UNIVERSIDAD NACIONAL DEL SUR
Departamento de Ciencias e Ingeniería de la Computación
San Andrés 800 (Campus Palihue) – Bahía Blanca – Buenos Aires - Argentina

Bahía Blanca, 05 de julio de 2023

Sr. Director Decano del
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur
Dr. Diego C. Martinez
S / D

De mi mayor consideración,

Tengo el agrado de dirigirme a Ud., y por su intermedio al Consejo Departamental, en relación al proyecto de creación de la Diplomatura en Ciberseguridad Inteligente. Adjunto a esta nota el documento con todos los detalles del proyecto.

Sin otro particular, saludo a Ud. atentamente,

Dr. Gerardo I. Simari
Profesor Adjunto
DCIC UNS
gis@cs.uns.edu.ar
Tel.: 459-5101 int. 2628

Proyecto de creación de la

Diplomatura en Ciberseguridad Inteligente

Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur

2023

05 de julio de 2023

Diplomatura en Ciberseguridad Inteligente

Resumen

Este documento presenta una propuesta para la creación de la Diplomatura en Ciberseguridad Inteligente, un programa a ser dictado por el Departamento de Ciencias e Ingeniería de Computación (DCIC) de la Universidad Nacional del Sur en colaboración con docentes de otros departamentos y actores del ámbito empresarial. Se trata de un programa que tiene previsto un 100% de su carga horaria a ser dictada a través de la modalidad de educación a distancia.

El DCIC propone la creación de un Programa de Diplomatura en Ciberseguridad Inteligente para profesionales y practicantes de distintas áreas de la ingeniería y las ciencias, así como también involucrados en el sector público o privado, que estén interesados en el desarrollo de capacidades asociadas con la gestión de sistemas seguros.

Este documento describe el programa de Diplomatura propuesto de acuerdo a la siguiente estructura. La sección 1 describe la introducción a la propuesta. La sección 2 analiza la fundamentación del programa, y lo contextualiza en relación con otros programas similares a nivel internacional y nacional. La sección 3 explica los objetivos del programa, y la Sección 4 especifica las características de la certificación otorgada y el perfil del egresado. Los apartados 5 y 6 describen la modalidad de enseñanza y las condiciones de ingreso, respectivamente. En la sección 7 se describe el plan de estudios, incluyendo la bibliografía de base, y en la sección 8 se detalla cómo se organizarán los cronogramas de dictado. Por último, la sección 9 brinda detalles acerca de la conformación del Comité Académico de Dirección y cuerpo docente, mientras que la sección 10 finaliza con la descripción de cuestiones presupuestarias que serán centrales al financiamiento del programa.

Datos de Contacto

Por consultas sobre la Diplomatura en Ciberseguridad Inteligente, contactarse con:

Departamento de Ciencias e Ingeniería de la Computación
San Andrés 800, UNS Campus de Palihue
(8000) Bahía Blanca, Argentina

e-Mail: diplo.ciber@cs.uns.edu.ar

Teléfono: +54 (291) 459-5135

Tabla de contenidos

1) Introducción

La pandemia del COVID-19 provocó que las empresas y los actores institucionales tuvieran que acelerar los procesos de digitalización de muchos de sus sectores. En muchos casos, estos avances no fueron acompañados por políticas de ciberseguridad adecuadas que permitieran custodiar los datos y las infraestructuras críticas de información y, por lo tanto, aumentaron la "superficie" expuesta. Más allá de los efectos directos de la pandemia, los ciberataques cada vez son más frecuentes, complejos y dirigidos, generando grandes costos en las empresas e instituciones para reparar los daños. A raíz de esto, la demanda de especialistas en ciberseguridad ha ido en aumento tanto en el sector público como en el privado, pero la oferta no alcanza para cubrir los puestos de trabajo disponibles. Una estimación de la fuerza laboral en ciberseguridad y su brecha sugiere que la fuerza global en ciberseguridad debe crecer por lo menos un 65%[1].

Los ataques a la infraestructura informática han crecido no sólo en cantidad, sino que han alcanzado una sofisticación que involucra elementos generales de la interacción humano-computadora. Por estas razones, esta Diplomatura se centrará no sólo en los aspectos "clásicos" de la ciberseguridad – aquellos comúnmente englobados bajo el nombre de Seguridad Informática – sino también en dos aspectos complementarios y que se incluyen como partes integrales en la investigación, desarrollo e innovación de vanguardia en la temática.

El primero de estos aspectos complementarios nace de la observación de que esta especialidad no solamente involucra a las disciplinas estrechamente ligadas a la digitalización, sino también a otras que se centran en aspectos humanos. Las personas típicamente se identifican como las partes más vulnerables a ataques dado que existen muchas técnicas que explotan la confianza, el tedio, la tendencia a ser abrumados por el volumen de datos, entre muchas otras vulnerabilidades humanas. Además, no puede ignorarse la preponderancia de las plataformas sociales (o funcionalidades que le agregan una componente social a muchos sistemas) en la vida de gran parte de la población mundial. Por lo tanto, cualquier profesional debe ser plenamente consciente no sólo de la existencia de estas vulnerabilidades, sino también de las principales formas de eliminarlas o al menos mitigarlas.

