Carrera de Especialización en Evaluación Universitaria

Universidad de Buenos Aires

Trabajo Final de Especialización en Evaluación Universitaria

Título

Análisis curricular de la Maestría en Seguridad Informática de la UBA

Subtítulo

Análisis del perfil del egresado, perspectivas respecto de normativas nacionales e/internacionales y de los docentes y/autoridades

Alumna: Lic. Graciela Norma Pataro

Tutor: Dr. Hugo Scolnik

Cotutor: Esp. Walter Viñas

Año de presentación: 2023

Cohorte: 2021

1. **Palabras clave**

Seguridad Informática (Information Security) – Currícula (Curriculum) – Habilidades y Competencias (Skills & Competency)

2. Resumen

En este trabajo se buscará abordar, partiendo de una evaluación curricular parcial, con especial referencia al perfil esperado de los egresados de la Maestría en Seguridad Informática, contrastándolo con los sentidos y criterios aportados por los docentes y autoridades de éste como referentes.
Se busca estudiar también de qué forma estos fundamentos (los que sustentan sus objetivos al momento de su creación) se relacionan con la normativa más reciente elaborada por el Estado Argentino en la Decisión Administrativa 641/21[1] de los Requisitos Mínimos de Seguridad de la Información para los Organismos del SPN (Sector Público Nacional) [DA 641; 2021] y normas internacionales tales como la ISO 27002:2022 (International Standard Organization) [ISO 27002; 2022].
Con estas normativas se busca construir los referentes para la evaluación del plan de estudios.
Los referentes seleccionados se utilizan para contrastar los objetivos de la Maestría con estándares nacionales e internacionales consensuados en cuanto a la regulación de la profesión de Seguridad Informática y corresponden a la International Standard Organization, institución que regula normativamente muchos estándares internacionales (entre ellos los de la Seguridad Informática), y el mismo gobierno argentino en sus disposiciones y normas locales.

This work will seek to address, based on a partial curricular evaluation, with special reference to the expected profile of the graduates of the Master's Degree in Computer Security, contrasting it with the senses and criteria provided by teachers and authorities of this as references.
It also seeks to study how these foundations (those that support its objectives at the time of its creation) relate to the most recent regulations developed by the Argentine Government in the Administrative Decision 641/21 of the Minimum Information Security Requirements for SPN Bodies and international standards such as ISO 27002:2022.
These regulations seek to build the benchmarks for the evaluation of the curriculum.
The selected referents are used to contrast the objectives of the master's degree with national and international standards agreed upon regarding the regulation of the Computer Security profession and correspond to the International Standard Organization, an institution that regulates many in-

[1] De ahora en más DA 641

ternational standards (including those of Information Security), and the Argentine government itself in its local provisions and regulations.

Índice general de contenidos

Índice de Imágenes

Índice de Tablas

3. Limitaciones al alcance: Nota sobre sesgo personal

Se hace necesario explicitar el propio sesgo personal de la autora respecto del contenido en el presente trabajo.

La autora colaboró en la creación de la currícula del presente Posgrado desde el año 2007 hasta su lanzamiento en el 2009. Luego se desempeñó como Coordinadora Académica del mismo hasta el año 2012 y desde el inicio es además docente de la materia "Marco Legal, Ética y Privacidad" dictando los contenidos referidos a la parte de Ética y Privacidad.

En tal tesitura se ha tratado de evitar en todo momento la emisión de juicios de valor que pudieran interferir con las conclusiones a las que podría arribar cualquier observador neutral. Esto se ha realizado manteniendo en todo momento una actitud imparcial y distanciada respecto de los comentarios que se han obtenido tanto de la CD como de los mismos docentes.

Afortunadamente con la ayuda de las perspectivas de los docentes y autoridades, este sesgo personal se mitiga grandemente. Es bien sabido que la inclusión de voces diferentes al momento de la realización de cualquier trabajo aporta una visión de diversidad que resulta en un trabajo más abarcativo, justo, transparente e inclusivo.

Además, el desempeño de la autora como Auditora de Sistemas Informáticos por 34 años coadyuva también para aportar una perspectiva más objetiva sobre el tema.

Por otra parte, las normativas son documentos estáticos de los cuales se extraen los conceptos para contrastar con los elementos del perfil de los egresados.

4. Orientación y Metodología utilizada en el presente TF

Se ha tomado como orientación básica del presente Trabajo Final el paper de Castañeda [Castañeda, 2012] en el cual la autora plantea la evaluación curricular de carreras pedagógicas. En su trabajo ella apunta:

> Uno de los desafíos centrales para las instituciones formadoras actualmente es acreditar la calidad de la formación ofrecida, para esto es clave lograr la coherencia del diseño curricular. En este marco, la creación de instrumentos para evaluar diseños curriculares se inscribe en la investigación evaluativa del currículum…. Tiene como propósito proponer procedimientos e instrumentos para el estudio del currículum formal o diseñado, por cuanto, se delinearon un conjunto de instrumentos que permitieron la indagación en torno a los componentes formales del currículum. [Castañeda; 2012, pág 73]

Para lograr esto la autora planteó instrumentos para investigar los componentes formales del curriculum con los que se "evaluó la coherencia de los principios pedagógicos, el perfil del egresado de la carrera de pedagogía, declarados y la revisión de la presencia o no de dichos referentes en los programas de las distintas asignaturas pertenecientes al área". [Castañeda; 2012, pág 73]

El presente trabajo solo presenta un análisis curricular de la Maestría en SI y no una evaluación curricular, rescatando algunos de los elementos que menciona Castañeda en su trabajo, siendo el objetivo de este análisis el coadyuvar a una evaluación interna que a posteriori podrá ser completada o complementada por las mismas autoridades del posgrado como parte de sus planes de actualización y evaluación de este Posgrado como modelo de educación superior.

Algunos autores indican que una evaluación curricular solo debe centrarse en algunos aspectos en tanto que otros [Lewy; 1976, Op cit p 37] sostienen que una evaluación curricular tiene que dar cuenta de todos y cada uno de los elementos que forman parte de un plan de estudios: Fundamentos, perfil, organización del contenido, etc. Los primeros consideran que es difícil evaluar la totalidad de un plan de estudios por la complejidad que subyace en el conocimiento de cada uno de los aspectos curriculares que son objeto de evaluación. [Barriga; 2005, pág. 7]

Para el análisis de la Maestría en SI es importante destacar que gran parte del difícil trabajo mencionado en el último párrafo se ve paliado por el hecho de que la autora de este TF formó parte del comité que originalmente desarrolló el currículo en cuestión y muchos de los fundadores son actualmente parte de la Comisión Directiva del Posgrado y/o además se desempeñan como docentes del mismo, lo que aporta un conocimiento mucho más profundo de los cómo, porqué y para qué se tomaron las diversas decisiones al momento de su creación.

"El diseño del currículum corresponde al currículum formal, pero no puede desconectarse lo que se ha denominado currículum real o desarrollo del currículum, sobre todo si se considera como criterio la coherencia curricular". [Castañeda; 2012, pág 76]

En este sentido el aporte de la visión de las autoridades de la Maestría en SI y los docentes de todas las asignaturas aporta una visión mucho más amplia que contempla ese curriculum real como menciona Castañeda y otros autores.

En el planteo de la metodología que utilizó Castañares [Castañares; 2012, pág. 78] ella menciona:

> "El objeto de estudio del presente trabajo fue el diseño curricular de las carreras de formación pedagógica, que consideró los siguientes componentes: principios orientadores de la formación docente, perfil de egreso, plan de estudios derivado del mismo, y programa de asignaturas."

En el presente trabajo final se utilizaron los mismos componentes que Castañares menciona para la maestría bajo análisis, los principios orientadores (objetivos), perfil de egreso, plan de estudios y programa de las asignaturas.

Nótese del cuadro que presenta Castañeda con su Plan de Evaluación curricular aquellos elementos que se han tenido en cuenta para desarrollar el presente análisis curricular [Castañeda; 2012, pág. 78] (se han resaltado en verde los elementos que se utilizan en este TF)

TABLA 1. PLAN DE EVALUACIÓN CURRICULAR

Evaluación curricular	Tipo de currículum	Objeto de evaluación	Elementos del currículum	Procedimientos de evaluación
Evaluación del currículum vigente	Currículum formal - Coherencia interna	-Principios pedagógicos declarados -Evaluación del perfil del egresado	-Orientaciones curriculares - Competencias	Matriz de coherencia curricular
		- Plan de Estudios	-Asignaturas -Objetivos -Contenidos -Metodología - Evaluaciones	Escala de mapeo curricular Rúbrica de evaluación

Ilustración 1 - Tabla de Evaluación curricular [Castañeda; 2012, pág 78]

Se ha reemplazado la escala de mapeo curricular en este trabajo por solamente la presencia de los contenidos formales establecidos y se ha buscado recuperar aquellos que deberían incluirse o excluirse contrastándolo con los pareceres y opiniones de los docentes respecto de los referentes mencionados anteriormente (DA/641 e ISO 27002:2022).

En este contexto de la investigación planteada por Castañeda,

> "el propósito de" su "investigación (análisis en este TF) consistió en evaluar la coherencia interna y correspondencia entre los diferentes componentes de la estructura curricular del área…, para los cuales se diseñaron, validaron y aplicaron instrumentos de evaluación curricular. El plan de evaluación curricular consideró dos categorías: la *Coherencia entre principios orientadores de la formación inicial*" (objetivos) "y el *Perfil de egreso* de la carrera…, y la *Coherencia* con el *Perfil de egreso* y los programas de asignaturas del área…". [Castañeda; 2012, pág 78]

En este TF se presentan dos matrices o tablas para analizar la coherencia de los principios orientadores u objetivos versus las competencias del perfil de egreso y, por otro lado, una matriz para contrastar la coherencia de las asignaturas con las competencias del perfil de egreso.

> "Para contrastar el currículum formal con la puesta en práctica del mismo, fueron entrevistados los directores de cada carrera como responsables de la gestión de éste, atendiendo con este análisis a la naturaleza interpretativa del currículum real o implementado." [Castañeda; 2012, pág 78]

Elemento este también presente en este TF ya que se realizaron las entrevistas a la Comisión Directiva y a los docentes de las diversas asignaturas.

> "Para ello, se estableció una definición operacional del concepto de coherencia como variable sustancial del estudio. Se entendió por coherencia el grado de relación existente entre los Principios orientadores de la formación inicial, el Perfil de egreso de la carrera de Pedagogía y los programas de asignaturas del área de Formación Pedagógica, declarados en los documentos curriculares evaluados." [Castañeda; 2012, pág 78]

En el presente trabajo final no se plantea ese "grado" de relación que menciona Castañeda en la coherencia definida por ella, sino que se limita solamente el análisis al planteamiento de la existencia de los sustentos relacionales entre los diferentes componentes (ausencia/presencia) dejando luego para un trabajo de mayor profundidad la investigación de hasta qué grado ese sustento habilita la relación entre los mismos (Objetivos, Perfil, Contenidos).

5. Historia y diseño del currículum del Posgrado en Seguridad Informática.

5.1. Historia de la creación del Posgrado

El posgrado en Seguridad Informática de la Universidad de Buenos Aires comenzó a funcionar en el año 2009. Luego de dos años de trabajo en la confección de este currículo éste fue aprobado por el Consejo Superior de la UBA mediante la resolución 4853/08[2] (Ver Anexo F) en la cual se creó la carrera, se aprobó el plan de estudios y su reglamento.

En el momento de su creación este posgrado fue único en el ámbito de la UBA ya que estas problemáticas no eran tratadas de forma unificada en ningún otro estudio.

Su creación obedeció a la necesidad de contar dentro de la UBA con un posgrado dedicado a la formación de profesionales en estas temáticas ya que "las aplicaciones informáticas son cada vez más importantes, los requerimientos de seguridad son cada vez mayores y esenciales en la opera-

[2] la Res. 4852/08 aprobó la Especialización en S.I. que forma parte de la Maestría en su primer año de cursada

toria de las organizaciones modernas... se hace evidente la necesidad de participar académicamente en la formación de los recursos humanos para que adquieran la capacidad de asistir a la conducción a conocer en detalle los riesgos, sus características, el efecto en las operaciones y, lo más importante, las formas de afrontarlo y, en lo posible, mitigarlos y/o neutralizarlos." [Anexo F; págs. 2 y 3].

Su creación fue propiciada por académicos de las facultades de Ciencias Exactas y Naturales, Ciencias Económicas e Ingeniería siendo los principales propulsores el Dr. Hugo Scolnik (FCEyN), Raul Saroka (FCE) e Ing. Alberto Dams (FI). Ellos convocaron a diversos profesionales y académicos de sus casas de estudio (la autora fue convocada por el Dr. Scolnik) y se comenzó en el año 2007 un ciclo de reuniones para definir la curricula y los contenidos de esta Maestría.

No existía en el país un modelo de posgrado similar dentro de la UBA, solo se contaban con estos dos estudios, a saber:

- "Posgrado de Especialización en Criptografía y Seguridad Teleinformática en el Instituto de Educación Superior del Ejército IESE
- Posgrado en Seguridad de la Información en la Universidad del Salvador" [Anexo F; pág. 4]

A nivel internacional se tomaron los ejemplos de los siguientes estudios:

- "University of Purdue, Indiana, EE.UU; Cerias (The Center for Education and Research in Information Assurance and Security).
- Norwich University Vermont USA; Infosec Graduate Program, Master in Science in Information Assurance.
- Kennesaw State University; Georgia, EE.UU. Center for Information security Education, que ha sido nominado como el National Center of Academic Excellence in Information Assurance Education por la National Security Agency (NSA)" [Anexo F; pág. 4]

Durante el diseño del currículum de este posgrado se utilizó una metodología similar a la indicada por Diaz Barriga en su trabajo [Barriga et al., 1990: pp. 46 – 52] en la que se ejemplifican las siguientes etapas:

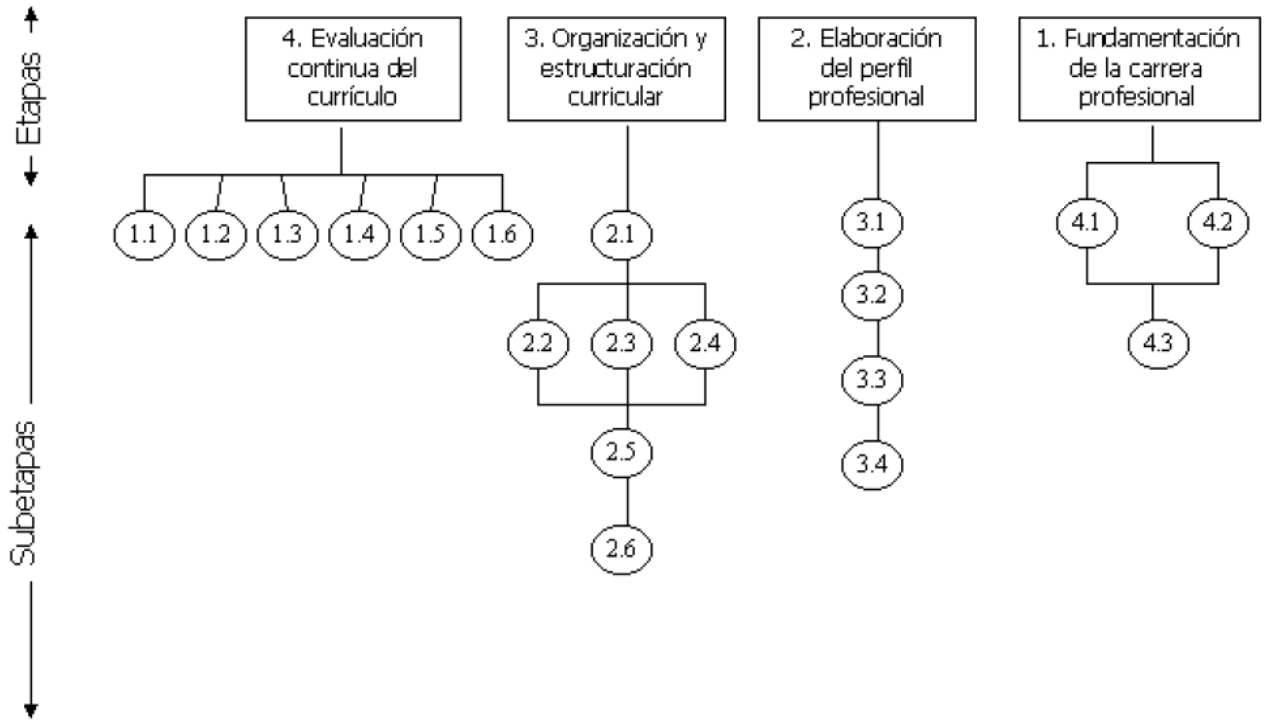


Ilustración 2 - Etapas de metodología de diseño curricular [Diaz Barriga et. al. 1990 p. 47]

Las etapas en el cuadro anterior se corresponden con lo utilizado en la elaboración del currículo de la Maestría, a saber:

- Etapa 1- Fundamentación de la carrera profesional: indicándose las necesidades del ámbito en el que se desempeñará el profesional, situando a la carrera en una realidad y un contexto social [Diaz Barriga et. al. 1990 p. 48] (Ver punto 5.2)
- Etapa 2- Elaboración del perfil profesional: donde se fijan las metas que se quieren alcanzar en relación con el tipo de profesional que se intenta formar. [Diaz Barriga et. al. 1990 p. 48] (Ver punto 5.3)
- Etapa 3- Organización del perfil profesional: Con base en los rubros (conocimiento y habilidades termina que contienen el perfil profesional, se enumeran los conocimientos y habilidades específicos que debe adquirir éste para que se logren los objetivos derivados de los rubros. Estos conocimientos y habilidades específicos se organizan en áreas de conocimientos, temas y contenidos de la disciplina, con base en los criterios derivados de ella. [Diaz Barriga et. al. 1990 p. 51]. Es decir, el currículo y sus contenidos específicos.
- Etapa 4- Evaluación continua del currículo: El currículo no se considera estático, pues está basado en necesidades que pueden cambiar y en avances disciplinarios, lo cual hace necesario actualizarlo permanentemente de acuerdo con las necesidades imperantes y los adelan-

tos de la disciplina. Se debe contemplar la evaluación externa, que en el caso de esta Maestría ocurrió ya en los años 2011 y 2016 por parte de la CONEAU, y la evaluación interna como logro académico de los objetivos enunciados en el perfil profesional. [Diaz Barriga et. al. 1990 p. 51]. El objetivo de este trabajo es colaborar como un elemento más para esa evaluación interna.

5.1.1. Datos generales de la Maestría

La duración de la Maestría es de dos años obteniéndose en el primer año el título de Especialista. La carga horaria de la maestría en su totalidad es de 752 horas.

Son requisitos de admisión:

1. *Los graduados de la Universidad de Buenos Aires con título de grado correspondiente a una carrera de CUATRO (4) años de duración como mínimo, de las carreras que se dictan en la Facultad de Ciencias Económicas, Facultad de Ciencias Exactas y Naturales y Facultad de Ingeniería, o*
2. *Los graduados de otras universidades argentinas con título de grado correspondiente a una carrera de CUATRO (4) años de duración como mínimo, con títulos afines a los señalados en a), o*
3. *Los graduados de universidades extranjeras que hayan completado, al menos, un plan de estudios de DOS MIL SEISCIENTAS (2.600) horas reloj o hasta una formación equivalente a master de nivel I, de carreras equivalentes en duración y temáticas a las indicadas, o*
4. *Los egresados de estudios de nivel superior no universitario vinculados a las áreas temáticas de la carrera, de CUATRO (4) años de duración o DOS MIL SEISCIENTAS (2.600) horas reloj como mínimo, serán evaluados individualmente y la Comisión de Maestría establecerá los requisitos previos que correspondan en cada caso, a fin de asegurar que su formación resulte compatible con las exigencias del posgrado al que aspiran.*
5. *aquellas personas que cuenten con antecedentes de investigación o profesionales relevantes, aun cuando no cumplan con los requisitos reglamentarios citados, podrán ser admitidos excepcionalmente para ingresar a la Maestría con la recomendación de la Comisión de Maestría y con la aprobación del Consejo Directivo de la Unidad Académica Sede de la Maestría o del Consejo Superior.*

Además, el postulante deberá superar el proceso de selección que implica:

1. *Antecedentes: acreditar la posesión de antecedentes académicos y profesionales suficientes a criterio de la Universidad, que guarden relación con el área disciplinaria objeto de estudio de la Maestría.*
2. *Examen de admisión: aprobar un examen de admisión donde se evalúan las aptitudes y capacidad lógica, como así también conocimientos de informática y redes.*
3. *Idioma: se exige dominio de la lectura en idioma inglés técnico. El postulante deberá acreditar ante el Director o quien el designe dicha aptitud o aprobar un examen de comprensión de textos. Se confeccionará un acta consignando la aprobación firmada por el Director.*
4. *Cartas de recomendación: el aspirante debe presentar dos cartas de recomendación que avalen sus antecedentes académicos y profesionales.*
5. *En la entrevista se evaluará el grado de motivación para el cual el postulante solicita su inscripción, compromiso con la finalización de la maestría, disponibilidad de tiempo, antecedentes y capacidad para abordarla íntegramente.* [Anexo G; pág. 12]

Son requisitos para acceder al título de Magister de la Universidad de Buenos Aires en Seguridad Informática:

- *Aprobar las materias y otras actividades establecidas en el diseño curricular o fijado por la Comisión de Maestría que contribuyan a su formación integral y superior en las disciplinas involucradas.*
- *Aprobar el Trabajo Final de Integración. Este trabajo de carácter integrador, será individual y consistirá en un análisis crítico de un tema de las materias del primer año y será expuesto para su aprobación ante un jurado.*
- *Aprobar la Tesis o el Trabajo Final de Maestría. El maestrando realizará una defensa oral y pública del Trabajo presentado en la que deberá demostrar el dominio y aplicación de métodos científicos y de los conocimientos específicos del campo de la Seguridad Informática.*

La Tesis o Trabajo Final de Maestría consistirá en la exposición de una problemática actualizada de un Área temática de Seguridad Informática, que incluya una elaboración del estado de la cuestión, la presentación de los datos empíricos si correspondiere y una exposición fundada de las conclusiones a las que hayan arribado. El mismo será individual y total o parcialmente escrito que podrá adquirir formato de proyecto, obra, estudios de casos, ensayo, informe de trabajo de campo u otras que permitan evidenciar la integración de aprendizajes realizados en el proceso formativo, la profundización de conocimientos en un campo profesional y el manejo de destrezas y perspectivas in-

novadoras en la profesión. La Tesis o Trabajo Final de Maestría se desarrollará bajo la dirección de un Director de trabajo final de Maestría. [Anexo G; pág. 14]

La modalidad de cursada comenzó a realizarse en forma virtual desde el inicio de la pandemia en 2020 y si bien continúa manteniéndose la cursada virtual la Escuela de Estudios de Posgrados de la Facultad de Ciencias Económicas (donde actualmente tiene su sede la Maestría) permite el dictado de clases presenciales previa coordinación con la EEP.

Las correlatividades de la cursada de las diferentes asignaturas se ejemplifican en el siguiente cuadro junto con la carga horaria de las diferentes asignaturas: [Anexo G; págs. 7 y 8]

Tabla 1 - CUADRO DE LAS ASIGNATURAS

Primer Año

Primer cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Ejes Temáticos de la Seguridad	48	-	48	-
Criptografía I	32	16	48	-
Seguridad en Redes I	32	16	48	-
Gestión Estratégica de la Seguridad I	32	16	48	-

Segundo cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Documentación y Proyectos de Seguridad	16	16	32	Gestión Estratégica de la Seguridad I
Seguridad en Sistemas Operativos y Aplicaciones	32	16	48	Ejes Temáticos de la Seguridad
Comportamiento Organizacional	16	8	24	Gestión Estratégica de la Seguridad I
Seguridad en Redes II	16	16	32	Seguridad en Redes I / Criptografia I
Marco Legal, Ética y Privacidad	32	-	32	Gestión Estratégica de la Seguridad I
Taller de Trabajo Final de Integración	16	8	24	-
Total Horas Primer Año	**272**	**112**	**384**	-

Segundo Año

Primer cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Seguridad Física	12	4	16	Seguridad en Sistemas Operativos y Aplicaciones

Gestión Estratégica de la Seguridad II	16	16	32	Documentación y Proyectos de Seguridad/ Marco Legal, Ética y Privacidad
Criptografía II	32	16	48	Criptografía I / Seguridad en Redes II
Taller de Trabajo Final de Maestría	32	32	64	Aprobación de todas las asignaturas del primer año

Segundo cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Auditoria	48	16	64	Gestión Estratégica de la Seguridad II
Informática forense y delitos informáticos	32	16	48	Criptografía II
Taller de Desempeño de Competencias Gerenciales		16	16	Comportamiento Organizacional
Taller de Trabajo Final de Maestría	32	48	80	Propuesta de TF aceptada
Total horas segundo año	**204**	**164**	**368**	-
Carga Horaria Total del Plan de Estudios	**476**	**276**	**752**	-

La Maestría será dirigida por un Director y dos Subdirectores, y una Comisión de Maestría. El Director y los Subdirectores integran la Comisión de Maestría. La Comisión de Maestría será la encargada de asesorar y colaborar con la gestión de la carrera.

