G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S

"2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Resolución

Número: RESOL-2026-9-GCABA-IUS

Buenos Aires, Lunes 9 de Marzo de 2026

Referencia: Sustituye el Plan de Estudios de la Carrera de Posgrado "Especialización en Gobernanza y Gestión de la Seguridad Informática" aprobado por el artículo 2 de la Resolución N° 18-GCABA-IUS/25.

VISTO:

La Ley Nacional N° 24.521, la Ley N° 5.689 (texto consolidado por Ley N° 6.764), el Decreto N° 507-PEN/23, las Resoluciones N° 14-GCABA-IUS/24, N° 23-GCABA-IUS/24, N° 13-GCABA-IUS/25 y N° 18-GCABA-IUS/25, el Expediente Electrónico N° 11799953-GCABA-SADIUS/26, y

CONSIDERANDO

Que mediante Ley N° 5.689 (texto consolidado según Ley N° 6.588) se creó el Instituto Universitario de Seguridad -IUSE-, como institución de educación superior con jurisdicción en la Ciudad Autónoma de Buenos Aires, cuya oferta académica se encuentra circunscripta al área disciplinar de la Seguridad, en el marco de la Ley Nacional de Educación Superior N° 24.521;

Que el IUSE tiene como visión posicionarse como Institución Universitaria innovadora signada por el paradigma de seguridad humana, con reconocimiento en el nivel jurisdiccional nacional, regional e internacional en materia de investigación, formación e inserción de profesionales en el campo de la seguridad;

Que el artículo 69 de la citada Ley Nacional N° 24.521 reza: *"Los títulos y grados otorgados por las instituciones universitarias provinciales tendrán los efectos legales previstos en la presente ley, en particular los establecidos en los artículo 41 y 42, cuando tales instituciones: a) Hayan obtenido el correspondiente reconocimiento de Poder Ejecutivo Nacional, el que podrá otorgarse previo informe de la Comisión Nacional de Evaluación y Acreditación Universitaria, siguiendo las pautas previstas en el artículo 63…";*

Que por medio del Decreto N° 507/2023 el Poder Ejecutivo Nacional otorgó el reconocimiento a esta casa de estudios, en los términos del mencionado artículo 69, inciso a), con la recomendación realizada por la Comisión Nacional de Evaluación y Acreditación Universitaria –CONEAU-;

Que por su parte a través de la Resolución N° 14-GCABA-IUS/24 –modificada mediante Resolución Nº 23-GCABA-IUS/24– se aprobó el Estatuto Provisorio del IUSE, estableciéndose en su artículo 57 que *"El régimen de enseñanza y aprendizaje abarcará los siguientes niveles: … c) formación de posgrado";*

Que asimismo, el mencionado Estatuto Provisorio dispone en su artículo 19 inciso j) que es atribución del Consejo Superior *"aprobar los títulos, carreras, planes de estudio, programas, proyectos académicos, proyectos de investigación y de extensión, transferencia y servicios, a propuesta del Rector"*, siendo en la misma línea, facultad del Rector conforme el artículo 27 inciso h) *"proponer al Consejo Superior la creación, suspensión o cierre de carreras de pregrado, grado y posgrado";*

Que la Disposición Transitoria N° 6 del mencionado Estatuto, estipula que hasta tanto se lleve a cabo la normalización del Instituto Universitario, su gobierno será asumido por el Rector Organizador, quien podrá ser eximido del cumplimiento de los requisitos establecidos en el artículo 24, y que, a su vez, ejercerá las funciones del Consejo Superior y demás órganos de gobierno y gestión, o las delegará en el Vicerrector y/o Secretarios;

Que por Resolución N° 13-GCABA-IUS/25 fue aprobado el *"Reglamento de Posgrado del Instituto Universitario de Seguridad"*, a efectos de contar con un marco normativo que establezca los criterios, lineamientos y procedimientos que regulan la organización y funcionamiento de los programas de Posgrado ofrecidos por esta alta casa de estudios;

Que en esa inteligencia, y a solicitud del Director de Posgrado en el ejercicio de sus funciones, previa intervención de la Secretaría Académica y de la Dirección General de Planeamiento y Desarrollo Universitario, mediante Resolución N° 18-GCABA-IUS/25 se aprobó la Carrera de Posgrado *"Especialización en Gobernanza y Gestión de la Seguridad Informática";*

Que el artículo 26 del citado Reglamento de Posgrado prescribe que *"En el caso de carreras de posgrado, tras su aprobación, la Dirección de Posgrado, en conjunto con la Dirección General de Planificación y Desarrollo Universitario, gestionará los trámites correspondientes ante la Secretaría de Educación y la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU), o los organismos que en el futuro los reemplacen, con el fin de obtener su reconocimiento y acreditación";*

Que en dicho marco, desde la Secretaría Académica a través de la NO-2026-11799670-GCABA-SAIUS e IF-2026-11798344-GCABA-SAIUS, se elevó a consideración de esta instancia una propuesta de adecuación integral del diseño curricular y la actualización del plan de estudios de la citada Carrera de Posgrado *"Especialización en Gobernanza y Gestión de la Seguridad Informática"*, en virtud de lo observado en el Informe de Evaluación emitido por la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU) que luce por IF-2026-11783480-GCABA-SADIUS en el Expediente Electrónico citado en el visto, y en el Expediente EX-2025-56445017-APN-DAC#CONEAU por IF-2026.14038153-APN-DAC#CONEAU, dado que en tal contexto se dio vista a esta institución a fin de subsanar aspectos de la citada carrera de especialización, vinculados principalmente con: la organización y secuenciación progresiva del plan de estudios; la incorporación de contenidos fundamentales para la gobernanza y gestión de la seguridad informática; la reformulación y fortalecimiento de las actividades prácticas y la actualización y ampliación de las referencias bibliográficas;

