CS - 305 / 2025

HURLINGHAM, 10/12/2025

VISTO el Estatuto, la RCS. N° 101/25 que establece la estructura orgánico- funcional de la Universidad Nacional de Hurlingham, la RCD N° 051/25 y el Expediente N° 1010/25 del registro de esta Universidad, donde se tramitan las actuaciones referidas a la creación del Plan de Estudios de la carrera denominada Licenciatura en Ciberseguridad con título intermedio de Técnico/a Universitario/a en Redes y operaciones informáticas; y

CONSIDERANDO:

Que corresponde al Consejo Superior aprobar los planes de estudio de acuerdo al artículo Nro. 58 inciso l) del Estatuto de la UNIVERSIDAD NACIONAL de HURLINGHAM.

Que según la RCS. N° 101/25 es un objetivo general del Instituto de Tecnología e Ingeniería Orientar

la formación de los estudiantes, mediante las funciones de docencia, investigación, extensión y gestión, para que sean capaces de ejercer un rol profesional activo en el desarrollo económico sustentable y el progreso social y cultural de la sociedad, desde una perspectiva que integre la competencia profesional con el humanismo y la solidaridad social y con conciencia de las necesidades y particularidades locales y nacionales.

Que según el art. 78 inc. c) del Estatuto de esta Universidad, es una función del Consejo Directivo del Instituto elevar al Rector, para su presentación al Consejo Superior, los planes de estudio que se desarrollen en su ámbito de incumbencia y sus posibles modificaciones.

Que la Resolución Ministerio de Educación N° 2598/23, y su modificatoria a través de la Resolución del Ministerio de Capital Humano N° 556/25, establece el Sistema Argentino de Créditos Académicos Universitarios (SACAU), el cual fija al Crédito de Referencia del/la estudiante (CRE) como el valor

organizador del diseño y rediseño de los planes de estudio.

Que a través de la RCS N° 351/24 se aprueba el Reglamento del Sistema Argentino de Créditos Académicos Universitarios (SACAU) de la Universidad Nacional de Hurlingham.

Que el desarrollo industrial nacional necesita dotarse de recursos humanos altamente especializados que cubran los aspectos integrales del sector productivo, desde el conocimiento tecnológico específico hasta el inherente al planeamiento y gestión, considerando los aspectos de seguridad, éticos, sociales y ambientales, como la capacidad de generación de políticas públicas para el área.

Que particularmente en el ámbito de la seguridad informática y de su importancia en el desarrollo de software, hay una amplia variedad de empresas con distintas características y tamaños que trabajan tanto en el mercado local como en el internacional. Se trata de una

disciplina presente en todo tipo de actividad productiva, con impactos en asuntos que van desde la intimidad y la vida cotidiana de las personas hasta en materia de soberanía y seguridad nacional.

Que en este contexto que la Universidad Nacional de Hurlingham se propone aportar al tejido productivo local y al sector de las TICs nacional, recursos humanos en los que se destaque la capacidad de proveer servicios de alta calidad. En tiempos donde es cada vez más importante garantizar la integridad y privacidad de la información, tanto personal o comercial como en materia forense, defensa, u otras cuestiones de Estado, resulta fundamental contar con profesionales expertos en ciberseguridad.

Que la carrera aborda contenidos y habilidades de seguridad informática, a partir de una sólida base de administración de redes, sistemas de comunicación, operaciones y desarrollo de software seguro.

CS - 305 / 2025

Que se propicia un diseño curricular flexible, con la incorporación de créditos para validar actividades de participación de las/los estudiantes en diferentes ámbitos profesionales, sociales y de la vida universitaria, y amalgamando de forma integral el paso del Curso de Preparación Universitaria a la cursada específica del primer cuatrimestre.

Que a través del expediente N° 1010/25, el Instituto de Tecnología e Ingeniería tramita la propuesta de creación de la carrera Licenciatura en Ciberseguridad con título intermedio de Técnico/a Universitario/a en Redes y operaciones informáticas.

Que mediante la Resolución Nro. 051/25 el Consejo Directivo del Instituto de Tecnología e Ingeniería elevó al Rector la propuesta de creación de la carrera Licenciatura en Ciberseguridad con título intermedio de Técnico/a Universitario/a en Redes y operaciones informáticas.

CS - 305 / 2025

Que según el Estatuto de esta Universidad, es una función del Consejo Directivo del Instituto elevar al Rector, para su tratamiento en Consejo Superior, los planes de estudio.

Que analizando el mismo, el Rector lo remite para su tratamiento por la comisión de Enseñanza atento a lo establecido en el artículo Nro. 30 del Reglamento Interno del Consejo Superior.

Que reunidas las comisiones permanentes en sesión conjunta, emiten dictamen favorable.

Que en virtud del Artículo 55 del Estatuto de la Universidad, el Rector integrará el Consejo Superior de la Universidad.

Que la presente medida se dicta en uso de las atribuciones conferidas por el Estatuto de la UNIVERSIDAD NACIONAL de HURLINGHAM, el Reglamento Interno del Consejo Superior y luego de haberse resuelto en reunión del día 10 de diciembre de 2025 de este Consejo Superior.

CS - 305 / 2025

Por ello,

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD NACIONAL DE HURLINGHAM

RESUELVE:

ARTÍCULO 1°- Aprobar la creación de la carrera denominada Licenciatura en Ciberseguridad con título intermedio de Técnico/a Universitario/a en Redes y operaciones informáticas, junto con su plan de estudio correspondiente, conforme a lo detallado en el Anexo Único de la presente propuesta

ARTÍCULO 2°- Regístrese, comuníquese y archívese.

UNIVERSIDAD NACIONAL DE HURLINGHAM

(Ley N° 27.016, sancionada el 19 de noviembre de 2014 y promulgada el 2 de diciembre de 2014)

Plan de Estudios:

Año: **2026**

UNIVERSIDAD NACIONAL DE HURLINGHAM

Instituto de Tecnología e Ingeniería

Universidad Nacional de Hurlingham
Licenciatura en Ciberseguridad

1. Presentación

1.1. Denominación de la carrera:

Licenciatura en Ciberseguridad

1.2. Títulos que otorga:

Intermedio: *Técnico/a Universitario/a en Redes y Operaciones Informáticas*

Final: *Licenciado/a en Ciberseguridad*

1.3. Cantidad de horas de interacción pedagógica totales:

Titulación intermedia: 1.120 horas

Titulación Final: 2.240 horas

1.4. Cantidad de horas y créditos totales:

Titulación intermedia: 3.000 horas - 120 créditos

Titulación Final: 6.000 horas - 240 créditos

1.5. Modalidad de cursado:

Presencial

1.6. Institucionalidad de la carrera:

Instituto de Tecnología e Ingeniería

2. Fundamentación de la carrera

La UNAHUR es una universidad pública y gratuita que estructura su desarrollo académico y científico en base a cuatro ejes de estudio e investigación: salud, educación, tecnología e ingeniería y biotecnología. Tiene como misión contribuir a través de la producción y distribución equitativa de conocimientos e innovaciones científico-tecnológicas al desarrollo local y nacional, con un fuerte compromiso con la formación de excelencia y la inclusión al servicio del acceso, permanencia y promoción de sus estudiantes.

Esta misión, atenta a las demandas sociales y al desarrollo de la región, la calidad de vida y los valores democráticos, que valoriza los saberes de las comunidades locales, delinea un modelo de institución que refuerza el compromiso de la universidad para con su medio y, con ello, no subordina su labor a tareas solamente científico-tecnológicas sino que se asume como espacio de articulación entre el territorio y la institución universitaria que le pertenece.

La Universidad Nacional de Hurlingham se propone ofrecer una propuesta académica que permita atender las diferentes áreas vocacionales de sus potenciales estudiantes, sin perder de vista las necesidades locales de profesionales cualificados, a fin de asegurar tanto el desarrollo humano de su propia comunidad universitaria como de la local en su conjunto.

Desde la docencia se apunta a brindar educación superior de calidad, formando profesionales de alto nivel, actualizados y en constante búsqueda de conocimientos, con un alto sentido ético-social.