La carrera cuenta también con un Coordinador que es nombrado por el Decano de la Facultad Sede a propuesta de la Comisión de Maestría. [Anexo G; pág. 6]

Como el primer año corresponde a la Especialización, la que cuenta asimismo con sus propias autoridades y su propia Comisión, la Comisión Directiva en su totalidad cuenta en la actualidad con 6 miembros en total (Directores más dos subdirectores). Uno de los subdirectores de la Especialización es un miembro externo perteneciente, en la actualidad, a la FCEyN.

Actualmente el Coordinador académico es parte de la Comisión Directiva, completando un total de 7 miembros.

5.2. Fundamentación de la carrera profesional

Como parte de la justificación de la creación de este posgrado (etapa 1: Fundamentación de la carrera profesional) se pueden resumir en algunas cuestiones, a saber:

- *Una mayor complejidad del contexto actual de las actividades públicas y privadas y la universalización de la utilización de las tecnologías informáticas en las organizaciones públicas y privadas.*
- *Un mayor impacto de las TIC en la gestión de las organizaciones.*
- *El incremento notorio de los problemas de seguridad en materia de la gestión de la información.*
- *Un crecimiento de las formas de delitos mediante el uso de la tecnología.*
- *La existencia de entes, disposiciones, estándares que exigen a las organizaciones el cumplimiento de normas de seguridad y la generación de responsabilidad emergente para quienes conducen esas organizaciones.*
- *La escasa oferta en la República Argentina de formación universitaria en materia de Seguridad Informática.*
- *La necesidad de proveer una oferta académica de alto nivel para capacitar a profesionales desde una perspectiva tecnológica, legal, ética y psicosocial.*
- *La necesidad de mejorar la formación universitaria de los profesionales que buscan dedicarse a la especialidad de la Seguridad Informática.*
- *La importancia que adquiere la protección de los activos informáticos de las organizaciones y personas, y la información acerca de los individuos.*[3]

El campo de la Seguridad Informática, o Seguridad de la Información como también suele denominárselo hoy en día, es un área de profesión en constante cambio, incluso a una aceleración aún mayor que muchas otras profesiones.

Baste pensar por ejemplo como en los dos años de pandemia la comisión de fraudes y estafas por medios informáticos se han duplicado, desbordando a instituciones bancarias, crediticias y organismos de contralor con reclamos y denuncias.

> *"El delito económico ya existía: fraude, estafa, robo. Pero se exacerbó cuando la vi-da mutó a modo virtual: "Más operaciones bancarias y en plataformas de compra-venta, generó más fraude"*, afirma Horacio Azzolín, desde la Unidad Fiscal Especializada en Ciberdelincuencia (Ufeci)."
>
> *Las denuncias en la Unidad Especializada de Ciberdelincuencia (Ufeci) aumentaron, entre marzo de 2020 y 2021, un 6.550 por ciento*. [Página 12; 2021]

[3] Res 2513/15 punto B) JUSTIFICACIÓN DE LA MAESTRÍA EN SEGURIDAD INFORMÁTICA

Asimismo, “la mayoría de las personas ajenas a la profesión de la ciberseguridad no se dan cuenta ni aprecian por completo la complejidad del trabajo de los profesionales de la seguridad” [CISO Mindmap; 2021], en el Mapa mental desarrollado desde hace más de 10 años por el especialista Rafeeq Rehman se incluye una enumeración de las tareas que un profesional de seguridad realiza. Este mapa sirve no solo como herramienta educativa (SANS[4] lo utiliza como parte de su poster de Liderazgo en Seguridad) sino también para que los profesionales diseñen y refinen sus programas de seguridad.
En solo un año (¡1 año!) de la realización del MindMap del 2021 se incluyeron 7 nuevas habilidades o skills para los profesionales de seguridad de la información.

Las finalidades establecidas en la resolución de su creación[5] son:

- “*Preparar recursos humanos capacitados en todos los ámbitos relacionados con la Seguridad Informática.*
- *Generar la capacitación de recursos humanos de excelencia para la docencia de grado y posgrado*
- *Promover el desarrollo de la investigación en materia de Seguridad Informática, a partir de la adquisición de rigurosidad científica para el análisis e interpretación del campo disciplinario*
- *Crear conciencia de la importancia y los alcances que esta área de conocimiento tiene actualmente en prácticamente todas las actividades de la sociedad, impulsando y fomentando una cultura de Seguridad Informática.*
- *Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos a la sociedad.*
- *Incorporar el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.*
- *Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.*
- *Formar egresados éticos capaces de generar, aplicar y transmitir los conocimientos adquiridos.”*

[4] SANS: Systems Administrator Network Security, asociación norteamericana ampliamente reconocida y creada en 1989, cuya misión es la de empoderar a los profesionales de seguridad
[5] Res 2513/15 punto III

La Maestría ha pasado por dos procesos de acreditación satisfactoriamente que fueron plasmados en las siguientes resoluciones de la CONEAU con las recomendaciones que se indican para cada caso:

- Res. 847/11 de fecha 1/11/2011 [Res. 847/11 CONEAU; pág. 7]
  - Se asegure el desarrollo de manera perentoria de actividades de investigación en la temática de la carrera, y la participación de los alumnos en estas actividades.
  - Se trabaje en el fortalecimiento de los antecedentes y se incremente la proporción de docentes con titulación igual o superior a magister.
  - Se especifique mediante normativa la exigencia de un integrante externo a la institución en el jurado de tesis.
- Res. 282/16 de fecha 21/4/2016 [Res. 282/16 CONEAU; pág. 1]
  - No tuvo recomendaciones y las realizadas en la evaluación anterior fueron subsanadas.

En ninguna de ambas acreditaciones se solicitó aún la categorización de CONEAU.
Luego, por medio de la Res. CS N° 2513/15 (Ver Anexo G) se aprobó la modificación del plan de estudios.
Uno de los cambios importantes incluidos en esta resolución fue la definición de este posgrado adecuado a lo establecido por el art 1 de la resolución CS 5284/12 en la que se indica: "*la Maestría será de tipo Profesional ya que, se vincula específicamente con el fortalecimiento y consolidación de competencias propias de una profesión o un campo de aplicación profesional."* [Anexo G; pág. 4]
La definición expresa del posgrado como de tipo "profesional" fue un hito importante ya que posibilitó dejar en claro esa vinculación de las competencias propias de los profesionales de seguridad de la información (nótese el subrayado) y como lo menciona expresamente ya que "a lo largo de su proceso de formación profundiza en competencias vinculadas con marcos teóricos disciplinares o multidisciplinares que amplían y cualifican las capacidades de desempeño que apunte a formar profesionales capaces de participar tanto de la fase de instrumentación como de diseño y decisión"
Otros cambios introducidos pueden resumirse en:

1.1.1. "*incorporación de tres nuevas asignaturas,* [Anexo G; pág. 6]

Se incorporaron las asignaturas de Seguridad Física porque se detectó que estas temáticas no habían sido tenidas en cuenta en el currículo original. Se agregó también un Taller para la realización del Trabajo Final de la Especialización (1er año) para aquellos estudiantes que solo desean obtener su título intermedio y por ende deben presentar su trabajo final necesi-

tando el correspondiente apoyo académico. Este apoyo a los estudiantes solo estaba definido a nivel de la cursada de la Maestría en el segundo año. Se agregó también un Taller de Competencias Gerenciales complementando la asignatura de Comportamiento Organizacional del primer año. Este Taller de Competencias Gerenciales se definió como exclusivamente práctico ya que aborda casos de estudio concretos con los estudiantes. (Ver cuadro de asignaturas)

1.1.2. Ajuste de las horas teóricas y de práctica de varias de las materias,

El ajuste de horas asignadas surgió naturalmente de la experiencia recabada en los años del dictado (recordar que el posgrado comenzó en el 2009 a funcionar como un posgrado totalmente nuevo en la UBA) ya que se estimaron originalmente las horas en valores de más abundantes en algunos casos (por ejemplo Criptografía I pasa de tener 64 horas totales a 48 horas) y en cambio a otras asignaturas fue necesario otorgarles más carga horaria (por ejemplo, Informática Forense pasó de tener 32 horas a 48 horas)

1.1.3. el reordenamiento de la secuencia de dictado en algunos casos y cambios de designación de otras asignaturas." [Anexo G; pág. 6 y 7]

Los cambios de designación obedecieron principalmente a la incorporación de la materia de Taller de TF para diferenciar su dictado de la asignatura similar de la Maestría y homogeneizarla respecto de las asignaturas de Taller ya existentes (anteriormente denominadas "Seminario"). Los reordenamientos en la secuencia pueden visualizarse en el cuadro de asignaturas siendo lo más destacable el cambio de los contenidos mínimos de la primera asignatura "Ejes Temáticos de la Seguridad" que mutó su contenido de materia introductoria a una asignatura en la cual se vuelcan los conocimientos mínimos necesarios para el resto de la cursada, hecho este que se evidenció con las diferentes cohortes al observarse una falta de nivelación de los conocimientos de los estudiantes.

Se incorporó asimismo la función del Coordinador Académico que, si bien en la práctica existía desde el comienzo del posgrado, no contaba con un respaldo específico formal en la resolución de creación de la Maestría.

También se incluyó el reglamento de Trabajos de Tesis de la Maestría como parte de la nueva resolución, como lo observara el informe de evaluación de la CONEAU emitido por Resolución 847/11[6] agregando, además, la obligatoriedad de la existencia de un jurado externo para la evaluación de los trabajos presentados.

[6] https://www.coneau.gob.ar/archivos/resoluciones/Res847-11C30185.pdf; consultada 24/2/2022

La carga horaria se mantuvo en la original de su creación, 752 horas.

Siendo éste un posgrado de temática tan novedosa en la Universidad de Buenos Aires su funcionamiento despertó gran interés en los estudiantes locales y también en los de muchos países latinoamericanos que han cursado el mismo desde el inicio de su funcionamiento.
Como bien lo indica en los postulados de su fundamentación:

> "El uso masivo de las TIC (tecnologías de la información y comunicaciones) como medios para generar, almacenar, transferir y procesar información se ha incrementado espectacularmente en los últimos años, y es un elemento indispensable para el funcionamiento de la sociedad actual. La información en todas sus formas y estados se ha convertido en un activo estratégico, al cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad." [7]

A casi más de 13 años de su inicio e incluyendo los cambios curriculares realizados en 2015 se considera conveniente rever si los postulados y/o contenidos originariamente establecidos al momento de su creación continúan siendo vigentes para el mercado profesional y académico en el cual funciona este posgrado en nuestro país.

5.3. Elaboración del perfil profesional

En cuanto a la elaboración del perfil profesional que ha sido la segunda etapa en el diseño curricular de la MSI podemos indicar, como apunta Vicente Santivañez Lima [V. Santivañez Lima; 2012; pág 90]

"El Perfil Profesional del Egresado a partir de Competencias, constituye la alternativa para afrontar el reto de establecer el canal que une la institución universitaria con las exigencias del entorno laboral de la sociedad, exigencias que los nuevos profesionales que egresan puedan absolverlas con éxito y calidad en los diversos campos ocupacionales y desempeños específicos que les toque desenvolverse, cualquiera sea su profesión."

Como comentara Diaz Barriga [Barriga et al., 1990: p. 6] en la etapa de realización del perfil del egresado se realizan las siguientes tareas:

- Investigación de los conocimientos, técnicas y procedimientos de la disciplina aplicables a la solución de problemas que se compone de:

a) Investigación de las áreas en las que podría trabajar el profesional

[7] Res. 2513/15, II Fundamentación del Posgrado, A) Antecedentes, a) Razones que determinan la necesidad de creación del proyecto del posgrado

b) Análisis de las tareas potenciales del profesional

c) Determinación de poblaciones donde podría trabajar el profesional

Para finalmente lograr el Desarrollo de un perfil profesional a partir de la integración de las áreas, tareas y poblaciones determinadas.

La utilización del perfil del egresado es parte del análisis interno como lo ejemplifica Diaz Barriga [Diaz Barrriga, 2005, imagen parcial tomada de la pág. 13]:

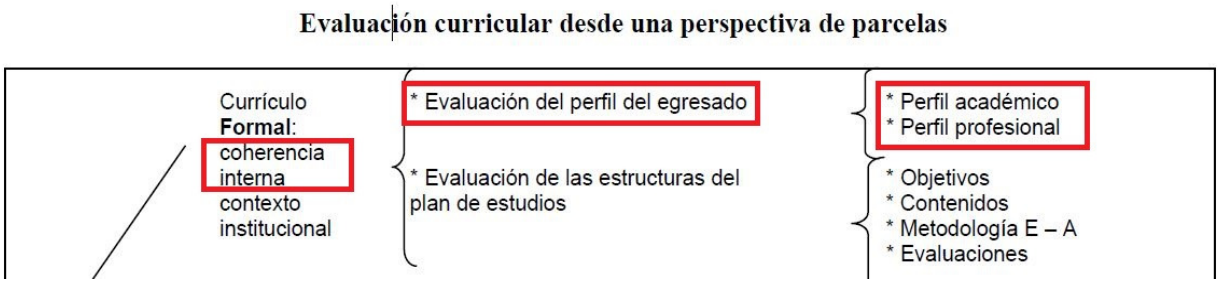


Ilustración 3 - [Diaz Barrriga, 2005, imagen parcial tomada de la pág. 13]

De la lectura de la resolución de su creación pueden observarse en la misma que los componentes necesarios para la definición de este perfil profesional han sido tomados en cuenta, a saber:

5.3.1. Investigación de las áreas en las que podría trabajar el profesional

Este componente es importante porque ayuda a dar soporte a la fundamentación del posgrado en cuestión y a situarlo en una realidad y en un contexto social.

Se indica en la resolución de su creación que su justificación cuenta con un amplio marco de referencia:

a) *Complejidad del contexto actual de las actividades públicas y privadas.*
b) *Impacto de las TIC en la gestión de las organizaciones.*
c) *Incremento notorio de los problemas de seguridad en materia de la gestión de la información.*
d) *Crecimiento de las formas de delitos mediante el uso de la tecnología.*
e) *Existencia de entes, disposiciones, estándares que exigen a las organizaciones el cumplimiento de normas de seguridad y la generación de responsabilidad emergente para quienes conducen esas organizaciones.*
f) *La escasa oferta en la República Argentina de formación universitaria en materia de Seguridad Informática.*

g) *La importancia que adquiere la protección de los activos informáticos de las organizaciones y personas, y la información acerca de los individuos.*[8] *(*)*

5.3.2. Análisis de las tareas potenciales del profesional

Dentro de las competencias esperadas del egresado de la Maestría se indican:

h) *Definir e instrumentar un plan integral de Seguridad Informática de la organización.*

i) *Definir estrategias y políticas de Seguridad Informática.*

j) *Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)*

k) *Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.*

l) *Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.*

m) *Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico.*

n) *Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones.*

o) *Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.*

p) *Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática.*

q) *Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas.*

r) *Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática.*

s) *Ejercer la docencia en materia de Seguridad Informática.*[9]

Estas competencias fueron ampliamente discutidas por los fundadores del posgrado (que la autora de este trabajo presenció en persona) para cual se realizó un análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) y del cual participaron académicos y profesionales de áreas de estudio muy diversas y transversales, lo que enriqueció ampliamente el resultado final.

[8] Res 2513/15 II. Fundamentación del Posgrado, B) Justificación de la MSI.

Este proceso tuvo lugar durante los años 2007 y 2008 mediante reuniones de los fundadores del posgrado (algunos de los cuales continuamos dentro del mismo como autoridades o docentes) en diferentes facultades y se realizaron intercambios de opiniones, consultas a otros currículos de universidades nacionales e internacionales.

También se realizaron consultas a profesionales y académicos que no formaban parte de los fundadores originales como lo menciona la Resolución de su creación: "Juan Pedro Hecht (criptógrafo), Julio Ardita (conocido especialista en seguridad), Edgardo Marcelo Ohman (doctor en psiquiatría), Pablo Kaufer Barbe (abogado), y Adrián Amigo (especialista en seguridad)" [Anexo G; pág. 3]

Se incluye aquí a los efectos puramente descriptivos el análisis FODA realizado en el mes de Abril/2009 en una en charla de presentación en sociedad del Posgrado frente a autoridades de la Escuela de Estudios de Posgrado de la FCE, otras de la UBA y potenciales estudiantes del PSI.

Tabla 2 - Análisis FODA. Posgrado en Seguridad Informática – UBA 28/4/2009	
Misión: Formar profesionales y ejecutivos con una visión integral y multidisciplinaria de la problemática de la Seguridad de la Información en las organizaciones	
Visión: Ser referentes académicos nacionales e internacionales en la especialidad de Seguridad de la Información	
Valores	• Estar a la vanguardia del conocimiento. • Fomentar la ética profesional y la integridad individual de nuestros alumnos. • Proveer diferentes visiones de la seguridad informática con independencia de compromiso comercial. • Trabajar en equipo
Fortalezas	• Posgrado desarrollado en forma conjunta por tres universidades nacionales de alto prestigio académico y respaldo de la UBA • Docentes con larga trayectoria profesional y académica • Enfoque interdisciplinario • Único en el país en su tipo
Debilidades	• Formación heterogénea de los asistentes • La falta de historia previa (por ser la primera promoción) • Dificultades en la coordinación administrativa. • Infraestructura edilicia.

	• Alta carga horaria.
Amenazas	• Aparición de nuevas propuestas educativas • Desactualización en los programas de las materias por la dinámica cambiante de la tecnología y del delito informático

En referencia a la amenaza de la desactualización, que es un peligro constante en el rubro de la SI, se sugirió en el inicio del posgrado la inclusión de Talleres de actualización que proveen un esquema menos rígido, ya que el circuito de actualización de los planes de estudio en nuestro país conlleva un gran trabajo administrativo entre las presentaciones al Consejo Superior de la UBA y posteriores verificaciones por parte de la CONEAU. En este sentido esto se mantiene aún hoy en día como una sugerencia de mejora de esta curricula.

5.3.3. Determinación de poblaciones donde podría trabajar el profesional

Las poblaciones donde podría desempeñarse el profesional de SI son prácticamente todas las imaginables considerando la gran expansión que las TICs han tenido durante los últimos años.
Prácticamente **todo tipo de empresas**, desde una PyME hasta una gran transnacional poseen sistemas de información que hacen a su desempeño comercial y humano.
Por ende, los activos de información deben resguardarse, protegerse, evolucionar y concomitantemente con ello, los recursos humanos que los utilizan y mantienen deben encontrarse conscientes y capacitados para afrontar los retos y amenazas que suceden en el día a día.

En resumen, el perfil de esta Maestría establece que el egresado debe ser un

> "***profesional*** *con aptitud para promover y aplicar metodologías actualizadas que conduzcan a la práctica de la Seguridad Informática; capaz de discernir entre las ventajas y desventajas asociadas con el diseño y gestión de políticas de seguridad; capaz de diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos, basado en estándares nacionales e internacionales y aspectos éticos-legales*".[10]

6. Interrogantes por responder en el presente trabajo: ¿Qué relación presentan los contenidos en relación con las competencias del perfil del graduado?

[10] Res 2513/15 punto IV Perfil del egresado

A los efectos de popular las competencias mencionadas en el perfil con los contenidos mínimos de las diferentes asignaturas se realiza primero una enumeración de las asignaturas con sus mnemotécnicos y comentarios en cada caso:

Tabla 3 – Grilla de Mnemotécnicos de las asignaturas (comentada)

Asignatura	**Código Asignatura**	**Observaciones**
Ejes Temáticos de la Seguridad	ET	Esta asignatura es de tipo introductorio a la temática y de nivelación de conocimientos. Se la excluye del análisis
Criptografía I	CRIPT1	
Seguridad en Redes I	RED1	
Gestión Estratégica de la Seguridad I	GEST1	
Documentación y Proyectos de Seguridad	DyPS	
Seguridad en Sistemas Operativos y Aplicaciones	SSOyA	
Comportamiento Organizacional	CO	
Seguridad en Redes II	RED2	
Marco Legal, Ética y Privacidad	MLEP	
Seguridad Física	SF	
Gestión Estratégica de la Seguridad II	GEST2	
Criptografía II	CRIPT2	
Taller de Trabajo Final de Integración / Taller de Trabajo Final de Maestría	TTFM	Asignaturas de apoyo a la realización del Trabajo final de la Especialización y de la Maestría. Se las excluye del análisis (excepto lo mencionado a continuación)
Auditoria	AUDIT	
Informática forense y delitos informáticos	IF	
Taller de Desempeño de Competencias Gerenciales	TDCG	

El corazón del posgrado se centra en tres áreas básicas de estudio, a saber:

a) Criptografía: CRIPT1 y CRIPT2

b) Redes: RED1, RED2 y SSOyA

c) Gestión: GEST1, GEST2 y DyPS

Para completar la formación técnica se requiere asimismo otra formación en temáticas que suelen denominarse “soft skills” o habilidades blandas y asignaturas de tipo transversal a las áreas básicas debido a que su formación técnica impacta en varias de las áreas básicas:

a) MLEP, CO y TDCG (habilidades blandas)
b) SF, AUDIT e IF (asignaturas transversales)
c) TTFM: Se incluyen de estas asignaturas contenidos necesarios a las habilidades blandas, a saber: Prácticas de redacción, Referencias y plagio, Selección de las fuentes bibliográficas y Fuentes de información: búsqueda y selección (estos últimos dos contenidos son equivalentes).

6.1. Coherencia curricular

6.1.1. Competencias

En cuanto a las competencias en términos muy generales se podría definir a la competencia como un *saber en acción*. [Camillioni, 2017, pág 74].

El informe del Proyecto Tuning de Reflexiones y Perspectivas de la Educación Superior en América Latina [Beneitone et al.; 2007; p. 320] define el término Competencias como:

> *“*Conjunto de conocimientos, habilidades y destrezas, tanto específicas como transversales, que debe reunir un titulado para satisfacer plenamente las exigencias de los contextos sociales… Las competencias son capacidades que la persona desarrolla en forma gradual y a lo largo de todo el proceso educativo y son evaluadas en diferentes etapas. Pueden estar divididas en competencias relacionadas con la formación profesional en general (competencias genéricas) y con un área de conocimiento (específicas de un campo de estudio).”

Así también Castañeda [Castañeda, 2012, pág. 76] nos indica: “*Los campos que conforman el perfil de egreso –académico y profesional– hacen referencia a competencias conceptuales, procedimentales y actitudinales donde se integran el saber, el hacer y el ser. Desde esta perspectiva, un perfil de egreso se constituye con los conocimientos, habilidades, actitudes y valores requeridos para satisfacer las necesidades éticas, políticas y económicas en los ámbitos laboral y social. Se concreta en tareas, funciones, actividades y acciones susceptibles de llevarse a cabo por parte del egresado*.”

Barriga menciona que [Barriga; 1999, pág. 1]

> “En los objetivos puede reconocerse tres componentes: a) la intencionalidad que proviene del agente de la acción, en este caso del educador, b) el referente de esta intencionalidad, que son la serie de comportamientos que se consideran valiosos de ser poseídos por los

educandos, e) el tiempo, corto, medio o largo, en el que se pretende lograr esos comportamientos y d) la realidad en la que se quiere lograr esos comportamientos, que son los educandos."

Esa serie de comportamientos que el educador busca lograr que el educando adquiera son las denominadas competencias, es decir, para el caso de las competencias profesionales que se espera que un profesional adquiera en materia de Seguridad Informática estas son los comportamientos que el educando debe adquirir a lo largo de la cursada de la Maestría.

Se busca verificar la congruencia de la propuesta curricular en el sentido que indica Brovelli al "*analizar el equilibrio entre los diferentes elementos que la integran (objetivos, contenidos, formatos curriculares, etc.), confrontándolos con los fundamentos y con el perfil profesional que se pretenda, a fin de detectar omisiones, incongruencias, contradicciones, que puedan afectar a la calidad de la propuesta*." [Brovelli, 2001, pág. 113]

6.1.2. Principios versus Competencias

Para realizar el análisis de la coherencia curricular interna se construye una matriz con los principios orientadores (objetivos) y las competencias específicas planteadas en el perfil del egresado siguiendo lo indicado por Castañeda [Castañeda, 2012, pág. 79] similar a la que se muestra en la siguiente imagen.

	Principios orientadores de la formación	Competencias del perfil de egreso	Asignaturas de malla de formación pedagógica
Coherencia (grado de relación)	Principios 1. 2. 3. 4.	Competencia 1. 2. 3. 4.	Asignatura 1. 2. 3. 4.

Ilustración 4 - Matriz de Coherencia curricular

A continuación, se realiza la primera etapa con las dos primeras columnas de la matriz mapeando los principios con las competencias mencionadas en el perfil de egreso del posgrado en MSI.

El contenido de esta tabla fue corroborado mediante consultas a la Comisión de la MSI (Ver Anexo B – Encuestas).

