLAN de ESTUDIOS**

**2024**

## Índice

I – DENOMINACIÓN, JUSTIFICACIÓN Y OBJETIVOS .....	5
1.1. Denominación: .....	5
1.2. Justificación:.....	5
1.3. Objetivos de la especialización en ciberseguridad: .....	6
1.3.1- Objetivo general.....	6
1.3.2- Objetivos específicos.....	6
II – PERFIL DE EGRESO .....	7
III – REQUISITOS DE INGRESO, DURACIÓN, REQUISITOS DE EGRESO .....	8
3.1. Requisitos de Ingreso:.....	9
3.2. Duración de la Especialización en Ciberseguridad: .....	9
3.3. Requisitos de Egreso para obtención del título: .....	9
IV – PLAN CURRICULAR .....	10
4.1. Créditos, organización y modalidad de cursado:.....	10
4.2. Metodología: .....	11
4.3- Sistema de calificaciones y evaluación final: .....	13
V - NÚMERO DE CUPOS Y COSTO.....	13
ANEXO .....	14

## **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)<sup>2</sup>, 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 los 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 UTEC, 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.

En el caso de títulos de grado emitidos en el extranjero, Se requiere apostilla del título a presentar de forma obligatoria que incorpore código de verificación electrónica. Fecha límite de entrega del apostillado: 31 de diciembre de 2024.

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. Para ello deben cumplir con los requisitos de conocimientos y experiencia profesional comprobable de al menos 2 años en el ámbito TIC, con carta de certificación de la empresa donde se desarrollaron las tareas.

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**<sup>1</sup> (900 horas) organizados en:

- 55 créditos de cursos virtuales
- 2 créditos de Taller de *Cyber Range* 1 crédito de Taller de Normativa Legal, 2 créditos de Taller de Emprendimientos

---

<sup>1</sup> De acuerdo con la Res. 384/23 – Ordenanza de Posgrados - UTEC

UNIDADES CURRICULARES	HORAS SINCRÓNICAS /ASINCRÓNICAS	HORAS AUTÓNOMAS	HORAS CRONOLÓGICAS TOTALES	Créditos
Fundamentos de ciberseguridad	85	80	165	11
Seguridad y <i>pentesting</i> de servidores de datos	55	110	165	11
Seguridad y <i>pentesting</i> de sistemas	55	110	165	11
Arquitecturas y protocolos de seguridad	75	90	165	11
Seguridad <i>en cloud computing</i>	55	110	165	11
Taller <i>Cyber Range</i>	15	15	30	2
Taller Normativa Legal	13	2	15	1
Taller Emprendimientos	23	7	30	2
<b>Subtotal</b>	<b>376</b>	<b>524</b>	<b>900</b>	<b>60</b>

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:

<b>Planificación</b>	Espacio de acceso al plan docente o guía de aprendizaje así como al calendario semestral donde se encuentra la temporalización prevista de las actividades.
<b>Comunicación (docencia)</b>	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.
<b>Recursos</b>	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.
<b>Evaluación</b>	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.

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

- **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 cómo protegerlas?

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**



<b>PLAN DE ESTUDIOS</b>	Especialización en Ciberseguridad 2024	
<b>NOMBRE DE LA UNIDAD CURRICULAR</b>	Seguridad y <i>pentesting</i> de servidores de datos	
<b>MODALIDAD</b>	Asincrónico y a distancia	
<b>CARÁCTER</b>	Obligatorio	
<b>CRÉDITOS</b>	11	
<b>CARGA HORARIA TOTAL (en horas)</b>	165 horas totales	
<b>DEDICACIÓN (en horas)</b>	TRABAJO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	55 horas	110 horas
<b>❖ DESCRIPCIÓN DE LA UNIDAD CURRICULAR</b>		
<ul style="list-style-type: none"> <li>● <b>Presentación de la Unidad Curricular:</b> <p>En esta unidad se verán ejemplos de algunos de los métodos más habituales para atacar formularios de aplicativos <i>web</i> que interactúan con alguna base de datos. Se harán ataques a las Bases de datos, así como a los aplicativos que hacen las consultas.</p> <p>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.</p> </li> <li>● <b>Objetivos de aprendizaje</b> <p>Se espera que los estudiantes puedan:</p> <ul style="list-style-type: none"> <li>○ Conocer las herramientas y los métodos de <i>pentesting</i> en los servidores de datos.</li> <li>○ Fortalecer los diferentes tipos de bases de datos, para asegurar la integridad, la disponibilidad y la confidencialidad de la información almacenada.</li> </ul> </li> </ul>		
<b>❖ CRITERIOS DE EVALUACIÓN</b>		

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*
- Booleanización 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.