El segundo aspecto es el de la incidencia que tienen hoy en día los sistemas inteligentes como parte de, prácticamente, cualquier sistema socio-técnico en producción a nivel mundial. La Inteligencia Artificial (IA) puede utilizarse para ayudar a los profesionales de la ciberseguridad a tratar la complejidad cada vez mayor de los sistemas modernos de IT, industria 4.0, infraestructura del Internet de las Cosas (IoT, por sus siglas en inglés), e intentar estar por delante de los ciberataques. Debido a las diferentes amenazas que pueden surgir en torno a la ciberseguridad es que se están explorando modelos de IA que faciliten el análisis y la toma de decisiones en tiempo real para detectar y reaccionar más rápidamente ante ciberataques. Lamentablemente, las funciones de la IA no solamente se limitan a la ciberseguridad defensiva, sino que también pueden ser utilizadas de manera

[1] https://www.openaccessgovernment.org/plugging-cybersecurity-skills-gap-security-professionals/155418/

ofensiva; de este modo, los ciberatacantes pueden explotar vulnerabilidades conocidas, encontrar nuevas o crearlas con mayor facilidad, conocer patrones de comportamiento de sus víctimas, romper con mayor facilidad contraseñas y captchas o buscar lugares donde esconderse y no ser detectados, e incluso adaptarse con mayor rapidez a las contramedidas que los defensores puedan tomar, entre otras posibilidades. Es imprescindible conocer y comprender estas actividades maliciosas para poder desarrollar contramedidas defensivas efectivas.

La Diplomatura en Ciberseguridad Inteligente está diseñada para que cualquier persona con conocimientos básicos de Informática obtenga una introducción a todos estos aspectos a un nivel suficiente como para incorporar su tratamiento en diferentes actividades en un amplio espectro de funciones laborales. En total consiste en 216 horas de dictado sincrónico y asincrónico organizadas en dos trimestres, con cobertura de aspectos teóricos, actividades prácticas e intercambios con docentes expertos en las diferentes áreas de estudio y con profesionales que brindarán puntos de vista actualizados desde sus respectivas perspectivas.

2) Fundamentación

Como ya se mencionó en el apartado anterior, el uso de las tecnologías de la información permea actualmente a prácticamente la población mundial entera. Con el avance del desarrollo y despliegue de estas tecnologías, surgen nuevas amenazas que nacen a partir de muchos orígenes, tales como las vulnerabilidades incluidas inconscientemente durante el desarrollo de software y hardware, pero también – cada vez más – por las debilidades inherentes a las componentes humanas de los sistemas socio-técnicos.

El Gobierno Nacional desarrolló recientemente el Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos (2021-2024)[2] del Ministerio de Seguridad de la Nación. Entre las áreas prioritarias identificadas se encuentran:

- Fortalecer los recursos humanos del Estado Nacional y las herramientas tecnológicas.
- Creación y actualización normativa.
- Acciones de campaña de prevención del ciberdelito.
- Crear equipos de respuesta específicamente capacitados.

[2] Resolución 75/2022 del Ministerio de Seguridad de la Nación. Texto completo del anexo disponible en: https://www.argentina.gob.ar/sites/default/files/infoleg/res75.pdf

Estrategia nacional:
https://www.boletinoficial.gob.ar/detalleAviso/primera/279103/20230105
https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf

- Incremento de cooperación público-privado.

En el ámbito de Ciberseguridad Ciudadana, el Gobierno Nacional ha implementado diferentes leyes, decretos y resoluciones que permitieron implementar herramientas como firma digital, como así también definir marcos de protección tanto para el estado nacional como para los ciudadanos. La cronología de ello se detalla a continuación:

- Ley nº 25326 de Protección de Datos, del 4 de octubre de 2000 (publicado en el Boletín Nacional de 2 de noviembre de 2000).
- Ley nº 25506, del 14 de enero de 2001, de Firma Digital.
- Decreto 1558/2001, del 3 de diciembre de 2001. Aprueba la reglamentación de la Ley nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.
- Decreto Reglamentario nº 2628/2002, del 19 de diciembre de 2002. Reglamentación de la Ley nº 25506. (Abrogado por el artículo 5º del Decreto nº 182/2019.)
- Resolución nº 580/2011, del 27 de noviembre de 2011, de Creación del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad.
- Disposición ONTI nº 3/2013, del 27 de agosto de 2013. Aprobación de la Política Modelo de Seguridad de la Información.
- Ley nº 26904, del 13 de noviembre de 2013, de Grooming
- Decreto nº 577/2017 del 28 de julio de 2017 y su modificatorio, que crea el Comité de Ciberseguridad en la órbita de la Secretaría de Gobierno y Modernización de la Jefatura de Gabinete de Ministros, estableciendo entre las tareas a su cargo la de “Desarrollar la Estrategia Nacional de Ciberseguridad en coordinación con las áreas competentes de la Administración Pública Nacional” y “Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad”.
- Decreto nº 182/2019 (Boletín Oficial 12 de marzo de 2019), que abroga el Decreto Reglamentario 2628/2002.
- Resolución nº 829/2019 del 24 de mayo de 2019, de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros. Aprobación de la Estrategia Nacional de Ciberseguridad.
- Decreto nº 480/2019, del 11 de julio de 2019, que actualizó la conducción del Comité de Ciberseguridad (Modificación del Decreto nº 577/2017).
- Resolución nº 1523/2019, del 12 de septiembre de 2019. Definición de Infraestructuras Críticas.

- Disposición 1/2021, del 19 de febrero de 2021. Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad.
- Disposición nº 6/2021, del 8 de abril de 2021. Creación del Comité Asesor para el Desarrollo e Implementación de aplicaciones seguras.
- Decisión Administrativa nº 641/2021, del 28 de junio de 2021. Establece los requisitos mínimos de seguridad de la información para organismos públicos.
- Resolución 1/2023, del 2 de enero de 2023. Resolución 1/2023-1-APN-SDG#JGM. sobre procedimiento de Consulta respecto del documento Segunda Estrategia Nacional de Ciberseguridad.