Por otra parte, la investigación se nutrirá de las problemáticas docentes que se releven, así como de los núcleos de interés del estudiantado. El desarrollo industrial nacional necesita dotarse de recursos humanos altamente especializados que cubran los aspectos integrales del sector productivo, desde el conocimiento tecnológico específico hasta el inherente al planeamiento y gestión, considerando los aspectos de seguridad, éticos, sociales y ambientales, como la capacidad de generación de políticas públicas para el área.

El Instituto de Tecnología e Ingeniería de la Universidad Nacional de Hurlingham será el responsable de la transferencia de conocimiento necesaria para cubrir las vacancias del sector público y privado, y el escenario natural donde discutir la planificación estratégica de desarrollo tecnológico, incluyendo docencia, investigación y extensión.

El aumento sostenido que se espera en la demanda nacional y global de servicios asociados a las tecnologías de la información y las comunicaciones (TICs), necesita dotarse de recursos humanos altamente especializados que cubran los aspectos integrales del sector productivo en estas áreas. El país cuenta con varios de los factores necesarios para aprovechar este potencial. Particularmente en el ámbito de

la seguridad informática y su importancia en el desarrollo de software donde hay una amplia variedad de empresas con distintas características y tamaños que trabajan tanto en el mercado local como en el internacional. Se trata de una disciplina presente en todo tipo de actividad productiva, con impactos en asuntos que van desde la intimidad y la vida cotidiana de las personas hasta en materia de soberanía y seguridad nacional.

Es en este contexto que la Universidad Nacional de Hurlingham se propone aportar al tejido productivo local y al sector de las TICs nacional, recursos humanos en los que se destaque la capacidad de proveer servicios de alta calidad. En tiempos donde es cada vez más importante garantizar la integridad y privacidad de la información, tanto personal o comercial como en materia forense, defensa, u otras cuestiones de Estado, resulta fundamental contar con profesionales expertos en ciberseguridad. La singularidad de la carrera es que llega a abordar contenidos y habilidades de seguridad informática, a partir de una sólida base de administración de redes, sistemas de comunicación, operaciones y desarrollo de software seguro.

Esta propuesta de cuatro años de duración se centra en formar Licenciados/as en Ciberseguridad. Además, otorga el título intermedio de Técnico/a Universitario/a en Redes y operaciones informáticas, que se obtiene a los dos años de cursada.

3. Objetivos de la carrera

Los objetivos de la carrera son:

- Formar profesionales con habilidades prácticas para planificar, gestionar y dirigir la implementación de planes de ciberseguridad; así como disponer de conocimiento teórico, capaces de analizar problemáticas e intervenir en situaciones concretas con herramientas y tecnologías apropiadas.
- Contribuir a la mejora de los sistemas de seguridad informática de instituciones públicas y privadas de la comunidad.
- Contribuir a la mejora de los sistemas de seguridad informática de entidades públicas y privadas de la comunidad.
- Brindar una formación comprometida con los valores éticos y democráticos de participación, libertad, solidaridad, resolución pacífica de conflictos, respeto a los derechos humanos, responsabilidad, honestidad, valoración y preservación del patrimonio natural y cultural.
- Ofrecer un sólido marco ético y legal de deontología profesional que regule el accionar en un campo de alto impacto social y con acceso a información sensible.
- Generar núcleos de investigación que promuevan la creación de conocimiento y la innovación científico-tecnológica en el ámbito de la disciplina.

- Aportar elementos técnicos a la reflexión social sobre el acceso a la información pública, la privacidad de datos personales, la confiabilidad e integridad de la información en soportes digitales, y otros aspectos de la vida cotidiana donde influyen los criterios y políticas de seguridad informática.

4. Perfil del egresado/a

4.1 Perfil del Técnico/a Universitario/a en Redes y Operaciones Informáticas

Un/a técnico/a universitario/a en redes y operaciones informáticas tiene como área de acción principal atender problemáticas de redes y operaciones ya sea para instalaciones de infraestructuras específicas o para dar soporte a equipos que desarrollan software o gestionan soluciones informáticas que integran tecnologías de información y comunicación.

El recorrido de la carrera abarca conceptos, herramientas, prácticas y resolución de problemas para que los/las estudiantes dispongan de conocimientos y experiencia al momento de insertarse laboralmente.

De acuerdo al perfil propuesto, el técnico/a deberá:

- Tener una base conceptual sólida que le permita participar en organismos, empresas, instituciones, como parte de los equipos de Gestión Informática, tanto respecto a tareas de comunicaciones como de gestión de ambientes para ejecutar aplicaciones y sistemas.
- Contar con las capacidades y competencias que le permitan adaptarse a las nuevas herramientas que van apareciendo en el ámbito laboral.
- Comprender adecuadamente la pertinencia de realizar las tareas bajo diferentes parámetros de calidad, entre los que destacamos: claridad, mantenimiento, robustez frente a fallos, uso eficiente de recursos y de la energía; también manejar los principales conceptos y herramientas requeridos para que sus productos cuenten con grados adecuados de calidad.
- Comprender la conveniencia de valorar y tener en cuenta los conceptos de estándares abiertos y software libre en los entornos operativos que se utilizan.

4.2 Perfil del Licenciado/a en Seguridad Informática

El licenciado/a en Ciberseguridad de la Universidad Nacional de Hurlingham está enfocado en dar respuestas a necesidades de la sociedad, empresas y organismos a través de procesos de puesta en funcionamiento de herramientas informáticas relacionadas la ciberseguridad ya sea desde la construcción de éstas, como así también desde la adaptación de soluciones existentes. Posee una formación ética profesional, y una estrecha relación con el sector productivo con capacidad de

desarrollo de proyectos propios. Combina el dominio técnico profundo con la capacidad de gestión, liderazgo y visión de negocio. Está preparado para intervenir en el ámbito público, privado y académico.

- Está capacitado para diseñar, planificar y liderar la estrategia de ciberseguridad de una organización.
- Tiene la capacidad de resolver problemas y liderar proyectos técnicos de ciberseguridad como líder de equipo o como consultor.
- Dispone de saberes que le permiten intervenir en el aspecto de seguridad del desarrollo de sistemas de información de distinta índole.
- Posee conocimiento para promover la construcción de software de acuerdo a normas y estándares de seguridad en los entornos operativos.
- Adquiere capacidades para integrarse en equipos multidisciplinarios de desarrollo o investigación que requieran soluciones de informática segura.
- Dispone de conocimientos sobre la gerencia de empresas u organismos cuyos principales procesos y plataformas se sustenten en tecnologías de ciberseguridad de pequeña, mediana y gran escala.
- Tiene la mirada crítica, la idoneidad profesional y la conciencia social para gestionar con responsabilidad el acceso y manipulación de información sensible para la vida de las personas y el funcionamiento de entidades públicas y privadas.
- Desarrolla una actitud propositiva que le permite alcanzar capacidades de innovación, liderazgo y dirección de proyectos.

5. Alcances

5.1. Alcances al título de Técnico/a Universitario/a

En particular, se espera que un/a técnico/a pueda

1. Diseñar, implementar, gestionar y mantener redes de datos.
2. Analizar aspectos básicos de seguridad en redes informáticas.
3. Integrar hardware y software para la correcta operación de redes de computadoras en soluciones que impliquen tecnologías de la información y la comunicación.
4. Configurar, implantar y desplegar servicios que permitan la operación de diferentes entornos para el desarrollo y la ejecución de software.
5. Integrar equipos interdisciplinarios que desarrollen procesos de análisis,

diseño, despliegue y puesta en marcha de sistemas que integren tecnologías de la información.