Se remitió originalmente el presente cuadro con el cual la CD de la Maestría estuvo de acuerdo en principio. Ver Anexo C (Modelo de la encuesta a las autoridades). Las competencias están numeradas siguiendo la misma numeración del punto 5.3.2

Tabla 4 - COHERENCIA CURRICULAR (Borrador aprobado originalmente)

OBJETIVO/PRINCIPIO	COMPETENCIAS ESPECÍFICAS
1. Preparar recursos humanos capacitados en todos los ámbitos relacionados con la Seguridad Informática.	a. Definir e instrumentar un plan integral de Seguridad Informática de la organización
	f. Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico
	l. Ejercer la docencia en materia de Seguridad Informática.
2. Generar la capacitación de recursos humanos de excelencia para la docencia de grado y posgrado	l. Ejercer la docencia en materia de Seguridad Informática.
	g. Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones
3. Promover el desarrollo de la investigación en materia de Seguridad Informática, a partir de la adquisición de rigurosidad científica para el análisis e interpretación del campo disciplinario	b. Definir estrategias y políticas de Seguridad Informática
	d. Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.
	a. Definir e instrumentar un plan integral de Seguridad Informática de la organización
4. Crear conciencia de la importancia y los alcances que esta área de conocimiento tiene actualmente en prácticamente todas las actividades de la sociedad, impulsando y fomentando una cultura de Seguridad Informática.	e. Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.
	g. Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones
	k. Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática
5. Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos a la sociedad.	a. Definir e instrumentar un plan integral de Seguridad Informática de la organización
6. Incorporar el conocimiento de las normas nacionales e internacionales	e. Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.

que regulan el área de la Seguridad Informática.	j. Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas
7. Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.	c. Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)
8. Formar egresados éticos capaces de generar, aplicar y transmitir los conocimientos adquiridos.	h. Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.
	i. Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática

Luego se recopilaron los comentarios al cuadro original los que se detallan a continuación.

6.1.2.1. Comentario 1: Inclusión de competencia nueva

En la realización de las encuestas a los docentes de las diferentes asignaturas se detectó que para la asignatura de Seguridad Física no existía una competencia que sustentara de manera concreta sus contenidos y el docente sugirió incorporar la siguiente competencia en la currícula:

- *Proteger físicamente los activos de la información, las personas y las instalaciones*

Esto es razonablemente lógico ya que dicha asignatura no estaba prevista cuando originalmente se creó el posgrado y luego se detectó dicho faltante incorporándola en la reforma de 2015. Se hace necesario, entonces, contar con una competencia que permita la adquisición de las habilidades o competencias que hacen a lo que suele denominarse “Seguridad Patrimonial”.

Esta competencia completa el sustento para el objetivo de “1. Preparar recursos humanos capacitados en <u>todos los ámbitos</u> relacionados con la Seguridad Informática.”

6.1.2.2. Comentario 2: Inclusión de otra competencia nueva

También uno de los miembros de la Comisión Directiva sugirió la inclusión de una competencia del estilo de:

- *Explorar y evaluar críticamente y adaptar normas internacionales/locales y/o buenas prácticas en relación a la S.I. en las organizaciones*

Justificando su existencia “*como extensión de su función (la de los profesionales egresados) de investigación, la exploración y evaluación crítica de normas internacionales y buenas prácticas que se*

generen, o actualicen, con relación a la SI, para interpretarlas e, incluso, plantear las adaptaciones y/o restricciones de aplicación en el medio local, acorde a sus características y distintos tipos de organizaciones dominantes."

Dicha competencia podría completar el sustento a los objetivos:

> 3.. *Promover el desarrollo de la investigación en materia de Seguridad Informática, a partir de la adquisición de rigurosidad científica para el análisis e interpretación del campo disciplinario*
>
> 6.. *Incorporar el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática*.

6.1.2.3. Comentario 3: Ligera modificación del objetivo 5)

Se planteó también una pequeña corrección de la redacción del objetivo:

> *5.. Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos a la sociedad*.

A una nueva forma de redacción que resulta más abarcativa, como:

> *5.. Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos en las organizaciones y, por extensión, a la sociedad.*

6.1.2.4. Comentario 4: Ligera modificación del objetivo 6)

Para brindarle un mayor espectro abarcativo se planteó la modificación del Objetivo:

> *6.. Incorporar el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.*

A una nueva redacción como:

> *6.. Incorporar <u>y aprehender</u> el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.*

Nótese que la inclusión del verbo "aprehender" concuerda con el significado que se indica en la web de [Significados.com] a diferencia del sencillo "aprender", donde se menciona:

> "*Aprender es adquirir conocimientos a través del estudio, la experiencia o la enseñanza. En cambio, aprehender es asimilar conocimientos sin necesidad de estudiar. Asimismo, los conocimientos adquiridos a través del aprender En referencia a estos 2 términos para una mejor comprensión, cuando se estudia se aprende y cuando se interactúa con el entorno se aprehende.*
>
> *Asimismo, los conocimientos adquiridos a través del aprender se pueden olvidar con el tiempo ya que el individuo no lo internaliza como el caso de que a los días no se recuerda la lec-*

ción estudiada en la universidad, muy diferente con el aprehender ya que los conocimientos obtenidos jamás se olvidan[11]*, por ejemplo: el colocarse unos zapatos*."

6.1.2.5. Versión final grilla Objetivos vs. Competencias

De los 7 profesores que desempeñan los cargos directivos de la Especialización y Maestría en Seguridad Informática el **86%** (6 de 7) validó esta grilla y sus comentarios fueron tenidos en cuenta en la elaboración de este nuevo cuadro en el cual se han resaltado en color amarillo la introducción de todos los comentarios descriptos anteriormente.

Tabla 5 - COHERENCIA CURRICULAR (Versión final con comentarios incluidos)

OBJETIVO/PRINCIPIO	COMPETENCIAS ESPECÍFICAS
1. Preparar recursos humanos capacitados en todos los ámbitos relacionados con la Seguridad Informática.	a. Definir e instrumentar un plan integral de Seguridad Informática de la organización
	f. Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico
	l. Ejercer la docencia en materia de Seguridad Informática.
	m. Proteger físicamente los activos de la información, las personas y las instalaciones
2. Generar la capacitación de recursos humanos de excelencia para la docencia de grado y posgrado	l. Ejercer la docencia en materia de Seguridad Informática.
	g. Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones
3. Promover el desarrollo de la investigación en materia de Seguridad Informática, a partir de la adquisición de rigurosidad científica para el análisis e interpretación del campo disciplinario	n. Explorar y evaluar críticamente y adaptar normas internacionales/locales y/o buenas prácticas en relación a la S.I. en las organizaciones
	b. Definir estrategias y políticas de Seguridad Informática
	d. Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.
	a. Definir e instrumentar un plan integral de Seguridad Informática de la organización
4. Crear conciencia de la importancia y los alcances que esta área de conocimiento tiene actualmente	e. Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.

[11] El subrayado corresponde a la autora

en prácticamente todas las actividades de la sociedad, impulsando y fomentando una cultura de Seguridad Informática.	g. Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones
	k. Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática
5. Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos en las organizaciones y, por extensión, a la sociedad.	a. Definir e instrumentar un plan integral de Seguridad Informática de la organización
6. Incorporar y aprehender el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.	e. Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.
	j. Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas
	n. Explorar y evaluar críticamente y adaptar normas internacionales/locales y/o buenas prácticas con relación a la S.I. en las organizaciones
7. Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.	c. Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)
8. Formar egresados éticos capaces de generar, aplicar y transmitir los conocimientos adquiridos.	h. Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.
	i. Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática

6.1.3. Competencias versus Asignaturas de la malla

Para poder completar la tabla de coherencia curricular se hace necesario indicar las diferentes asignaturas que cubren las competencias mencionadas en el perfil. Se utilizan los mnemotécnicos que se definieran en el punto 6 Tabla 3.

Como indica Díaz Barriga [Barriga et al., 1990: p. 51] *Con base en los rubros (conocimiento y habilidades) que contienen el perfil profesional, se enumeran los conocimientos y habilidades específicos que debe adquirir el profesional para que se logren los objetivos derivados de los rubros. Estos co-*

nocimientos y habilidades específicos se organizan en áreas de conocimientos, temas y contenidos de la disciplina, con base en los criterios derivados de ella.

Con este postulado presente se procede a asignar para cada una de las competencias definidas en el perfil del egresado, aquellos conocimientos que surgen de los contenidos de cada una de las asignaturas que componen este posgrado.

Se construye la siguiente tabla indicando para cada una de las competencias específicas aquellas asignaturas que las cubren en sus temáticas.

Tabla 6 - GRILLA DE COMPETENCIAS DEL PERFIL DEL EGRESADO Y ASIGNATURAS QUE LAS CUBREN EN LA CURRICULA

Nro	COMPETENCIAS	CRIPT1 y 2	RED1 y 2	GEST1 y 2	DyPS	SSOyA	SF	AUDIT	CO	MLEP	IF	TDCG	TTFM
1	Definir e instrumentar un plan integral de Seguridad Informática de la organización	X	X	X	X	X	X	X	X	X	X	X	X
2	Definir estrategias y políticas de Seguridad Informática	X	X	X	X	X	X	X	X	X	X	X	X
3	Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)	X	X	X	X	X	X	X	X	X	X	X	X
4	Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.	X	X	X	X	X	X	X	X	X	X		X
5	Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.	X	X	X	X	X	X	X	X	X	X	X	X
6	Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico	X	X	X	X	X	X	X	X	X	X	X	X
7	Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones	X	X	X	X	X	X	X	X	X	X		X

8	Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.	X	X	X	X		X	X	X	X	X	X	X
9	Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática	X	X	X	X		X	X	X	X	X	X	X
10	Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas	X	X	X	X	X		X	X	X	X		
11	Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática	X	X	X	X	X	X	X	X	X	X	X	X
12	Ejercer la docencia en materia de Seguridad Informática.	X	X	X	X	X		X	X	X	X		X

Esta grilla se construyó con la información brindada por todos los docentes que imparten las asignaturas de la MSI (100% de los encuestados respondieron la encuesta).

7. Resultados concretos de las encuestas de forma específica a docentes – Interrogantes del TF

Utilizando de base los interrogantes que se espera responder mediante el análisis curricular que se planteara en la propuesta del presente trabajo final se procedió a compaginar las respuestas brindadas por todos los docentes para cada uno de ellos.

Todas las respuestas pueden visualizarse en el Anexo E - Refundido de respuestas al cuestionario.

A continuación, los resultados hallados.

7.1. ¿Qué problemas sobre los contenidos y/o alcances del plan de estudios identifican o qué preocupaciones surgen en la perspectiva de los actores entrevistados?

Varios de los docentes manifestaron problemas con las cargas horarias asignadas a sus materias, se confecciona el siguiente cuadro:

Tabla 7 – Asignación de cargas horarias		
Asignatura	**Carga horaria original**	**Carga horaria solicitada por el docente**
Seguridad Física	16 hs (4 clases)	Solicita 2 clases más en la cursada
Auditoría	64 horas (17 clases)	Plantea la necesidad de agregar una materia corta de introducción que permita desarrollar mejor los temas previos necesarios
Informática Forense	48 horas (14 clases)	Solicita la realización de clases presenciales

y delitos informáticos		para los trabajos de laboratorio
Marco Legal, Ética y Privacidad	32 horas (9 clases)	Solicita 3 clases más en la cursada
Seguridad en los Sistemas Operativos y las Aplicaciones	48 horas (14 clases)	Si bien el docente no indicó cuántas horas o clases más necesitaría, manifestó la necesidad de incluir temas importantes que no pueden brindarse porque la carga horaria no lo permite (ver comentario en el punto siguiente)
Comportamiento Organizacional	24 horas (6 clases)	Agregar dos clases más para permitir el tratamiento con mayor profundidad y amplitud el tema de Comunicación.

Un comentario especial lo merecen las materias dedicadas al Taller de Trabajo Final de Integración y Taller de Trabajo Final de Maestría en donde el docente a cargo manifiesta que "*faltan herramientas metodológicas de investigación, los alumnos llegan al taller de TF sin tener metodología*."

7.1.1. Propuestas de mejoras

En cuanto a los interrogantes planteados a los docentes respecto de:

1. ¿Qué propuestas se plantean para resolver esos problemas?
2. Pensando en normativas nacionales e internacionales reconocidas (La decisión administrativa 641/2021 o la ISO 27002:2022) ¿considera usted que existen contenidos mínimos que podrían incluirse o excluirse en su asignatura?

7.1.2. Mejoras en cuanto a los contenidos

Respecto de los contenidos varios docentes indicaron la ampliación de estos con los que se consignan en el siguiente cuadro:

Tabla 8 – Mejoras a contenidos

Asignatura	**Contenidos mínimos a agregar**
Seguridad Física	Sistemas perimetrales y control de acceso Ciclo de vida de los soportes físicos de almacenamiento Seguridad de las Instalaciones de Suministro y del Cableado Mantenimiento de los componentes de la seguridad física Monitoreo de la seguridad
Marco Legal, Ética y Privacidad	Se sugiere desglosar el contenido mínimo de Ética y Privacidad en: Ética: Teorías éticas y su aplicación, Pensamiento crítico, Ética profesional.

	Privacidad: Teorías de Privacidad, Amenazas a la Privacidad, Leyes de Privacidad nacionales e internacionales. Regulación del comercio y Libertad de Expresión Nuevas tecnologías: su impacto ético y a la privacidad Y para la parte Legal se sugiere incorporar: Régimen legal atinente a la profesión de S.I., Cibercrimen
Auditoría	Conceptos básicos de las normas internacionales: NIST, COBIT, en lo pertinente y COSO, actualización 2013 y la versión actualizada de COSO Risk Management.
Seguridad en los Sistemas Operativos y las Aplicaciones	DevSecOps dentro de las clases del Ciclo de Vida de los Sistemas, e Ingeniería Inversa Desarrollo seguro
Gestión estratégica de la Seguridad 1	Actualización en estándares, frameworks y regulaciones
Gestión estratégica de la Seguridad 2	Metodologías internacionales de análisis de Riesgo (por ej. Magerit, etc.)
Seguridad en Redes 1	- SIEM: Gestion de eventos e incidentes de seguridad - SOC: Centro de Operaciones de Seguridad - Web Application Firewall - NIDS/NIPS Sistemas de detección y prevención de intrusos - Estrategias de seguridad en redes en ambientes cloud - Gestión de identidades [12] De la asignatura Redes 2 se incluyó el tema de IDS - Análisis de vulnerabilidades técnicas - Seguridad perimetral desde el punto de vista industrial
Seguridad en Redes 2	- Botnets - Seguridad en Arquitecturas de Servicios Web[13] Prevención de la fuga de datos

7.1.3. Otras propuestas de mejoras

Y como otras propuestas se pueden encontrar:

a) El docente a cargo de los Talleres de Trabajos Finales también manifestó una sugerencia de mejora en cuanto a la forma del dictado que actualmente está implementada en sus asignaturas: "*Creo que el taller podría estar desarrollado temporalmente de otra forma. Por ejemplo, un encuentro mensual desde el inicio de la maestría o especialización. Podría comenzar con algunos conceptos de metodología de la investigación, como para que puedan definir un problema de investigación, luego los objetivos e identificar las herramientas metodológicas que utilizarán. Esto se sumaría al contenido actual, ya que, como mencioné antes, la redac-*

[12] El docente indicó que estos temas ya se estaban dictando en la asignatura
[13] El docente indicó que estos temas anteriores ya se estaban dictando dentro de la asignatura

ción, búsqueda de información y referenciación son transversales al resto de las asignaturas. Se podrían organizar encuentros donde otros maestrandos cuenten su experiencia. También es muy útil que cada cátedra identifique una serie de temas posibles que orienten esta elección".

Los conceptos impartidos se ubican más en los contenidos de la ISO 27001:2022. Esta norma también fue utilizada como base para la DEA 641/2021

b) En la asignatura Comportamiento Organizacional se comentó:

Los conceptos impartidos se ubican más en los contenidos de la ISO 27001:2022. Esta norma también fue utilizada como base para la DEA 641/2021

Nótese que solo en el índice de esa norma ISO se establecen contenidos del tipo, a saber:

Contexto de la organización

- *Comprender las necesidades y expectativas de las partes interesadas*

Liderazgo

Tareas de Apoyo

- *Concientización*
- *Comunicación*

Esta norma da el sustento teórico conceptual para la creación del Sistema de Administración de Seguridad de la Información en una empresa y de esta norma se desprenden los controles que se mencionan en la ISO 27002.

c) En cuanto que en la asignatura Gestión Estratégica de la Seguridad 2 se sugirió: "*podrían ofrecerse seminarios en temas de seguridad de tecnologías emergentes, como la IA, la computación cuántica, los sistemas industriales, etc."*

d) En la asignatura Documentación de Proyectos de Seguridad el docente manifestó que *existe una necesidad, recabada a partir de la propia manifestación de los alumnos, de abordar la gestión de porfolios, programas y proyectos de Seguridad desde una óptica más generalista y no enfocada exclusivamente en la parte documental*, y por ende el docente sugiere: *Modificar el nombre de la asignatura a "Gestión de Proyectos de Seguridad" y preparar a los maestrandos como gestores con foco en conocimientos, técnicas y herramientas conectadas con experiencias profesionales reales.*

Asimismo, también comentó que: *El proyecto que utilizo en el curso es en sí mismo la implementación de un sistema de Gestión basado en familia ISO 27000. La materia no aborda específicamente 27001 (sistema de gestión) o 27002 (controles) pero usamos base de esos conocimientos que se trabajan en otra materia.*

7.2. ¿Qué relación presentan los contenidos en relación con las competencias del perfil del graduado y su relación con el mundo académico y el mercado laboral actual?

Las perspectivas y opiniones de los diferentes docentes se indican a continuación:

CRIPT1 y CRIPT2

Esta(s) asignatura(s) es(son) esencialmente técnica(s) (matemática discreta aplicada y álgebra abstracta aplicada) y por lo tanto ortogonal a las normas administrativas, siempre y cuando se siga dictando en el nivel actual, el que alcanza lo exigible en la implementación práctica de protocolos de seguridad que aseguren los tres pilares de la seguridad informática: **confidencialidad, integridad y disponibilidad.**

Todo es perfectible, pero no así el empeño puesto en el dictado de esta materia y que capacita a nivel competitivo en escala mundial a sus egresados. Seguiremos en esta línea docente, es nuestro compromiso.

CO

Desde el punto de vista de los contenidos para el mercado laboral, los estudiantes encuentran que la materia les resulta de suma utilidad ya que proponen casos propios de la vida real que les ocurren y esos casos, más casos elaborados por la cátedra, son tratados en clase lo que enriquece e incrementa el conocimiento y las competencias que los alumnos adquieren.

MLEP

Los estudiantes encuentran muy interesantes los conceptos vertidos en la materia ya que les habilitan un panorama mucho más amplio respecto de las habilidades blandas que un profesional de seguridad de la información debe conocer y manejar, tanto desde el punto de vista ético, los conocimientos de la privacidad y el manejo de la parte legal que un profesional debe conocer para poder desempeñarse en un cargo directivo en las empresas de hoy en día.

Los conceptos de esta asignatura cubren principalmente los controles que hacen al cumplimiento de las normas legales por parte de una empresa (control 5.31) pero también se incorporan aquellas habilidades blandas que hacen a un gerenciamiento ético y responsable no solo con los recursos propios de una empresa sino también con el público, terceros involucrados y la sociedad en general.

GEST1 y GEST2

Nosotros pasamos revista a la ISO 27002 para entender su contenido y misión dentro de la gestión de la seguridad. No entramos a analizar los controles sugeridos porque entendemos que es resorte de las materias de contenido técnico que forman parte del currículo.

Como participante activo en el desarrollo de la DA 641/2021, considero que sus contenidos están cubiertos mayormente en la cursada de la carrera. Esta norma se basó en la ISO/IEC 27002, versión 2013. La nueva versión 2022 de este estándar reordena y agrega algunos objetivos de control y controles, obteniéndose a mi entender, una norma más sencilla de interpretar y aplicar, pero que no contiene grandes cambios respecto a los contenidos de la versión anterior. Adicionalmente durante la cursada de GESI II, se recorren estándares tales como la ISO 27005, complementario de la ISO/IEC 27001, y metodologías utilizadas internacionalmente, como Magerit, para el dictado de las clases de Riesgo.

Entiendo que quien egresa de la carrera se encuentra preparado para ejercer roles técnicos, gerenciales y de liderazgo estratégico, según las motivaciones personales de cada cursante. Puede también desarrollar una carrera académica. A manera de sugerencia, podrían ofrecerse seminarios en temas de seguridad de tecnologías emergentes, como la IA, la computación cuántica, los sistemas industriales, etc.

TDCG

Considero que este Taller cubre ampliamente las competencias esperadas en los estudiantes para desempeñarse a nivel de cualquier empresa en posiciones de liderazgo de las áreas de Seguridad de la Información

IF

En relación a las normativas citadas, considero que se están dando mucho más que los contenidos mínimos y creo que es adecuado el plan de estudios diseñado en esta asignatura.

Las competencias del perfil del graduado son un conjunto de habilidades, conocimientos y actitudes que se espera que los estudiantes desarrollen a lo largo de su formación académica y que les permitan insertarse de manera exitosa en el mundo laboral actual. Entre estas

competencias se encuentran: la comunicación efectiva, el pensamiento crítico, la creatividad, la innovación, la colaboración, la responsabilidad social, la ética profesional, el aprendizaje autónomo, la adaptabilidad, el liderazgo, la gestión de proyectos y el uso de las tecnologías de la información y la comunicación. Estas competencias son relevantes tanto para el ámbito académico como para el profesional, ya que facilitan el desarrollo de procesos de investigación, generación de conocimiento, solución de problemas, trabajo en equipo y comunicación de resultados. Asimismo, estas competencias responden a las demandas y desafíos del mercado laboral actual, que requiere de profesionales capaces de adaptarse a los cambios constantes, innovar en sus campos de acción, colaborar con otros actores y asumir un compromiso ético y social con su entorno.

Dicho esto, considero que este posgrado cumple con esos postulados.

SSOyA

Inicialmente puedo mencionar que considero que los contenidos están bien seleccionados, considerando las restricciones del tiempo total de la materia.

Considero que las 12 competencias resultan pertinentes y acordes a las necesidades del mercado laboral actual. Esto fundamentado en que ofrecen al graduado la posibilidad de insertarse en el ámbito de la Seguridad de la Información o profundizar sus conocimientos en dicha temática.

Finalmente, y en relación al mundo académico, también ofrecen un fundamento interesante para empezar a ejercer la docencia dentro del ámbito. Una prueba de este punto, es la presencia de graduados como docentes o ayudantes en varias de las materias de la carrera.

TTFM

Considero que una de las habilidades más demandadas actualmente es la capacidad de trabajar en equipos interdisciplinarios. Si bien la maestría tiene un enfoque que orienta a los profesionales en tecnologías blandas, se podría complementar este perfil.

RED1 y RED2

Entiendo que las competencias que están contempladas en el Plan son suficientes y cubren ampliamente las necesidades de los futuros profesionales de SI (Redes 1)

Esta asignatura complementa lo dictado en la correlativa anterior. (Redes 2)

7.3. Tres focos conjuntos: ¿Los tres elementos analizados: plan de estudios, perspectivas y criterios de los docentes/directivos y normativa nacional conforman un conjunto armonioso y complementario?

Del análisis de todas las respuestas recabadas con sus comentarios y mejoras surge que el conjunto es en sí armonioso y complementario, aunque existen pequeños cambios que deberían introducirse, a saber:

a) La incorporación de la competencia mencionada en el punto 6.1.2.6. referida a "Proteger físicamente los activos de la información", las personas y las instalaciones y cuya necesidad surge de la asignatura de Seguridad Física.
b) Adecuar levemente la redacción de los objetivos números 5 y 6 de la Maestría en cuanto a:

   5. Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos en las organizaciones y, por extensión, a la sociedad.

   6. Incorporar y aprehender el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.

   Esto brindaría un mayor amplitud y precisión a dichos objetivos
c) Incorporar las clases solicitadas por algunas de las asignaturas (Ver Tabla 7)
d) Reordenar el tema del "Desarrollo seguro" que debería incluirse en la asignatura SSOyA y eliminarse de la asignatura RED2.
e) Ajustar los contenidos de algunas asignaturas incluyendo temáticas que actualmente ya se están dictando como parte de estas. Ver Tabla 8.
f) Ajustar las cargas horarias de las asignaturas que lo han solicitado. Ver Tabla 7.

7.4. ¿Qué valor asume el perfil del graduado de la MSI en función de lo planteado por docentes y directivos y por la normativa nacional?

En los términos indicados por los mismos docentes al responder respecto de este interrogante se puede comentar que (los subrayados son de la autora):

RED1 y RED2:

La materia aborda temas técnicos y brinda a los alumnos conocimientos y habilidades esenciales para establecer medidas de seguridad en una organización. Las herramientas son fundamentales para proteger la infraestructura, la red, las aplicaciones y los datos de la empresa, y su comprensión permite a los estudiantes desempeñar un rol activo al momento de definir e instrumentar un plan integral de Seguridad Informática de la organización.

Los conocimientos técnicos brindados sirven de base para que un directivo en una organización pueda tomar decisiones para definir un plan de seguridad, establecer las estrategias y elaborar los planes.