Para abordar efectivamente estas áreas (y las demás identificadas en el documento), se requieren programas de capacitación tanto de alcance nacional, para asegurar disponibilidad para toda persona interesada en adquirir los conocimientos, como internacional, para tender nuevos lazos que a futuro pueden traducirse en colaboraciones fructíferas entre actores de la academia, de gobierno y del sector privado.

A continuación, exploramos un conjunto de programas de estudio existentes tanto en Argentina como en otros países de habla hispana, con el objetivo de analizar la oferta en cuanto a tipo de institución, duración y modalidad. Luego, brindaremos detalles acerca de las capacidades existentes en la Universidad Nacional del Sur en las temáticas relacionadas.

Programas relacionados en países de habla hispana

Como paso inicial para el diseño del programa propuesto, se realizó un relevamiento de programas y cursos de diferente alcance en países de habla hispana; los resultados se encuentran en la siguiente tabla:

País	Institución	Programa	Duración	Modalidad	Info
Argentina	CEDSA (Centro de estudios a distancia de Salta)	Tecnicatura Superior en Ciberseguridad	2 años	Online	Link
	Universidad Fasta (Fraternidad de Agrupaciones Santo Tomás de Aquino)	Licenciatura en Ciberseguridad (con título intermedio de Analista en ciberseguridad)	4 años 3 años título intermedio)	Online	Link
	Universidad de Palermo	Diplomatura en Ciberseguridad	16 semanas (96 hs.)	Online	Link
	UBA (Facultad de Ingeniería)	Maestría en seguridad informática	2 años	Presencial	Link
	UNSO (Universidad nacional Scalabrini Ortiz)	Tecnicatura universitaria en Ciberseguridad	3 años	Presencial	Link
	UNLP Facultad de Informática)	Especialización en redes y seguridad	80 horas ciclo introductorio – 340 hs.	Presencial	Link

			especialidad		
	ITBA (Instituto Tecnológico de Buenos Aires)	Certificado profesional en ciberseguridad	12 semanas / 42 hs.	Online	Link
	Academia Numen (Avalado por Universidad Atlántida Argentina)	Diplomatura en Ciberseguridad	320 hs.	Online	Link
Bolivia	Universidad Católica Boliviana San Pablo	Diplomado en Ciberseguridad y Protección de Datos	6 meses	Online	Link
Chile	Universidad Mayor	Técnico Universitario en Ciberseguridad	3 años	Online	**Link**
	Saint Leo University	Ingeniería/Grado Profesional en Ciberseguridad	2 años	Online	Link
	Instituto profesional Diego Portales	Ingeniero en informática (título intermedio de Técnico de nivel superior en Informática)	8 semestres (4 semestres título interm.)	Semi-pres.	Link
	CIISA (Instituto de Ciencias Tecnológicas de la Universidad San Sebastián)	Ingeniería en Ciberseguridad	4 años	Online / Presencial	Link
		Diplomado en ciberseguridad	108 hs.	Online	Link
		Técnico en ciberseguridad	2 años y medio	Online	Link
	IPP Instituto Profesional Providencia	Técnico superior en ciberseguridad	3 años	Online	Link
España	Universidad Nacional de Educación a Distancia (UNED)	Máster Universitario en Ciberseguridad	1 año	Online	Link
	Universidad Politécnica de Catalunya	Maestría en Ciberseguridad	1 año	Presencial	Link
	Universidad en Internet (Universidad de La Rioja)	Maestría en Ciberseguridad	1 año	Online	Link
	Universidad Politécnica de Madrid	Máster Universitario en Ciberseguridad	1 año	Presencial	Link
	Universidad Europea	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones	10 meses	Online	Link
México	Instituto Politécnico Nacional	Especialidad en Seguridad Informática y Tecnologías de la Información	1 año	Presencial	Link
		Maestría en Ingeniería en Seguridad y Tecnologías de la Información	N/D	Presencial	Link
	Centro de Estudios Superiores Navales	Posgrado Maestría en Seguridad Nacional	Online: 1400 hs. / Presencial: 2100 hs.	Online o Presencial	Link
	TEC Monterrey	Maestría en ciberseguridad	2 años y medio	Presencial	Link

	Universidad Autónoma de Nuevo León	Licenciatura en Seguridad en Tecnologías de Información	5 años	Híbrida	Link
Paraguay	Universidad Autónoma de Asunción	Diplomado en Ciberseguridad Nivel Inicial	5 meses	Online	Link
Perú	Techtitute	Maestría en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)	1 año	Online	Link
	Saint Leo University	Ingeniería/Grado Profesional en Ciberseguridad	2 años	Online	Link
	Universidad en Internet	Maestría en Ciberseguridad	1 año	Online	Link
	Cibertec	Curso: Ciberseguridad de Servicios en Internet	64 hs.	Online	Link
	CEUPE (Centro Europeo de Postgrado)	Maestría en seguridad de la información y tecnología	1 año	Online	Link
	CAEN (Centro de Altos Estudios Nacionales)	Maestría en Ciberseguridad y Gestión de la Información	18 meses	Presencial	Link
	Universidad Continental	Programa de Especialización en Ciberseguridad	128 hs.	Online	Link
Uruguay	Universidad ORT Uruguay	Diploma de especialización en ciberseguridad	1 año	Presencial	Link
		Curso: Hacking Ético y Gestión de incidentes	4 meses	Online	Link

Se puede apreciar una preponderancia casi total de propuestas en modalidad online y de duración corta (un año o menos). Otra característica que se repite con frecuencia es el carácter privado de las instituciones que las ofrecen, existiendo muy pocas por parte de universidades públicas como la Universidad Nacional del Sur. Si bien el programa será arancelado, se considera importante que las universidades nacionales argentinas ocupen el espacio de nexo entre la academia, la industria y el gobierno para nutrir no sólo a los participantes de los programas que ofrecen, sino también a los docentes investigadores que aportan sus conocimientos durante los dictados.