5.2. Alcances de la Licenciatura en Ciberseguridad

La licenciatura forma profesionales con habilidades y conocimientos para:

- Formular, dirigir y validar políticas y mecanismos de seguridad en sistemas informáticos de todo, asegurando su alineación con los objetivos organizacionales.
- Desarrollar y gestionar el ciclo de vida de sistemas y tecnologías específicas de ciberseguridad para diferentes instancias de procesamiento, resguardo o comunicación de datos y aplicaciones informáticas en general.
- Establecer y auditar procedimientos de desarrollo seguro de acuerdo a las mejores prácticas y estándares de calidad de la industria del software.
- Gobernar proyectos integrales de ciberseguridad, administrar la gestión de riesgos corporativos, diseñar arquitecturas de seguridad complejas y coordinar equipos de defensa y de ataque simulado.
- Realizar tareas de investigación científica básica y aplicada en Ciberseguridad, participando como becario, Docente-Investigador o Investigador Científico/Tecnológico, en Laboratorios, Centros e Institutos de Investigación y Desarrollo en la materia.
- Planificar y supervisar auditorías de seguridad y de cumplimiento normativo, así como dirigir investigaciones complejas sobre nuevas amenazas y análisis de evidencia digital.
- Intervenir y dictaminar en pericias informáticas y brindar consultoría estratégica en asuntos de ciberseguridad y ciberdefensa en ámbitos oficiales y corporativos.

6. Condiciones de Ingreso

Los/as aspirantes a ingresar deberán:

- Poseer título de educación secundaria o equivalente expedido por escuelas de educación secundaria que cuenten con reconocimiento oficial. Excepcionalmente, podrán ingresar quienes tengan 25 (veinticinco) años o más (Art. 7 Ley de Educación Superior 24.521) y aprueben la evaluación establecida por la UNAHUR en la que se compruebe disponer de los conocimientos requeridos.

- Finalizar el Curso de Preparación Universitaria (CPU) que ofrece la Universidad.

7. Estructura curricular

7.1 Estructura por campos formativos

La carrera está estructurada por campos de formación. Estos refieren al modo en que se organizan y agrupan las unidades curriculares de acuerdo a las definiciones institucionales de la universidad. Los campos de formación son:

- CFC: campo de formación común.
- CFB: campo de formación básica.
- CFE: campo de formación específica.
- CIC: Campo de Integración curricular.

El **CFC** es común a todas las carreras de la UNAHUR y se compone de unidades curriculares que institucionalmente se considera que brindan los conocimientos y habilidades imprescindibles para el ejercicio de las profesiones. Se incluyen en el CFC las siguientes unidades curriculares:

- Cultura y alfabetización digital en la universidad
- Asignatura UNAHUR a elección entre las incluidas en la oferta definida anualmente por la Secretaría Académica.

El recorrido formativo de las materias del **CFB** plantea un abordaje profundo de contenidos fundamentales para poder abordar y conceptualizar desde el inicio mismo de la carrera principalmente los siguientes ejes transversales:

- Identificación, formulación y resolución de problemas matemáticos.
- Nociones básicas de los componentes y funcionalidades informáticas.
- Elementos de lógica y programación.
- Tecnologías de administración, resguardo y transmisión de información.
- Fundamentos para el desempeño en equipos de trabajo y comunicación efectiva
- Fundamentos para evaluar y actuar en relación con el impacto social de su actividad en el contexto global y local

A través del recorrido por las distintas unidades y actividades curriculares, se espera brindar a los y las estudiantes una formación teórica y práctica vinculada al contexto local, regional y global, comprometida socialmente y con una mirada política, crítica y reflexiva.

Se incluyen en el CFB las siguientes unidades curriculares:

- Matemática para informática I
- Matemática para informática II
- Introducción a lógica y problemas computacionales
- Taller de programación
- Lenguajes informáticos
- Bases de Datos
- Redes de computadoras
- Organización de computadoras I
- Organización de computadoras II
- Sistemas Operativos
- Tecnología y sociedad

El **CFE** es propio de la carrera y se compone de las unidades curriculares a las que refiere la especificidad de la titulación que se otorga.

Incluye saberes necesarios para la apropiación del conocimiento de la disciplina de Seguridad Informática. Incorpora la contextualización, la lógica y la legitimación de este conocimiento, así como los desarrollos científicos y técnicos propios; la articulación entre el campo específico y productivo, el contexto de desarrollo y su contribución al abordaje de problemáticas actuales.

Se incluyen en el CFE las siguientes unidades curriculares:

- Introducción a los sistemas de comunicación y seguridad
- Taller de intérpretes de comandos
- Operaciones
- Redes avanzadas
- Seguridad de la Información
- Laboratorio de sistemas operativos y redes
- Gestión integral de seguridad
- Desarrollo Seguro
- Ciberseguridad en la nube
- Ciberseguridad ofensiva
- Ciberseguridad defensiva
- Cibercrimen y análisis forense

- Criptografía
- Administración y respuesta a incidentes
- Ciberdefensa y ciberinteligencia

El **CIC** se enfoca en la integración de saberes mediante la aplicación práctica de los mismos en proyectos de integración. En este campo se desarrollan actividades curriculares en las que las y los estudiantes se vinculan con temas y problemas específicos de sus profesiones.

Son parte de este campo las siguientes unidades curriculares:

- Desarrollo, seguridad y operaciones
- Práctica profesional supervisada
- Proyecto final

Además, el plan de estudios incluye ***Actividades Curriculares Acreditables (ACA)***, las cuales son un aporte a la flexibilidad. Son un conjunto de actividades consideradas valiosas para la formación, referidas al ámbito de la investigación, la extensión, la cultura, los eventos académicos, el deporte, el trabajo y de unidades curriculares electivas que se van acreditando con asignación parcial de créditos a medida que se cumplimentan. En tanto flexibles, no se determinan de antemano sino que se ofrecen a elección del estudiantado dentro del conjunto de posibilidades que brinda y/o reconoce el Instituto de Tecnología e Ingeniería. Las ACA se regularán por medio de un reglamento específico.

Las ACA suman un total de 30 créditos (CRE), que se distribuyen de la siguiente manera:

- 10 créditos en unidades curriculares no incluidas en el plan de estudios.
- 10 créditos en experiencias formativas diversas.
- 10 créditos que se distribuirán según la definición del Instituto de tecnología e ingeniería.

Del total de créditos, el plan de estudios contempla que el porcentaje de las horas ACA que corresponden a interacción pedagógica supera ampliamente el 10% (75 horas), dependiendo de las actividades que desarrollen las y los estudiantes.

Se deben cumplimentar **12 créditos** para obtener el **título intermedio** y **18 créditos** más para obtener el **título de grado**.

La distribución de horas y créditos de las actividades por campo de formación son:

Campo de formación	Cantidad de actividades	Horas de interacción pedagógica	Horas de trabajo autónomo	Horas totales	Créditos
Común	2	64	111	175	7
Básica	11	704	896	1600	64
Específica	15	1056	1819	2875	115
Integración curricular	3	224	376	600	24
Actividades Curriculares Acreditables´		192	558	750	30

7.2 Estructura del plan de estudios

CRE: Unidad de tiempo total de trabajo académico - TAE: Horas de trabajo Autónomo del Estudiante - TTE: Horas de Trabajo Total del Estudiante (hs. IP + hs. TAE) (Carga horaria Total) - Hs. IP + Hs. TAE= TTE 1500 hs. Por año como mínimo - TTE dividido 25 horas= CRE. 60 por año promedio

Año	Campo	Nro	ASIGNATURA		HS. IP Semanal	HS. IP Total	HS. TAE	HS. TTE	CRE
1	CFB	1	Matemática para informática I	C	4	64	111	175	7
1	CFB	2	Introducción a lógica y problemas computacionales	C	4	64	111	175	7
1	CFE	3	Introducción a los sistemas de comunicación y seguridad	C	6	96	154	250	10
1	CFC	4	Cultura y alfabetización digital en la universidad	C	2	32	68	100	4
TOTAL PRIMER CUATRIMESTRE						256	444	700	28
1	CFE	5	Taller de intérpretes de comandos	C	4	64	161	225	9