Que en la mencionada propuesta, la Dirección de Posgrado junto con la coordinación de la carrera, han desarrollado un proceso sistemático de revisión académica y técnica del diseño curricular, atendiendo de manera exhaustiva cada una de las observaciones formuladas, con el objeto de reconfigurar la estructura curricular asegurando una progresión formativa coherente y gradual, fortalecer la articulación entre contenidos teóricos y actividades prácticas, actualizar y diversificar la bibliografía obligatoria y complementaria y consolidar la coherencia entre perfil del egresado, objetivos de la carrera y organización curricular, configurando así un nuevo diseño curricular que mantiene la identidad académica de la carrera, pero fortaleciendo sustantivamente su coherencia interna, rigurosidad disciplinar y adecuación a los estándares vigentes para carreras de posgrado, garantizando el cumplimiento de los criterios de calidad establecidos por la CONEAU;

Que la Directora Legal y Técnica del Instituto Universitario de Seguridad intervino en el marco de su competencia emitiendo el pertinente Dictamen Legal;

Que en virtud de lo expuesto, se impone dictar el acto administrativo correspondiente a efectos readecuar integralmente el diseño curricular y la actualizar el plan de estudios de la Carrera de Posgrado *"Especialización en Gobernanza y Gestión de la Seguridad Informática"*, conforme los criterios establecidos por la CONEAU.

Por ello, en uso de las facultades que le son propias,

EL RECTOR ORGANIZADOR

DEL INSTITUTO UNIVERSITARIO DE SEGURIDAD

RESUELVE:

Artículo 1°. – Sustituir el Plan de Estudios de la Carrera de Posgrado *"Especialización en Gobernanza y Gestión de la Seguridad Informática"* aprobado por el artículo 2 de la Resolución N° 18-GCABA-IUS/25, por el IF-2026-11798344-GCABA-SAIUS, que forma parte integrante de la presente Resolución, atendiendo a las observaciones efectuadas en el informe de evaluación de la Comisión Nacional de Evaluación y Acreditación Universitaria.

Artículo 2°. – Publíquese en el Boletín Oficial de la Ciudad Autónoma de Buenos Aires y comuníquese al Vicerrector, a la Secretaría de Administración, a la Secretaría Académica, a la Dirección de Posgrado y a la Dirección General de Planeamiento Universitario del Instituto Universitario de Seguridad. Cumplido, archívese.

Digitally signed by JUAN BAUTISTA MAHIQUES
Date: 2026.03.09 13:37:35 ART
Location: Ciudad Autónoma de Buenos Aires

Juan Bautista Mahiques
Rector
INSTITUTO UNIVERSITARIO DE SEGURIDAD
AREA JEFE DE GOBIERNO

Digitally signed by Comunicaciones Oficiales
Date: 2026.03.09 13:37:41 -03:00

Posgrado | Especialización en Gobernanza y Gestión de la Seguridad Informática
PLAN DE ESTUDIOS

1. Fundamentación

1.1 Posicionamiento epistemológico

Seguridad informática, seguridad cibernética, ciberseguridad, son conceptos que aluden a un proceso que no se agota en el plano técnico, sino que se encuentra influenciado por aspectos normativos, éticos, económicos y organizacionales. En general, los propósitos de la seguridad informática son, por un lado, proteger frente a fallas y amenazas cibernéticas y, por otro lado, fomentar el desarrollo económico y social basado en las Tecnologías de la Información y la Comunicación (TIC), todo ello en un marco de derecho a la privacidad y protección de datos personales (BID, 2016)[1].

El crecimiento exponencial del uso de las TIC ha traído grandes beneficios, así como desafíos permanentes en un mundo globalizado. Su integración a la vida y la economía son claves para el funcionamiento actual y el desarrollo tecnológico de la sociedad y las instituciones que la componen. Sin embargo, en nuestro país se observa una limitada capacidad de respuesta ante amenazas cibernéticas: a pesar de los avances en el marco jurídico, aún se plantean numerosos retos en materia de cultura organizacional y formación de recursos humanos.

A medida que aumentan los riesgos, y con ellos la sofisticación y el profesionalismo del cibercrimen, los ciudadanos, los gobiernos y las empresas se vuelven más vulnerables. Las amenazas cibernéticas tienen el potencial de comprometer la disponibilidad, integridad y capacidad de recuperación de las infraestructuras críticas para el desarrollo humano. Asimismo, la complejidad que plantea la transnacionalización de los delitos informáticos requiere de un esfuerzo multidimensional para abordarlos.

En este sentido, un líder en seguridad informática debe contar con las habilidades suficientes para comprender y aplicar los principios, herramientas y metodologías desde una perspectiva multidisciplinaria, que integre las dimensiones jurídicas, éticas y tecnológicas, sociales y económicas de la ciberseguridad.

La relevancia epistemológica de esta Especialización en Gobernanza y Gestión de la Seguridad Informática radica en su capacidad para integrar y articular conocimientos teóricos y prácticos que abordan los desafíos actuales de la ciberseguridad, promoviendo un enfoque interdisciplinario que vincula el diseño de arquitecturas seguras de redes y sistemas, la prevención a través de auditorías y estrategias de mitigación de riesgos, y la intervención e investigación cuando el incidente ha ocurrido.

Resulta esencial formar profesionales capaces de gestionar la seguridad informática desde una visión integral de gobernanza que, basándose en un marco conceptual riguroso, se centre en proporcionar las herramientas para actuar ante escenarios reales.

[1] Banco Interamericano de Desarrollo (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016.* Observatorio de la Ciberseguridad en América Latina y El Caribe.

En definitiva, la seguridad informática no es sólo una disciplina estratégica para proteger operaciones y fortalecer la confianza en el ecosistema digital, sino también un pilar fundamental para garantizar un desarrollo sostenible y seguro que beneficie tanto a las organizaciones como a la sociedad en su conjunto.