La materia (RED2) contribuye a fortalecer el grado de control interno de las organizaciones al educar y concientizar sobre los riesgos de seguridad, implementar controles mediante las herramientas técnicas aprendidas y preparar a los estudiantes para responder a incidentes de seguridad.

CRIPT1 y CRIPT2

Considero que los contenidos mínimos definidos son adecuados para la capacitación criptológica de los cursantes de la Maestría. En conjunto, el resultado es más que adecuado para la comprensión teórica y práctica de la criptografía y el criptoanálisis por parte de los profesionales IT cursantes en este posgrado.

Los graduados de la maestría reconocen y agradecen la formación adquirida en esta especialidad.

Esta asignatura técnica (CRIPT2) es dictada al nivel equivalente al de las dos primeras carreras equivalentes en los EEUU (MIT y Stanford) y las dos primeras carreras equivalentes en España (Universidad Politécnica de Madrid y Universidad Carlos III de Madrid). Esto ha sido verificado por el docente a cargo y sustentado por el Prof Emérito en Criptografía Dr. JORGE RAMIÓ AGUIRRE, creador de la mayor red iberoamericana de la especialidad tanto docente como en investigación (CRIPTORED). La idea es brindar formación criptológica de excelencia, 100% actualizada y revisada año a año y con enfoques que concilian la teoría con la práctica de la seguridad de la información. Ciertamente somos una de las asignaturas pilares de nuestra Maestría.

GEST1 y GEST2

Considero que resolvemos muy satisfactoriamente la demanda de las organizaciones en cuanto al perfil que hemos nosotros adoptado.

Entiendo que quien egresa de la carrera se encuentra preparado para ejercer roles técnicos, gerenciales y de liderazgo estratégico, según las motivaciones personales de cada cursante. Puede también desarrollar una carrera académica.

SSOyA

Considero que las 12 competencias resultan pertinentes y acordes a las necesidades del mercado laboral actual. Esto fundamentado en que ofrecen al graduado la posibilidad de insertarse en el ámbito de la Seguridad de la Información o profundizar sus conocimientos en dicha temática.

Finalmente, y en relación al mundo académico, también ofrecen un fundamento interesante para empezar a ejercer la docencia dentro del ámbito. Una prueba de este punto es la presencia de graduados como docentes o ayudantes en varias de las materias de la carrera.

TDCG

Considero que este Taller cubre ampliamente las competencias esperadas en los estudiantes para desempeñarse a nivel de cualquier empresa en posiciones de liderazgo de las áreas de Seguridad de la Información.

Los contenidos impartidos cubren las expectativas de las normas en los términos de Liderazgo, Concientización y Manejo de conflictos.

AUDIT

Creemos que se ajustan al perfil profesional, teniendo en cuenta que la Especialización y Maestría en Seguridad Informática ha sido diseñada específicamente para responder al mismo. Cubre una necesidad integradora que resulta imprescindible para formar personal jerarquizado especializado con las habilidades de gestión en el más amplio sentido del término.

IF

Las competencias del perfil del graduado son un conjunto de habilidades, conocimientos y actitudes que se espera que los estudiantes desarrollen a lo largo de su formación académica y que les permitan insertarse de manera exitosa en el mundo laboral actual. Entre estas competencias se encuentran: la comunicación efectiva, el pensamiento crítico, la creatividad, la innovación, la colaboración, la responsabilidad social, la ética profesional, el aprendizaje autónomo, la adaptabilidad, el liderazgo, la gestión de proyectos y el uso de las tecnologías de la información y la comunicación. Estas competencias son relevantes tanto para el ámbito académico como para el profesional, ya que facilitan el desarrollo de procesos de investigación, generación de conocimiento, solución de problemas, trabajo en equipo y comunicación de resultados. Asimismo, estas competencias responden a las demandas y desafíos del mercado laboral actual, que requiere de profesionales capaces de adaptarse a los cambios constantes, innovar en sus campos de acción, colaborar con otros actores y asumir un compromiso ético y social con su entorno.

Dicho esto, considero que este posgrado cumple con esos postulados.

CO

Desde el punto de vista de los contenidos para el mercado laboral, los estudiantes encuentran que la materia les resulta de suma utilidad ya que proponen casos propios de la vida real que les

ocurren y esos casos, más otros elaborados por la cátedra, son tratados en clase lo que enriquece e incrementa el conocimiento y las competencias que los alumnos adquieren.

MLEP

Los estudiantes encuentran muy interesantes los conceptos vertidos en la materia ya que les habilitan un panorama mucho más amplio respecto de las habilidades blandas que un profesional de seguridad de la información debe conocer y manejar, tanto desde el punto de vista ético, los conocimientos de la privacidad y el manejo de la parte legal que un profesional debe conocer para poder desempeñarse en un cargo directivo en las empresas de hoy en día.

8. Construcción de los referentes

8.1. Actualización de la DA 641/2021

El campo de la seguridad informática tiene un movimiento en el mercado de tipo vertiginoso, no solo por los inconvenientes a nivel de la seguridad que aparecen diariamente sino por los esfuerzos internacionales para su regulación y la mitigación de amenazas.

Al momento del planteamiento original de la propuesta del presente trabajo la DA 641 emitida el 4/6/2021 era lo más actualizado a nivel del gobierno argentino. Esa norma está basada primordialmente en los controles definidos en la norma ISO/IEC 27002:2013 [ISO27002 2013] y en el mes de febrero del año 2022 el organismo ISO emitió una nueva norma 27002 que modificó la estructura anterior siendo sus principales cambios:

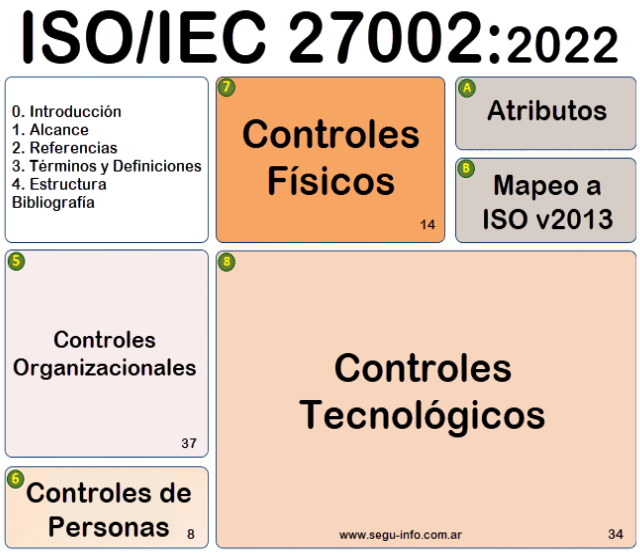


Ilustración 5 - – Nuevas áreas en la ISO 27002:2022 [Segu-Info; 2022]

- *"El cambio de nombre*
- *Incorporación de nuevos términos y definiciones*
- *La nueva estructura de temas de seguridad de la información*
- *La nueva estructura de atributos de los controles*
- *Cambios en controles desde la versión ISO 27002:2013"* [Segu-info; 2022]

Los 14 dominios de controles con los que contaba la ISO 27002:2013 se reestructuraron en esta nueva versión del 2022 en 4 grandes áreas proveyendo una estructura más simple, a saber: Controles Organizacionales, Controles de Personas, Controles Físicos y Controles Tecnológicos.
Asimismo, los 114 controles originales de la versión 2013 fueron reducidos a 93, siendo algunos controles fusionados en nuevos controles y se agregaron 11 nuevos controles que no estaban previstos en la ISO del año 2013.
Como también lo grafica la profesional Marcela Pallero [Pallero; 2023] esta agrupación puede ejemplificarse como:

Ilustración 6 – Dominios de la ISO 27002:2022 [Pallero; 2023]

En aras de proveer una mejor actualización de este referente se procedió entonces a determinar detalladamente todas las directrices incluidas en la DA 641 y se las comparó con los controles originales de la ISO 27002:2013 para luego encontrar sus equivalentes en la nueva norma ISO 27002:2022.
De dicha actualización surge que no quedan directrices de la DA 641 no previstas en la nueva norma ISO 27002:2022 y se agregan además los 11 nuevos controles más actuales.

De los 11 nuevos controles el control 5.30 de “Preparación de las TIC para la continuidad del negocio”, puede llegar a subsumirse en los controles de la DA 641 13.1 aunque en este control de la reglamentación argentina no se menciona el BIA (Análisis de Impacto del Negocio; Business impact Análisis) pero si se menciona en la introducción general de la DA 641 (introducción y Directriz 1.) como Análisis (o Evaluación) de Riesgos.
Esta actualización queda plasmada en el Anexo A para su posterior utilización en las Encuestas.

9. Conclusiones del presente trabajo

Luego de realizadas y evaluadas las respuestas tanto de la CD como de todos los docentes se han podido recabar diferentes cambios sugeridos para introducir en la actual curricula de la Maestría en SI.
A modo de compilación se indican aquí todos los cambios de forma resumida resaltando aquellos cambios concretos, ya sea por supresión o por agregado de contenidos y/o competencias.

9.1. Objetivos/Principios

Los objetivos y/o Principios de la Maestría se sugiere que sean las siguientes:
1. Preparar recursos humanos capacitados en todos los ámbitos relacionados con la Seguridad Informática.
2. Generar la capacitación de recursos humanos de excelencia para la docencia de grado y posgrado
3. Promover el desarrollo de la investigación en materia de Seguridad Informática, a partir de la adquisición de rigurosidad científica para el análisis e interpretación del campo disciplinario
4. Crear conciencia de la importancia y los alcances que esta área de conocimiento tiene actualmente en prácticamente todas las actividades de la sociedad, impulsando y fomentando una cultura de Seguridad Informática.
5. Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos en las organizaciones y, por extensión, a la sociedad.
6. Incorporar y aprehender el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.
7. Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.
8. Formar egresados éticos capaces de generar, aplicar y transmitir los conocimientos adquiridos.

9.2. Competencias

Se sugiere que las competencias de la Maestría sean las siguientes:

a. Definir e instrumentar un plan integral de Seguridad Informática de la organización

b. Definir estrategias y políticas de Seguridad Informática

c. Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)

d. Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.

e. Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.

f. Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico

g. Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones

h. Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.

i. Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática

j. Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas

k. Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática

l. Ejercer la docencia en materia de Seguridad Informática.

m. Proteger físicamente los activos de la información, las personas y las instalaciones

n. Explorar y evaluar críticamente y adaptar normas internacionales/locales y/o buenas prácticas en relación a la S.I. en las organizaciones

9.3. Contenidos de las asignaturas

Se confecciona la siguiente tabla comparada de los contenidos originales y los nuevos contenidos sugeridos. En la misma se consignan solamente aquellas asignaturas para las que se sugieren cambios. Los contenidos en amarillo son contenidos nuevos que se sugieren. Los contenidos que se han

movido de asignatura se resaltan en color rosa. Los contenidos suprimidos se han tachado en el texto del contenido original. En los casos de contenidos reformulados se los ha marcado en color verde claro.

Tabla 9 – Contenidos de las asignaturas comparado	
ASIGNATURA: **Seguridad en redes I**	
Esquemas de seguridad: distribución de claves simétricas. Administración de claves publicas: autoridad certificante y certificados. Administración de claves de sesión compartidas. Seguridad de redes e Internet: Single Sign On, Infraestructura de Clave Publica PKI. Seguridad de WWW; comercio electrónico, gateways de pago, ~~protocolo SET "Secure Electronic Transaction";~~ seguridad en IP IPSec: Firewalls, SSL. Seguridad en organizaciones: Firma Digital, ~~Factura Electrónica;~~ administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades.	Esquemas de seguridad: distribución de claves simétricas. Administración de claves públicas: autoridad certificante y certificados. Administración de claves de sesión compartidas. Seguridad Perimetral, firewalls. Web Application Firewall. NIDS/NIPS Sistemas de detección y prevención de intrusos (IDS). Seguridad de redes e Internet: Infraestructura de Clave Publica PKI, Estrategias de seguridad en redes en ambientes cloud. Protocolos de Autenticación: Single Sign On. Seguridad de WWW; Protocolo TLS/SSL, comercio electrónico, gateways de pago. Seguridad en IP IPSec. Seguridad en organizaciones: Firma Digital, Administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades. Análisis de vulnerabilidades técnicas. SIEM: Gestión de eventos e incidentes de seguridad. SOC: Centro de Operaciones de Seguridad. Seguridad perimetral: enfoque desde el punto de vista industrial. Optativos: SET, Factura Electrónica
ASIGNATURA: **Gestión estratégica de la seguridad I**	
Organización y estructura del área de seguridad: áreas, funciones y responsabilidades, perfiles, criterios de organización. Técnicas de gestión (estrategia, finanzas, marketing y recursos humanos). Ciclo de vida de los sistemas de seguridad. Gestión de proyectos de seguridad. Tercerización de servicios y gestión de proveedores. Evaluación económica de la seguridad. Métricas y performance. Estrategias, políticas, programas y normas de seguridad. Introducción al análisis y gestión del riesgo.	Organización y estructura del área de seguridad: áreas, funciones y responsabilidades, perfiles, criterios de organización. Técnicas de gestión (estrategia, finanzas, marketing y recursos humanos). Ciclo de vida de los sistemas de seguridad. Gestión de proyectos de seguridad. Tercerización de servicios y gestión de proveedores. Evaluación económica de la seguridad. Métricas y performance. Estrategias, políticas, programas y normas de seguridad. Introducción al análisis y gestión del riesgo.

	Actualización en estándares, frameworks y regulaciones
ASIGNATURA: ~~Documentación y proyectos de seguridad~~ Gestión de Proyectos de Seguridad	
Formulación y seguimiento de un proyecto de seguridad en base a un caso de estudio incluyendo el ciclo de vida de los sistemas de seguridad; fase inicial, fase de desarrollo y adquisición, fase de implementación, fase de operación y mantenimiento, fase de disposición.	Formulación y seguimiento de un proyecto de seguridad en base a un caso de estudio incluyendo el ciclo de vida de los sistemas de seguridad; fase inicial, fase de desarrollo y adquisición, fase de implementación, fase de operación y mantenimiento, fase de disposición. Gestión de porfolios, programas y proyectos de seguridad.
ASIGNATURA: **Seguridad en sistemas operativos y aplicaciones**	
Instalación y operación segura del sistema operativo. Ciclo de vida del desarrollo de sistemas. Desarrollo y gestión de bases de datos. Controles de los sistemas. Control en la operación y el mantenimiento de las aplicaciones. Aplicaciones distribuidas. Ataques y vulnerabilidades en aplicaciones y sistemas. Buffer Overflows, Format Strings, Race Conditions. Entornos protegidos (sandboxes, chroot). Mecanismos de protección: técnica del canario, segmento no ejecutable. Análisis de logs. HostIDS. Vulnerabilidades en web. Códigos maliciosos.	Instalación y operación segura del sistema operativo. Ciclo de vida del desarrollo de sistemas, DevSecOps. Desarrollo y gestión de bases de datos. Controles de los sistemas. Control en la operación y el mantenimiento de las aplicaciones. Aplicaciones distribuidas. Ataques y vulnerabilidades en aplicaciones y sistemas. Buffer Overflows, Format Strings, Race Conditions. Entornos protegidos (sandboxes, chroot). Mecanismos de protección: técnica del canario, segmento no ejecutable. Análisis de logs. HostIDS. Vulnerabilidades en web. Códigos maliciosos. Ingeniería inversa. Desarrollo seguro.
ASIGNATURA: **Seguridad en Redes II**	
Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, ~~Intrusión Detection Systems~~ Honeypots; análisis de vulnerabilidades, pruebas de penetración. ~~Desarrollo seguro.~~ Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de con-	Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, Botnets Honeypots; análisis de vulnerabilidades, pruebas de penetración. Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de con-

trol. Ubicación de Firewalls, ~~IDS.~~	trol. Ubicación de Firewalls. Seguridad en Arquitecturas de servicios Web. Prevención de la fuga de datos.
ASIGNATURA: **Marco legal, ética y privacidad**	
Introducción al Derecho Informático, conceptos y terminología legal. Sistemas legales en Argentina y otros países. Régimen jurídico de protección de la Propiedad Intelectual. Régimen de Firma Digital. Visión jurídica de los delitos informáticos. Derecho Internacional: legislación transfrontera. Jurisprudencia. Ética y privacidad.	Introducción al Derecho Informático, conceptos y terminología legal. Sistemas legales en Argentina y otros países. Régimen jurídico de protección de la Propiedad Intelectual. Régimen de Firma Digital. Visión jurídica de los delitos informáticos. Cibercrimen Régimen legal atinente a la profesión de S.I. Derecho Internacional: legislación transfrontera. Jurisprudencia. Ética: Teorías éticas y su aplicación, Pensamiento crítico, Ética profesional. Privacidad: Teorías de Privacidad, Amenazas a la Privacidad, Leyes de Privacidad nacionales e internacionales Regulación del comercio y Libertad de Expresión Nuevas tecnologías: su impacto ético y a la privacidad
Asignatura: **Seguridad Física**	
Administración y relevamiento de los riesgos. Planeamiento y gerenciamiento de la Seguridad Física. La tecnología y el diseño de procesos de trabajo. Aplicación de diseños. Sistemas de seguridad física.	Administración y relevamiento de los riesgos. Planeamiento y gerenciamiento de la Seguridad Física. La tecnología y el diseño de procesos de trabajo. Aplicación de diseños. Sistemas de seguridad física. Sistemas perimetrales y control de acceso Ciclo de vida de los soportes físicos de almacenamiento Seguridad de las Instalaciones de Suministro y del Cableado Mantenimiento de los componentes de la seguridad física Monitoreo de la seguridad
ASIGNATURA: **Gestión estratégica de la seguridad II**	
Análisis y gestión del riesgo, modelo de valor, mapa de riesgos, evaluación de salvaguardas, informe de insuficiencias, catálogo de elementos, estado de riesgo. Ciclo de vida: análisis y gestión, planificación,	Análisis y gestión del riesgo, modelo de valor, mapa de riesgos, evaluación de salvaguardas, informe de insuficiencias, catálogo de elementos, estado de riesgo. Metodologías internacionales de análisis de Riesgo (por ej. Magerit, etc.) Ciclo de vida: análisis y gestión, planificación,

implementación de salvaguardas, gestión de configuración y cambios. Relación y complementariedad entre los distintos estándares y/ modelos (frameworks), cumplimiento (compliance), regímenes e instituciones Internacionales y Nacionales: Cobit, Coso, BSI, ISO, ITIL, Basilea II, CMM, SOX, otros.	implementación de salvaguardas, gestión de configuración y cambios. Relación y complementariedad entre los distintos estándares y/ modelos (frameworks), cumplimiento (compliance), regímenes e instituciones Internacionales y Nacionales: Cobit, Coso, BSI, ISO, ITIL, Basilea II, CMM, SOX, otros.
ASIGNATURA: **Auditoría**	
Control y auditoría. Normas técnicas. Control y estructura organizativa. Separación de funciones y oposición de intereses. Análisis específico del área de Seguridad Informática. Controles en las entradas al sistema y sus almacenamientos. Transacciones rechazadas y observadas. Concepto de monitoreo. Planificación de las actividades de auditoría. Pruebas de cumplimiento. Evaluación de aplicación de políticas, planes, normas, procedimientos, esquemas, estándares y métricas. Pruebas y técnicas asociadas. Pistas de auditoría. Evaluación del nivel de respuesta ante incidentes. Test de penetración. Test de nivel de divulgación y comprensión de políticas, normas y procedimientos en la organización. Comprobaciones y simulaciones sobre planes de contingencia, continuidad de operaciones y recuperación.	Control y auditoría. Normas técnicas. Control y estructura organizativa. Separación de funciones y oposición de intereses. Análisis específico del área de Seguridad Informática. Controles en las entradas al sistema y sus almacenamientos. Transacciones rechazadas y observadas. Concepto de monitoreo. Planificación de las actividades de auditoría. Pruebas de cumplimiento. Evaluación de aplicación de políticas, planes, normas, procedimientos, esquemas, estándares y métricas. Pruebas y técnicas asociadas. Pistas de auditoría. Evaluación del nivel de respuesta ante incidentes. Test de penetración. Test de nivel de divulgación y comprensión de políticas, normas y procedimientos en la organización. Comprobaciones y simulaciones sobre planes de contingencia, continuidad de operaciones y recuperación. Conceptos básicos de las normas internacionales: NIST, COBIT en lo pertinente, COSO, COSO Risk Management, todas actualizadas.

9.4. Carga horaria de las asignaturas

En cuanto a las cargas horarias de las asignaturas varios docentes manifestaron la necesidad de ajustarla.

Se elabora el presente cuadro considerando las horas originalmente asignadas y a modo de propuesta, las horas extra que se podrían asignar para completar lo solicitado por los docentes.

Tabla 10 – Carga horaria de las asignaturas comparada

Asignatura	**Carga horaria original** (hs.)		**Carga horaria objetivo**		**Comentario**
	Teórica	Práctica	Teórica	Práctica	
Seguridad Física	12	4	16	8	De 4 clases pasa a 6 clases
Introducción a la Auditoría (nueva asignatura)	--	--	12	4	Se proponen 4 clases

Marco Legal, Ética y Privacidad	32		42		De 9 clases pasa a 12 clases
Seguridad en los Sistemas Operativos y las Aplicaciones	32	16	36	20	Se agregan 2 clases extra
Comportamiento Organizacional	16	8	20	12	Se agregan 2 clases extra

9.5. Otras problemáticas/propuestas planteadas

Se enumeran a continuación otras problemáticas planteadas por el cuerpo docente:

- En Informática Forense y delitos informáticos el docente solicitó la realización de clases presenciales para los trabajos de laboratorio
- En los Talleres para los Trabajos finales de la especialización y de la Maestría planteó la necesidad de replantear la forma de cursada de la materia proponiendo una cursada que cuente con encuentros de tipo mensual desde el inicio de la cursada.
- Desde la asignatura de Gestión de la Seguridad 2 se sugirió incorporar seminarios en temas de seguridad de tecnologías emergentes, como la IA, la computación cuántica, los sistemas industriales, etc. (Comentario de la autora: En la asignatura de Marco Legal, Ética y privacidad se han incorporado conceptos de tecnologías emergentes y la IA. Los sistemas industriales se planteó su futura incorporación en le asignatura Seguridad en redes 2)
- La Comisión sugirió la inclusión de Talleres de actualización como parte de la curricula como ya se mencionó al final del punto 5.3.2, para propender a una actualización constante en el área de Seguridad de la Información.

10. Colofón

Recapitulando lo presentado en este trabajo en cuanto a los Fundamentos y objetivos al momento de la creación de la Maestría en SI versus la Normativa nacional e internacional.

Al momento de la creación de la Maestría en el año 2008 los objetivos planteados cubrían ampliamente normas internacionales sobre el tema como ser las normas de la gama de las ISO 27000 (por ejemplo: ISO 27001: Gestión de Sistemas de Seguridad de la Información, ISO 27002: Seguridad de la Información, Ciberseguridad y Protección de la Privacidad (Controles)).

Incluso las normas ISO recién incorporaron como un pilar de la norma los conceptos de Privacidad (nótese la inclusión en el título de la misma norma) que en las versiones anteriores estaba en la norma, pero con una menor relevancia respecto de los otros pilares de la seguridad de la informa-

ción, mientras que la Maestría ya lo había incorporado como parte de sus objetivos y en su currícula en el 2008 al contar entre las competencias aquellas dirigidas a la temática de Privacidad.
En la búsqueda de ofertas similares internacionales se tomaron en cuenta ofertas de Universidades reconocidas a nivel mundial como ser el Cerias (The Center for Education and Research in Information Assurance and Security) de la University of Purdue, Indiana, EE.UU; el Master in Science in Information Assurance Infosec Graduate Program de la universidad de Norwich University Vermont USA, y la Universidad Kennesaw State University; Georgia, EE.UU; Center for Information security Education, que fue nominado como el National Center of Academic Excellence in Information Assurance Education por la National Security Agency (NSA).
Esto permitió contrastar las diversas tendencias internacionales para estas formaciones de posgrado entre universidades de renombre internacional.

En cuanto a la comparativa con la norma local DA 641/2021 [DA 641; 2021; pág. 2] pueden verse que sus objetivos, tanto el general (OG) como los específicos (OE) comparados con los objetivos enumerados en el presente trabajo en la tabla 4 de Coherencia Curricular punto 6.1.2 se corresponden como, por ejemplo, para mencionar algunos:
OG- Proteger los activos de información, frente a riesgos internos o externos, que pudieran afectarlos, para así preservar su confidencialidad, integridad y disponibilidad.

Se sustenta en los objetivos de la MSI:

O1- Preparar recursos humanos capacitados en todos los ámbitos relacionados con la Seguridad Informática.

O4- Crear conciencia de la importancia y los alcances que esta área de conocimiento tiene actualmente en prácticamente todas las actividades de la sociedad, impulsando y fomentando una cultura de Seguridad Informática.

O5- Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos a la sociedad.

O7- Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.

OE- Proteger la información, los datos personales y activos de información propios del conjunto de organismos que componen el Sector Público Nacional.

Se sustenta en los objetivos de la MSI:

O7- Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.

O8- Formar egresados éticos capaces de generar, aplicar y transmitir los conocimientos adquiridos.