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

- **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

<ul style="list-style-type: none"> <li>● Elementos redundantes</li> <li>● Políticas de copias de seguridad</li> <li>● Sistemas de recuperación en Windows Server</li> <li>● Planes de contingencia</li> </ul> <p>3) Seguridad activa</p> <ul style="list-style-type: none"> <li>● Certificados y sistemas de clave pública y privada</li> <li>● Certificados en GNU/Linux</li> <li>● Certificados en <i>Windows Server</i></li> <li>● IPSEC</li> <li>● Redes privadas virtuales</li> <li>● Monitorización de la red</li> <li>● Herramientas de comprobación</li> </ul> <p>4) Configuración de servicios</p> <ul style="list-style-type: none"> <li>● Servidores de ficheros e impresoras</li> <li>● Cortafuegos</li> <li>● Servidor de correo</li> <li>● Servidor de web y FTP</li> <li>● Protección de los puertos</li> </ul> <p>5) Mantenimiento</p> <ul style="list-style-type: none"> <li>● Actualizaciones</li> <li>● Monitorización de eventos</li> <li>● Automatización de tareas</li> </ul> <p>Un docente de UTEC brindará acompañamiento semanal sincrónico a los estudiantes en formato de clases de apoyo.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Arquitecturas y protocolos de seguridad</b>	
<b>PLAN DE ESTUDIOS</b>	Especialización en Ciberseguridad - 2024
<b>NOMBRE DE LA UNIDAD CURRICULAR</b>	Arquitecturas y protocolos de seguridad
<b>MODALIDAD</b>	Asincrónico y a distancia
<b>CARÁCTER</b>	Obligatorio
<b>CRÉDITOS</b>	11

<b>CARGA HORARIA TOTAL (en horas)</b>	165 horas totales	
<b>DEDICACIÓN (en horas)</b>	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	75 horas	90 horas
<b>❖ DESCRIPCIÓN DE LA UNIDAD CURRICULAR</b>		
<ul style="list-style-type: none"> <li>● <b>Presentación de la Unidad Curricular:</b> <p>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.</p> <p>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 <i>Single Sign On</i>. 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.</p> </li> <li>● <b>Objetivos de aprendizaje</b> <p>Se espera que los estudiantes puedan:</p> <ul style="list-style-type: none"> <li>○ Comprender el funcionamiento de protocolos básicos de red para securizar sistemas informáticos.</li> <li>○ Comprender el funcionamiento de protocolos de autenticación y autorización para poder diseñar arquitecturas complejas de control de acceso y sistemas de <i>Single Sign On</i>.</li> <li>○ 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.</li> </ul> </li> </ul>		
<b>❖ CRITERIOS DE EVALUACIÓN</b>		
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.

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



- **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.

<b>❖ CRITERIOS DE EVALUACIÓN</b>	
<p>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).</p>	
<b>❖ MODALIDAD y CONTENIDOS</b>	
<p>Los contenidos del curso que se trabajarán en esta asignatura son:</p> <p>1) El <i>Cloud Computing</i>: Un nuevo paradigma de servicios</p> <p>Módulo 1 - Fundamentos y plataformas de <i>cloud computing</i>  Módulo 2 - Introducción a la seguridad en <i>cloud computing</i></p> <p>2) Gestión de riesgos en <i>Cloud Computing</i>: Un modelo, por defecto, distribuido</p> <p>Módulo 3 - Gestión del riesgo en cloud computing  Módulo 4 - Seguridad en entornos IaaS públicos</p> <p>3) Gobierno de las aplicaciones <i>Cloud</i> y modelos DevSecOps</p> <p>Módulo 5 - Seguridad de aplicaciones en la nube: gestión de la identidad digital  Módulo 6 - Fundamentos de DevSecOps</p> <p>4) Aspectos legales de <i>Cloud Computing</i>: Una visión global</p> <p>Módulo 7 - Cumplimiento legal</p> <p>Un docente de UTEC brindará acompañamiento semanal sincrónico a los estudiantes en formato de clases de apoyo.</p>	

<b>Taller de Emprendimientos</b>	
<b>PLAN DE ESTUDIOS</b>	Especialización en Ciberseguridad - 2024
<b>NOMBRE DE LA UNIDAD CURRICULAR</b>	Taller de Emprendimientos

<b>MODALIDAD</b>	Sincrónico, asincrónico y a distancia	
<b>CARÁCTER</b>	Obligatorio	
<b>CRÉDITOS</b>	2	
<b>CARGA HORARIA TOTAL (en horas)</b>	30 horas totales	
<b>DEDICACIÓN (en horas)</b>	TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO	TRABAJO AUTÓNOMO
	23 horas	7 horas
<b>❖ DESCRIPCIÓN DE LA UNIDAD CURRICULAR</b>		
<ul style="list-style-type: none"> <li>● <b>Presentación de la Unidad Curricular:</b> <p>Esta unidad se compone de dos cursos/talleres ofrecidos por el área de UTEC Innova, denominados “Actitud Emprendedora” y “Generación de Ideas de Negocio”.</p> <p>Con ambos cursos/talleres, se busca abordar conceptos claves para el desarrollo de una actitud emprendedora con el objetivo de que el participante internalice aptitudes, operaciones y comportamientos estratégicos personales necesarios, que le faciliten un buen desempeño en el mundo emprendedor; así como brindar herramientas para la generación e identificación de oportunidades de negocios, a través de una metodología basada en actividades y dinámicas participativas.</p> </li> <li>● <b>Objetivos de aprendizaje</b> <ul style="list-style-type: none"> <li>○ Lograr que el participante se empodere con sus fortalezas emprendedoras.</li> <li>○ Potenciar al emprendedor para que pueda identificar un punto de partida personal con relación a su actitud emprendedora.</li> <li>○ Identificar ideas de negocios, evaluar si las ideas identificadas son oportunidades y diseñar un modelo de negocio inicial.</li> </ul> </li> </ul>		
<b>❖ CRITERIOS DE EVALUACIÓN</b>		
<p>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.</p>		