1.2 Antecedentes y pertinencia de la creación de la carrera

El Instituto Universitario de Seguridad (IUSE), con sede en la Ciudad Autónoma de Buenos Aires, fue creado mediante la Ley N° 5.689 el 17 de noviembre de 2016, promulgada por el Decreto N° 646/016 y publicada en el Boletín Oficial de la Ciudad de Buenos Aires. Desde sus inicios, el IUSE se ha orientado a ofrecer formación de grado en el área de la seguridad, con un fuerte énfasis en el compromiso ético, la innovación y el respeto por los derechos humanos. En 2023, el IUSE fue reconocido como Institución Universitaria mediante el Decreto PEN N° 507/2023, tras la evaluación favorable de la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU) en el año 2020.

El IUSE tiene como antecedente institucional al Instituto Superior de Seguridad Pública (ISSP) el cual, además de capacitar a miembros de la Policía y el Cuerpo de Bomberos de la Ciudad, ofrece programas de formación técnica y capacitación para diversos actores del Sistema Integral de Seguridad Pública. La experiencia acumulada en el ISSP permitió identificar la necesidad de ampliar la oferta educativa en seguridad, adoptando un enfoque integral y multidisciplinar que no se limitara a la formación policial. En este contexto, el IUSE se configura como una pieza clave en la formación continua de todos los actores de la seguridad pública en la Ciudad de Buenos Aires, contribuyendo con conocimiento técnico y científico a la comunidad y a los cuerpos de seguridad.

Desde su creación, el IUSE ha planificado su oferta académica en ciclos de estudio que incluyen carreras de tecnicaturas universitarias y licenciaturas, así como ciclos de complementación curricular, además de prever en su proyecto institucional programas de posgrado que complementen estas propuestas. A la fecha, se dictan las tecnicaturas en Seguridad Pública, en Investigación Criminal, en Criminalística, y en Protección contra Incendios. Sobre las carreras de grado, el instituto ofrece la Licenciatura en Seguridad Pública, la Licenciatura en Criminalística, la Licenciatura en Protección Contra Incendios y la Licenciatura en Investigación Criminal, con los correspondientes ciclos de complementación curricular, orientadas a formar profesionales competentes en el análisis, diseño y ejecución de políticas de seguridad ciudadana, así como en la prevención de riesgos. Estas licenciaturas fomentan una visión interdisciplinaria, con un enfoque humanista y un claro compromiso con el Estado de Derecho y los derechos humanos. Sumado a ello, se incorporan desde el área de extensión diplomaturas de pregrado que constituyen cursos cortos y enfocados en brindar conocimientos prácticos y habilidades concretas especializadas en áreas específicas de la seguridad.

La creación de la Especialización en Gobernanza y Gestión de la Seguridad Informática responde a una necesidad concreta en el campo, aportando una perspectiva multidimensional para la gestión organizacional y, a la vez, un enfoque disciplinar específico en gestión de riesgos, auditoría y análisis forense en materia de seguridad informática. Esta orientación resulta pertinente en tanto contribuye al fortalecimiento de capacidades para la formulación

de estrategias preventivas y de intervención, tanto en organizaciones públicas como privadas. De igual forma, el perfil del graduado propuesto se alinea en su totalidad con los objetivos del IUSE, aportando saberes y competencias específicas para los gestores de la seguridad informática a nivel local y nacional.

2. Organización de la carrera

2.1. Denominación: Especialización en Gobernanza y Gestión de la Seguridad Informática.

2.2. Título que otorga: Especialista en Gobernanza y Gestión de la Seguridad Informática.

2.3 Objetivos de la carrera

1. Formar a profesionales especializados en seguridad informática, desde una perspectiva multidimensional, que incluya aspectos legales, éticos, tecnológicos, económicos y sociales. Los graduados estarán capacitados para comprender y gestionar de manera estratégica las interacciones entre estos aspectos en organizaciones públicas y privadas, con el propósito de liderar de manera efectiva los desafíos emergentes de la ciberseguridad.

2. Fomentar el diseño y la gobernanza de estrategias de seguridad informática que optimicen la toma de decisiones, a través de un enfoque integrado de la auditoría, la gestión de riesgos, la informática forense y la comunicación en situaciones de crisis, con el objeto de prevenir y actuar ante amenazas cibernéticas, y garantizar la integridad y protección de los sistemas de información.

2.4 Perfil del egresado

El graduado de la Especialización en Gobernanza y Gestión de la Seguridad Informática estará preparado para liderar áreas, equipos y programas de seguridad informática en organizaciones tanto públicas como privadas. Con un enfoque integral y multidisciplinario, comprenderá las dimensiones jurídicas, éticas y tecnológicas de la ciberseguridad, siendo apto para desempeñarse en la gestión de riesgos, auditorías de sistemas informáticos y respuestas ante ataques y delitos informáticos. Además, el graduado será capaz de liderar estrategias de comunicación institucional de manera efectiva en situaciones de crisis.

Al finalizar la Especialización, los participantes habrán adquirido un conjunto de conocimientos y habilidades que les permitirán:

- Supervisar, diseñar y desarrollar políticas de ciberseguridad que integren la gestión de riesgos, la auditoría y el análisis forense, alineadas con los objetivos estratégicos de la organización, con el propósito de garantizar la protección de la información y la infraestructura crítica.
- Implementar políticas y programas de seguridad informática que integren los aspectos normativos, éticos, tecnológicos, sociales y económicos relacionados con la ciberseguridad, con el fin de promover prácticas responsables en el entorno digital.
- Liderar equipos de seguridad informática, con la gestión de recursos humanos y presupuestos, y el fomento de una conducción organizacional basada en la toma de decisiones informada y la comunicación efectiva en situaciones de riesgo y crisis en el contexto de ciberseguridad.