1	CFB	6	Organización de computadoras I	C	4	64	61	125	5
1	CFB	7	Bases de Datos	C	4	64	111	175	7
1	CFB	8	Taller de programación	C	4	64	86	150	6
TOTAL SEGUNDO CUATRIMESTRE						256	419	675	27
TOTAL PRIMER AÑO						**512**	**863**	**1375**	**55**
2	CFB	9	Redes de computadoras	C	4	64	61	125	5
2	CFB	10	Organización de computadoras II	C	4	64	61	125	5
2	CFB	11	Sistemas Operativos	C	4	64	86	150	6
2	CFE	12	Operaciones	C	4	64	161	225	9
TOTAL PRIMER CUATRIMESTRE						256	369	625	25
2	CFC	13	Materia UNAHUR	C	2	32	43	75	3
2	CFE	14	Redes avanzadas	C	6	96	154	250	10
2	CFE	15	Seguridad de la Información	C	4	64	61	125	5
2	CIC	16	Desarrollo, seguridad y operaciones	C	6	96	154	250	10
TOTAL SEGUNDO CUATRIMESTRE						288	412	700	28
TOTAL SEGUNDO AÑO						**544**	**781**	**1325**	**53**
ACTIVIDADES CURRICULARES ACREDITABLES (ACA)						**64**	**236**	**300**	**12**
TOTAL Tecnicatura Universitaria en Redes y Operaciones informáticas						**1120**	**1880**	**3000**	**120**
Año	**Campo**	**Nro**	**ASIGNATURA**		**HS. IP Semanal**	**HS. IP Total**	**HS. TAE**	**HS. TTE**	**CRE**
3	CFB	17	Lenguajes informáticos	C	4	64	61	125	5
3	CFE	18	Laboratorio de sistemas operativos y redes	C	4	64	111	175	7
3	CFB	19	Matemática para informática 2	C	4	64	111	175	7

3	CFE	20	Gestión integral de seguridad	C	4	64	111	175	7
TOTAL PRIMER CUATRIMESTRE						256	394	650	26
3	CFB	21	Tecnología y sociedad	C	4	64	36	100	4
3	CFE	22	Desarrollo Seguro	C	4	64	136	200	8
3	CFE	23	Cibercrimen y análisis forense	C	4	64	111	175	7
3	CFE	26	Criptografía	C	4	64	111	175	7
TOTAL SEGUNDO CUATRIMESTRE						256	394	650	26
TOTAL TERCER AÑO						**512**	**788**	**1300**	**52**
4	CFE	25	Ciberseguridad en la nube	C	4	64	111	175	7
4	CFE	24	Ciberseguridad ofensiva	C	4	64	111	175	7
4	CFE	27	Administración y respuesta a incidentes	C	4	64	111	175	7
4	CIC	28	Práctica Profesional Supervisada	C	4	64	111	175	7
TOTAL PRIMER CUATRIMESTRE						256	444	700	28
4	CFE	29	Ciberdefensa y ciberinteligencia	C	4	64	111	175	7
4	CFE	30	Ciberseguridad defensiva	C	6	96	104	200	8
4	CIC	31	Proyecto final	C	4	64	111	175	7
TOTAL SEGUNDO CUATRIMESTRE						224	326	550	22
TOTAL CUARTO AÑO						**480**	**770**	**1250**	**50**
ACTIVIDADES CURRICULARES ACREDITABLES (ACA)						128	322	450	18
TOTAL 3° y 4° AÑO						**1120**	**1880**	**3000**	**120**
TOTAL Licenciatura						**2240**	**3760**	**6000**	**240**

8. Seguimiento curricular

El seguimiento curricular es un proceso continuo de monitoreo y evaluación para asegurar que el plan de estudios cumpla con los cometidos para los que fue pensado.

El objetivo es contar con un insumo que permita identificar aspectos a mejorar y tomar decisiones para optimizar los procesos de enseñanza y de aprendizaje.

La Comisión de Carrera en conjunto con la Secretaría Académica será la encargada de realizar el seguimiento curricular.

9. Formación Práctica

La formación práctica es concebida en este plan de estudios, de manera tal de permitir que el estudiante a lo largo de su carrera, incorpore saberes teóricos y prácticos, que les permitan desarrollar competencias profesionales para un adecuado desempeño en relación a las actividades reservadas al título y a los alcances definidos para el perfil de egresado de la carrera.

Los criterios que rigen la intensidad de la formación práctica son:

- Gradualidad y complejidad. El aprendizaje constituye un proceso de reestructuraciones continuas, que posibilita de manera progresiva alcanzar niveles cada vez más complejos de comprensión e interpretación de la realidad.
- Integración de teoría y práctica. La intervención en la problemática específica contempla ámbitos o modalidades curriculares de articulación e integración teórico-práctica que, además de recuperar el aporte de diferentes disciplinas, propicien la permanente reflexión sobre la práctica en situaciones concretas que requieren el desarrollo de soluciones a problemas del mundo real.
- Resolución de situaciones problemáticas. El proceso de apropiación del conocimiento científico o tecnológico requiere el desarrollo de la capacidad de identificar y resolver problemas del mundo real que requieren de la disciplina, dentro de un enfoque sistémico e interdisciplinario.

En este sentido la intensidad de la formación práctica garantiza que el estudiante logre introducirse a los estudios universitarios en seguridad informática, interpretar los problemas del mundo real relacionados con la aplicación de la disciplina e intervenir de manera efectiva para resolver los mismos.

La formación práctica se desarrollará en diferentes dimensiones. Por un lado, facilitando que el estudiante se familiarice con la Universidad, la organización y funcionamiento de las instituciones de enseñanza y su vinculación con la realidad. Asimismo, en esta dimensión se desarrollan habilidades prácticas en actividades experimentales y de resolución de problemas que acercan la realidad del ambiente profesional.

Por otro lado, se promueve la interpretación de la realidad vinculada con el profesional a través del diagnóstico y análisis de problemas, articulando la teoría con la práctica. Por último, la intervención crítica se promueve a partir de prácticas

formativas contextualizadas. Estas prácticas incluyen la participación del estudiante en actividades de carácter científico, tecnológico y/o experiencias de intervención profesional, que permitan resolver problemas del sector, en el contexto del perfil del graduado definido institucionalmente.

La formación práctica se consolida e integra mediante las actividades curriculares:

- La Práctica Profesional Supervisada (PPS) es una actividad formativa en la cual el alumno realiza una incorporación supervisada y gradual al trabajo profesional, a través de su inserción a una realidad o ambiente laboral específico relacionado con la seguridad informática y de esta manera aplica integralmente los conocimientos adquiridos a lo largo de su formación académica. El Reglamento de Práctica Supervisada de la Universidad de Hurlingham regula los objetivos, metodología, acciones, plan de trabajo, actividades, evaluación, docente responsable y lugar de realización. La supervisión la realiza un tutor docente y deberá acreditarse un tiempo mínimo de horas de práctica profesional dentro de la misma universidad, en instituciones, organismos, sectores productivos, y/o de servicios.
- El Proyecto Final consta de la realización de un trabajo técnico y/o científico y/o desarrollo tecnológico y/o aquel trabajo de carácter analítico - científico, de elaboración y conclusiones personales relacionado con las incumbencias profesionales e integrador de los conocimientos adquiridos, que debe realizar y presentar todo alumno/a para obtener el grado de Licenciado. El reglamento de Proyectos integradores de la Universidad de Hurlingham regula los objetivos, características, requisitos previos, elección del tema, dirección, responsable de la asignatura, desarrollo del proyecto, finalización y examen.El Proyecto será guiado y supervisado por un docente tutor.

10. Contenidos mínimos

Cultura y alfabetización digital en la universidad:

Derechos y ciudadanía digital. Reflexión crítica sobre la cultura contemporánea. Entornos y plataformas digitales de aprendizaje. Herramientas de colaboración en ambientes digitales. Recursos de información en la era digital: búsquedas efectivas y evaluación crítica de fuentes. Producción, uso y distribución de contenidos digitales académicos. Exploración y apropiación de tendencias y tecnologías emergentes.

Asignatura UNAHUR:

Son propuestas flexibles que realiza la Universidad atendiendo a coyunturas y propósitos particulares y los/las estudiantes pueden elegir entre las incluidas en la oferta definida anualmente por la Secretaría Académica. En el Anexo 1 se detallan los contenidos mínimos de algunos ejemplos de asignaturas UNAHUR actualmente ofrecidas.