Experiencia de la UNS en Ciberseguridad y Sistemas Inteligentes

La Universidad Nacional del Sur, a través de su Departamento de Ciencias e Ingeniería de la Computación, posee amplias capacidades para ofrecer un programa de las características que se proponen. En particular, se destacan las colaboraciones internacionales que existen con laboratorios e individuos con larga trayectoria en Ciberseguridad, como lo son:

- Dr. V.S. Subrahmanian (Northwestern University, EE.UU.)
- Dr. Paulo Shakarian (Arizona State University, EE.UU.)
- Dr. Sushil Jajodia (George Mason University, EE.UU.)

- Dr. Andrea Pugliese (Università della Calabria, Italia)

A su vez, a través de convenios de colaboración, el DCIC también posee sólidas conexiones con empresas del medio, las cuales aportarán al programa en diferentes medidas.

La UNS tiene una amplia trayectoria en la Investigación, Desarrollo e Innovación en Inteligencia Artificial, contando con varios grupos de investigación con proyección internacional asociados a su vez con el Instituto de Ciencias e Ingeniería de la Computación (ICIC UNS–CONICET). Desde el punto de vista de la disciplina de la Inteligencia Artificial, la Ciberseguridad es un campo de aplicación formidable dado que, en general, presenta simultáneamente las características que hacen que la construcción de sistemas inteligentes eficientes y efectivos sea muy complejo, como lo son:

- La incertidumbre, que surge del manejo de inconsistencia, incompletitud y conocimiento probabilístico o inherentemente incierto.
- La necesidad de integrar fuentes heterogéneas de datos, información y conocimiento.
- Procesamiento de información en flujos potencialmente no acotados y de un caudal que implica la imposibilidad de almacenar los contenidos en su totalidad.
- Intratabilidad computacional de las soluciones que arrojan resultados exactos en casos generales. Esto obliga al estudio de restricciones que permitan garantizar la obtención de soluciones tratables dados los recursos de tiempo, espacio y poder de cómputo disponibles.
- La necesidad de desarrollar soluciones que sean interpretables (es decir, que exista la posibilidad de saber cómo derivan una solución) y explicables (concepto relacionado con los usuarios del sistema, los cuales pueden requerir explicaciones para poder tomar soluciones en base a los resultados arrojados).

Dados estos fundamentos, la Diplomatura contará con el apoyo de estos grupos para el dictado de los contenidos asociados a la Inteligencia Artificial, pero también para brindarle a éstos aplicaciones para las herramientas que desarrollan, creando así nuevos vínculos entre grupos de trabajo en ambas instituciones (DCIC e ICIC).

Por último, el programa contará con la intervención de expertos de otras Unidades Académicas de la UNS y otras UUNN para brindar aportes en temáticas más específicas, como por ejemplo Derecho, Economía y Humanidades. En el apartado 9 se incluye una lista de personas que ya fueron consultadas y expresaron interés en colaborar con el DCIC para el desarrollo del programa.

3) Objetivos

Objetivo general

La Diplomatura en Ciberseguridad Inteligente se propone como un espacio de educación continua, con foco en la actualización de saberes desde el punto de vista tecnológico, metodológico, y científico. Dado que el campo de la Ciberseguridad es amplio, se busca iniciar a los recursos humanos en la creación de capacidades, tanto en amplitud cognitiva como en profundidad conceptual, en los principales verticales que lo atraviesan. Se concibe como un programa de educación a distancia que sea accesible a personas que se encuentren ejerciendo actividades laborales sin la posibilidad de acercarse a la Universidad de manera física.

Objetivos específicos

El programa tiene los siguientes objetivos específicos:

- Formar a estudiantes de cualquier disciplina – con conocimientos básicos de Informática – en las competencias de la Ciberseguridad moderna, con foco en las necesidades del mercado laboral actual.
- Explorar la amplia gama de aristas que tiene la Ciberseguridad en sistemas socio-técnicos actuales, incluyendo no sólo la Seguridad Informática sino también los aspectos humanos y aquellos que surgen del despliegue de los sistemas inteligentes.
- Generar conciencia en los participantes sobre los peligros que supone tener medidas de ciberseguridad vulnerables.
- Brindarle a los participantes los conocimientos necesarios para una pronta inserción laboral en roles relacionados con la Ciberseguridad.
- Crear un espacio de educación continua que sirva de nexo entre la comunidad académica de la Universidad y los entornos profesionales de Argentina y otros países hispanohablantes, con el objetivo de facilitar colaboraciones de mutuo beneficio.

4) Certificación a otorgar y perfil del egresado

Diploma de finalización

Al culminar exitosamente el programa, los estudiantes recibirán un diploma en formato digital expedido por el Departamento de Ciencias e Ingeniería de la Computación de la Universidad Nacional del Sur, firmado por sus autoridades y la persona directora del programa. Habrá tres tipos posibles de diploma:

- **Aprobación:** Certifica que la persona asistió a un mínimo del 80% de las clases sincrónicas y resolvió satisfactoriamente las actividades de evaluación.
- **Aprobación con distinción:** Certifica que la persona asistió a un mínimo del 80% de las clases sincrónicas y resolvió exitosamente las actividades de evaluación, con un rendimiento destacado por el nivel de excelencia demostrado.
- **Asistencia:** Certifica que la persona asistió a un mínimo del 80% de las clases sincrónicas y tuvo acceso al material asincrónico del programa.