2.5 Tipo de carrera: Posgrado.

2.6 Modalidad de dictado

La carrera se dicta bajo modalidad presencial con asignaturas de carácter trimestral. La interacción pedagógica combina clases presenciales físicas en el espacio-aula en sede y presenciales sincrónicas en el espacio-aula de video comunicación.

2.7 Requisitos de admisión

Podrán solicitar la admisión a la Especialización en Gobernanza y Gestión de la Seguridad Informática, quienes acrediten alguna de las situaciones que se detallan a continuación:

a) Egresados de carreras de Nivel Superior Universitario, cuya obtención se derive de un plan de estudios con una duración mínima de cuatro (4) años y dos mil seiscientas (2.600) horas reloj; en el área de ciencias sociales y/o disciplinas específicas asociadas al derecho y la seguridad, tales como: Seguridad Pública, Seguridad Ciudadana, Criminalística, Investigación Criminal, Abogacía y Ciencia Política; así como en el área de informática, tales como: Ciencias de la Computación, Sistemas de Información, Ingeniería en Sistemas, Ingeniería en Software.

b) Egresados de carreras de Nivel Superior Universitario, cuya obtención se derive de un plan de estudios con una duración mínima de cuatro (4) años y dos mil seiscientas (2.600) horas reloj; de disciplinas no mencionadas en el punto a) que en su desempeño profesional se vinculen con la temática de la Especialización.

c) Graduados de universidades extranjeras que otorguen títulos reconocidos de carreras de grado universitario en línea con lo referido en los puntos a) y b). En el caso de que los estudios de grado se hubieran cursado en universidades extranjeras, la admisión a la Carrera de Especialización no implicará la reválida de los títulos previamente obtenidos.

d) Aquellas personas que no cuenten con título universitario de grado o de nivel superior no universitario de cuatro (4) años de duración mínima, podrán ser admitidas con carácter excepcional, de acuerdo con lo establecido en el artículo 39 bis de la Ley de Educación Superior N° 24.521 cumplimentando los requisitos compensatorios que el Comité Académico considere necesarios.

Los interesados deberán presentar una solicitud de admisión dirigida a la Coordinación de la Carrera adjuntando título/s y diploma/s que certifiquen los grados obtenidos y un currículum vitae actualizado. La Coordinación de la carrera decidirá sobre la admisión de los candidatos con base en una evaluación de los antecedentes presentados, quedando a su criterio citar a los postulantes a una entrevista personal.

Los requisitos administrativos de inscripción se encuentran establecidos en el Reglamento de Posgrado.

2.8 Inserción institucional y lugar de dictado

La carrera se inserta institucionalmente en la Secretaría Académica - Dirección de Posgrado.

Las actividades se llevarán a cabo en la sede de la institución localizada en Av. Roca N° 4.170, Ciudad Autónoma de Buenos Aires.

3. Plan de Estudios

3.1 Estructura

El plan de estudios tiene una duración de un (1) año y medio, distribuido en cinco (5) trimestres. La estructura curricular responde a un plan de estudios semi estructurado compuesto por nueve (9) materias y un Taller de Trabajo Integrador Final (TIF), en un tramo común a todos los estudiantes, y una materia electiva (a elegir entre un menú de asignaturas disponibles en los posgrados afines dictados en la casa de estudios), la cual puede tener treinta y seis (36) o cuarenta y ocho (48) horas. En consecuencia, la carga horaria mínima del plan de estudios es de cuatrocientas cuarenta y un (441) horas mientras que la máxima alcanza las cuatrocientas cincuenta y tres (453) horas, según la selección de asignatura electiva que se realice y sin contar las horas dedicadas a la elaboración del trabajo integrador final.

El plan se organiza en tres trayectos curriculares. A saber:

- Formación Básica: Este primer trayecto ofrece las bases conceptuales y metodológicas para la comprensión del campo de la seguridad informática. Se abordan los fundamentos técnicos, normativos, éticos y sociales, necesarios para que los estudiantes adquieran una visión integral de las problemáticas de seguridad informática. Además, los estudiantes se introducen en las tecnologías y prácticas esenciales para proteger redes y sistemas dentro de infraestructuras críticas.
- Formación Específica: En este trayecto, los estudiantes se sumergen en los temas específicos de la Especialización, como el régimen legal sobre manejo y protección de datos, las principales formas de cibercrimen y de los marcos jurídicos y procesales que sustentan su investigación y persecución penal. Además, se abordan las oportunidades y el uso estratégico del Big Data para la gobernanza en ciberseguridad. La formación profesional incluye el estudio de estrategias comunicacionales que permitan responder eficazmente en situaciones de riesgo y crisis.
- Formación Práctica: Este trayecto está centrado en el diseño y desarrollo de políticas y programas de ciberseguridad desde un rol de liderazgo, con integración de la gestión de riesgos, la auditoría y el análisis forense. Con un enfoque práctico, a través del desarrollo de proyectos de planificación, estudios de casos y simulaciones, los estudiantes se enfrentan a escenarios reales de gestión de intervenciones en seguridad informática, con el fin de desarrollar competencias para el análisis, la planificación, la ejecución y la supervisión de políticas y programas en este ámbito, tanto en organizaciones públicas como privadas.

Taller de Trabajo Integrador Final

El Taller para el Trabajo Integrador Final incluye seis (6) encuentros a lo largo de un trimestre, con el objeto de acompañar al alumno en la integración de los saberes adquiridos y la elaboración de una propuesta de Trabajo Integrador Final.

Requisito de Graduación

Para graduarse, el estudiante deberá aprobar la totalidad de las asignaturas del plan de estudios y presentar y aprobar un Trabajo Integrador Final (TIF) en los términos establecidos en el Reglamento de Trabajo Integrador Final, como así también cumplimentar con las exigencias o requisitos establecidos en la normativa vigente del IUSE.