Matemática para informática I:

Elementos de lógica proposicional y de primer orden: Enfoque sintáctico y semántico. Técnicas de prueba. Teoría de la Estructuras Discretas. Cuantificadores. Condicionales Asociados. Razonamientos Deductivos. Leyes de Inferencia. Teoría básica de conjuntos. Problemas de Conteo. Números enteros: Teoría de número.

Introducción a lógica y problemas computacionales:

Qué es la informática: hardware vs. software, historia de las computadoras, presente, posibles escenarios futuros. Historia del software y los lenguajes de programación: qué son los paradigmas de programación: imperativo, orientado a objeto y funcional.

Qué es un programa. Entornos de desarrollo y ejecución. Principios de la programación imperativa: comandos (acciones), estructuras de control de flujo de programas (secuencia, repetición simple, repetición condicional, alternativa condicional en comandos). Sensores booleanos. Conectivas booleanas. Sensores numéricos. División en subtareas como metodología para la resolución de problemas complejos, y necesidad de dar estructura a un programa no trivial.

Introducción a los sistemas de comunicación y seguridad:

Introducción a Redes y Sistemas de Comunicaciones. Concepto y características principales. Informática y comunicaciones. Arquitectura de Sistemas: Relación entre hardware, sistema operativo y red. Operaciones informáticas y componentes básicos.

Introducción a la Ciberseguridad. Elementos de programación segura. Riesgos y vulnerabilidades. Integridad y privacidad de la información. Distinción conceptual entre Seguridad de la Información (activos y gobierno) y Ciberseguridad (protección de infraestructuras y ciberespacio). La tríada CIA (Confidencialidad, Integridad, Disponibilidad).

Teoría de Comunicaciones y Seguridad: Conceptos de transmisión analógica y digital, ruido y ancho de banda enfocados en la Disponibilidad e Integridad de la información. Canales de comunicación y medios físicos (cobre, fibra, inalámbrico) como vectores de ataque y defensa (capa física). Introducción a la terminología de

riesgo, amenaza y vulnerabilidad en el contexto de las comunicaciones. Panorama general de controles técnicos. Evolución histórica: del perímetro físico a la seguridad lógica. Políticas de seguridad.

Taller de intérpretes de comandos:
Interfaz operativas de usuario, GUIs vs CLIs. Sistemas CLIs en diferentes sistemas operativos. Formato de comandos: argumentos, flags. Comandos comunes. Directorios, rutas absolutas y relativas. Gestionar archivos con CLI. Permisos y privilegios. Piping y redireccionado. Búsquedas. Acciones por lotes. Concepto de variables de entorno y archivos de configuración. Creación de scripts para la automatización de procesos complejos. Scripting simple con Bash.

Organización de las computadoras 1:

Historia de la computación. Definición de computadora. La "información" en el mundo real (magnitudes analógicas y cantidades discretas) y su representación como "datos" binarios dentro del computador. Sistemas de representación numérica (SRN) decimales y binarios. Generalización a SRN posicionales en otras bases (octal, hexa o genérico "r"). Representación de números enteros (con signo) y racionales en sistemas de punto fijo y punto flotante. Errores al representar números racionales e irracionales en un sistema de ancho finito. Sistemas de representación alfanumérica. Representación de variables lógicas. Álgebra binaria: suma, resta y conceptos de multiplicación. Lógica digital: Axiomas y propiedades del álgebra de Boole, operaciones y compuertas lógicas. Circuitos combinacionales genéricos. Equivalencia entre la tabla de verdad y las funciones canónicas. Semisumadores y sumadores. Flags. Introducción conceptual a los módulos funcionales en los que se organiza una computadora: ALU, registros, bancos de registros, memoria y dispositivos de entrada/salida. Los caminos de datos (buses de datos, direcciones y control). Conceptos de lenguaje de máquina y ensamblador. Programas ensambladores. Relación entre lenguajes de alto nivel y código de máquina. Programas compiladores e intérpretes. Ejemplos de arquitecturas reales. Diferencias entre microprocesadores, microcontroladores y sistemas embebidos.

Bases de datos:

Qué es un modelo de datos, modelos conceptuales, lógicos y físicos. Modelo de entidad-relación: conceptos básicos. Modelo relacional: tabla, atributo, dominio, valor, fila; restricciones de integridad; operaciones que se pueden hacer. SQL: concepto de lenguaje de consulta, sintaxis, concepto de join, agrupamientos, subqueries, joins parciales. Sistemas de Bases de Datos. Diseño y administración de Sistemas de Bases de Datos. Escalabilidad, eficiencia y efectividad. Lenguajes de DBMS. Transacción: concepto, demarcación de transacciones.

Taller de programación:

Valores y expresiones, tipos, estado. Terminación y parcialidad. Metodología para desarrollo de software robusto. Principios de la programación estructurada: funciones y procedimientos. Resolución de problemas mediante programas. Tipos de datos estructurados, arreglos y registros. Herramientas y lenguajes para el procesamiento de datos. Entornos integrados de desarrollo.

Redes de computadoras:

Concepto de red de computadoras, redes y comunicación. Modelos OSI y TCP/IP. Conceptos de protocolo y de servicio. Nivel físico: repetidor y hub, cableado estructurado. Nivel de enlace: concepto de medios físicos, tramas, bridge y switch, enlaces inalámbricos, vlans, spanning tree. Nivel de red: concepto de ruteo, topologías, ruteo estático, algoritmos y protocolos de ruteo dinámico, protocolo IPv4, resolución de direcciones. Nivel de transporte: funciones, protocolos UDP y TCP, multiplexación, concepto de socket, control de congestión, servicios de capa de aplicación (http, dhcp, dns, smtp, etc.). El modelo computacional de la Web. Estándares utilizados en Internet, concepto de RFC. Concepto e implementación de las VPN. Administración de redes: servicios, firewalls. Sistemas cliente/servidor y sus variantes.

Organización de computadoras II:

Combinacionales genéricos. Circuitos combinacionales específicos: Sumador, decodificador, multiplexor, demultiplexor, detector de paridad, comparador de magnitud y codificador de prioridades. Biestables. Circuitos secuenciales. Celda de memoria, registro de desplazamiento y contador. Organización y arquitectura del computador. Unidades funcionales. Unidad aritmético lógica (ALU). Memoria y sus niveles de jerarquía. Subsistemas de entrada y salida. Unidad de control y camino de datos.

Arquitectura. ISA. Instrucciones en código de máquina. Von Neumann. Harvard. RISC. CISC. Ciclos de instrucción. Tipos de direccionamiento. Lenguaje de transferencia de registros(RTL). Lenguaje de máquina. Lenguaje ensamblador. Código fuente y código objeto.Ensambladores, intérpretes y compiladores. Conceptos de arquitecturas superescalares y multiprocesamiento."

Sistemas operativos:

Introducción a los sistemas operativos: función de abstracción del hardware; organización, estructura y servicios de los SO. Sistemas operativos: de tiempo real, embebidos (embedded), distribuidos. Sistemas batch / Multiprogramación / / Sistemas paralelos. Conceptos de proceso, thread y planificación. Concurrencia de ejecución. Interbloqueos. Comunicación y cooperación entre procesos. Deadlocks. Planificación: Algoritmos, criterios. Multiprocesamiento. Administración de memoria: Espacio lógico y físico, swapping, alocación contigua, paginación, segmentación. Memoria virtual: Paginación bajo demanda, algoritmos de reemplazo de página, thrashing. Sistemas de archivos: Sistemas de archivos. Protección. Manejo de directorios. Concepto de Proceso. Planificación de Procesos. Protección: objetivos, dominio de protección, matriz de acceso y sus implementaciones. Prácticas con distintos sistemas operativos.

Operaciones:

Introducción a operaciones en los contextos de las tecnologías de la información (IT). Ambientes. Sistemas de producción. Conceptos de despliegue e integración. Despliegue continuo. Buenas prácticas, gestión del proyecto. Herramientas. Métricas.

Redes avanzadas:

El modelo computacional de la Web. Estándares utilizados en Internet, concepto de RFC. Concepto e implementación de las VPN. Administración de redes: servicios, firewalls. Sistemas cliente/servidor y sus variantes.