Nótese que el objetivo O3 de la MSI no sustenta ningún objetivo de la DA 641: *Promover el desarrollo de la investigación en materia de Seguridad Informática, a partir de la adquisición de rigurosidad científica para el análisis e interpretación del campo disciplinario*; ya que, si bien no es un objetivo explicitado en dicha norma, es necesario para promover una continua capacitación de los profesionales de la Seguridad de la Información y, por ende, es parte de los objetivos de la Maestría.

El presente análisis ha contado con la amplia colaboración de todos los integrantes de la Maestría en Seguridad Informática, tanto la Comisión Directiva como todos los docentes que la conforman.
Se ha logrado arribar a propuestas de mejoras que incrementarían el perfil del egresado a nuevas tecnologías y problemáticas dentro de la profesión en un entorno en constante cambio.
Si bien este análisis es parcial ya que no se han analizado aspectos tales como la modalidad de la cursada, formas de evaluación, cuestiones administrativas, etc., quedan los mismos para un proceso de evaluación más profundo.
Como un dato extra, se obtuvo el promedio de las evaluaciones al cuerpo docente realizadas por los alumnos cursantes en el año 2022 siendo el mismo de 9 puntos sobre una escala de 10, lo que constituye un importante logro desde la óptica de los cursantes.

11. Referencias Bibliográficas

[Anguita et al., 2003 parte I] J. Casas Anguita, J.R. Repullo Labrador y J. Donado Campos; La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I); Aten Primaria 2003;31(8):527-38; https://es.scribd.com/document/219294154/Diseno-de-Cuestionarios-Casas-Anguita#; consultado 18/1/2023

[Anguita et al., 2003 parte II] J. Casas Anguita, J.R. Repullo Labrador y J. Donado Campos; La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (II); Aten Primaria 2003;31(9):592-600; https://es.scribd.com/document/329078241/Anguita-Repullo-y-Campos-La-Encuesta-Como-Tecnica-de-Investigacion-II; consultado 18/1/2023

[Barriga et al., 1990] Díaz Barriga, F., Lule, M. Rojas, S. y Saád, S. (1990) Metodología de Diseño Curricular para la Educación Superior. México. Trillas; https://etrillas.mx/libro/metodologia-de-diseno-curricular-para-educacion-superior_4232

[Barriga; 1999] Algo más sobre Objetivos y Competencias; Carlos Barriga Hernández; https://es.scribd.com/document/244472835/Arequipa-BARRIGA-CARLOS-ALGO-MAS-SOBRE-OBJETIVOS-Y-COMPETENCIAS-Dr-CARLOS-1-doc#; consultado el 16/4/2023

[Barriga, 2005] Barriga, Ángel Díaz; Evaluación curricular y evaluación de programas con fines de acreditación. Cercanías y desencuentros; Conferencia para el Congreso Nacional de Investigación Educativa. Sonora, 2005.

[Beneitone et al.; 2007] Beneitone, P., Esquetini, C., González, J., Maletá, M. M., Siufi, G., & Wagenaar, R. (2007). Reflexiones y perspectivas de la Educación Superior en América Latina. Informe Final – Proyecto Tuning – América Latina 2004-2007. Universidad de Deusto & Universidad de Groeningen; http://erasmusplusriesal.org/es/contenido/reflexiones-y-perspectivas-de-la-educacion-superior-en-america-latina; consultado 7/4/2023

[Brovelli, 2001] Brovelli, Marta; Evaluación curricular; Fundamentos en Humanidades, vol. II, núm. 4, primavera, 2001; Universidad Nacional de San Luis; San Luis, Argentina

[Camillioni, 2017] Camillioni, Alicia W. de; Ensayos: Tendencias y formatos en el currículo universitario; Mayo 2017; Itinerarios Educativos; DOI: 10.14409/ie.v0i9.6536; https://www.researchgate.net/publication/316653153_EnsayosTendencias_y_formatos_en_el_curriculo_universitario

[Castañeda, 2012] Castañeda, M., Castro Rubilar, F. & Mena Bastías, C. (2012). Instrumentos para evaluar el currículum formal en carreras pedagógicas. Panorama, 6 (10), 71-85. Adaptándolo a la temática del presente posgrado. (Trabajo principal)

[CISO Mindmap; 2021] CISO MindMap 2021: ¿Qué hacen realmente los profesionales de InfoSec?; 24/1/2022; https://blog.segu-info.com.ar/2022/01/ciso-mindmap-2021-que-hacen-realmente.html

[DA 641; 2021] Decisión Administrativa 641/2021 Jefatura de Gabinetes de Ministros; 25/6/2021; http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=351345, consultada 19/6/2022

[Guillermet; 2007] El Proyecto TUNING sobre Educación Superior en América Latina: Objetivos, acciones, conclusiones generales y resultados específicos en el área Física; Dr. Amando Fernández Guillermet; https://www.researchgate.net/publication/273774647_El_Proyecto_TUNING_sobre_Educacion_Superior_en_America_Latina_Objetivos_acciones_conclusiones_generales_y_resultados_especificos_en_el_area_Fisica; consultado el 7/4/2023

[ISO 27002 2013] https://www.iso.org/standard/54533.html; consultada el 5/2/2023

[ISO 27002; 2022] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, https://www.iso.org/standard/75652.html, consultada 18/1/2023

[Lewy; 1976] Lewy, A. "Naturaleza de la evaluación del currículo" en Manual de evaluación formativa del currículo. Bogotá, Voluntad-UNESCO, 1976.

[Página 12; 2021] Qué hacer ante los nuevos delitos virtuales. Guía del ciberdelito, desde las estafas con el CBU a los hackeos al WhatsApp; https://www.pagina12.com.ar/391628-guia-del-ciberdelito-desde-las-estafas-con-el-cbu-a-los-hack; 26/12/2021; consultada el 8/1/2022

[Pallero; 2023] ISO 27002 de 2022; https://twitter.com/Marce_I_P/status/1691140592460247044?t=clJ4VcAm24t2GyyMuwV9fQ&s=03, consultado 15/8/2023

[Res. 282/16 CONEAU] Res. 282/16; Acreditar la carrera de Maestría en Seguridad Informática, de la Universidad de Buenos Aires, Facultad de Ingeniería, Facultad de Ciencias Exactas y Naturales y Facultad de Ciencias Económicas, que se dicta en la Ciudad Autónoma de Buenos Aires; https://www.coneau.gob.ar/archivos/resoluciones/Res282-16C30477-15.pdf; consultada 10/7/2023

[Res. 847/11 CONEAU] Res. 847/11; Acreditar la carrera de Maestría en Seguridad Informática, de la Universidad de Buenos Aires, Facultad de Ingeniería, Facultad de Ciencias Exactas y Naturales y Facultad de Ciencias Económicas, que se dicta en la Ciudad Autónoma de Buenos Aires; https://www.coneau.gob.ar/archivos/resoluciones/Res847-11C30185.pdf; consultada 10/7/2023

[Segu-Info; 2022] Cambios en la nueva ISO/IEC 27002/2022; 25/1/2022; Blog Segu-Info; https://blog.segu-info.com.ar/2022/01/cambios-en-la-nueva-isoiec-270022022.html; consultada el 18/1/2023

[Significados.com]. Disponible en: https://www.significados.com/aprehender/ Consultado: 10 de julio de 2023, 11:13 am.

[V. Santiváñez Lima; 2012] Vicente Santivañez Lima; Diseño curricular a partir de competencias; 2012; Bogotá: Ediciones de la U

12. Otra bibliografía consultada

- Análisis Curricular plan de estudios 1993 y 2009; Taxadhó, Ixmiquilpan, Hugo., 16 de junio del 2010; https://es.scribd.com/document/385511797/Analisis-Curricular-plan-de-estudios-1993-y-2009
- Casarini Ratto, Marta; Teoría y diseño curricular; Edit. Trillas; 1997
- Delgado Villca, M.Sc. Lic. Jimmy; Unidad Didáctica I: Aspectos Conceptuales de la Teoría Curricular; UNIVERSIDAD MAYOR DE SAN SIMÓN, Facultad de Humanidades y Cs. de la Ed., Carrera de Ciencias de la Educación (presentación ppt)
- Diaz-Barriga Arceo, Frida; Lule Gonzalez, Ma de Lourdes; Metodología de diseño curricular para educación superior; Edit. Trillas
- Diaz Barriga, Angel; El enfoque de competencias en la educación. ¿Una alternativa o un disfraz de cambio?; Perfiles Educativos, vol. XXVIII, núm. 111, enero-marzo, 2006, pp. 7-36; Instituto de Investigaciones sobre la Universidad y la Educación; Distrito Federal, México
- Frida, A. (1990); Evaluación Curricular; FUENTE: DIAZ BARRIGA; Metodología del diseño curricular para educación superior. México: Trillas. UNIDAD. 5: "ETAPA CUATRO: EVALUACIÓN CURRICULAR". (presentación ppt) https://es.scribd.com/presentation/552292785/Evaluacion-Curricular

- Garza-González, Beatriz; Ma. Alejandra Hernández-Castañón y Aurora Zamora-Mendoza; Competencias profesionales para la atención de las adicciones, en los programas de licenciatura en enfermería de la universidad autónoma de Querétaro, México; Revista Iberoamericana para la Investigación y el Desarrollo Educativo; ISSN 2007 – 7467; Vol. 6 Num. 11; Junio – Diciembre 2015
- Manual de revisión y diseño curricular universitario; 2013-2013; Universidad de Santiago de Chile; Vicerrectoría académica; equipo: Pamela Urra Sepúlveda, Javier Jiménez Badaracco, Claudia Oliva Leiva, Alicia Pérez Lorca, Patricia Pallavicini Magnère
- Peña Sáenz, Alexander; Análisis curricular (George Posner); https://es.scribd.com/document/438592823/Analisis-Curricular
- Perez Perez, Maribel; Síntesis de ELABORACIÓN DEL PERFIL PROFESIONAL, Basado en Diaz-Barriga Arceo (2011); Universidad Autónoma del Estado de Hidalgo, Sistema de Universidad Virtual Licenciatura en Innovación y Tecnología Educativa; Teoría, Diseño y Evaluación Curricular, Unidad III. Diseño Curricular
- Stake, Robert (2006); Evaluación basada en criterios y evaluación interpretativa; https://campusacademica.rec.uba.ar/mod/resource/view.php?id=252305; del libro Evaluación comprensiva y evaluación basada en estándares. Barcelona: Editorial Graó.

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Alumna: Lic. Graciela N. Pataro

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
5 Políticas de seguridad de la información	1. **Política de Seguridad de la Información del organismo** a) desarrollar una Política de Seguridad de la Información compatible con la responsabilidad primaria y las acciones de su competencia, sobre la base de una evaluación de los riesgos que pudieran afectarlos.		**5.30 (nuevo que menciona el BIA)**
5.1.1 Políticas para la seguridad de la información	1.1.	aprobada por las máximas autoridades	**5.1**
	1.2.	notificada y difundida a todo el personal y a terceros	
5.1.2 Revisión de las políticas para la seguridad de la información	1.3	revisada y eventualmente actualizada, (periodicidad no superior a DOCE (12) meses).	**5.1**
	1.4	utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos	
6 Organización de la seguridad de la información 6.1 Organización interna	2. **Aspectos Organizativos de la Seguridad** a) desarrollar e implementar un marco organizativo que habilite una efectiva gestión y operación de la seguridad de la información en el organismo.		
6.1.1 Roles y responsabilidades en seguridad de la información	2.1.	asignar a un área del organismo con competencia en la materia las responsabilidades relativas a la seguridad de la información	**5.2**
6.1.2 Segregación de tareas	2.2.	segregar las funciones y áreas de responsabilidad en conflicto	**5.3**
	2.3.	impulsar las iniciativas que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona.	**Cubierta por las "Propiedades de seguridad de la información" que están embebidas en todos los controles**
6.1.5 Seguridad de la información en la gestión de proyectos	2.4.	abordar los aspectos referidos a la seguridad de la información en el diseño y la gestión de todos los proyectos que lleve adelante el organismo, dejando evidencia de tal intervención.	**5.8**
	2.5.	establecer como falta, el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos contenidos en el presente documento.	**Incluida en 6.4 y 5.28. También tiene relevancia en 8.17**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
	2.6.	incluir en los contratos, Términos de Referencia o en el instrumento mediante el cual se materialice la contratación del personal, cláusulas que contemplen el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos	**Incluida en 6.4, 6.2 y 6.6**
6.2 Los dispositivos móviles y el teletrabajo			
6.2.1 Política de dispositivos móviles	2.7.	establecer mecanismos adecuados de seguridad para el trabajo remoto y para el uso de dispositivos móviles.	**8.1**
6.2.2 Teletrabajo			**6.7**
7 Seguridad relativa a los recursos humanos 7.1 Antes del empleo	3. **Seguridad Informática de los Recursos Humanos** a) adoptar una perspectiva sistémica para proteger sus activos de información, dentro de la cual el personal debe ser considerado un recurso central. b) establecer una política de respeto de los derechos individuales de los empleados y resguardar su privacidad. c) Los agentes y funcionarios deben ser concientizados y capacitados para desarrollar habilidades y conocimientos en seguridad de la información, y hacer un uso responsable de la información y de los recursos utilizados en su gestión con el fin de prevenir riesgos		
7.1.1 Investigación de antecedentes			**6.1**
7.1.2 Términos y condiciones del empleo			**6.2**
7.2.2 Concienciación, educación y capacitación en seguridad de la información	3.1.	realizar e implementar planes de concientización en el uso seguro y responsable de los activos de información, diseñándolos para cada tipo de público y con distintas temáticas.	**6.3**
	3.2.	promover el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información, desarrollo de software e infraestructura.	**Incluida en 6.3**
7.2 Durante el empleo 7.2.1 Responsabilidades de gestión 7.3 Finalización del empleo o cambio en el puesto de trabajo 7.3.1 Responsabilidades ante la finalización o cambio	3.3.	establecer la obligatoriedad de la suscripción de actas o compromisos respecto a la seguridad de la información para todos los empleados del organismo, cualquiera sea su modalidad de contratación, teniendo en cuenta que las responsabilidades correspondientes pueden exceder la vigencia de la relación laboral.	**5.4** **6.5**
9 Control de acceso			

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
9.1 Requisitos de negocio para el control de acceso	3.4.	establecer claramente los requerimientos de seguridad de la información, que incluya niveles de acceso a la información para cada perfil de trabajo.	
9.1.1 Política de control de acceso			**5.15**
	3.5.	incluir los aspectos de seguridad en las etapas de inducción de los agentes, y evaluarlos durante toda la relación laboral.	**Incluida en 6.3**
	3.6.	requerir a los agentes y funcionarios, la firma de un acuerdo de confidencialidad.	**Incluida en 6.6**
7.2.3 Proceso disciplinario	3.7.	incorporar dentro de los procesos disciplinarios cualquier violación a las políticas de seguridad del organismo	**6.4**
8 Gestión de activos 8.1 Responsabilidad sobre los activos	**4. Gestión de Activos** a) Los activos de información del organismo deben ser gestionados y protegidos en forma efectiva. b) deben ser clasificados según su criticidad para el organismo desde la perspectiva de su confidencialidad, integridad y disponibilidad, lo que permitirá adoptar las medidas de protección adecuadas.		
8.2 Clasificación de la información 8.2.1 Clasificación de la información	4.1.	clasificar los activos de información, en línea con el tipo y la importancia de la información que gestionan para el organismo.	**5.12**
8.1.1 Inventario de activos	4.2.	llevar un inventario actualizado en el que se detallen los datos necesarios para conocer la ubicación, el propietario y las responsabilidades correspondientes de cada activo.	**5.9**
8.1.2 Propiedad de los activos			**5.9**
8.2.2 Etiquetado de la información			**5.13**
8.2.3 Manipulado de la información			**5.10**
8.1.4 Devolución de activos	4.3.	exigir a todos los agentes y empleados la devolución de los activos de información en su poder al finalizar la relación laboral o cuando un cambio en las funciones lo requiera.	**5.11**
8.3 Manipulación de los soportes	4.4.	efectuar una destrucción segura de cualquier medio que pueda contener información o datos personales, en función de su nivel de criticidad, sobre la base de un procedimiento documentado, una vez que se haya catalogado como defectuoso o rezago.	
8.3.1 Gestión de soportes extraíbles			**7.10**
8.3.2 Eliminación de soportes			**7.10**
11.2.7 Reutilización o eliminación segura de equipos			**7.14**
	5. Autenticación, Autorización y Control de Accesos		

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
	a) El acceso a los activos de información del organismo debe realizarse a partir de procesos y mecanismos de seguridad definidos e implementados según su nivel de criticidad, con el fin de proveer un nivel apropiado de protección. b) Los privilegios de acceso deben ser otorgados en forma expresa y formalmente autorizada a quienes los requieran para sus funciones		
9.4 Control de acceso a sistemas y aplicaciones 9.4.1 Restricción del acceso a la información 9.4.2 Procedimientos seguros de inicio de sesión	5.1.	utilizar en todos los casos el principio de "necesidad de saber", es decir que solo se otorguen privilegios de acceso en la medida en que sean requeridos para las actividades y tareas que cada empleado o funcionario debe llevar adelante.	**8.3** **8.5**
9.2 Gestión de acceso de usuario 9.2.1 Registro y baja de usuario	5.2.	hacer una adecuada y oportuna gestión de las altas y bajas de cuentas de usuario y privilegios, coordinando con las áreas de Recursos Humanos y aquellas en las que el empleado se desempeña toda novedad que pudiera impactar en ellos.	**5.16**
9.2.2 Provisión de acceso de usuario			**5.18**
9.2.6 Retirada o reasignación de los derechos de acceso			**5.18**
9.2.3 Gestión de privilegios de acceso 9.4.4 Uso de utilidades con privilegios del sistema	5.3.	realizar un seguimiento detallado sobre las cuentas con privilegios especiales.	**8.2** **8.18**
9.2.5 Revisión de los derechos de acceso de usuario	5.4.	revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.	**5.18**
9.4.3 Sistema de gestión de contraseñas			**5.17**
8.1.3 Uso aceptable de los activos	5.5.	requerir a los agentes, funcionarios y demás usuarios un uso responsable de sus dispositivos y datos de autenticación, dejando sentado que se encuentra estrictamente prohibido compartirlos y que deben ser mantenidos seguros en forma permanente.	**5.10**
9.3 Responsabilidades del usuario			
9.3.1 Uso de la información secreta de autenticación			**5.17**
9.2.4 Gestión de la información secreta de autenticación de los usuarios	5.6.	restringir y controlar la asignación y uso de derechos de accesos privilegiados.	**5.17**
9.4.5 Control de acceso al código fuente de los programas	5.7.	limitar y monitorear el acceso al código fuente de los programas	**8.4**
10 Criptografía	6. **Uso de herramientas criptográficas** a) La confidencialidad, integridad, autenticidad y/o no repudio de la información del organismo debe ser protegida mediante técnicas de cifrado, tanto si los datos se encuentran almacenados como cuando son transmitidos.		

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
10.1.1 Política de uso de los controles criptográficos 10.1 Controles criptográficos	6.1.	requerir el cifrado de cualquier dispositivo del organismo que contenga información considerada crítica y cuando involucre datos personales, especialmente cuando este se lleve fuera de la institución.	**8.24**
10.1.2 Gestión de claves	6.2.	proteger adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.	**8.24**
	6.3.	utilizar certificados digitales en todos los sitios de Internet del organismo.	**Incluida en 8.26**
11 Seguridad física y del entorno	**7. Seguridad física y ambiental** a) Los activos de información del organismo deben ser protegidos mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados.		
11.1 Áreas seguras 11.1.1 Perímetro de seguridad física 11.1.4 Protección contra las amenazas externas y ambientales	7.1.	la identificación y protección de áreas seguras contra desastres naturales, ataques maliciosos o accidentales	**7.1** **7.5**
11.1.2 Controles físicos de entrada	7.2.	la incorporación de controles físicos de ingreso/egreso, con los respectivos controles de identificación, cronológicos y de funcionamiento asociados, en aquellas áreas donde se encuentren resguardados los activos de información.	**7.2**
11.2 Seguridad de los equipos 11.2.1 Emplazamiento y protección de equipos	7.3.	el registro de los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.	**7.8**
11.1.6 Áreas de carga y descarga	7.4.	la adopción de medidas de seguridad para que el equipamiento sea ingresado o retirado del organismo con una autorización previa y habiéndose adoptado todos los recaudos del caso.	**7.2**
11.1.3 Seguridad de oficinas, despachos y recursos 11.2.8 Equipo de usuario desatendido 11.2.9 Política de puesto de trabajo despejado y pantalla limpia	7.5.	el cuidado de los puestos de trabajo, mediante mecanismos de bloqueo de sesión y escritorio despejado.	**7.3** **8.1** **7.7**
	7.6.	la adopción de medidas para evitar la pérdida, daño, robo o el compromiso de los activos de información del organismo y la interrupción de sus operaciones.	**Imcluida en 7.8, 7.12 y 7.13**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
11.2.3 Seguridad del cableado	7.7.	la protección frente a interrupciones, interferencia o daños de los cables eléctricos y de red que transporten datos o apoyen los servicios de información.	**7.12**
11.2.2 Instalaciones de suministro 11.2.4 Mantenimiento de los equipos	7.8.	el mantenimiento del equipamiento para contribuir a su disponibilidad e integridad continuas.	**7.11** **7.13**
8.3.3 Soportes físicos en tránsito 11.2.5 Retirada de materiales propiedad de la empresa	7.9.	la adopción de medidas de seguridad para los activos informáticos que deben llevarse fuera del organismo, considerando los distintos riesgos de trabajar fuera de sus dependencias, en lo que hace al resguardo de la información y a la seguridad física de los dispositivos.	**7.10** **7.10**
11.2.6 Seguridad de los equipos fuera de las instalaciones			**7.9**
12 Seguridad de las operaciones	**8. Seguridad operativa** a) Las operaciones del organismo deben desarrollarse en forma segura, en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos		
12.1 Procedimientos y responsabilidades operacionales 12.1.1 Documentación de procedimientos de los operación	8.1.	establecer las responsabilidades y los procedimientos para la gestión y la operación para todas las instalaciones de procesamiento de información.	**5.37**
12.1.3 Gestión de capacidades	8.2.	revisar, monitorear y ajustar los requerimientos de capacidad desde la perspectiva de la seguridad de la información.	**8.6**
12.1.2 Gestión de cambios 12.1.4 Separación de los recursos de desarrollo, prueba y operación	8.3.	minimizar los riesgos de acceso o de cambios no autorizados en entornos productivos, separando los entornos de desarrollo, prueba y producción, en los casos que corresponda.	**8.32** **8.31**
14.2.8 Pruebas funcionales de seguridad de sistemas	8.4.	implementar un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo.	**8.29**
12.2 Protección contra el software malicioso (malware) 12.2.1 Controles contra el código malicioso	8.5.	proteger las instalaciones contra infecciones de código malicioso	**8.7**
12.3 Copias de seguridad 12.3.1 Copias de seguridad de la información	8.6	realizar copias de resguardo del software y la información con una periodicidad y modalidad acordes con su criticidad de los datos y con los procesos que se lleven a cabo, probándolas periódicamente y estableciendo	**8.13**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
14.2.9 Pruebas de aceptación de sistemas	8.6.	procesos que se lleven a cabo, probándolas periódicamente y estableciendo un registro de las pruebas de restauración que permitan conocer quién participó del proceso, cuándo y cómo lo hizo y dónde se encuentra la copia.	**8.29**
12.4.4 Sincronización del reloj			**8.17**
12.4 Registros y supervisión	8.7.	llevar registro de todos los eventos de seguridad y revisarlo periódicamente con el fin de detectar posibles incidentes	
12.4.1 Registro de eventos			**8.15**
12.4.2 Protección de la información del registro			**8.15**
14.2.4 Restricciones a los cambios en los paquetes de software	8.8.	mantener un control estricto sobre el software y su integridad, en entornos productivos.	**8.32**
12.6 Gestión de la vulnerabilidad técnica	8.9.	identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el software utilizado. En los casos que el mismo sea provisto por terceros, contar con una política de actualización para evitar que se afecte la operación.	
12.6.1 Gestión de las vulnerabilidades técnicas			**8.8**
12.6.2 Restricción en la instalación de software			**8.19**
	8.10.	gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.	
12.4.3 Registros de administración y operación	8.11.	registrar y revisar periódicamente las actividades de los administradores y operadores.	**8.15**
	9. Seguridad en las comunicaciones a) La información de las redes del organismo debe ser protegida y controlada adecuadamente, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del organismo.		
9.1.2 Acceso a las redes y a los servicios de red	9.1.	Segregar, en la medida de las posibilidades, los grupos de servicios de información, usuarios y sistemas en las redes.	**5.15**
13.1.2 Seguridad de los servicios de red			**8.21**
13.1.3 Segregación en redes			**8.22**
13 Seguridad de las comunicaciones 13.1 Gestión de la seguridad de redes 13.1.1 Controles de red	9.2.	proteger adecuadamente la información que se transfiera dentro del organismo y hacia cualquier entidad externa, incluyendo aquella que se transmita a través de servicios de correo electrónico.	**8.20**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
13.2.3 Mensajería electrónica	9.3.	exigir el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del organismo para toda comunicación vinculada con sus funciones, informando los riesgos de este incumplimiento.	**5.14**
13.2 Intercambio de información			
13.2.1 Políticas y procedimientos de intercambio de información	9.4.	incluir mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados	**5.14**
13.2.2 Acuerdos de intercambio de información	9.5.	incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban.	**5.14**
13.2.4 Acuerdos de confidencialidad o no revelación	9.6.	incorporar acuerdos y cláusulas de confidencialidad y no divulgación cuando el organismo entienda que resulta conveniente para el tipo de información que trate.	**6.6**
14 Adquisición, desarrollo y mantenimiento de los sistemas de información 14.1 Requisitos de seguridad en los sistemas de información	**10. Adquisición, desarrollo y mantenimiento de sistemas de información** a) La seguridad de la información debe contemplarse como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites a través de Internet		
14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	10.1	especificar lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño), cuando el proceso de contratación sea gestionado por el propio organismo.	**5.8**
14.2 Seguridad en el desarrollo y en los procesos de soporte 14.2.1 Política de desarrollo seguro 14.2.5 Principios de ingeniería de sistemas seguros	10.2.	utilizar una metodología de desarrollo seguro, capacitando a los desarrolladores e incorporando cláusulas en las especificaciones técnicas de los pliegos de bases y condiciones particulares.	**8.25** **8.27**
14.2.6 Entorno de desarrollo seguro			**8.31**
14.2.2 Procedimiento de control de cambios en sistemas	10.3.	controlar los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción e incorporando efectivos controles cruzados o por oposición.	**8.32**
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo			**8.32**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
14.3 Datos de prueba 14.3.1 Protección de los datos de prueba	10.4.	proteger los datos utilizados en las pruebas, evitando la utilización de bases de datos reales.	**8.33**
14.1.3 Protección de las transacciones de servicios de aplicaciones	10.5.	utilizar protocolos que garanticen la transmisión o enrutamiento adecuados que eviten la divulgación, alteración o duplicación no autorizadas de transacciones.	**8.26**
12.5 Control del software en explotación 12.5.1 Instalación del software en explotación	10.6.	evaluar la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.	**8.19**
14.1.2 Asegurar los servicios de aplicaciones en redes públicas	10.7.	proteger la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.	**8.26**
14.2.7 Externalización del desarrollo de software	10.8.	controlar y supervisar el efectivo cumplimiento y las actividades realizadas por el cocontratante en aquellas contrataciones de bienes y servicios efectuadas por el organismo.	**8.30**
15 Relación con proveedores 15.1 Seguridad en las relaciones con proveedores	**11. Relación con proveedores** a) La contratación, cualquiera sea la modalidad, realizada por el organismo para la provisión de un bien o servicio debe incluir en el pliego de bases y condiciones particulares cláusulas de cumplimiento efectivo por parte del cocontratante, relacionadas con la seguridad de la información, desde el inicio del procedimiento contractual y hasta la efectiva finalización del contrato.		
15.1.1 Política de seguridad de la información en las relaciones con los proveedores	11.1	la consideración de aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.	**5.19**
15.1.2 Requisitos de seguridad en contratos con terceros	11.2	el establecimiento e inclusión en el pliego de bases y condiciones particulares de todos los requisitos de seguridad de la información pertinentes, en los acuerdos que se suscriban con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura tecnológica al organismo.	**5.20**
15.2 Gestión de la provisión de servicios del proveedor			