Se pondrá a disposición a su vez la opción de solicitar una copia impresa con firmas holográficas, con un costo adicional para cubrir la gestión y envío.

Perfil del egresado

Los egresados del programa tendrán una formación básica en una amplia gama de aspectos que componen la Ciberseguridad moderna, con un foco en alcanzar la capacidad de continuar su formación en los aspectos más específicos que requiera su desarrollo profesional.

En particular, el egresado estará capacitado para:

- Comprender los conceptos fundamentales de la Ciberseguridad, incluyendo gestión de amenazas, legislación y buenas prácticas, gestión de riesgos y gestión de identidades.
- Desplegar efectivamente herramientas defensivas, tales como la gestión de incidentes, Centros de Operaciones de Ciberseguridad, redes seguras y aquellas asociadas con el cómputo en la nube.
- Comprender el funcionamiento y alcance de las principales herramientas ofensivas, tales como pruebas de penetración, ingeniería social y ataques en redes OT e IoT.
- Realizar una gobernanza efectiva de la Ciberseguridad, incluyendo el desarrollo de un plan rector, cuestiones relacionadas con privacidad y gobernanza de datos, gestión de costos y planes de inversión en Ciberseguridad.
- Analizar las ventajas y riesgos asociados al despliegue de herramientas de Inteligencia Artificial en el ámbito de la Ciberseguridad, tanto en modalidad defensiva, ofensiva o relacionada con su gobernanza.

5) Modalidad de enseñanza

El contenido de la Diplomatura se dictará con una modalidad combinada que incluye encuentros sincrónicos y material para ser abordado de manera asincrónica. Se prevé un encuentro semanal de 3 horas (organizado en dos bloques, con un descanso entre ellos), y la puesta a disposición de material multimedial para ser abordado de manera asincrónica.

Todos los encuentros sincrónicos serán programados con anterioridad al comienzo de cada bloque trimestral de dictado, y serán grabados para que puedan acceder aquellas personas que no hayan podido asistir.

Las actividades se organizarán a través del Campus Virtual de la UNS, el cual se implementa a través de la plataforma de educación a distancia Moodle-UNS. En conjunto con el Campus Virtual – según la necesidad – se utilizarán plataformas de videoconferencia (tales como Zoom, Google Meet, Microsoft Teams, Gather, etc.) y de interacción y colaboración multimedial (tales como Discord y Slack), favoreciendo dentro de lo posible la utilización de espacios institucionales adquiridos por la UNS.

Los temas teóricos serán dictados por docentes a cargo en forma sincrónica y asincrónica. Se incluirán presentaciones de expertos reconocidos en ciberseguridad e inteligencia artificial, tanto de entornos académicos como de la industria. Dichas presentaciones serán complementadas durante las sesiones sincrónicas con la posibilidad de realizar un intercambio entre alumnos y docentes a fin de analizar en conjunto el material o la experiencia presentados, como así también evacuar dudas y enriquecer la discusión con experiencias propias. Para el material asincrónico, se utilizarán las funcionalidades de la plataforma de educación a distancia para poner a disposición de los alumnos material multimedial (texto, audio y video) de la manera más cómoda posible (explorando el uso de plataformas de uso generalizado tales como YouTube y Spotify, entre otras).

La aprobación de cada módulo se realizará en base a:

- El desarrollo y entrega de trabajos prácticos. La cantidad por módulo será definida según la naturaleza de los temas incluídos.
- Para garantizar que los alumnos que asisten a las clases sincrónicas estén al día con los contenidos, se requerirá la aprobación de un cuestionario periódico en línea (tipo quiz) durante el dictado del curso.

En cada caso, el umbral de aprobación se fijará en 60% de los puntos totales en los que se divide la actividad. Se utilizarán las funcionalidades de gestión de evaluaciones de la plataforma a distancia para incluir aleatoriedad en las actividades, administrar el tiempo y realizar actividades variadas. Cada instancia de evaluación estará acompañada por la posibilidad de recuperar en caso de no aprobar o no asistir a la misma.

Para aprobar la Diplomatura, se deberán aprobar todos los módulos y tener una asistencia mínima del 80% a las actividades sincrónicas.

6) Condiciones de ingreso

Los aspirantes deberán contar con título secundario. Para el caso de aquellas personas que no posean título o experiencia laboral relacionada con el área de informática, se requieren las siguientes condiciones para poder cursar exitosamente y aprovechar el contenido del Programa:

- Comprensión de conceptos básicos relacionados con la temática: Red de dispositivos, nube, algoritmo (concepto básico, pseudocódigo vs. lenguaje de programación), programa, proceso, sistema operativo, base de datos, almacenamiento.
- Tener habilidades analíticas (por ejemplo para comprender conceptos abstractos, resolver problemas de manera creativa, etc.).
- Tener capacidad para adquirir nuevos conocimientos y ponerlos en práctica rápidamente.

Los aspirantes deberán notificarse de estas condiciones al momento de inscribirse al programa, y poner a disposición del Comité Académico un curriculum vitae donde pueda apreciarse la experiencia del postulante en relación a ellas.