Protocolo IPv6 - Sistemas Autónomos / ISPs / NAPs - Ruteo Interno y Externo en sistemas autónomos. Características de los ISPs (proveedores de servicios de Internet). Servicios distribuidos. Seguridad en Redes de Computadoras y Dispositivos. Optimizaciones de ruteo y servicios. Redes basadas en software. Virtualización de redes. Redes iOT.

Seguridad de la información:

Introducción a la Seguridad de la Información. Conceptos fundamentales y objetivos. Gestión de la Seguridad de la Información. Riesgo: análisis y tratamiento. Seguridad en Redes, elementos de criptografía. Criptografía Simétrica y Asimétrica. Algoritmos de Hash. Infraestructura de Clave Pública. Certificados digitales. Seguridad en Redes. Objetivos. Ataques, Servicios y Mecanismos de Seguridad. Seguridad en Redes Inalámbricas. Control de Acceso Lógico. Controles físicos de seguridad: seguridad en el centro de cómputos. Seguridad en las operaciones. Gestión de usuarios. Control de cambios. Métodos de Evaluación de seguridad:

Auditorías, Evaluaciones funcionales, Vulnerability Assessment y Penetration Test. Gestión de Incidentes. Seguridad en Aplicaciones. Vulnerabilidades. Software malicioso. Problemática de las aplicaciones WEB. Leyes, regulaciones y estándares. Marcos legales nacional e internacional. Privacidad, Integridad y seguridad en sistemas de información.

Desarrollo, seguridad y operaciones (Integradora):

Metodologías y herramientas de desarrollo, seguridad y operaciones (Dev-Sec-Ops)

Operaciones y modelos de gestión ágiles. Fundamentos de integración y despliegues continuos. Infraestructura de nube. Herramientas. Arquitecturas de contenedores (Docker, otras). Automatizaciones. Trabajo con contenedores. Contenedores y nube. El Software como Servicio. Alternativas abiertas para servicios en la nube. Monitoreo.

Planificación y realización de proyectos de seguridad informática. Trabajo de integración profesional.

Lenguajes informáticos:

Estudio de los fundamentos de la programación concurrente, el paralelismo y la programación basada en eventos. Modelos de concurrencia y sus motivaciones; diferencias conceptuales y operativas entre concurrencia, paralelismo y eventos. Modelos de memoria compartida y pasaje de mensajes, incluyendo mecanismos de sincronización, exclusión mutua y comunicación entre procesos e hilos. Análisis de problemas asociados a la concurrencia: condiciones de carrera, inanición, interbloqueos, seguridad y progreso. Exploración de modelos de interacción como cliente-servidor y productor-consumidor. Programación orientada a eventos en entornos concurrentes. Aplicación de técnicas de concurrencia, paralelismo y programación basada en eventos en lenguajes de programación contemporáneos. Introducción a la programación sobre unidades de procesamiento gráfico (GPU) y estudio de criterios de eficiencia energética en entornos de ejecución concurrente y paralelo.

Laboratorio de sistemas operativos y redes:

Instalación, configuración y operación de distintos servicios relacionados con Internet: servidores de aplicaciones, servidor y cliente de mail, servidor y cliente FTP, firewalls, etc. Servicios de directorio, servidores LDAP, uso desde aplicaciones. Gestión de usuarios y control de accesos en un entorno operativo, impacto en la

instalación de aplicaciones, posibilidad de compartir recursos. Sistemas de backup automatizados, políticas de criticidad. Instalación, configuración y operación de repositorios de código. Monitoreo de redes, protocolo SNMP. Técnicas de transmisión de datos, modelos, topologías, algoritmos de ruteo y protocolos. Sistemas operativos de redes. Computación orientada a redes. Sistemas colaborativos.

Gestión integral de seguridad:

Gobierno de la seguridad de la información. Modelos de gobierno. Roles y responsabilidades. Políticas de seguridad. Marcos normativos y estándares internacionales. Gestión de riesgos. Métricas e indicadores. Auditoría y mejora continua. Legislación y normativa sobre sistemas de gestión, seguridad de la Información, cybersecurity framework, protección de datos, portabilidad y responsabilidad de transacciones monetarias. Implementación y auditoría de estándares en organizaciones.

Fraude y protección de Datos Personales. Tipificación y modelos de prevención. Medidas de protección de los datos personales. Normativas y organismos de aplicación. Compliance.

Deontología Profesional. Problemática actual de los profesionales del sector de ciberseguridad. Ética y toma de decisiones en el marco de organizaciones públicas y privadas. Regulaciones de la profesión y otras profesiones relacionadas al sector. Interés público.

Desarrollo Seguro:

Principios de Programación Segura: Diseño seguro. Validación de entradas y salidas. Gestión segura de errores y excepciones. Autenticación y autorización. Gestión de sesiones.

Vulnerabilidades Comas: Análisis profundo de vulnerabilidades. Revisión de Código: Pruebas de seguridad. Revisiones manuales de código. Dev Sec Ops (aplicación de proyecto).

Scripting para Seguridad: Uso de lenguajes para automatizar tareas de defensa, ataque y análisis. Análisis de código en aplicaciones móviles.

Cómo desarrollar de forma segura. Framework OWASP. Ciclo de Vida de Desarrollo Seguro (SSDLC): Integración de la seguridad en el desarrollo (DevSecOps). Análisis de código malicioso (OWASP, CWE, automatización de SI DevSecOpsetc)

Tecnología y sociedad:
Computación y Sociedad. Modelos de desarrollo científico y tecnológico. El proceso de producción de conocimiento. Etapas históricas. Historia de la computación. Ciencia, tecnología y economía. Sus interrelaciones. Etapas del desarrollo científico y tecnológico. El papel de la Universidad. La investigación científica y tecnológica en la actualidad. Software libre y sociedad. El posicionamiento del software libre y el código abierto. Cuestiones éticas y sociales. Sesgos algorítmicos. Impacto del uso de la IA. Definiciones de principios éticos. Regulaciones nacionales e internacionales. Posicionamiento de los/las profesionales en la resolución de problemas mediante IA.

Matemática para informática II:

Números naturales: Inducción matemática. Relaciones binarias. Estudio de las propiedades de una relación binaria. Clasificación. Relaciones de orden. Relaciones de equivalencia. Principios básicos de recuento: Regla del producto y regla de la suma. Factorial de un número. Propiedades. Análisis Combinatorio simple y con repetición.

Cibercrimen y análisis forense:

Análisis forense. Hardware, Software. Técnica y Método. Peritaje, normativa, implicancias y técnicas. Simulaciones. Informática Forense: Principios y metodología. Cadena de custodia.

Adquisición de Evidencia Digital: Adquisición de medios no volátiles. Adquisición de medios volátiles. Forensia en dispositivos móviles y en la nube.

Análisis Forense: Análisis de sistemas de archivos. Recuperación de datos. Análisis de artefactos de sistemas operativos (logs, registros, prefetch). Técnicas Anti-Forenses: Esteganografía, cifrado, ofuscación y métodos de evasión.

Informe Pericial: Estructura y validez legal del informe pericial informático. Investigación de Informática Forense. Aspectos legales y Deontología en CiberSeguridad.

Ciberseguridad ofensiva

Ciberseguridad en infraestructura y redes. Introducción al análisis de vulnerabilidades y pentesting. Tipos de vulnerabilidades. Metodologías de evaluación de seguridad ofensiva. Fases del pentesting: reconocimiento, escaneo, explotación, post-explotación y reporte. Herramientas de pentesting. Pruebas en

entornos controlados. Elaboración de informes técnicos. Hacking ético. Identificación y explotación de vulnerabilidades, en aplicaciones web, redes, servidores y otros sistemas informáticos.

Modelos de Ataque: Análisis de Tácticas, Técnicas y Procedimientos. Marcos de referencia. Caza de amenazas.

Autenticación de mensajes y autenticación de transmisores: conceptos y diferencias. Esquemas de autenticación.