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
15.2.1 Control y revisión de la provisión de servicios del proveedor	11.3.	la supervisión y revisión por parte de los responsables asignados al proyecto de todos los niveles de seguridad acordados	**5.22**
15.2.2 Gestión de cambios en la provisión del servicio del proveedor			**5.22**
15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	11.4.	la inclusión de cláusulas para mantenimiento del nivel de servicio, especialmente en servicios de provisión crítica, que permitan mantener su disponibilidad.	**5.21**
	11.5.	la inclusión en el pliego de bases y condiciones de estipulaciones tendientes al cumplimiento de todas las normas legales y contractuales que sean aplicables.	**Incluida en 5.20**
16 Gestión de incidentes de seguridad de la información 16.1 Gestión de incidentes de seguridad de la información y mejoras	**12. Gestión de incidentes de seguridad** a) El organismo debe adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.		
16.1.1 Responsabilidades y procedimientos	12.1.	identificar las debilidades en los procesos de gestión de información del organismo, de manera de adoptar las medidas que prevengan la ocurrencia de incidentes de seguridad.	**5.24**
16.1.3 Notificación de puntos débiles de la seguridad			**6.8**
16.1.4 Evaluación y decisión sobre los eventos de seguridad de información			**5.25**
16.1.5 Respuesta a incidentes de seguridad de la información	12.2	contar con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.	**5.26**
6.1.3 Contacto con las autoridades	12.3.	adoptar una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.	**5.5**
6.1.4 Contacto con grupos de interés especial			**5.6**
	12.4.	instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.	**Incluida en 6.3**
16.1.2 Notificación de los eventos de seguridad de la información	12.5.	notificar a la Dirección Nacional de Ciberseguridad de la ocurrencia de incidentes de seguridad, en un plazo no superior a CUARENTA Y OCHO (48) horas de su detección.	**6.8**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
16.1.6 Aprendizaje de los incidentes de seguridad de la información 16.1.7 Recopilación de evidencias	12.6.	recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia.	**5.27** **5.28**
16.1.2 Notificación de los eventos de seguridad de la información	12.7.	en el caso en que el incidente de seguridad hubiere afectado activos de información y hubiere comprometido información y/o datos personales de terceros, se deberá informar públicamente tal ocurrencia.	**6.8**
17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio 17.1 Continuidad de la seguridad de la información	**13. Aspectos de seguridad para la continuidad de la gestión** a) Los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales deben contemplar todos los aspectos de seguridad de la información involucrada.		
17.1.1 Planificación de la continuidad de la seguridad de la información	13.1.	identificar los requisitos necesarios para cumplir todos los requerimientos de seguridad de la información ante un evento inesperado que impida seguir operando, con foco en los servicios esenciales que preste el organismo.	**5.29 y el 5.30 (nuevo que menciona el BIA)**
17.1.2 Implementar la continuidad de la seguridad de la información	13.2.	establecer, documentar, implementar y mantener los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.	**5.29**
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	13.3.	verificar, revisar y evaluar a intervalos regulares los controles de continuidad de la seguridad de la información.	**5.29**
11.1.5 El trabajo en áreas seguras 17.2 Redundancias 17.2.1 Disponibilidad de los recursos de tratamiento de la información	13.4.	implementar mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.	**7.6** **8.14**
18 Cumplimiento	**14. Cumplimiento**		

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
	a) En todos los casos el organismo debe cumplir con las disposiciones legales, normativas y contractuales que le sean aplicables, con el fin de evitar sanciones administrativas y/o legales y que los empleados incurran en responsabilidades civiles o penales como resultado de su incumplimiento.		
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	14.1.	la identificación, documentación y actualización periódica de los requisitos legales y contractuales para cada sistema de información que utilice.	**5.31**
18.1 Cumplimiento de los requisitos legales y contractuales 18.1.4 Protección y privacidad de la información de carácter personal	14.2.	el cumplimiento de la Ley No 25.326 de Protección de los Datos Personales y sus normas reglamentarias y complementarias.	**5.34**
18.1.5 Regulación de los controles criptográficos	14.3.	la revisión periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.	**5.31**
18.2 Revisiones de la seguridad de la información 18.2.1 Revisión independiente de la seguridad de la información			**5.35**
18.1.2 Derechos de propiedad intelectual (DPI)	14.4	la supervisión del cumplimiento de todos los requisitos de seguridad contenidos en la legislación aplicable, incluyendo las directrices del presente documento, y en las políticas y procedimientos del organismo, por parte de los responsables de cada área del organismo, respecto a su personal y a la información que gestiona.	**5.32**
18.1.3 Protección de los registros de la organización			**5.33**
18.2.2 Cumplimiento de las políticas y normas de seguridad	14.5.	considerar la adopción de las medidas correctivas que surjan de auditorías y revisiones periódicas de cumplimiento de los presentes requisitos, sean estas realizadas por personal del área, de organismos competentes o de terceros habilitados a tal fin.	**5.36**
12.7 Consideraciones sobre la auditoria de sistemas de información 12.7.1 Controles de auditoría de sistemas de información			**8.34**
18.2.3 Comprobación del cumplimiento técnico			**5.36, 8.8**
NUEVOS CONTROLES INCLUIDOS EN LA ISO 27002/2022			
		Inteligencia de Amenazas (ecolección de información para inteligencia)	**5.7**
		Seguridad de la información para el uso de servicios en la nube	**5.23**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Anexo A - Correspondencia de los controles de las ISO 27002:2013 y 2022 versus la DEA 641/2021

Trabajo Final de Especialización en Evaluación Universitaria (2023)

CONTROL ISO 27002/2013	DIRECTRICES DEA 641/2021		CONTROL ISO 27002/2022
		Preparación de las TIC para la continuidad del negocio (puede subsumirse en el DA 13.1 y 1)	**5.30**
		Monitoreo de la seguridad física	**7.4**
		Gestión de la configuración (Configuraciones de seguridad, hardware, software, servicios y redes deben establecerse, documentarse, implementarse, supervisarse y revisarse)	**8.9**
		Eliminación de la información (refiere a la información no al medio de almacenamiento)	**8.10**
		Enmascaramiento de datos (de acuerdo a políticas de la empresa, requerimientos del negocio y legislaciones vigentes)	**8.11**
		Prevención de la fuga de datos (en sistemas, redes y aplicaciones que procesen/transmitan información sensible)	**8.12**
		Actividades de monitoreo (en redes, sistemas y applicaciones por comportamientos anómalos)	**8.16**
		Filtrado Web (reducir la exposición en el acceso a sitios con contenido malicioso)	**8.23**
		Codificación Segura (aplicación de principios de programación segura en las aplicaciones)	**8.28**

En verde controles de la ISO 27002:2013 que se han fusionado en la nueva version // En amarillo controles de la DEA 641 asimilados a controles en la ISO 27002:2022

Trabajo Final de Especialización en Evaluación Universitaria

Título: Análisis curricular de la Maestría en Seguridad Informática de la UBA

Subtítulo: Análisis del perfil del egresado, perspectivas respecto de normativas nacionales e/internacionales y de los docentes y/autoridades

Alumna: Lic. Graciela N. Pataro

ANEXO B – ENCUESTAS

Como se ha planteado en el presente trabajo final se han realizado encuestas tanto a la Comisión del Posgrado en MSI como a los docentes de las diferentes asignaturas.

A continuación, se indican las características y el marco teórico utilizado para la realización de estas.

1. Universo de estudio

Se indican a continuación las diferentes autoridades de la Comisión de la MSI[1]:

1) Dr. Hugo Scolnik (director MSI)
2) Raul Saroka (subdirector MSI)
3) Dr. Pedro Hecht (coordinador académico)
4) Ing. Alberto Dams (subdirector MSI)
5) Ricardo Rivas (subdirector ESI)
6) Ing. Hugo Pagola (director ESI[2])
7) Dr. Diego Garbervetsky (subdirector ESI)

El cuerpo docente se compone como se indica en la tabla que sigue (se utilizan los mnemotécnicos que se indican en la Tabla 1):

Nro.	Apellido y nombres	Asignaturas que participa en I y II año
1	SAROKA, Raúl	ET, GEST1, TTFM
2	DEVINCENZI, Juan Alejandro	ET, SSOyA, RED2
3	PAGOLA, Hugo	ET, RED1, RED2
4	HECHT, Pedro	ET, CRIPT1, CRIPT2, TTFM
5	MISTO MACIAS, Mara	GEST1

[1] Maestría en Seguridad Informática
[2] Especialización en Seguridad Informática

6	SCOLNIK, Hugo	CRIPT1
7	MASNATTA, Néstor	CRIPT1
8	CARRALBAL, Diego	DyPS
9	ARDITA, Julio	SSOyA
10	MONETTI, Mónica	CO, TDCG
11	CARACOCHE, Juan Manuel	RED2
12	VALLEJOS, Javier	RED1, RED2
13	PATARO, Graciela	MLEP
14	SUMER ELIAS, Miguel	MLEP
15	ERRECALDE, Myrian	TTFM
16	PRANDINI, Patricia	GEST2
17	SILBERFICH, Pablo	GEST2, AUD
18	RIVAS, Ricardo	AUDIT
19	GAGLIARDI, Sebastián	AUDIT
20	BENDINELLI, Maximiliano	IF
21	PUIG, Eduardo	SF

Queda definida de esta forma el universo a encuestar. Las encuestas no se realizan por muestreo, sino que todos los integrantes, docentes y autoridades, han sido encuestados.
Siguiendo los lineamientos que indica Anguita [Anguita et al., 2003 parte I] se procede a indicar cada uno de los pasos que se han tomado para la realización de las encuestas.

2. Identificación del problema

Como ya se mencionara, se ha buscado abordar, partiendo de una evaluación curricular parcial, con especial referencia al perfil esperado de los egresados de esta Maestría tal cual como figura en la Resolución de creación de esta (actualizada al 2015) contrastándolo con los sentidos y criterios aportados por los docentes y autoridades de éste como referentes.
También, de qué forma estos fundamentos (que surgen de las percepciones de docentes y autoridades) se relacionan con la normativa más reciente elaborada por el Estado Argentino plasmada en la Decisión Administrativa 641/21 referida a los Requisitos Mínimos de Seguridad de la Información para los Organismos del SPN (Sector público Nacional). Esta norma, asimismo, se encuentra basada

en la internacionales IRAM-ISO/IEC 27001 (Requisitos para los sistemas de gestión de seguridad de la información), 27002 (Buenas prácticas) y 20000-1 (Especificación formal para la gestión de servicios de TI), con lo cual se cubren también normativas internacionales reconocidas en nuestro país.

3. Determinación del diseño de la investigación

Se ha optado por un diseño de tipo "analítico observacional o correlacional". Como indica Anguita [Anguita et al., 2003 parte I, pág. 1]

"En el caso de los estudios analíticos observacionales, las variables de interés son seleccionadas para conocer la relación que existe entre ellas, aprovechando su presencia o ausencia en grupos de sujetos escogidos cuidadosamente, de modo que sea posible el control sobre las variables identificadas por el investigador."

Las principales variables identificadas son:

3.1. Objetivos/Principios del perfil del egresado

3.2. Competencias específicas establecidas en el plan de estudios

3.3. Contenidos de las asignaturas

3.4. Referentes nacionales e internacionales

4. Especificación de la hipótesis

El interrogante principal que se busca responder es si los estudiantes que se están formando, o quienes ya han finalizado el posgrado Maestría en Seguridad Informática (MSI) de la UBA están respondiendo a las necesidades del mercado profesional y académico actual.

El interés es analizar las competencias laborales que propicia la MSI en función de los criterios que definen la misma normativa de su creación (Res. 2513/15) contrastándolas con la normativa nacional (DA 641/21) e internacional, y desde las percepciones de la Comisión del Posgrado y el cuerpo docente.

Y desglosando este interrogante en cuestiones más específicas sobre las tres áreas de análisis que se plantean realizar, podríamos cuestionarnos:

4.1. Plan de estudios

¿Qué relación presentan los contenidos en relación con las competencias del perfil del graduado?

4.2. Perspectiva docente/Comisión directiva

¿Qué problemas sobre los contenidos y/o alcances del plan de estudios identifican o qué preocupaciones surgen en la perspectiva de los actores entrevistados? ¿qué propuestas se plantean para resolver esos problemas?

¿Cuáles son las perspectivas de directivos y docentes de la MSI en relación con el perfil del graduado y su relación con el mundo académico y el mercado laboral actual?

4.3. Normativa nacional

¿Qué relación/es se identifican entre el perfil del graduado de la carrera MSI y lo planteado por la normativa nacional sobre competencias necesarias en la formación de los profesionales del rubro de SI?

4.4. Tres focos conjuntos

¿Los tres elementos analizados: plan de estudios, perspectivas y criterios de los docentes/directivos y normativa nacional conforman un conjunto armonioso y complementario?

¿Qué valor asume el perfil del graduado de la MSI en función de lo planteado por docentes y directivos y por la normativa nacional/internacional?

5. Definición de las variables.

Las variables identificadas a tratar son:

5.1. Objetivos/Principios del perfil del egresado vs. las Competencias específicas establecidas en el plan de estudios (dirigida a la Comisión Directiva o autoridades)

5.2. Competencias específicas vs. Contenidos de las asignaturas (dirigida a todo el cuerpo docente)

5.3. Competencias específicas vs. Referentes nacionales e internacionales (dirigida a las autoridades y el cuerpo docente)

6. Selección de la muestra.

Como se ha indicado en el punto 1) el universo de estudio son todos los docentes y autoridades de la MSI.

7. Diseño del cuestionario.

Se ha optado por dos tipos de preguntas al universo de estudio:

a) Cerradas: Cuando se han planteado tanto a los directivos como al cuerpo docente la identificación de las competencias esperadas respecto de los objetivos del posgrado (¿qué com-

petencias sustentas a cuáles objetivos?) y también cuando a los docentes se los interroga sobre los contenidos específicos de las asignaturas respecto de las competencias. Para ello se han presentado grillas que el encuestado simplemente debe completar con cruces. Se reservan espacios para comentarios y/o observaciones por parte del encuestado.

b) Abiertas: Toda vez que se ha otorgado libertad a los encuestados para acrecentar las selecciones concretas que surgen de las preguntas cerradas, permitiéndoles ampliar los conceptos allí vertidos e indicar, a su criterio, si existen competencias y/o contenidos específicos a suprimir o a agregar al plan de estudios.

Los cuestionarios presentados se incluyen como los:

- Anexo C – Consulta a las autoridades
- Anexo D – Consultas al cuerpo docente

Para el cuestionario del anexo D se utilizó como prueba piloto la asignatura Criptografía 1 que cuenta con 3 docentes a cargo.

8. Organización del trabajo de campo.

8.1. Primera etapa: Objetivos vs. Competencias

Para esta primera encuesta se contactó a las autoridades del Posgrado y se sometió a su análisis y opinión una grilla que contrasta los Objetivos/Principios de la Resolución de creación versus las competencias el perfil del egresado. El resultado de esa encuesta se presenta en el cuerpo principal de este trabajo. Ver Anexo C – Consulta a las autoridades.

8.2. Segunda etapa: Contenidos versus las competencias de la Maestría

En la segunda etapa se contactaron a los docentes de todas las materias presentándoles un cuestionario tipo grilla con las 12 competencias del posgrado y los contenidos específicos de la asignatura en cuestión.

Se contactaron a todos los docentes y algunos manifestaron su participación parcial en el dictado de algunas de las asignaturas, luego de lo cual se centró el foco en el docente a cargo de esta.

Además de la grilla se incluyeron 5 preguntas cuyo contenido puede visualizarse en el Anexo D – Consultas al cuerpo docente.

9. Obtención y tratamiento de los datos.

De la consulta a las autoridades hubo varios feedbacks que provocaron un proceso de refinamiento y precisión llegando finalmente al cuadro que puede visualizarse en el texto principal de este trabajo en la Tabla 5 dentro del punto 6.1.2.5. Versión final grilla Objetivos vs. Competencias
En las consultas a los docentes de las distintas asignaturas hubo también varios procesos de retroalimentación para explicarles el objetivo del presente trabajo y asesorarlos en el llenado de las respuestas buscando siempre orientar y respetar sus puntos de vista.

10. Análisis de los datos e interpretación de los resultados.

A medida que se recopilaban las respuestas se fue construyendo el Anexo E - Refundido de respuestas al cuestionario en el cual se volcaron todas las respuestas a las 5 preguntas plateadas como así también los comentarios generales de los contenidos y otros comentarios vertidos por los docentes.
Para incluir en el Trabajo Final se hizo necesario ordenar algunas de las respuestas por temática para mejor proveer al objetivo buscado de verter las opiniones específicas respecto de los contenidos y el sustento que ellos brindan a las diferentes competencias.

Con las respuestas referidas a los contenidos y si los mismos sustentan las diferentes competencias de la Maestría se confeccionó el Anexo H - Contenidos vs Competencias detallado lo que permitió detectar cuáles asignaturas no sustentan alguna de las competencias. Esta grilla también sirvió para detectar el problema del contenido “Desarrollo Seguro” que estaba asignado a la asignatura Seguridad en Redes II cuando debía estar en la asignatura Seguridad en los Sistemas Operativos y las Aplicaciones (Luego consultado y corroborado por los docentes de ambas asignaturas).
Con el Anexo H detallado se refundió el sustento en una grilla más reducida que se confeccionó y se muestra en el Anexo I - Contenidos vs Competencias. Esta grilla fue volcada como resultado en el Trabajo final en la Tabla 6 GRILLA DE COMPETENCIAS DEL PERFIL DEL EGRESADO Y ASIGNATURAS QUE LAS CUBREN EN LA CURRICULA dentro del punto 6.1.3.

Finalmente, con todos estos elementos se construyen los cuadros finales que figuran en las conclusiones del trabajo, a saber:

- Tabla 9 – Contenidos de las asignaturas comparado
- Tabla 10 – Carga horaria de las asignaturas comparada

Trabajo Final de Especialización en Evaluación Universitaria

Título: Análisis curricular de la Maestría en Seguridad Informática de la UBA

Subtítulo: Análisis del perfil del egresado, perspectivas respecto de normativas nacionales e/internacionales y de los docentes y/autoridades

Alumna: Lic. Graciela N. Pataro

ANEXO C – Consulta a las autoridades

Texto de la consulta a la Comisión Directiva de la MSI:

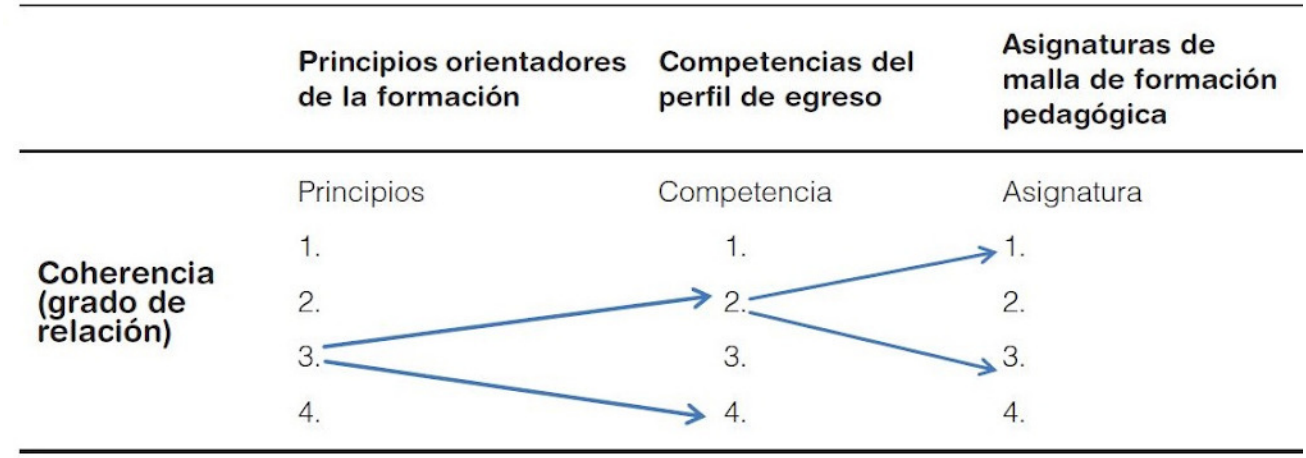
A. Asunto del mail:

Consulta por objetivos y competencias de la Maestría en SI

B. Cuerpo del mensaje:

Hola gente!

Algunos de ustedes saben que estuve cursando en el 2021 la Especialización en Evaluación Universitaria de la UBA y completé la cursada y me queda el TF por hacer y por suerte este año pude encontrar un poco de tiempo para empezar a escribir.
El tema de mi TF es un Análisis Curricular de nuestro posgrado MSI
Espero poder lograr un trabajo que ayude a mejorar la currícula nuestra :-)
Una de las cosas que tengo que hacer para el análisis curricular de la Maestría es verificar la coherencia interna del curriculum.
Tomé la última resolución de la maestría, la del 2015 e hice un mapeo entre los objetivos o principios del
posgrado y las competencias del perfil de egresados.
Eso es algo que saco de la bibliografía que uso y que es parecido a este gráfico



MATRIZ DE COHERENCIA CURRICULAR

Con esa idea armé esta grilla que les paso y que les consulto si están de acuerdo en ese esquema o si tienen

comentarios para hacerme.

Una de las cosas que prevé mi TF es entrevistas o encuestas a docentes y a la Comisión directiva así que este

es un primer approach y a medida que avance los volveré a contactar.

Yo la armé a mi buen saber y entender y con los conocimientos que poseo.

Todo el texto está tomado tal cual de lo que dice la resolución, no saqué ni agregué nada.

Aguardo sus comentarios y sugerencias a ver qué les parece.