7) Plan de estudio

El plan de estudios está estructurado con una duración total de 24 semanas, el cual se organiza en dos bloques de 12 semanas cada uno (ver cronograma tentativo en la sección correspondiente de este documento).

El contenido se organiza en cuatro módulos que cubren cada una de las dimensiones principales del tema de estudio. A continuación, se brinda una descripción de los temas que componen cada módulo.

Módulo 1: Fundamentos

- **Introducción a la Ciberseguridad:** Motivación. Definiciones: Ciberseguridad, Seguridad Informática y Seguridad de la Información.
- **Legislación y buenas prácticas:** Leyes de protección de datos personales: Casos de estudio en diferentes países. Norma ISO 270001 y sus derivadas. Modelo NIST (National Institute of Standards and Technology de EE.UU.) y otros esfuerzos por parte del Gobierno del Reino Unido.
- **Ciclo de vida de gestión de amenazas:** Identificación de vulnerabilidades. Clasificación de vulnerabilidades. Priorización de vulnerabilidades. Mitigación de vulnerabilidades.
- **Gestión de riesgos:** Introducción a métodos de gestión de riesgos. Magerit (Gobierno de España) como caso de estudio. Activos. Criterios. Amenazas. Salvaguardas. Diseño de casos de uso. Revisión de casos de uso.
- **Gestión de identidades:** Concepto. Modelos. Elementos. Tecnologías.
- **Introducción a la Inteligencia Artificial:** Conceptos básicos. Las dos ramas de la Inteligencia Artificial, más su combinación. Aprendizaje automático: Procesamiento de

datos; Conceptos principales (Inferencia y Predicción); Categorías (supervisado, no supervisado, por refuerzo, representacional, evolutivo); Tipos (Regresión, Clasificación, Clustering); Desempeño (Matrices de confusión, precisión, cobertura, F1, curvas ROC). Dos ejemplos de modelos de aprendizaje automático: Árboles de decisión y Redes Neuronales. La National Vulnerability Database (NVD de NIST, EE.UU.) como fuente abierta de datos y conocimiento para alimentar el desarrollo y despliegue de herramientas inteligentes.

- **Intervenciones por parte de profesionales invitados.**

Módulo 2: Ciberseguridad Defensiva

- **Gestión de incidentes:** Detección de incidentes. Notificación de incidentes. Clasificación de incidentes. Análisis de incidentes. Contención, erradicación y recuperación ante incidentes. Reportes sobre incidentes.
- **Gestión de Centros de Operaciones de Ciberseguridad:** Identificación de activos y riesgos. Protección. Detección. Respuesta. Recuperación.
- **Gestión de redes seguras:** Introducción. Casos prácticos.
- **Gestión de microsegmentación:** Conceptos. Casos de uso. Tecnologías.
- **Ciberseguridad en la nube:** Introducción. Plataformas de protección de cargas de trabajo en la nube (CWPP). Gestión de postura de seguridad en la nube (CSPM). Uso de tecnologías.
- **Implementación de Zero Trust:** Concepto y filosofía. Actores y alcance. Modelos de implementación.
- **Inteligencia Artificial para Ciberseguridad Defensiva:** Aplicaciones de inteligencia artificial para detección de incidentes y amenazas. Uso de técnicas de inteligencia artificial para el engaño (“*deception*”) defensivo de actores maliciosos: honeypots, oscurecimiento de valor, exposición de intención. Detección de contenido y actores maliciosos en plataformas sociales.
- **Intervenciones por parte de profesionales invitados.**

Módulo 3: Ciberseguridad Ofensiva

- **Introducción a las pruebas de penetración:** Concepto. Tipo de pruebas. Modelos de informes.
- **Herramientas para pruebas de penetración:** Burp Suite, NMAP, Metasploit, Maltego, Ophcrack, entre otras.
- **Simulación de ataques de penetración:** Metodología para simulación de ataques. Tecnologías de simulación.

- **Ejercicios de pruebas de penetración:** Casos de uso.
- **Riesgos en OT e IoT:** Análisis de riesgo en redes OT. Análisis de riesgo en redes IoT.
- **Ingeniería Social:** Concepto. Técnicas de ingeniería social. Casos de uso.
- **Inteligencia Artificial para Ciberseguridad Ofensiva:** Aplicaciones de inteligencia artificial para identificación ofensiva de vulnerabilidades: Fuzzing, métodos formales, aprendizaje por refuerzo, grandes modelos de lenguaje (LLMs, como por ejemplo ChatGPT, Bard, Galactica, etc.) y otros de IA generativa multimodal. Ataques a sistemas inteligentes (Inteligencia Artificial Adversarial).
- **Intervenciones por parte de profesionales invitados.**

Módulo 4: Gobernanza de la Ciberseguridad

- **Desarrollo de plan rector de Ciberseguridad:** Diagnóstico. Adecuación. Mejora. Introducción a la norma ISO 27032.
- **Privacidad de la información y Gobernanza de datos:** Componentes del gobierno de datos. Actores. Órganos. Mejores prácticas. Blockchain.
- **Gestión de costos de ciberseguridad:** Metodología basada en riesgos. Análisis de costos. Modelo de costos.
- **Desarrollo seguro de Software:** Software on premise. Aplicaciones nativas de la nube.
- **Planes de Inversión en Ciberseguridad:** Concepto. Modelos de plan de inversión. Diseño de plan de inversión.
- **Inteligencia Artificial y gobernanza de la ciberseguridad:** Ciclo de vida de proyectos de inteligencia artificial para ciberseguridad. Documentación y entregables de proyectos de IA. Sistemas inteligentes fiables**:** Fundamentos, Realización, Evaluación. Inteligencia Artificial explicable e interpretable. Aspectos éticos del uso de la inteligencia artificial. Regulación de los sistemas inteligentes.
- **Intervenciones por parte de profesionales invitados.**

Bibliografía

Los profesores a cargo de cada módulo brindarán material bibliográfico actualizado, tales como artículos publicados en eventos científicos y tecnológicos, la prensa especializada, documentación preparada por empresas, como así también por expertos en las áreas pertinentes.