<b>❖ MODALIDAD y CONTENIDOS</b>
<p>El curso/taller “Actitud Emprendedora” se realiza de forma asincrónica, virtual, y se divide en 4 módulos secuenciales: Autoconocimiento Emprendedor, Las competencias del Siglo XXI, La cuestión del riesgo, del éxito y la tolerancia al fracaso, El propósito.</p> <p>El curso/taller “Generación de Ideas de Negocio” se realiza de forma sincrónica, asincrónica y autónoma, todo virtual. Las instancias sincrónicas se realizan durante 2 días, 4 horas cada día. Y se complementa con horas asincrónicas y trabajo autónomo para un entregable final. Al completarlo los estudiantes podrán identificar ideas de negocios, evaluar si las ideas identificadas son oportunidades y validar las necesidades de sus potenciales clientes. Se desarrolla con una modalidad que apunta al “aprender haciendo” como estrategia para el desarrollo de los conocimientos, habilidades y actitudes en los participantes, que favorecen la generación de ideas para la concepción de emprendimientos exitosos.</p>

<b>Taller de Simulación con Cyber Range</b>		
<b>PLAN DE ESTUDIOS</b>	Especialización en Ciberseguridad - 2024	
<b>NOMBRE DE LA UNIDAD CURRICULAR</b>	Taller de Simulación con <i>Cyber Range</i>	
<b>MODALIDAD</b>	Sincrónico, autónomo y a distancia	
<b>CARÁCTER</b>	Obligatorio	
<b>CRÉDITOS</b>	2	
<b>CARGA HORARIA TOTAL (en horas)</b>	30 horas totales	
<b>DEDICACIÓN (en horas)</b>	<b>TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO</b>	<b>TRABAJO AUTÓNOMO</b>
	15 horas	15 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 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, y un entregable final La nota final será de Aprobado/No Aprobado.

## ❖ MODALIDAD y CONTENIDOS

El taller consta de ejercicios de simulación realizados de forma sincrónica, presencial, Se realizarán 6 simulaciones, distribuidas en 2 jornadas, y se deberá realizar un entregable final que de cuenta del proceso de resolución de las simulaciones.

Las actividades de entrenamiento en ciberseguridad están diseñadas para proporcionar un entorno seguro, realista y controlado donde los estudiantes pueden aprender, practicar y perfeccionar sus habilidades frente a amenazas cibernéticas reales.

Se simulan entornos de TI, replicando casos reales, donde pueden estar incluidos servidores, endpoints, dispositivos de red y aplicaciones. Los participantes son expuestos a diversos tipos de amenazas, emulando técnicas avanzadas de intrusión. Las actividades ofrecen escenarios prácticos para seguridad defensiva, intrusiva y ejercicios colaborativos, facilitando un aprendizaje integral.

--

<b>Taller de Normativa en Ciberseguridad</b>		
<b>PLAN DE ESTUDIOS</b>	Especialización en Ciberseguridad - 2024	
<b>NOMBRE DE LA UNIDAD CURRICULAR</b>	Taller de Normativa en Ciberseguridad	
<b>MODALIDAD</b>	Sincrónico y a distancia	
<b>CARÁCTER</b>	Obligatorio	
<b>CRÉDITOS</b>	1	
<b>CARGA HORARIA TOTAL (en horas)</b>	15 horas totales	
<b>DEDICACIÓN (en horas)</b>	<b>TRABAJO SUPERVISADO SINCRÓNICO/ASINCRÓNICO</b>	<b>TRABAJO AUTÓNOMO</b>
	13 horas	2 horas
<b>❖ DESCRIPCIÓN DE LA UNIDAD CURRICULAR</b>		
<ul style="list-style-type: none"> <li>● <b>Presentación de la Unidad Curricular:</b> <p style="margin-left: 40px;">Este taller 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.</p> </li> <li>● <b>Objetivos de aprendizaje</b> <ul style="list-style-type: none"> <li>○ Comprender las leyes y regulaciones específicas relacionadas con la seguridad cibernética</li> </ul> </li> </ul>		

- 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, 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