El TIF será individual y escrito, y podrá adoptar diversos formatos, tales como: plan de auditoría informática, informes periciales, propuesta de intervención, plan de monitoreo, plan de comunicación, ensayo, estudio de caso o estudio comparado, u otros que oportunamente se establezcan en el Reglamento de Trabajo Integrador Final, siempre que realicen un aporte a la disciplina. Se espera que este trabajo evidencie la integración de los aprendizajes adquiridos durante la carrera.

El TIF deberá entregarse en un plazo máximo de doce (12) meses desde la finalización de la cursada y la aprobación de todas las asignaturas. Los trabajos serán dirigidos por un docente de la carrera, a elección del alumno, y evaluados por un tribunal convocado para tal fin. No se requiere una instancia de defensa oral. Las especificaciones sobre su desarrollo se encuentran establecidas en el Reglamento de Trabajo Integrador Final.

3.2 Malla curricular

Trayecto	Trimestre	Materia	Modalidad	Carga horaria total de interacción pedagógica					Cant. de semanas	Carga horaria semanal de interacción pedagógica
				Total	Prácticas	Teóricas	En sede	Sincrónicas		
Formación Básica	1	1. Introducción a la seguridad informática	Teórico - Práctico	36	10	26	27	9	12	3
Formación Básica	1	2. Fundamentos de ciberseguridad en redes e infraestructuras críticas	Teórico - Práctico	48	10	38	32	16	12	4
Formación Específica	2	3. Derecho informático	Teórico - Práctico	48	10	38	32	16	12	4
Formación Práctica	2	4. Gestión de riesgos y auditoría de seguridad informática	Teórico - Práctico	48	30	18	32	16	12	4
Formación Específica	3	5. Política criminal y cibercrimen	Teórico - Práctico	36	10	26	27	9	12	3
Formación Específica	3	6. Gobernanza de datos y seguridad informática	Teórico - Práctico	36	10	26	27	9	12	3
Formación Práctica	4	7. Diseño de estructuras y programas en seguridad informática	Teórico - Práctico	48	30	18	32	16	12	4
Formación Específica	4	8. Comunicación y gestión de crisis en seguridad	Teórico - Práctico	36	10	26	27	9	12	3
Formación Práctica	5	9. Informática forense	Teórico - Práctico	48	30	18	32	16	12	4

Formación Práctica	5	10. Taller de TIF	Práctico	21	21	0	21	0	6	3,5
				405	**171**	**234**	**289**	**116**		
Total Tramo Común				**100%**				**29%**		
Electiva opción 1*										
Formación Específica		11. Electiva	Teórico - Práctico	36	x	X	27	9	12	3
				441			**316**	**125**		
Total				**100%**				**28%**		
Electiva opción 2*										
Formación Específica		11. Electiva	Teórico - Práctico	48	x	X	32	16	12	4
				453			**321**	**132**		
Total				**100%**				**29%**		

* Con el objetivo de fomentar la interdisciplinariedad en el perfil de los egresados de carreras de posgrado IUSE, el estudiante deberá optar por cursar en cualquier momento de su trayecto de formación una asignatura de las ofertadas en otras carreras de posgrado que se dicten en la casa de estudios, cuyo listado será actualizado y definido para cada cohorte por el Comité Académico, o bien en otra institución universitaria a través del sistema de créditos, conforme el presente plan de estudios y/o la normativa que en un futuro lo reemplace. Esta puede corresponder a un curso de treinta y seis (36) o cuarenta y ocho (48) horas, respetando la misma distribución horaria a la establecida en las dos opciones de la malla curricular. Debido a que el IUSE es un Instituto especializado en el abordaje de la seguridad se garantiza que la oferta disponible se encuentre vinculada a la disciplina.

3.3 Correlatividades

Trayecto	Trimestre	Materia	Correlatividades
Formación Básica	1	1. Introducción a la seguridad informática	
Formación Básica	1	2. Fundamentos de ciberseguridad en redes e infraestructuras críticas	
Formación Específica	2	3. Derecho informático	
Formación Práctica	2	4. Gestión de riesgos y auditoría de seguridad informática	
Formación Específica	3	5. Política criminal y cibercrimen	Materia 4
Formación Específica	3	6. Gobernanza de datos y seguridad informática	
Formación Práctica	4	7. Diseño de estructuras y programas en seguridad informática	Materias 2 y 4
Formación Específica	4	8. Comunicación y gestión de crisis en seguridad	
Formación Práctica	5	9. Informática forense	Materias 3, 4 y 5
Formación Práctica	5	10. Taller de TIF	Materias 1 a 8
Formación Específica		11. Electiva	

3.4 Sistema de créditos universitarios

Con el objeto de visibilizar la labor autónoma que realizan los estudiantes en sus trayectos formativos y con la intención de ajustar la duración teórica de la carrera con su duración real se incorpora la noción de créditos universitarios.

Los créditos representan la unidad de tiempo total de trabajo académico que estimativamente dedican los/as estudiantes para alcanzar los objetivos formativos de cada una de las actividades curriculares que componen el plan de estudios. En esta unidad de tiempo se incluyen: a) las horas de docencia o interacción pedagógica docente-estudiantes, independientemente de la modalidad, y b) las horas de trabajo autónomo del estudiante que son adicionales a las de docencia o interacción docente-estudiantes. Al respecto, un (1) crédito equivale a veinticinco (25) horas reloj de trabajo total del/la estudiante.

Para esta Especialización se calcula una dedicación del alumno equivalente a dos mil trescientas un (2.301) horas totales, que representan noventa y dos (92) créditos; los cuales se distribuyen durante cinco (5) trimestres de dictado de las asignaturas, más los doce (12) meses otorgados para la elaboración del TIF.