El núcleo del material se basa en las siguientes fuentes:

- McCumber, John. Assessing and managing security risk in IT systems: A structured methodology. CRC Press, 2004. Disponible en: https://dl.acm.org/doi/10.5555/1036257
- Helfrich, James N. Security for Software Engineers. CRC Press, 2018. Disponible en: https://doi.org/10.1201/9780429506475
- Takanen, A., Demott, J. D., Miller, C., & Kettunen, A. (2018). Fuzzing for software security testing and quality assurance. Artech House. Disponible en: https://ieeexplore.ieee.org/document/9100404
- Parisi, Alessandro. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd, 2019. Disponible en: https://www.packtpub.com/product/hands-on-artificial-intelligence-for-cybersecurity/9781789804027. Repositorio de código asociado disponible en: https://github.com/PacktPublishing/Hands-On-Artificial-Intelligence-for-Cybersecurity
- Ventre, Daniel. Artificial Intelligence, Cybersecurity and Cyber Defence. John Wiley & Sons, 2020. Disponible en: https://www.wiley.com/en-ie/Artificial+Intelligence,+Cybersecurity+and+Cyber+Defence-p-9781119788188
- Sikos, Leslie F., and Kim-Kwang Raymond Choo, eds. Data science in cybersecurity and cyberthreat intelligence. Cham: Springer, 2020. Disponible en: https://link.springer.com/book/10.1007/978-3-030-38788-4
- Sikos, L. F. (ed.) (2018) AI in Cybersecurity. Cham, Switzerland: Springer. DOI: 10.1007/978-3-319-98842-9. Disponible en: https://link.springer.com/book/10.1007/978-3-319-98842-9
- Mead, Nancy R., and Carol Woody: “Cyber Security Engineering: A Practical Approach for Systems and Software Assurance”. Addison-Wesley Professional, 2016. Disponible en: https://www.oreilly.com/library/view/cyber-security-engineering/9780134189857/
- International Standards Organization (ISO): Serie de normas internacionales ISO 27000:2022 – Gestión de la Seguridad de la Información. Disponible en: https://webstore.ansi.org/standards/iso/isoiec27000information
- Russell, S. and Norvig, P.: “Artificial Intelligence: A Modern Approach”, 4th edition, Pearson, 2020. Disponible en: https://aima.cs.berkeley.edu/global-index.html
- Ministerio de Administraciones Públicas, Gobierno de España: “MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, 2012. https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html
- European Commission: “Ethics Guidelines for Trustworthy AI”, 2018. https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf

- OWASP (Open Web Application Security Project). https://dev.owasp.org/projects/
- Jason Garbis, Jerry W. Chapman. Zero Trust Security, An Enterprise Guide. Berkeley, CA: Apress, 2021. Disponible en: https://link.springer.com/book/10.1007/978-1-4842-6702-8
- Liz Rice, Michael Hausenblas. Kubernetes Security. O'Reilly Media, Inc., 2018. Disponible en: https://www.oreilly.com/library/view/kubernetes-security/9781492039075/

8) Cronograma tentativo

El dictado se organiza en dos bloques de aproximadamente 3 meses cada uno, con clases a distancia en modalidad sincrónica una vez por semana con una duración de 3 horas reloj; la duración total del dictado en modalidad sincrónica es, por lo tanto, de *72 horas*. Además, se pondrá a disposición de los alumnos material multimedial que complementa a las clases y será abordado de manera asincrónica. Se espera que cada alumno le dedique 6 horas semanales al estudio del material, como así también a participar de las discusiones, actividades y evaluaciones en línea, lo cual arroja un total de *144 horas* a lo largo del programa. Así, en total, el cursado de la Diplomatura es de **216 horas**.

El cronograma del dictado de cada módulo se organiza de la siguiente manera:

Bloque 1:

- Comienzo: Primera mitad de abril
- Finalización: Finales de junio

Bloque 2:

- Comienzo: Segunda mitad de agosto
- Finalización: Mediados de noviembre

Distribución en semanas del dictado de módulos:

- Semanas 1 a 6 Bloque 1: Módulo 1
- Semanas 7 a 13 Bloque 1: Módulo 2
- Semanas 14 a 18 Bloque 2: Módulo 3
- Semanas 19 a 24 Bloque 2: Módulo 4

9) Comité Académico de Dirección y cuerpo docente

Se establecerá un Comité Académico de Dirección integrado por cinco (5) profesores de la UNS u otras Universidades Nacionales vinculados a la carrera, como así también actores del ámbito empresarial que sean idóneos. Uno de sus miembros actuará como Director de la Diplomatura.

Inicialmente, el Comité Académico de Dirección estará integrado por:

- Dr. Gerardo I. Simari (Universidad Nacional del Sur y CONICET)
- Dr. Marcelo Falappa (Universidad Nacional del Sur y CONICET)
- Dr. Carlos Chesñevar (Universidad Nacional del Sur y CONICET)
- Lic. Mariano P. Russo (CuBit, S.A. – Ex-Director Nacional de Cberseguridad)

Luego de la creación de la Diplomatura, se incorporará un quinto miembro al Comité Académico, el cual será externo a la UNS.