Seguimos en contacto

Saludos, Graciela

Coherencia curricular.xlsx

C. Miembros de la CD encuestados y sus respuestas

Miembro CD	Respuesta	Observaciones
Dr. Hugo Scolnik	Aprueba grilla	
Raul Saroka		

Dr. Pedro Hecht	Aprueba grilla	No soy experto en diseño curricular pero te anticipo que me gustó lo que armaste. No sabría cómo mejorar-lo.
Ing. Alberto Dams		
Ricardo Rivas	Aprueba grilla	Hizo varios comentarios volcados en el trabajo
Ing. Hugo Pagola	Aprueba grilla	Contenido razonable
Dr. Diego Garbervetsky		

Trabajo Final de Especialización en Evaluación Universitaria

Título: Análisis curricular de la Maestría en Seguridad Informática de la UBA

Subtítulo: Análisis del perfil del egresado, perspectivas respecto de normativas nacionales e/internacionales y de los docentes y/autoridades

Alumna: Lic. Graciela N. Pataro

Anexo D – Consultas al cuerpo docente (Formulario base)

Texto del mail de consulta enviado a todos los docentes

A. Asunto del mail:

Encuesta sobre contenidos materia **XXXXXXXX**

B. Cuerpo del mensaje:

Estimado docente de la asignatura **XXXXXXXXXX:**

En el marco de mi Trabajo Final de la Especialización en Evaluación Universitaria me encuentro abocada en la realización de un **Análisis Curricular** de nuestro Posgrado en Seguridad Informática.
Para lograr ese cometido estoy recabando las opiniones y comentarios de todos los docentes en cuanto a de qué forma los contenidos que usted imparte en su asignatura sustentan las competencias del Perfil del egresado.
Su opinión es muy importante no solo para el trabajo en sí, sino que ayudará para refinar, perfeccionar y actualizar los contenidos impartidos.
Todas las respuestas y opiniones serán tratadas con la máxima confidencialidad.
La idea es obtener finalmente un cuadro similar al que le muestro aquí (esto es solo un fragmento ilustrativo):

Nro	COMPETENCIAS	1 ASIGNAT	2 ASIGNAT	3 ASIGNAT	4 ASIGNAT	5 ASIGNAT
1	Definir e instrumentar un plan integral de Seguridad Informática de la organización			1	1	
2	Definir estrategias y políticas de Seguridad Informática		1	1	1	

En esta tesitura le agrego aquí un cuadro en el que se incluyen todos los contenidos mínimos de la asignatura que usted imparte y las competencias del perfil del egresado (tomados de la Resolución de creación del Posgrado 2513/15).
Algunos de los contenidos mínimos pueden resultar muy específicos o técnicos y usted puede agruparlos según su criterio y preferencia.

Asimismo, no es necesario que el contenido sustente la competencia en un 100% ya que la unión de los contenidos que aportan otras asignaturas coadyuva en ese cometido, así que con indicar simplemente en la casilla correspondiente una "X" se puede considerar que el contenido sustenta en todo o en parte la competencia indicada.
Se ha dejado un espacio luego de las competencias donde solo se mencionan los contenidos mínimos para observaciones o comentarios que usted desee realizar.
A continuación, sus contenidos para cada una de las competencias.
Al final se le plantean una serie de preguntas que son importantes para enriquecer el resultado del análisis. Se le agradece enormemente el leerlas con atención y aportar sus comentarios de considerarlo oportuno.

COMPETENCIAS DEL PERFIL DEL EGRESADO (Son 12 competencias)

1. **Definir e instrumentar un plan integral de Seguridad Informática de la organización**

CONTENIDOS MÍNIMOS	**¿SUSTENTA COMPETENCIA?**
Contenido 1	
Contenido 2	
….	
Contenido N	

2. **Definir estrategias y políticas de Seguridad Informática**

CONTENIDOS MÍNIMOS	**¿SUSTENTA COMPETENCIA?**
Contenido 1	
Contenido 2	
….	
Contenido N	

3. **Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)**

CONTENIDOS MÍNIMOS	**¿SUSTENTA COMPETENCIA?**
Contenido 1	
Contenido 2	
….	
Contenido N	

4. **Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.**

CONTENIDOS MÍNIMOS	¿SUSTENTA COMPETENCIA?
Contenido 1	
Contenido 2	
….	
Contenido N	

5. **Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes**.

CONTENIDOS MÍNIMOS	¿SUSTENTA COMPETENCIA?
Contenido 1	
Contenido 2	
….	
Contenido N	

6. **Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico**

CONTENIDOS MÍNIMOS	¿SUSTENTA COMPETENCIA?
Contenido 1	
Contenido 2	
….	
Contenido N	

7. **Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones**

CONTENIDOS MÍNIMOS	¿SUSTENTA COMPETENCIA?
Contenido 1	
Contenido 2	
….	
Contenido N	

8. **Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática**.

CONTENIDOS MÍNIMOS	¿SUSTENTA COMPETENCIA?
Contenido 1	
Contenido 2	
….	
Contenido N	

9. Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática

CONTENIDOS MÍNIMOS	**¿SUSTENTA COMPETENCIA?**
Contenido 1	
Contenido 2	
….	
Contenido N	

10. Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas

CONTENIDOS MÍNIMOS	**¿SUSTENTA COMPETENCIA?**
Contenido 1	
Contenido 2	
….	
Contenido N	

11. Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática

CONTENIDOS MÍNIMOS	**¿SUSTENTA COMPETENCIA?**
Contenido 1	
Contenido 2	
….	
Contenido N	

12. Ejercer la docencia en materia de Seguridad Informática.

CONTENIDOS MÍNIMOS	**¿SUSTENTA COMPETENCIA?**
Contenido 1	
Contenido 2	
….	
Contenido N	

ESPACIO PARA COMENTARIOS U OBSERVACIONES RESPECTO DE LOS CONTENIDOS MÍNIMOS DE LA ASIGNATURA

CONTENIDOS MÍNIMOS	**OBSERVACIONES**
Contenido 1	
Contenido 2	
….	
Contenido N	
Contenido 1	

CUESTIONARIO ESPECÍFICO (5 preguntas)

a) ¿Qué problemas sobre los contenidos y/o alcances del plan de estudios identifica usted respecto de su asignatura?

b) ¿Posee alguna preocupación en particular con los contenidos del plan de estudios?

c) ¿Tiene alguna propuesta para resolver estos problemas?

d) ¿Cuáles son sus perspectivas en relación con las competencias del perfil del graduado (los 12 mencionados anteriormente) y su relación con el mundo académico y el mercado laboral actual?

e) Finalmente, pero no menos importante, pensando en normativas nacionales e internacionales reconocidas (La decisión administrativa 641/2021[1] o la ISO 27002:2022) ¿considera usted que existen contenidos mínimos que podrían incluirse o excluirse en su asignatura? Por favor, elabore su respuesta. (Se adjunta un cuadro comparativo de estas normativas y una nómina de los controles de la ISO 27002:2022[2] que puede resultarle de utilidad para responder esto último).

[1] REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL
[2] Seguridad de la Información, Ciberseguridad y Protección de la Privacidad

C. **Cuerpo docente entrevistado para cada asignatura**

Nro.	Apellido y nombres	Asignaturas que participa en I y II año/OK (si completó la encuesta)
1	SAROKA, Raúl	GEST1, TTFM
2	DEVINCENZI, Juan Alejandro	SSOyA, RED2
3	PAGOLA, Hugo	RED1, RED2
4	HECHT, Pedro	CRIPT1, CRIPT2, TTFM
5	MISTO MACIAS, Mara	GEST1
6	SCOLNIK, Hugo	CRIPT1, SF
7	MASNATTA, Néstor	CRIPT1
8	CARRALBAL, Diego	DyPS
9	ARDITA, Julio	SSOyA
10	MONETTI, Mónica	CO, TDCG
11	CARACOCHE, Juan Manuel	RED2
12	VALLEJOS, Javier	RED1, RED2
13	PATARO, Graciela	MLEP
14	SUMER ELIAS, Miguel	MLEP
15	ERRECALDE, Myrian	TTFM
16	PRANDINI, Patricia	GEST2
17	SILBERFICH, Pablo	GEST2, AUD
18	RIVAS, Ricardo	AUD
19	GAGLIARDI, Sebastián	AUD
20	BENDINELLI, Maximiliano	IF

Trabajo Final de Especialización en Evaluación Universitaria

Título: Análisis curricular de la Maestría en Seguridad Informática de la UBA

Subtítulo: Análisis del perfil del egresado, perspectivas respecto de normativas nacionales e/internacionales y de los docentes y/autoridades

Alumna: Lic. Graciela N. Pataro

ANEXO E - Refundido de respuestas al cuestionario a docentes

COMENTARIOS GENERALES SOBRE LOS CONTENIDOS

CRIPT1

Considero que los contenidos mínimos definidos son adecuados para la capacitación criptológica de los cursantes de la Maestría. Se presentan los algoritmos y protocolos básicos y esenciales y que luego serán ampliados y fundamentados en Criptografía II. En conjunto, el resultado es más que adecuado para la compresión teórica y práctica de la criptografía y el criptoanálisis por parte de los profesionales IT cursantes en este posgrado.

CRIPT2

OBSERVACION= La siguiente opinión es subjetiva pero absolutamente fiel, a mi leal saber y refrendada por las encuestas recibidas por los cursantes de los últimos diez años en la maestría y que nunca terminaron calificando integralmente a Cripto II con menos de 9.90 (sobre 10 puntos).

Esta asignatura técnica es dictada al nivel equivalente al de las dos primeras carreras equivalentes en los EEUU (MIT y Stanford) y las dos primeras carreras equivalentes en España (Universidad Politécnica de Madrid y Universidad Carlos III de Madrid). Esto ha sido verificado por el docente a cargo y sustentado por el Prof Emérito en Criptografía Dr. JORGE RAMIÓ AGUIRRE, creador de la mayor red iberoamericana de la especialidad tanto docente como en investigación (CRIPTORED). La idea es brindar formación criptológica de excelencia, 100% actualizada y revisada año a año y con enfoques que concilian la teoría con la práctica de la seguridad de la información. Ciertamente somos una de las asignaturas pilares de nuestra Maestría.

GEST2

CONTENIDOS MÍNIMOS	OBSERVACIONES
Análisis y gestión del riesgo: mapa de riesgos, evaluación de salvaguardas, informe de insuficiencias, catálogo de elementos, estado de riesgo.	Sobre la base de lo dictado en materia de riesgos en GESI I, se profundiza en la materia respecto a casos concretos de gestión de riesgo y se revisan estándares internacionales relacionados.
Ciclo de vida: análisis y gestión, planificación, implementación de salvaguardas, gestión de configuración y cambios	Al explicarse el tema de gobierno de la seguridad de la información, se lo diferencia de la gestión y se establecen roles y funciones diferenciadas. Si bien no se profundiza en aspectos técnicos, la gestión de estas temáticas conlleva un conocimiento de temas tales como gestión de configuraciones, de cambios, de accesos, de activos, etc., en materia de planificación, construcción, ejecución y monitoreo.
Relación y complementariedad entre los distintos estándares y/ modelos (frameworks), cumplimientos (compliance), regímenes e instituciones Internacionales y Nacionales: Cobit, Coso, BSI, ISO, ITIL, Basilea II, CMM, SOX, otros.	Se profundiza especialmente en COBIT, presentándose el marco desde el punto de vista del gobierno y la gestión pero se presentan otros estándares ISO, como la 27014, la 27032, la subserie 27100, etc.

CO

El tema de la Motivación es troncal con los conocimientos impartidos en esta asignatura.

TDCG

Siendo esta asignatura de tipo Taller se trabajan casos puntuales durante la cursada. Esos casos son muchas veces aportados por los mismos estudiantes y se muestran formas de resolución y tratamiento de estos a todos los cursantes, enriqueciendo el conocimiento y el intercambio para todos ellos.

AUDIT

CONTENIDOS MÍNIMOS	OBSERVACIONES
Control y auditoría.	Cubierto, faltaría tiempo, o deberían darse conceptos generales de Auditoría en asignaturas anteriores.
Normas técnicas.	Se trabajan varias normas nacionales, internacionales y de industrias/mercados verticales.

Control y estructura organizativa.	Se asume que se vio en otras asignaturas. Se profundiza y detalla en Seguridad Informática y de la Información.
Separación de funciones y oposición de intereses.	Conceptos generales, ejemplos.
Análisis específico del área de Seguridad Informática.	Cubierto.
Controles en las entradas al sistema y sus almacenamientos.	En ejemplos.
Transacciones rechazadas y observadas.	En casos.
Planificación de las actividades de auditoria.	Muy desarrollado, basado en Auditoría sustentada en Riesgos con impacto tecnológico y del Negocio. GTAG 11, etc, Trabajos Prácticos.
Pruebas de cumplimiento.	En casos prácticos de integración
Evaluación de aplicación de políticas, planes, normas, procedimientos, esquemas, estándares y métricas.	En casos prácticos de integración
Test de penetración.	Vía ejemplos de aplicación
Comprobaciones y simulaciones sobre planes de contingencia, continuidad de operaciones y recuperación	Se desarrolla con ejemplos de Auditoría de Plan de Contingencia y de Auditoría de Prueba de Plan de Contingencia.

TTFM

CONTENIDOS MÍNIMOS	OBSERVACIONES
Prácticas de redacción.	La c□nsider□ una c□mpetencia transversal, facilita el aprendizaje y la c□mprensión. N□ s□l□ es necesaria para la redacción del TF, la deben aplicar en muchas materias de la carrera.
Referencias y Plagi□.	L□s alumn□s deben c□n□cer las n□rmas de referenciación para n□ c□meter plagi□. N□ se dimensi□na c□rrectamente que es una falta grave y que se puede c□meter en f□rma n□ intenci□nal, s□l□ p□r n□ citar c□rrectamente.

SSOyA

Título general que se desarrolla en varias clases (para los contenidos): Ciclo de vida del desarrollo de sistemas, Ataques y vulnerabilidades en aplicaciones y sistemas, Análisis de logs, Vulnerabilidades en web.

Contenido general, se aborda desde diversas perspectivas (para los contenidos): Controles de los sistemas, Control en la operación y el mantenimiento de las aplicaciones, Aplicaciones distribuidas.

Contenido técnico específico: Buffer Overflows, Format Strings, Race Conditions, Entornos protegidos (sandboxes, chroot), Mecanismos de protección: técnica del canario, segmento no ejecutable, HostIDs.

Se sugiere la incorporación como contenido mínimo el tema general de “Diseño seguro”, el cual se da en distintos contenidos como ser: entornos protegidos, vulnerabilidades web, códigos maliciosos, seguridad en bases de datos, Seguridad en el SDLC, ataques y vulnerabilidades, buffer overflow, etc.

MLEP

Este contenido mínimo no abarca la totalidad de temas que se imparten, ver comentarios en las preguntas (Comentando sobre el contenido mínimo: Ética y Privacidad)

RED 1

El protocolo SET si bien es de interés histórico no se está dando actualmente por razones de tiempo.

El tema de Factura Electrónica no se está dando, aunque se ven los protocolos de base para sustentar el mismo.

De la asignatura Redes 2 se incluyó el tema de IDS en esta materia.

Se incorporaron los siguientes contenidos:

*) SIEM: Gestion de eventos e incidentes de seguridad

*) SOC: Centro de Operaciones de Seguridad

*) Web Application Firewall

*) NIDS/NIPS Sistemas de detección y prevención de intrusos

*) Estrategias de seguridad en redes en ambientes cloud

Se propone una nueva enumeración de los contenidos mínimos, en la que ya se hacen los comentarios vertidos en el relevamiento (reordenamiento, temas incluidos como optativos y nuevos temas incorporados), a saber:

- Esquemas de seguridad: distribución de claves simétricas.
- Administración de claves publicas: autoridad certificante y certificados. Administración de claves de sesión compartidas.
- Seguridad Perimetral, firewalls. Web Application Firewall, NIDS/NIPS Sistemas de detección y prevención de intrusos
- Seguridad de redes e Internet: Infraestructura de Clave Publica PKI, Estrategias de seguridad en redes en ambientes cloud
- Protocolos de Autenticación: Single Sign On.
- Seguridad de WWW; Protocolo TLS/SSL, comercio electrónico. gateways de pago.
- Seguridad en IP IPSec.
- Seguridad en organizaciones: Firma Digital, administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades.
- Análisis de vulnerabilidades técnicas
- SIEM: Gestion de eventos e incidentes de seguridad
- SOC: Centro de Operaciones de Seguridad
- Otros temas optativos: protocolo SET “Secure Electronic Transaction”, Factura Electrónica.

RED 2

El tema IDS se está dando en Redes 1

Se incorporó el tema Botnets.

Se incorporó el tema de “Seguridad en Arquitectura de Servicios WEB”

El tema “Desarrollo seguro” pertenece a la materia Seguridad en Sistemas Operativos y aplicaciones.

La enumeración de los contenidos mínimos excluyendo los que se han pasado a la asignatura Redes 1 y los nuevos temas incorporados son:

- Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, Honeypots; análisis de vulnerabilidades, pruebas de penetración
- Botnets.
- Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de control.
- Ubicación de Firewalls.
- Seguridad en Arquitectura de Servicios WEB.

CUESTIONARIO ESPECÍFICO

a) ¿Qué problemas sobre los contenidos y/o alcances del plan de estudios identifica usted respecto de su asignatura?

SF

La carga horaria asignada a la materia (16 horas: 4 clases aproximadamente) resulta insuficiente para poder abarcar la cantidad de temas que deben impartirse desde el punto de vista de la Seguridad Física.

AUDIT

Restricciones de tiempo para desarrollar conjuntamente los fundamentos de la asignatura y los distintos escenarios de aplicación, frente a nuevas tecnologías, o su grado de evolución con impacto en seguridad y control. La selección de prioridades resulta cada vez más difícil, y se debe optar por eliminar temas, con sustitución parcial vía trabajos de investigación adicionales a cargo de los alumnos.

TTFM

Considero que faltan herramientas metodológicas de investigación, los alumnos llegan al taller de TF sin tener metodología.

IF

En particular, creo que se deberían poder realizar laboratorios presenciales.

MLEP

El tema de Ética y Privacidad abarca una miríada de temas que en la realidad se están impartiendo como parte de la asignatura y no se encuentran detallados a este nivel.

DyPS

Puede existir un sesgo excesivo hacia la documentación. Desde el propio nombre de la materia se condiciona el enfoque.

RED 1

En el apartado “Espacio para comentario y observaciones” se identifican temas que se deberían incorporar y/o eliminar de la nómina de contenidos mínimos.

b) ¿Posee alguna preocupación en particular con los contenidos del plan de estudios?

SF

Los contenidos mínimos no incluyen algunos temas importantes según mi criterio.

GEST1

Considero que debemos actualizarlo a la luz de los cambios que se han producido en los temas de seguridad. Si bien las materias se actualizan permanentemente, seguramente hay temas que no se están ofreciendo.

En nuestro caso, se han considerado las actualizaciones de los estándares, frameworks y regulaciones. Así supongo y espero que el resto de las asignaturas. Habría que ver que pasa, por ejemplo, temas referidos a Computación en la Nube ya que esta modalidad ha avanzado significativamente en los últimos tiempos.

GEST2

No se identifican problemas específicos. Se trabaja en forma coordinada con los docentes de GESI I, prerrequisito de la materia.

AUDIT

El tiempo asignado a la materia resulta insuficiente debido a que se hace necesario introducir conceptos generales de base durante la cursada consumiendo tiempo necesario para desarrollar los temas más complejos.

TTFM

El plan es flexible e incorpora en forma permanente nuevas tendencias.

Una de las causas principales del TMT (todo menos tesis) es que los alumnos no tienen orientación y seguimiento luego de finalizar la cursada. También les cuesta definir el tema.

IF

La dinámica de la materia hace que se deban actualizar continuamente los contenidos ya sea por cuestiones tecnológicas o por marcos normativos

SSOyA

Es importante que los contenidos técnicos del plan de estudio se mantengan actualizados para que la oferta del posgrado continue siendo interesante y dado el avance tecnológico constante, lo cual se hace más crítico en materias con alto contenido técnico.

CO

Al ser el tema de Motivación tan importante para los conocimientos del manejo de los estudiantes en las empresas tanto públicas como privadas, se ha observado en el transcurso del dictado, durante varios años, que no resulta suficiente la carga horaria asignada a la materia para poder abarcarlo con mayor detalle y profundidad.

MLEP

Lo mencionado en el punto a)

También se debe mencionar el hecho de que la carga horaria asignada a la cursada resulta insuficiente para cubrir los temas impartidos. Se necesitan 3 clases más para poder cubrir los temas para impartir los conocimientos deseados.

DyPS

Entiendo que existe una necesidad, recabada a partir de la propia manifestación de los alumnos, de abordar la gestión de porfolios, programas y proyectos de Seguridad desde una óptica más generalista y no enfocada exclusivamente en la parte documental.

RED 1

Además, lo planteado en cuanto al reordenamiento de los contenidos brindaría una mejor y mayor especificidad técnica a la asignatura.

c) ¿Tiene alguna propuesta para resolver estos problemas?

SF

Si, por un lado, se sugiere agregar un par más de clases a la cursada y además se completa esta respuesta en las preguntas d) y e)

AUDIT

Consideramos que se podría agregar una asignatura de tipo introductorio para desarrollar los conceptos de base para nuestra asignatura de Auditoría, con una carga horaria menor

TTFM

Creo que el taller podría estar desarrollado temporalmente de otra forma. Por ejemplo, un encuentro mensual desde el inicio de la maestría o especialización. Podría comenzar con algunos conceptos de metodología de la investigación, como para que puedan definir un problema de investigación, luego los objetivos e identificar las herramientas metodológicas que utilizarán. Esto se sumaría al contenido actual, ya que, como mencioné antes, la redacción, búsqueda de información y referenciación son transversales al resto de las asignaturas. Se podrían organizar encuentros donde otros maestrandos cuenten su experiencia. También es muy útil que cada cátedra identifique una serie de temas posibles que orienten esta elección.

Asimismo, el docente a cargo sugiere estos contenidos para agregar en la asignatura.

Contenidos a agregar para TALLER DE TRABAJO FINAL DE INTEGRACION:

- Tipos de trabajo final (TF).
- Disposiciones individuales para el desarrollo del TF.
- Plan de trabajo para el desarrollo del TF.
- Criterios genéricos y normativos.
- Consideraciones acerca del plagio.

Contenidos a agregar para TALLER DE TRABAJO FINAL DE MAESTRÍA (todos contenidos relevantes):

- Tutorías grupales e individuales.
- Organización de Trabajos Finales de Maestría con orientación académica y con orientación profesional.
- Importancia del aporte personal y originalidad de los objetivos perseguidos.
- Desarrollo de un Plan de Trabajo de Maestría.
- Selección de potenciales Directores de Trabajo Final de Maestría.
- Estructura de los capítulos y contenidos a incluir en los mismos (Hay una relación estrecha entre objetivos específicos del TF y capítulos o contenidos. Si están bien definidos los objetivos, el contenido es la respuesta a ese objetivo).
- Declaración Jurada de origen de los contenidos. Plazos reglamentarios para la presentación de Planes de Trabajo Final de Maestría y del propio Trabajo Final.
- El proceso de habilitación para la defensa.
- La defensa del Trabajo Final de Maestría (Es algo que inquieta a los alumnos, también se brinda información sobre el tema y sirve mucho la experiencia de quienes ya han pasado por esa instancia.)

IF

Es inherente a la materia, no es un problema en sí mismo.

GEST1

Incluir como contenido mínimo un ítem referido a “Actualización en estándares, frameworks y regulaciones”

SSOyA

Cada docente, tomando en cuenta las especificidades de su materia, debería mantener los contenidos actualizados y de interés para los cursantes.

CO

Agregar dos clases más para permitir el tratamiento con mayor profundidad y amplitud el tema de Comunicación.

MLEP

Se sugiere incorporar como desglose de los contenidos mínimos los siguientes:

Ética:

- Teorías éticas y su aplicación
- Pensamiento crítico
- Ética profesional

Privacidad:

- Teorías de Privacidad
- Amenazas a la Privacidad
- Leyes de Privacidad nacionales e internacionales

Regulación del comercio y Libertad de Expresión

Nuevas tecnologías: su impacto ético y a la privacidad

También se sugiere incorporar como contenido mínimo para la parte Legal:

- Régimen legal atinente a la profesión de S.I.
- Cibercrimen

DyPS

Modificar el nombre de la asignatura a “Gestión de Proyectos de Seguridad” y preparar a los maestrandos como gestores con foco en conocimientos, técnicas y herramientas conectadas con experiencias profesionales reales.

RED 1

Lo ya mencionado en el apartado “Espacio para comentario y observaciones”.

d) ¿Cuáles son sus perspectivas en relación con las competencias del perfil del graduado (los 12 mencionados anteriormente) y su relación con el mundo académico y el mercado laboral actual?

CRIPT1

Los graduados de la maestría reconocen y agradecen la formación adquirida en esta especialidad.

CRIPT2

Se trata de una enseñanza imprescindible en nuestra Maestría.

SF

Los temas planteados en las competencias resultan incompletos ya que es necesario ampliarlos para que los contenidos mínimos, que se sugieren en la respuesta e), encuentren su sustento.