Por un lado, la carga horaria mínima de interacción pedagógica del plan de estudios es de cuatrocientos cuarenta y un (441) horas, para lo que se estima una dedicación horaria de trabajo autónomo del alumno de mil quinientas diez (1.510) horas, correspondiente a setenta

y ocho (78) créditos. Por otro lado, el alumno deberá dedicar trecientas cincuenta (350) horas, correspondientes a catorce (14) créditos, a la elaboración del Trabajo Integrador Final una vez finalizadas y aprobadas todas las asignaturas comprendidas en el plan de estudios.

Para la elaboración del TIF, el alumno dispondrá de un plazo máximo de entrega de doce (12) meses, prorrogable por seis (6) meses a solicitud del alumno y posterior consideración del Comité Académico. Se entiende que estas horas son estimadas ya que la dedicación horaria efectiva puede variar en función de las particularidades del estudiante.

El reconocimiento de créditos externos podrá otorgarse únicamente en la asignatura electiva que se propone en el plan de estudios. El reconocimiento de créditos de seminarios o cursos de posgrado se otorgarán sobre la base de los siguientes requisitos:
a. Que los docentes a cargo del desarrollo de las actividades de posgrado presenten título de posgrado o mérito equivalente.
b. Que la actividad por la que se solicitan créditos presente contenidos pertinentes con el perfil del graduado y los objetivos de la carrera, y haya sido aprobada por el Comité Académico.
c. Que la obligación académica acreditada tenga una duración no inferior a treinta y seis (36) horas.
d. Que el programa de estudio se encuentre legalizado por la Institución en la que se desarrolló la actividad y contenga: el nombre de la obligación académica, la carga horaria, los contenidos, la bibliografía y la modalidad de evaluación.
e. Que la Institución en la que se haya dictado la actividad lo haya hecho a través de una plataforma oficial y tenga avalado su SIED por CONEAU si correspondiere.
f. Que en el certificado de aprobación otorgado por la Institución figuren: el nombre de la obligación académica, la nota final de aprobación y los correspondientes datos de registro.

Trayecto	Materia	Modalidad	Horas Interacción pedagógica	Horas Autónomas	Horas totales	CRE
Formación Básica	1. Introducción a la seguridad informática	Teórico - Práctico	36	90	126	5
Formación Básica	2. Fundamentos de ciberseguridad en redes e infraestructuras críticas	Teórico - Práctico	48	120	168	7
Formación Específica	3. Derecho informático	Teórico - Práctico	48	160	208	8
Formación Práctica	4. Gestión de riesgos y auditoría de seguridad informática	Teórico - Práctico	48	192	240	10
Formación Específica	5. Política criminal y cibercrimen	Teórico - Práctico	36	120	156	6
Formación Específica	6. Gobernanza de datos y seguridad informática	Teórico - Práctico	36	120	156	6

Formación Práctica	7. Diseño de estructuras y programas en seguridad informática	Teórico - Práctico	48	192	240	10
Formación Específica	8. Comunicación y gestión de crisis en seguridad	Teórico - Práctico	36	120	156	6
Formación Práctica	9. Informática forense	Teórico - Práctico	48	192	240	10
Formación Práctica	10. Taller de TIF	Práctico	21	84	105	4
Formación Específica	11. Electiva*	Teórico-práctico	36	120	156	6
	Elaboración TIF		0	350	350	14
Totales			**441**	**1.860**	**2.301**	**92**

*Para la materia electiva, se toma como referencia la carga horaria de asignatura mínima aceptada equivalente a treinta y seis (36) horas de interacción pedagógica.

El sistema de créditos establecido en el presente plan de estudios deberá ajustarse a aquellas normativas institucionales sobre la materia que IUSE elabore oportunamente.

3.5 Contenidos mínimos

1. Introducción a la seguridad informática

I) Fundamentos de la seguridad informática. Conceptos fundamentales de seguridad informática. Normas ISO/IEC 27001:2022 y ISO/IEC 27002:2022 como marco de referencia. Ciberseguridad en contexto: perspectiva integral para la comprensión del impacto de la ciberseguridad en diferentes áreas de la organización. Introducción a la gestión de incidentes. Amenazas, riesgos y vulnerabilidades.

II) Herramientas básicas y normativas en ciberseguridad. Conceptualización y tipologías de sistemas operativos, redes y bases de datos. Aspectos éticos y legales: introducción a las normativas nacionales e internacionales sobre ciberseguridad. Auditoría y análisis forense: conceptos básicos de auditoría de sistemas y análisis forense digital. Ciberseguridad y cibercrimen en contexto de globalización.

2. Fundamentos de ciberseguridad en redes e infraestructuras críticas

I) Redes de computadoras, arquitecturas, topologías, protocolos de comunicación y análisis de tráfico. Principios de seguridad de la información aplicados a redes e infraestructuras críticas. Ataques por capas del modelo OSI, ataques a nivel de aplicación y marcos de referencia para desarrollo y despliegue seguro (OWASP, DevSecOps).

II) Seguridad en redes: segmentación, filtrado, firewalls, IDS/IPS, VPN y políticas de seguridad. Fundamentos sobre el análisis de riesgos, amenazas, vulnerabilidades y gestión de exposiciones en entornos críticos. Autenticación, control de acceso, administración de

identidades y privilegios (IAM). Criptografía: cifrado simétrico y asimétrico, funciones hash, firmas digitales, PKI, certificados digitales, gestión de claves y protocolos criptográficos aplicados. Gestión de vulnerabilidades, métricas de criticidad, procesos de priorización y remediación. Protección de datos y prevención de fuga de información (DLP). Gestión, integridad, retención y trazabilidad de logs. Control de contenidos y articulación con el marco normativo vigente, incluyendo la Ley N° 26.388. Monitoreo de operaciones digitales y trazabilidad con fines de cumplimiento, prevención e investigación.