La diplomatura cuenta con el siguiente plantel docente que estará a cargo del dictado de clases sincrónicas y producción de material asincrónico:

- Lic. Leonardo De Matteis, Depto. de Cs. e Ing. de la Computación, UNS
- Dr. Fernando Delbianco, Departamento de Economia, UNS
- Lic. Gustavo C. Distel, Depto. de Cs. e Ing. de la Computación, UNS
- Dra. Elsa Estevez, Depto. de Cs. e Ing. de la Computación, UNS
- Dra. Maria Vanina Martinez, IIIA, CSIC, España
- Lic. José Moyano, Depto. de Cs. e Ing. de la Computación, UNS
- Lic. Mariano P. Russo, CuBit, S.A.
- Ing. Claudio A. Salamanca, Depto. de Cs. e Ing. de la Computación, UNS
- Dr. Gerardo I. Simari, Depto. de Cs. e Ing. de la Computación, UNS
- Dr. Axel Soto, Depto. de Cs. e Ing. de la Computación, UNS
- Mg. Alejandro Stankevicius, Depto. de Cs. e Ing. de la Computación, UNS

Asimismo, para contribuir con el dictado del contenido, se cuenta con la colaboración de los siguientes expertos profesionales con amplia experiencia en los tópicos cubiertos en la Diplomatura:

- Dr. Juan G. Corvalán, Facultad de Derecho UBA
- Dra. Lorena De Matteis, Departamento de Humanidades, UNS
- Dr. Mario A. Leiva, Depto. de Cs. e Ing. de la Computación, UNS
- Dr. José N. Paredes, The Black Puma, S.A.S.
- Ab. Alejandro Puglia, Ministerio de Justicia y Seguridad, CABA
- Mg. Pamela Tolosa, Departamento de Derecho, UNS
- Mg. Julio Ardita, Consultor, ex Socio Deloitte
- Carlos Ibañez, Consultor, NSG Corp
- CA Pablo Sorrentino, Comodoro de Marina Director General de Comunicaciones, Informática y Ciberdefensa de la Armada Argentina.

10) Presupuesto

Principales componentes presupuestarias

La Diplomatura tiene los siguientes gastos de funcionamiento previstos:

- **Pago de licencias:** Software específico, plataformas de videoconferencia y comunicación, etc.
- **Honorarios (calculados por hora):**
    - Persona que cumpla el rol de *Administrador General* del programa.
    - Persona que cumpla el rol de *Community Manager* para llevar adelante campañas en redes sociales, responder consultas, etc.
    - Profesores para el preparado y dictado de clases sincrónicas.
    - Profesores para el preparado y producción de material asincrónico.
    - Auxiliares de práctica para el preparado y corrección de actividades prácticas y de evaluación.
    - Editores de audio y video.
    - Ayudantes de videoconferencia (punto de contacto con los alumnos, moderador general, monitoreo del chat, etc.).
- **Becas** parciales y/o totales para alumnos (por ejemplo, internas a la UNS y/o DCIC para nutrir el plantel docente futuro, Municipalidad de Bahía Blanca, Polo Tecnológico Bahía Blanca, para sponsors, etc.).
- **Campañas de marketing** en plataformas sociales.

El programa será autofinanciado; es decir, será financiado principalmente por las matrículas de los participantes y, en la medida de la disponibilidad, por sponsors.

Cálculo de matrícula

Antes del comienzo de cada cohorte, se realizarán cálculos pesimistas, intermedios y optimistas de la cantidad de participantes con los que se contará; éstos se harán en base a llamados a preinscripción y el conocimiento obtenido de otras cohortes y de programas en la UNS. Una vez obtenidos dichos valores y la suma de los gastos esperados, se podrá fijar el monto que deberá abonar cada participante, contemplando una adecuada gestión del riesgo.

Financiación

Las siguientes componentes presupuestarias requieren alguna medida de financiación:

- Pago de licencias
- Campañas de marketing en plataformas sociales

Las medidas de financiación serán cubiertas por fondos provenientes de sponsors o, en su defecto, por adelantos provistos por el Departamento de Ciencias e Ingeniería de la Computación. En ambos casos, los gastos que se realicen serán calculados en función de la disponibilidad de fondos. En el caso de licencias, se dará preferencia a herramientas que dispongan de versiones gratuitas o que ya estén disponibles en la UNS.

A su vez, los honorarios serán abonados una vez que se disponga de fondos, sean de sponsors o de matrículas. Esto implica que las personas deban comenzar a trabajar antes de recibir sus honorarios, lo cual es una práctica habitual en este tipo de programas.

Sponsors

Se buscará la participación en la Diplomatura de una serie de sponsors que colaborarán tanto con material para el dictado de los diferentes módulos como con aportes de índole económica. Como retribución, se ofrecerán becas, la inclusión de logos, spots, etc. en el material de la Diplomatura, como así también espacio en clases sincrónicas o material asincrónico para que la empresa divulgue entre los participantes sus prácticas asociadas a la temática, oportunidades laborales u otro contenido que el comité académico considere apropiado. Se prevé establecer una serie de niveles (por ejemplo: oro, plata, bronce), cada uno con un nivel de aporte y de acceso a espacios acorde.

La siguiente lista incluye potenciales empresas sponsor, según los vínculos ya existentes con los integrantes del comité académico:

- Red Hat
- Illumio
- CuBIt
- Radical
- IBM
- Oracle
- Amazon
- Tenable