Ciberseguridad en la nube:

Conceptos básicos de despliegue en infraestructura en nube y pautas de seguridad en Nube. Cloud híbrido, seguridad en contenedores y Kubernetes. Gestión de identidades.

Ejemplos de ataques. Inyección. Fallas criptográficas. Diseño inseguro. Configuración de seguridad. Componentes vulnerables y obsoletos. Fallos de identificación y autenticación.

Baselines de ejemplo: Cloud Security Alliance AWS Baseline PCI DSS, AWS 18CIS.

Criptografía:

Algoritmos y criptografía. Protocolos y técnicas. Aplicación. Conceptos Fundamentales: Historia y terminología. Criptografía clásica. Principios de Kerckhoffs. Necesidad de encriptar la información.

Métodos clásicos de encriptación. Criptografía Simétrica: Cifradores de bloque y modos de operación. Cifradores de flujo. Gestión de claves simétricas. Criptografía Asimétrica: Fundamentos matemáticos. Algoritmos. Funciones Hash. Códigos de autenticación de mensajes. Criptografía de curva elíptica.

Infraestructura de Clave Pública: Firma digital. Certificados digitales. Autoridades Certificantes. Cadena de confianza. Block Chains. Criptografía en redes y bases de datos.

Administración y respuesta a incidentes:

Continuidad del negocio y recuperación ante desastres (BCP, DRP, IRP) Normativas y estándares internacionales

Análisis de Impacto al Negocio (BIA). Identificación de procesos críticos. - Evaluación de riesgos y vulnerabilidades. Determinación de RTO y RPO. Plan de Continuidad del Negocio (BCP) Componentes del BCP. Estrategias de continuidad. Desarrollo, implementación y mantenimiento del plan. Plan de Recuperación ante

Desastres (DRP) Tipos de desastres: naturales, tecnológicos, humanos. - Estrategias de recuperación. Infraestructura de respaldo y redundancia.

Respuesta ante Incidentes (IRP) Ciclo de vida de la gestión de incidentes. - Equipos de respuesta (CSIRT). - Comunicación y reporte de incidentes (ej. de Playbooks y respuestas)

Simulacros, pruebas y mejora continua. Tipos de pruebas: simulaciones, ejercicios de escritorio, pruebas completas. Indicadores de desempeño. Actualización y mejora continua de los planes.

Práctica profesional supervisada:

Integración en contextos reales de trabajo. Reconocimiento de roles en esos contextos. Aplicación en el marco de empresas, instituciones, organismos y sectores productivos. Vinculación con problemáticas concretas, metodologías vigentes y entornos tecnológicos reales. Procesos de acceso al mercado laboral.

Roles y funciones dentro de un equipo. Trabajo en equipo. Autoaprendizaje. Buenas prácticas en la gestión de recursos. Planificación y gestión de seguridad. Trabajo en forma remota. Normas, estándares y criterios de seguridad informática. Elaboración de Informes. Exposición de informes.

Ciberdefensa y Ciberinteligencia:

Evolución de la Ciberdefensa. Ciberguerra. Ciberterrorismo. Mejores Prácticas en Ciberdefensa. Principal normativa nacional e internacional. Ciberguerra y el derecho internacional humanitario. Manual de Tallin. Ciberoperaciones.

Ciberinteligencia. Ciclo de la Inteligencia. Ingeniería Social. OSINT. HUMINT. SIGINT. MASINT. Inteligencia financiera. Ingeniería Inversa. Tipos de Inteligencia: Estratégica, Táctica y Operativa. Fuentes de Inteligencia: OSINT, HUMINT, SIGINT. Inteligencia en la Deep y Dark Web.

Análisis y Atribución: Análisis de TTPs. Indicadores de Compromiso (IoCs). Atribución de ataques. Plataformas y Estándares. Relaciones internacionales en ciberseguridad. Principales actores globales. Redes y organizaciones. Alianzas estratégicas de nuestro país y tendencias en comercio internacional. Procesos de integración económica y el rol de la seguridad de la información. Escenarios de conflicto.

Seguridad defensiva:

Defensa de Redes y Arquitecturas Seguras. Arquitecturas de Seguridad: Defensa en profundidad. Modelo de Confianza Cero (Zero Trust).

Tecnologías de Detección y Prevención: IDS/IPS (basados en firmas y comportamiento). Firewalls de nueva generación (NGFW) y aplicaciones web (WAF). Monitoreo y Correlación. Gestión de logs. Plataformas de seguridad y gestión de eventos.

Seguridad inalámbrica y protección en entornos distribuidos. Conceptos de Honeypots y Honeynets. Soluciones EDR (Endpoint Detection and Response) y XDR. Caza de Amenazas.

Simulación y colaboración: Red Team / Blue Team / Purple Team.

Proyecto final:

Determinación de un tema de investigación y/o desarrollo: pertinencia y factibilidad.

Objetivos e hipótesis. Estado del arte, revisión y búsqueda bibliográfica sistematizada. Modelización de un proyecto. Etapas de un proyecto. Estructura de escritura final y formatos de presentación.

Desarrollo y publicación de productos. Conformación de equipos y roles. Plan de trabajo. Documentos de producción y diseño. Estimación de recursos. Prototipos. Métricas.

10.1 Actividades Curriculares Acreditables (ACA)

El Instituto de Instituto de Tecnología e Ingeniería definirá periódicamente el catálogo de *Actividades Curriculares Acreditables (ACA)*, que incluirá tanto unidades curriculares electivas como otro tipo de actividades académicas, investigativas, culturales, deportivas o de vinculación con la comunidad, sean estas organizadas por la UNAHUR o por otras instituciones y espacios reconocidos. También se definirán los requisitos de reconocimiento de las distintas ACA y los criterios para la ponderación y otorgamiento de créditos.

Anexo I - Contenidos mínimos de Asignaturas UNAHUR

Arte y tecnología. Escuela de espectadores

La mirada del espectador. Exploración de las múltiples conexiones que existen entre la literatura, el cine, el teatro y las artes plásticas y su relación con la tecnología. Artes plásticas. Lengua y literatura. Teatro y representación. Cine y tecnología. Fotografía.

Astro: relación de la humanidad con el cosmos

Temas y problemas de Astronomía, en una visión general, contextual e histórica. La Astronomía en la Antigüedad. La Esfera Celeste. Elementos de sistemas de coordenadas esféricos. El Tiempo Astronómico. Sistema Solar. Elementos de Astrofísica. Estrellas. Sistemas Estelares. Elementos de Cosmología. Nuevos mundos: Sistemas Extrasolares.

Ciencia, tecnología e innovación para el desarrollo

Definiciones fundamentales de ciencia, tecnología e innovación, incluyendo su importancia en el desarrollo económico y social. Los contextos y desafíos de la innovación en diversos sectores y entornos son explorados, junto con estrategias para la identificación de oportunidades y la transferencia de tecnología. Se examina el impacto ético y social de la tecnología, así como los aspectos legales y políticas públicas relacionados. Además, se fomenta el desarrollo de habilidades de trabajo en equipo y comunicación efectiva en el contexto de la innovación.

Cine documental: miradas desde el Sur

Cambios en el mundo contemporáneo y en la Argentina. El cine documental y la representación de esos acontecimientos. Las vivencias en los cambios individuales y colectivos en perspectiva de derechos humanos, de género, de nuevos hábitos y costumbres en torno al trabajo, la familia, la convivencia entre generaciones, las rupturas y los nuevos acuerdos que se producen entre jóvenes y adultos en relación con la forma de entender el mundo contemporaneo. El documental y la representación de “la justicia” y sus instituciones en el cine nacional. El documental y la representación de “la justicia” y sus instituciones en el cine internacional.

Ciudadanía activa y compromiso social

Las políticas de infancias, el rol del Estado y las nuevas prioridades de agenda en derechos de la niñez y en la reducción de las desigualdades en la Argentina y en el contexto latinoamericano. Las políticas sociales de infancias, la igualdad de oportunidades y de resultados; los paradigmas de políticas de infancia y adolescencia en Argentina y América Latina; la desigualdad y la pobreza en la infancia y adolescencia; la inversión social.