III) Identificación y análisis de infraestructuras críticas en sectores estratégicos. Seguridad física y lógica en entornos críticos. Amenazas persistentes avanzadas (APT), defensa en profundidad, Zero Trust y respuesta básica ante incidentes. Estándares y marcos regulatorios aplicables a la ciberseguridad de infraestructuras críticas: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27019, NIST Cybersecurity Framework y buenas prácticas internacionales.

3. Derecho informático

I) Fundamentos jurídicos del derecho informático y protección de datos. Introducción al Derecho Informático, conceptos y terminología legal. Legislación en Argentina y análisis comparado con otros países. Régimen legal del manejo y protección de datos personales: bases de datos, normativa, obligaciones legales del Estado, de las empresas y derecho de los ciudadanos. Aspectos jurídicos del correo electrónico. Firma digital y su regulación. Gestión de la seguridad de la información: Normas ISO 27001 e ISO 27002.

II) Programas de Compliance en seguridad informática: normativas, principios y aplicación en entornos organizacionales. Mecanismos y procedimientos internos de supervisión y control para la prevención y detección de ataques informáticos externos. Estrategias para la gestión y mitigación de riesgos informáticos en el ámbito empresarial. Identificación y evaluación de factores de riesgo asociados a los recursos humanos en la seguridad informática.

III) Delitos informáticos, responsabilidad legal y desafíos éticos en la era digital. Intrusismo informático, daño informático y responsabilidad penal. Propiedad intelectual en el entorno digital. Legislación sobre cibercrimen, jurisprudencia y delitos relacionados con el uso de Internet. Cuestiones legales relacionadas con Internet: nombres de dominio, cookies, datos de tráfico y aspectos legales asociados a la seguridad y privacidad en redes y plataformas digitales. Ética social, profesional y ciudadana: manejo de datos, privacidad y uso responsable de la tecnología. Responsabilidad social en el entorno digital. Desafíos legales de tecnologías emergentes como inteligencia artificial (IA), el Internet de las Cosas (IoT) y Blockchain.

4. Gestión de riesgos y auditoría de seguridad informática

I) Políticas y gestión de riesgos. Principios y procedimientos que alineen las prácticas de ciberseguridad con los objetivos estratégicos de la organización. ISO/IEC 27002:2022 como referencia para la selección de controles en procesos de tratamiento de riesgos. Metodologías de análisis de riesgos.

II) Auditorías de seguridad informática. Aspectos éticos, normativos, presupuestarios y organizacionales. Planificación e implementación de auditorías. El impacto en la gestión y la toma de decisiones a nivel estratégico. Herramientas de análisis de vulnerabilidades y

auditorías en el ámbito de la seguridad informática: conceptos básicos y ejemplos prácticos. Gestión de riesgos y desarrollo de planes de mitigación.

III) Ciberinteligencia y monitoreo de amenazas. Técnicas de recopilación de información sobre amenazas potenciales y actores del cibercrimen. Uso de herramientas de monitoreo y detección de intrusiones. Estrategias de colaboración interinstitucional entre sector público y privado, y entre los diferentes poderes públicos (judicial, ejecutivo y legislativo).

5. Política Criminal y Cibercrimen

I) La interrelación entre el sistema de justicia, el sistema penitenciario, el derecho penal y los sistemas de seguridad en la prevención del delito. Elementos e instrumentos de la política criminal. Política criminal y Derechos Humanos. Política Criminal en Argentina. Política Criminal y sistema penal.

II) Introducción al cibercrimen y delitos informáticos: Tipologías de cibercrimen, ciberdelincuencia económica, y su impacto en la política criminal. Marco jurídico y procedimientos penales: Aspectos procedimentales y probatorios en la investigación de cibercrímenes, incluyendo legislación nacional e internacional. Convenio de Budapest sobre el Delito Cibernético. Ciberterrorismo y Ciberguerra: enfoques estratégicos y contramedidas tecnológicas frente a amenazas como ciberterrorismo, ciberespionaje y ciberguerra.

III) Criminología y victimología en entornos digitales. Perfilación criminal: concepción, tipologías y características conductuales generales del ciberdelincuente. Análisis criminal y técnicas de perfilación digital. Análisis de la escena del crimen física y digital. Fases del delito. Técnicas de reconstrucción. Conceptos e instrumentos para la gestión de políticas victimológicas en el ecosistema digital. Perspectivas de género y Derechos Humanos en victimología. Grooming: definición y tipologías. Marco legal y políticas públicas. Procedimientos penales y evidencia digital. Herramientas y estrategias de prevención en plataformas digitales.

6. Gobernanza de datos y seguridad informática

I) Introducción a la gobernanza de datos y seguridad informática: políticas, principios, roles y responsabilidades. ISO/IEC 27002:2022 como marco de gobernanza y la implementación de controles organizacionales y técnicos en la gestión segura de la información. El impacto del Big Data en la gestión de datos y su relevancia en ciberseguridad. Big Data y su gobernanza en ciberseguridad. Estrategias de recolección, almacenamiento y análisis seguro de datos masivos. Data Mining, Data Warehousing y Seguridad: técnicas de minería de datos para extraer información valiosa de grandes bases de datos, con foco en la protección de la información frente a amenazas cibernéticas.

II) Arquitecturas y tecnologías seguras: exploración de arquitecturas y tecnologías clave (IoT, Cloud Computing) para la gobernanza de datos con un enfoque en la ciberseguridad. Control en ciberseguridad: uso de paneles de control para la gestión de grandes fuentes de datos en el contexto de la ciberseguridad. Paneles de control y gestión de riesgos de seguridad: uso de paneles de control en la gestión de datos masivos para monitorear amenazas de

seguridad. Procesos y procedimientos para asegurar la protección de los datos en entornos críticos.