Cuando los pasados no pasan: lugares de memoria

La memoria. La noción de "lugares de memoria". Genocidios del siglo XX: un acercamiento histórico y conceptual. El terrorismo de Estado en Argentina. Políticas de memoria: derechos humanos ayer y hoy. El memorial de Berlín; la historia de vida de Soghomon Tehlirian; la fecha del 24 de marzo; el pañuelo de las Madres; el Himno Nacional Argentino o el Museo/sitio de memoria ESMA pensados críticamente para conocer el pasado y construir una economía general del pasado en el presente.

Debates políticos actuales. Ideas para pensar el mundo de hoy

Introducción al debate político. El debate político contemporáneo y las singularidades del momento histórico-ideológico actual. Algunos debates políticos actuales, tales como la justicia social, la igualdad de género, la ecología, el avance tecnológico, el populismo y la antipolítica.

Educación sexual integral. Cuando lo esencial es visible a los ojos

Introducción a la Educación sexual integral: enfoques y tradiciones de la educación sexual. El paradigma de derechos como marco para las prácticas pedagógicas de ESI: Declaración de los Derechos Humanos y otras leyes que cambiaron paradigmas. La Ley Nacional N° 26.150/06. Nuevas/os sujetos/as: niñez y adolescencia; autonomía progresiva; superación del paradigma tutelar. Educación Sexual Integral con perspectiva de género. Géneros y diversidades. El cuerpo como construcción política.

Filosofía. Problemas filosóficos

Orígenes de la Filosofía: Grecia. La filosofía entre el arte y la ciencia. La pregunta por el todo. La duda radical. Definiciones críticas de la filosofía. El poder. La multiplicidad de relaciones de poder. El poder y el discurso. La voluntad de poder. Posmodernidad y la sociedad del espectáculo. El fin de los grandes relatos. El cuestionamiento de la idea de progreso y de la teleología de la historia.

Posmodernidad y posverdad, sociedad de la comunicación, sociedad de consumo, sociedad del espectáculo. El otro. Existencia precaria y política. La idea de libertad y la ética de la responsabilidad. El debate en torno a los conceptos de tolerancia y hospitalidad. El extranjero.

Innovación y creatividad

Creatividad, e innovación. La innovación y el desarrollo en los campos del conocimiento asociados a las especialidades o de las carreras de la Unahur. El contexto sociocultural de la innovación. ¿Para quiénes innovamos desde la Universidad? Proceso creativo. Diagnóstico de la problemática. Técnicas de generación de ideas. Nociones básicas de neuroeducación para aplicarlas a la generación de ideas-proyecto. Innovación Social Sustentable. Nuevos modelos de liderazgo. Conceptos y desarrollo. Difusión. Formas de organización. Apoyo y financiamiento. Modelos de inversión actuales. Modelos de presupuesto. Financiamiento. Innovación Colaborativa. Organización. Modelo Canvas. Cómo cuento mi proyecto. Cómo muestro mi proyecto.

Introducción a la imagen. De la imagen fija a la imagen en movimiento

Enfoque semiótico y giro pictórico. El problema de la representación. La imagen como signo. La relación entre el significado y el referente. El lenguaje de los nuevos medios. La cultura visual y el estudio de la visualidad. La imagen mediática. La retórica de la imagen. El acto fotográfico. La potencia política de las imágenes. Collage y montaje. El lugar del espectador emancipado. Herramientas del lenguaje visual. Artes y medios visuales y audiovisuales. La estética de lo performativo y la teatralidad.

Introducción al Latín

Nociones básicas sobre los orígenes de la lengua latina. El latín y las lenguas romances. la vida cotidiana en Roma. Epitafios y graffitis. La construcción de la identidad romana. La condición de la mujer en la antigüedad latina. Palabras flexivas. Morfología nominal. Hechiceras, magas y diosas en la cultura latina. Representaciones para la mujer en la tragedia latina. La puella culta elegíaca. Su contexto de aparición: una nueva manera de ser mujer en Roma.

La vida secreta de las rocas

Introducción a la geología: origen y evolución del universo, el Sistema Solar y la Tierra. El tiempo geológico. Introducción a la paleontología: evolución e historia de

la vida en la Tierra. Registro geológico. Cambio climático. Mineralogía: propiedades de los minerales. Métodos de identificación de minerales. Introducción a la sistemática mineral. El ciclo de las rocas: Procesos endógenos y exógenos. Geología e hidrocarburos: Sistema petrolero convencional y no convencional. Importancia estratégica e implicancias ambientales de las actividades.

Malvinas: una causa de nuestra América Latina

Los principales argumentos históricos. Descubrimiento, colonización y usurpación. Los argumentos jurídicos: de la usurpación a las Naciones Unidas. Malvinas como causa política de Estado. Integridad territorial y Libre determinación de los pueblos. Otros casos de colonialismo bajo la bandera de la libre determinación.

El Atlántico Sur en la geopolítica de América Latina: recursos naturales, depredación y militarización. Soberanía sobre el Atlántico Sur. La Antártida como espacio de disputa.

Historia contemporánea de la causa Malvinas: guerra y posguerra. Inglaterra y los problemas de financiamiento de las islas. Intercambios en materia de comunicación, recursos energéticos y educación. El golpe cívico militar de 1976 y el cambio de perspectiva. La decisión de tomar Malvinas y la derrota. Los ochenta y los noventa: la “desmalvinización”. Posneoliberalismo y remalvinización. Malvinas como causa regional. Un nuevo período de desmalvinización.

Métodos participativos de transformación de conflictos

El diálogo colaborativo y la construcción de consensos. Convivencia ambiental. Teoría del Conflicto. Su apreciación y tratamiento como oportunidad de cambio. Comunicación. Conocimientos básicos y aplicación a la vida comunitaria y profesional. Negociación. Técnicas y herramientas. Mediación. Procesos de mediación y su incidencia en la cultura. Facilitación en procesos de abordaje de conflictos intra e inter institucionales. Procesos participativos de prevención temprana y adecuado abordaje de conflictos comunitarios.

Pensamiento ambiental latinoamericano

Introducción al pensamiento ambiental latinoamericano (PAL). La educación y el desarrollo como dos ejes y preocupaciones centrales del PAL. El rol de la educación superior: avances y desafíos. Las concepciones del desarrollo que se disputan al Norte global. La incorporación de la dimensión ambiental en la educación superior. De la EA a la Educación para el Desarrollo Sustentable: un desplazamiento que no

sólo es conceptual sino político. El postdesarrollo como alternativa al desarrollo. La ecología política y la propuesta de descolonizar la naturaleza.

Robótica

Tipos de robots y campos de uso.Partes que componen un dispositivo robótico. Conceptos de tinkercad y su uso. Conceptos básicos de arduino. Algebra de Boole y lógica digital. Introducción a la programación en bloques y C++. Robótica y automatización de objetos.

Una historia del rock nacional

Los orígenes del Rock Nacional. Las derivas urbanas como método compositivo. El núcleo fundador. Espacios de sociabilidad. La jerga del rock. Rock y marginalidad. El Cordobazo. La década del 70. Inspiraciones bajo el látigo de la violencia. El apogeo del Rock Nacional. Concepto de “música progresiva”. Folklore y rock. El rock sinfónico. La década del 80. Modernidad o muerte. La guerra de Malvinas como separatoria de aguas. La recuperación democrática. La rebelión punk. De los teatros y estadios al pub y los lugares emblemáticos. El canto popular urbano. La década del 90. La balsa a la deriva. La canción neoliberal. Año 2000 y después. La vuelta de Boedo y Florida: la movida sónica y el rock chabón. Las tribus urbanas. Experimentación y poesía social. Cumbia y protesta social. Últimos años: La producción independiente y las nuevas tecnologías. La muerte del disco.

Hoja de firmas

Sistema: sudocu
Fecha: 10/12/2025 16:56:57
Cargado por: Valeria Maidana

Sistema: sudocu
Fecha: 10/12/2025 17:24:23
Autorizado por: Nicolas Vilela

Sistema: sudocu
Fecha: 10/12/2025 18:28:26
Autorizado por: Jaime Perczyk