7. Diseño de estructuras y programas en seguridad informática

I) Estructura organizacional del área de seguridad. Funciones, responsabilidades y perfiles del equipo técnico, técnicas de gestión estratégica, presupuesto y recursos humanos. Ciclo de vida de los sistemas de seguridad y la gestión de proyectos, evaluación económica de la seguridad y el uso de métricas de rendimiento. Tercerización de servicios y gestión de proveedores.

II) Cultura y clima organizacional en la seguridad. Gestión del cambio y resolución de conflictos. Teoría y psicología organizacional en el entorno de ciberseguridad. Desarrollo de competencias gerenciales: liderazgo, comunicación y toma de decisiones. Gestión de riesgos en ciberseguridad y marcos de referencia aplicables

III) Arquitectura segura de redes y sistemas. Principios de diseño. Controles técnicos relevantes de ISO/IEC 27002:2022. Monitoreo, detección y respuesta. Comparación de enfoques de seguridad en sistemas operativos. Buenas prácticas para proteger datos en entornos diversos (cloud, dispositivos personales), documentación, estandarización, auditoría y cumplimiento en seguridad de la información.

8. Comunicación y gestión de crisis en seguridad

I) La comunicación y la información. La comunicación institucional: externa e interna. Lenguaje y tipos de acciones comunicativas. La comunicación como elemento constitutivo de la gestión pública y privada. Medios de comunicación y opinión pública. La construcción social del delito en/desde los mass media. Redes sociales. Desinformación.

II) Planificación y gestión de la comunicación institucional. Confección de protocolos de comunicación en materia de seguridad. Diseño estratégico de la comunicación de gestión. Storytelling.

III) Comunicación de riesgo y comunicación de crisis. Errores habituales. La gestión de la comunicación en la crisis. Estrategias de preparación, explicación y legitimación. Recomendaciones sobre la mirada multidisciplinar.

9. Informática forense

I) Principios fundamentales de la forensia digital. Diferencias entre evidencia física y digital. Preservación de la cadena de custodia. Desafíos técnicos y legales asociados a la recolección de datos. Normativas internacionales y regulaciones de cumplimiento. Consideraciones legales para asegurar la admisibilidad de la evidencia en juicios. Elaboración de informes periciales.

II) Conceptos básicos de la adquisición y análisis de imágenes forenses en sistemas y dispositivos móviles, y herramientas de código abierto. Análisis de datos e interpretación de resultados forenses en un contexto estratégico. Traducción de hallazgos técnicos en recomendaciones estratégicas.

10. Taller de TIF

Definición de marcos analíticos y metodológicos. Relevancia. Fundamentación. Objetivos. Cronograma. Estructura de los capítulos y contenidos a incluir en los mismos. Selección de las fuentes. Referencias. Selección de potenciales Directores/Tutores de TIF. Plazos para la presentación de Planes de TIF y Trabajo Integrador Final de Especialización.

11. Electiva

Con el objeto de fomentar la interdisciplinariedad en el perfil de los egresados de carreras de posgrado IUSE, el estudiante deberá optar por cursar una asignatura de las carreras de posgrado que se dicten en la casa de estudios. El menú de asignaturas electivas será actualizado y definido para cada cohorte por el Comité Académico a partir de la oferta académica de posgrado que presente el IUSE o a partir del reconocimiento de créditos.

3.6 Estrategia de seguimiento curricular

El seguimiento curricular forma parte de la evaluación permanente de la carrera, la cual está a cargo del Comité Académico y el Coordinador de la carrera, quien lo preside, y tiene por objeto proponer acciones para la mejora en la calidad de la carrera y en la graduación de los estudiantes a lo largo del tiempo. Esta comprende la sistematización de información académica que permita el análisis del avance, rendimiento y egreso de los estudiantes; la revisión de la pertinencia y actualización de los contenidos dictados y su integración horizontal y vertical; y la actualización de los materiales didácticos, biblioteca y/o soportes tecnológicos.

Las fuentes y mecanismos para su concreción se encuentran establecidos en el Reglamento de Posgrado.

3.7 Modalidad pedagógica

La carrera desarrollará una modalidad pedagógica teórico-práctica, orientada a fomentar la participación activa de los estudiantes y a aplicar los conceptos teóricos en situaciones concretas.

Las clases combinarán exposiciones teóricas con actividades prácticas, tales como análisis de casos, debates grupales, trabajos prácticos y simulaciones. Estas dinámicas permitirán profundizar en el estudio de problemáticas actuales de seguridad informática, y diseñar e implementar políticas y programas de ciberseguridad desde una perspectiva multidisciplinaria.

Además, en las asignaturas del trayecto de Formación Práctica se promoverá la realización de proyectos de diseño de intervenciones vinculados con contextos reales de seguridad informática, en el marco de la promoción de habilidades prácticas clave para el análisis, la planificación, la ejecución y la supervisión estratégica y operativa de áreas y proyectos de seguridad informática, incluidos planes de mitigación de riesgos, auditorías informáticas e investigaciones forenses digitales.

El dictado de las asignaturas contará con carga horaria presencial donde hasta un treinta por ciento (30%) de las horas podrá ser mediada por tecnología de videoconferencia.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S

"2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Hoja Adicional de Firmas
Anexo

Número: IF-2026-11798344-GCABA-SAIUS

Buenos Aires, Lunes 9 de Marzo de 2026

Referencia: Anexo - Carrera de Posgrado “Especialización en Gobernanza y Gestión de la Seguridad Informática”.

El documento fue importado por el sistema GEDO con un total de 15 pagina/s.

Digitally signed by Comunicaciones Oficiales
Date: 2026.03.09 11:08:28 -03:00

P/P Paola Lechuga
Secretaria de Administración
SECRETARIA DE ADMINISTRACION IUS
AREA JEFE DE GOBIERNO

Digitally signed by Comunicaciones Oficiales
Date: 2026.03.09 11:08:29 -03:00