Competencia sugerida para inclusión:

- Proteger físicamente los activos de la información, las personas y las instalaciones

GEST1

Considero que resolvemos muy satisfactoriamente la demanda de las organizaciones en cuanto al perfil que hemos nosotros adoptado. Más aún habiendo visto varias ofertas últimamente es notorio que han ido incorporando temas de gestión que estaban ausentes con anterioridad.

GEST2

Entiendo que quien egresa de la carrera se encuentra preparado para ejercer roles técnicos, gerenciales y de liderazgo estratégico, según las motivaciones personales de cada cursante. Puede también desarrollar una carrera académica. A manera de sugerencia, podrían ofrecerse seminarios en temas de seguridad de tecnologías emergentes, como la IA, la computación cuántica, los sistemas industriales, etc.

TDCG

Considero que este Taller cubre ampliamente las competencias esperadas en los estudiantes para desempeñarse a nivel de cualquier empresa en posiciones de liderazgo de las áreas de Seguridad de la Información.

TTFM

Considero que una de las habilidades más demandadas actualmente es la capacidad de trabajar en equipos interdisciplinarios. Si bien la maestría tiene un enfoque que orienta a los profesionales en tecnologías blandas, se podría complementar este perfil.

IF

Las competencias del perfil del graduado son un conjunto de habilidades, conocimientos y actitudes que se espera que los estudiantes desarrollen a lo largo de su formación académica y que les permitan insertarse de manera exitosa en el mundo laboral actual. Entre estas competencias se encuentran: la comunicación efectiva, el pensamiento crítico, la creatividad, la innovación, la colaboración, la responsabilidad social, la ética profesional, el aprendizaje autónomo, la adaptabilidad, el liderazgo, la gestión de proyectos y el uso de las tecnologías de la información y la comunicación. Estas competencias son relevantes tanto para el ámbito académico como para el profesional, ya que facilitan el desarrollo de procesos de investigación, generación de conocimiento, solución de problemas, trabajo en equipo y comunicación de resultados. Asimismo, estas competencias responden a las demandas y desafíos del mercado laboral actual, que requiere de profesionales capaces de adaptarse a los cambios constantes, innovar en sus campos de acción, colaborar con otros actores y asumir un compromiso ético y social con su entorno.

Dicho esto, considero que este posgrado cumple con esos postulados.

SSOyA

Considero que las 12 competencias resultan pertinentes y acordes a las necesidades del mercado laboral actual. Esto fundamentado en que ofrecen al graduado la posibilidad de insertarse en el ámbito de la Seguridad de la Información o profundizar sus conocimientos en dicha temática.

Finalmente, y en relación al mundo académico, también ofrecen un fundamento interesante para empezar a ejercer la docencia dentro del ámbito. Una prueba de este punto, es la presencia de graduados como docentes o ayudantes en varias de las materias de la carrera.

CO

Desde el punto de vista de los contenidos para el mercado laboral, los estudiantes encuentran que la materia les resulta de suma utilidad ya que proponen casos propios de la vida real que les ocurren y esos casos, más casos elaborados por la cátedra, son tratados en clase lo que enriquece e incrementa el conocimiento y las competencias que los alumnos adquieren.

MLEP

Los estudiantes encuentran muy interesantes los conceptos vertidos en la materia ya que les habilitan un panorama mucho más amplio respecto de las habilidades blandas que un profesional de seguridad de la información debe conocer y manejar, tanto desde el punto de vista ético, los conocimientos de la privacidad y el manejo de la parte legal que un profesional debe conocer para poder desempeñarse en un cargo directivo en las empresas de hoy en día.

RED 1

Entiendo que las competencias que están contempladas en el Plan son suficientes y cubren ampliamente las necesidades de los futuros profesionales de SI.

RED 2

Esta asignatura complementa lo dictado en la correlativa anterior.

e) Finalmente, pero no menos importante, pensando en normativas nacionales e internacionales reconocidas (La decisión administrativa 641/2021[1] o la ISO 27002:2022) ¿considera usted que existen contenidos mínimos que podrían incluirse o excluirse en su asignatura? Por favor, elabore su respuesta. (Se adjunta un cuadro comparativo de estas normativas y una nómina de los controles de la ISO 27002:2022[2] que puede resultarle de utilidad para responder esto último).

CRIPT1

Esta asignatura es esencialmente técnica (matemática discreta aplicada y álgebra abstracta aplicada) y por lo tanto ortogonal a las normas administrativas, siempre y cuando se siga dictando en el nivel actual, el que alcanza lo exigible en la implementación práctica de protocolos de seguridad que aseguren los tres pilares de la seguridad informática: **confidencialidad, integridad y disponibilidad**.

CRIPT2

Todo es perfectible, pero no así el empeño puesto en el dictado de esta materia y que capacita a nivel competitivo en escala mundial a sus egresados. Seguiremos en esta línea docente, es nuestro compromiso.

SF

Se sugiere la inclusión de los contenidos mínimos que se indican a continuación:

1. Sistemas perimetrales y control de acceso
2. Ciclo de vida de los soportes físicos de almacenamiento
3. Seguridad de las Instalaciones de Suministro y del Cableado
4. Mantenimiento de los componentes de la seguridad física
5. Monitoreo de la seguridad

GEST1

[1] REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL
[2] Seguridad de la Información, Ciberseguridad y Protección de la Privacidad

Nosotros pasamos revista a la ISO 27002 para entender su contenido y misión dentro de la gestión de la seguridad. No entramos analizar los controles sugeridos porque entendemos que es resorte de las materias de contenido técnico que forman parte del currículo.

GEST2

Como participante activo en el desarrollo de la DA 641/2021, considero que sus contenidos están cubiertos mayormente en la cursada de la carrera. Esta norma se basó en la ISO/IEC 27002, versión 2013. La nueva versión 2022 de este estándar reordena y agrega algunos objetivos de control y controles, obteniéndose a mi entender, una norma más sencilla de interpretar y aplicar, pero que no contiene grandes cambios respecto a los contenidos de la versión anterior. Adicionalmente durante la cursada de GESI II, se recorren estándares tales como la ISO 27005, complementario de la ISO/IEC 27001, y metodologías utilizadas internacionalmente, como Magerit, para el dictado de las clases de Riesgo.

TDCG

Considero que este Taller cubre ampliamente las competencias esperadas en los estudiantes para desempeñarse a nivel de cualquier empresa en posiciones de liderazgo de las áreas de Seguridad de la Información.

AUDIT

Consideramos conveniente contemplar los contenidos básicos de las normas internacionales: NIST, COBIT, en lo pertinente y COSO, actualización 2013 y la versión actualizada de COSO Risk Management.

IF

En relación a las normativas citadas, considero que se están dando mucho más que los contenidos mínimos y creo que es adecuado el plan de estudios diseñado en esta asignatura.

SSOyA

Inicialmente puedo mencionar que considero que los contenidos están bien seleccionados, considerando las restricciones del tiempo total de la materia.

Acompañando las tendencias tecnológicas actuales, podría ser adecuado incluir más contenidos de DevSecOps dentro de las clases de Ciclo de vida del desarrollo de sistemas.

Además, sería interesante poder desarrollar con profundidad la temática de ingeniería inversa para brindar conocimientos detallados sobre el funcionamiento del software y los mecanismos arquitectónicos y de los sistemas operativos que lo sustentan.

Sin embargo, el desarrollo de esta temática se encuentra limitada por la longitud total (en horas) de la materia.

CO

Los conceptos impartidos se ubican más en los contenidos de la ISO 27001:2022. Esta norma también fue utilizada como base para la DEA 641/2021

Nótese que solo en el índice de esa norma ISO se establecen contenidos del tipo, a saber:

Contexto de la organización

- Comprender las necesidades y expectativas de las partes interesadas

Liderazgo

Tareas de Apoyo

- Concientización
- Comunicación

Esta norma da el sustento teórico conceptual para la creación del Sistema de Administración de Seguridad de la Información en una empresa y de esta norma se desprenden los controles que se mencionan en la ISO 27002.

MLEP

Los conceptos de esta asignatura cubren principalmente los controles que hacen al cumplimiento de las normas legales por parte de una empresa (control 5.31) pero

también se incorporan aquellas habilidades blandas que hacen a un gerenciamiento ético y responsable no solo con los recursos propios de una empresa sino también con el público, terceros involucrados y la sociedad en general.

DyPS

El proyecto que utilizo en el curso es en sí mismo la implementación de un sistema de Gestión basado en familia ISO 27000. La materia no aborda específicamente 27001 (sistema de gestión) o 27002 (controles) pero usamos base de esos conocimientos que se trabajan en otra materia.

RED 1

Se podrían incorporar como contenidos mínimos los que corresponden de la ISO 27002:

- Gestión de vulnerabilidades técnicas (8.8): parcialmente solo en cuanto al "análisis de vulnerabilidades". Por lo tanto, se sugiere la incorporación de un contenido del tipo de: "Análisis de vulnerabilidades técnicas"

Los temas que se indican a continuación ya fueron incorporados en la asignatura según se desprende de lo comentado en observaciones del espacio para comentarios

- Seguridad de la información para el uso de servicios en la nube (5.23)
- Gestión de identidades (5.16)
- Registro de eventos (8.15), tema ya incorporado al tratar el tema de SIEM

Por todo lo expuesto anteriormente se sugiere que la nómina de contenidos mínimos de la asignatura Seguridad en Redes I sea (se repite lo consignado en la parte de comentarios generales):

- Esquemas de seguridad: distribución de claves simétricas. Administración de claves públicas: autoridad certificante y certificados. Administración de claves de sesión compartidas.
- Seguridad Perimetral, firewalls. Web Application Firewall. NIDS/NIPS Sistemas de detección y prevención de intrusos.
- Seguridad de redes e Internet: Infraestructura de Clave Publica PKI, Estrategias de seguridad en redes en ambientes cloud.

- Protocolos de Autenticación: Single Sign On.
- Seguridad de WWW; Protocolo TLS/SSL, comercio electrónico, gateways de pago.
- Seguridad en IP IPSec.
- Seguridad en organizaciones: Firma Digital, Administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades.
- Análisis de vulnerabilidades técnicas.
- SIEM: Gestión de eventos e incidentes de seguridad.
- SOC: Centro de Operaciones de Seguridad.

Se está pensando incluir dentro del tema de seguridad perimetral el enfoque desde el punto de vista industrial.

RED 2

Podrían incorporarse como contenidos mínimos de la ISO 27002:

- Prevención de la fuga de datos (8.12)

Por todo lo mencionado se sugiere que los contenidos mínimos de la asignatura Seguridad en Redes II sean:

- Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención.
- Botnets.
- Honeypots, análisis de vulnerabilidades, pruebas de penetración.
- Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de control.
- Ubicación de Firewalls
- Seguridad en Arquitectura de Servicios WEB.
- Prevención de la fuga de datos.

Universidad de Buenos Aires Buenos Aires, 10 de setiembre de 2008.

Exptes. Nros. 342.484/08, 492.400/08 y
912.233/08

VISTO las actuaciones presentadas por las Facultades de Ciencias Económicas, de Ciencias Exactas y Naturales y de Ingeniería mediante las cuales solicitan la creación de la Carrera de Especialización en Seguridad Informática, organizada en conjunto entre las tres Facultades, y

CONSIDERANDO:

Lo establecido por las resoluciones (CS) nros. 6649/97 y 807/02.

Que resulta indispensable jerarquizar la temática de la Seguridad Informática en una actividad académica en el marco de la Universidad de Buenos Aires;

Lo informado por la Dirección de Títulos y Planes.

Lo aconsejado por la Comisión de Estudios de Posgrado.

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD DE BUENOS AIRES,
R e s u e l v e:

ARTICULO 1º.- CREAR LA CARRERA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA, organizada conjuntamente entre la Facultad de Ciencias Económicas, la Facultad de Ciencias Exactas y Naturales y la Facultad de Ingeniería.

ARTICULO 2º.- Aprobar la reglamentación general, los objetivos, el plan de estudios y los contenidos mínimos de las asignaturas de la carrera a que se refiere el artículo 1º, y que como Anexo 1 forma parte de la presente resolución y el Reglamento específico obrante en el Anexo 2.

ARTICULO 3º.- Regístrese, comuníquese, notifíquese a la Secretaría de Asuntos Académicos, a la Subsecretaría de Posgrado y a la Dirección de Títulos y Planes. Cumplido, archívese.

RESOLUCION Nº 4852
NES

Rubén Eduardo Hallú
Rector

Carlos Esteban Mas Vélez
Secretario General

Universidad de Buenos Aires

ANEXO 1

I. INSERCIÓN INSTITUCIONAL DEL POSGRADO

Denominación del posgrado: **Carrera de Especialización en Seguridad Informática**
Denominación del Título que otorga: **Especialista en Seguridad Informática**
Unidades Académicas de las que depende el posgrado: Facultades de Ciencias Económicas, de Ciencias Exactas y Naturales y de Ingeniería.
Sede/s de desarrollo de las actividades académicas del posgrado: Facultad de Ciencias Económicas (según las resoluciones (CD) nros. 1966/08 de la Facultad de Ciencias Exactas y Naturales; 3522/08 de la Facultad de Ingeniería y 2932/08, de la Facultad de Ciencias Económicas)
Resoluciones del CD de la/s Unidad/es Académica/s de aprobación del proyecto de posgrado: Facultad de Ciencias Económicas, res. (CD) nro. 2499/08; Ciencias Exactas y Naturales, res. (CD) nro 408/08 y Facultad de Ingeniería res. (CD) nro 2900/08

II FUNDAMENTACION DEL POSGRADO

A) ANTECEDENTES

a) Razones que determinan la necesidad de creación del proyecto de posgrado:

El uso masivo de las TIC (tecnologías de la información y comunicaciones) como medios para generar, almacenar, transferir y procesar información se ha incrementado espectacularmente en los últimos años, y es un elemento indispensable para el funcionamiento de la sociedad actual. La información en todas sus formas y estados se ha convertido en un activo estratégico, al cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad.

La sociedad ha adquirido una gran dependencia respecto del manejo apropiado de la información. Las aplicaciones informáticas son cada vez más importantes, los requerimientos de seguridad son cada vez mayores y esenciales en la operatoria de las organizaciones modernas.

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

Un componente fundamental en toda clase de actividades es la información. Los recursos informáticos se encuentran permanentemente sujetos a distintas situaciones de riesgo. Múltiples personas en diferentes lugares del mundo, se especializan en realizar toda clase de ataques a la seguridad, para lo cual muchas de las organizaciones no están adecuadamente preparadas.

Asegurar la información de una organización requiere instalar una cultura de seguridad e implementar una adecuada combinación de conceptos, tecnologías, metodologías, estándares, herramientas de gestión y recursos humanos capacitados.

Un profesional en Seguridad Informática debe saber aplicar adecuadamente elementos tecnológicos como técnicas biométricas, técnicas criptográficas, modelos formales de seguridad, arquitectura del computador, sistemas operativos y redes, informática forense, como así también, habilidades y herramientas gerenciales de planeamiento, de continuidad de las operaciones, manejo de incidentes, recursos humanos, auditoria, seguridad física e incluso la adecuada comprensión de los aspectos legales nacionales e internacionales.

Uno de los mayores retos de las organizaciones es garantizar la seguridad de los recursos informáticos y de las personas. Actualmente existen en el mercado regulaciones específicas que imponen entidades de contralor, bancos centrales, bolsas de valores y otros organismos. Estas regulaciones implican que las organizaciones deben respetar normas impuestas, ponerlas en práctica y demostrar que cumplen con ellas.

La gestión del riesgo es un elemento fundamental en el logro de los propósitos y objetivos de las organizaciones. La explosiva evolución de la tecnología ha creado nuevos factores de riesgo que son prácticamente desconocidos por los niveles de conducción.

En tales circunstancias, se hace evidente la necesidad de participar académicamente en la formación de los recursos humanos para que adquieran la capacidad de asistir a la conducción a conocer en detalle los riesgos, sus características, el efecto en las operaciones y, lo más importante, las formas de afrontarlo y, en lo posible, mitigarlos y/o neutralizarlos.

La gestión de los riesgos informáticos constituye una necesidad ineludible para cualquier organización que quiera administrar y utilizar su información de manera confiable, segura y funcional para el logro de sus objetivos.

Los recursos humanos especializados en Seguridad Informática en nuestro país son escasos y las carreras de grado no contemplan en sus planes de estudio un enfoque integral para solucionar las crecientes necesidades en este área. Dado este escenario la Carrera en Seguridad Informática es una nueva opción académica que representa el esfuerzo de un grupo de especialistas de la UBA por ofrecer capacitación de alto nivel.

La carrera es el espacio ideal de convergencia de experiencias, tecnologías y metodologías, en donde los estudiantes puedan prepararse para enfrentar el reto de seguridad que significa vivir en un mundo globalmente interconectado.

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

Esta carrera, además de un sólido marco teórico, busca ofrecer a los estudiantes escenarios con casos reales sobre el tema de la seguridad informática y los riesgos a los que se está expuesto, que busquen construir un contexto de aprendizaje práctico alrededor de la vulnerabilidad intrínseca de los sistemas. Se procura establecer un marco de gestión adecuado y coherente de la información crítica de la organización.

Los profesionales en informática deben repensar los conceptos tradicionales en el área de seguridad, para procurar mayores y mejores niveles de aseguramiento de la información.

b) Antecedentes en instituciones nacionales y/o extranjeras de ofertas similares:

A nivel nacional existen en la actualidad dos ofertas que apuntan a objetivos similares pero no con el mismo contenido. Ellas son:

- Posgrado de Especialización en Criptografía y Seguridad Teleinformática en el Instituto de Educación Superior del Ejército IESE
- Posgrado en Seguridad de la Información en la Universidad del Salvador

Se ha tomado en cuenta, además, el Currículo de Seguridad de la Información presentado en el Congreso Segurinfo 2007 organizado por USUARIA.

A nivel internacional se han evaluado programas de posgrado en diversas universidades de los EE.UU., Europa y Latinoamérica. Finalmente se trabajó sobre varios programas de las universidades de los Estados Unidos por ser los más adelantados en la materia. Los programas más calificados y tomados en cuenta por este grupo de trabajo han sido los siguientes:

- University of Purdue, Indiana, EE.UU.:Cerias (The Center for Education and Research in Information Assurance and Security).
- Norwich University, Vermont, EE.UU; Infosec Graduate Program, Master in Science in Information Assurance.
- Kennesaw State University, Georgia, EE.UU: Center for Information Security Education, que ha sido nominado como el National Center of Academic Excellence in Information Assurance Education por la National Security Agency.

CARLOS ESTEBAN MAS VELEZ
Secretario General

c) Comparación con otras ofertas existentes en la Universidad: establecer similitudes, diferencias y posibilidades de articulación

No existe en la Universidad de Buenos Aires una oferta comparable con la que contiene esta presentación.

d) Consultas a las que fue sometido el proyecto de posgrado, indicando personas e instituciones (adjuntar documentación pertinente)

Se han realizado numerosas reuniones con la activa participación de los siguientes docentes:

Facultad de Ciencias Económicas

- Raúl Saroka; Ricardo Rivas; Leopoldo Cansler

Facultad de Ciencias Exactas y Naturales

- Hugo Scolnik; Graciela Pataro; Rodolfo Baader

Facultad de Ingeniería

- Alberto Dams; Hugo Pagola; Luis Marrone

Además, se ha consultado a los siguientes expertos del ámbito profesional:

- Juan Pedro Hecht; Julio Ardita; Edgardo Marcelo Ohman, Pablo Kaufer Barbe; Adrián Amigo

e) Convenios con instituciones

Se ha acordado con la Dirección de Relaciones Internacionales de la Universidad Politécnica de Cataluña explorar la posibilidad de realizar la carrera en forma conjunta.

B) JUSTIFICACIÓN DE LA CARRERA DE ESPECIALIZACION EN SEGURIDAD INFORMÁTICA.

De acuerdo con el artículo 11° de la Resolución (CS) Nº 6649/7, esta es una carrera de especialización.

Este posgrado tiene amplia justificación dentro del siguiente marco de referencia:

- Complejidad del contexto actual de las actividades públicas y privadas
- Universalización de la utilización de las tecnologías informáticas en las organizaciones públicas y privadas.
- Impacto de las TIC en la gestión de las organizaciones.
- Incremento notorio de los problemas de seguridad en materia de la gestión de la información.

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

- Crecimiento de las formas de delitos mediante el uso de la tecnología.
- Existencia de entes, disposiciones, estándares que exigen a las organizaciones el cumplimiento de normas de seguridad y la generación de responsabilidad emergente para quienes conducen esas organizaciones.
- La escasa oferta en la Republica Argentina de formación universitaria en materia de Seguridad Informática.
- La necesidad de proveer una oferta académica de alto nivel para capacitar a profesionales desde una perspectiva tecnológica, legal, ética y psico-social.
- La necesidad de mejorar la formación universitaria de los profesionales que buscan dedicarse a la especialidad de la Seguridad Informática.
- La importancia que adquiere la protección de los activos informáticos de las organizaciones y personas, y la información acerca de los individuos.

III OBJETIVOS DEL POSGRADO

- Preparar recursos humanos capacitados en todos los ámbitos relacionados con la Seguridad Informática.
- Crear conciencia de la importancia y los alcances que esta área de conocimiento tiene actualmente en prácticamente todas las actividades de la sociedad, impulsando y fomentando una cultura de Seguridad Informática.
- Formar especialistas en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos a la sociedad.
- Incorporar el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.
- Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.
- Formar profesionales éticos capaces de generar, aplicar y transmitir los conocimientos adquiridos.

IV PERFIL DEL EGRESADO

El especialista en Seguridad Informática debe ser un profesional con aptitud para promover y aplicar metodologías actualizadas que conduzcan a la práctica de la Seguridad Informática, capaz de discernir entre las ventajas y desventajas asociadas con el diseño y gestión de políticas de seguridad, y de diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos, basado en estándares nacionales e internacionales y aspectos éticos-legales.

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

Competencias esperadas del egresado de la carrera de especialización en Seguridad Informática:

- Instrumentar un plan integral de Seguridad Informática de la organización.
- Colaborar en definir estrategias y políticas de Seguridad Informática.
- Entender en los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)
- Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y aplicar las medidas de protección adecuadas a cada situación.
- Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa.
- Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico.
- Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones.
- Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática.
- Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática.

V ORGANIZACIÓN DEL POSGRADO

a) INSTITUCIONAL: REGLAMENTO DEL PROYECTO DE POSGRADO.

1. Modalidad de designación de las autoridades del posgrado y funciones.

La Carrera de Especialización será dirigida por la Comisión de Maestría en Seguridad Informática. El director y los subdirectores de la Maestría serán el director y subdirectores de la Carrera.

La Comisión será la encargada de supervisar el funcionamiento de la carrera.

Serán sus funciones:

a) Seleccionar los profesores y tutores.

b) Definir los requisitos previos para el ingreso de los aspirantes.

c) Estudiar los antecedentes de los aspirantes.

d) Proponer al Consejo Directivo de la Facultad sede de la Carrera la aceptación o rechazo, con dictamen fundado, de los aspirantes como candidatos a la Carrera.

CARLOS ESTEBAN MAS VELEZ
Secretario General

e) Definir el plazo máximo durante el cual el aspirante podrá completar la Carrera, incluida la aprobación del trabajo final. Dicho plazo no se podrá prolongar más de cuatro años a contar desde la fecha de admisión.

f) Evaluar periódicamente el nivel académico de los cursos, seminarios y programas específicos de la Carrera.

g) Emitir opinión fundada sobre los programas analíticos de las diferentes actividades académicas.

h) Evaluar los aspectos relacionados con la metodología y evaluación de las actividades de enseñanza y aprendizaje

i) Aprobar informes periódicos y la memoria anual de la Carrera que presenta el Director.

j) Determinar, cuando sea pertinente, los cursos previos de nivelación, que deberán cursar y aprobar los aspirantes de la Carrera, y las unidades académicas en las que deberán cumplimentar dichos cursos...

k) Proponer al Consejo Directivo de la Facultad sede de la Carrera la aprobación por equivalencia de las materias de posgrado que los estudiantes cursen fuera de la Carrera. En ningún caso el total de cursos aprobados por equivalencia debe superar el 30% de las materias de la Carrera.

2. Modalidad de selección y designación de profesores

- Podrán ser docentes aquellos que sean profesores de universidades argentinas o extranjeras y/o en su caso expertos de reconocido prestigio en la temática.

b) ACADÉMICA: PLAN DE ESTUDIOS. CONTENIDOS MÍNIMOS.

100 - Ejes temáticos de la seguridad

Concepto de seguridad. Servicios básicos de seguridad: Confidencialidad, integridad, disponibilidad, autenticación, no repudio. Elementos a proteger. Amenazas, riesgos, vulnerabilidades. El factor humano. Estrategias de seguridad: normas, políticas y procedimientos; fuentes de amenazas; niveles de seguridad; seguridad lógica y física. Controles de acceso: modelos discrecionales, mandatorios, por roles; Bell-Lapadula, Clark-Wilson, pared china. Identificación, autenticación, autorización. Incidentes de seguridad: prevención, detección, recupero.

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

200 - Criptografía

Fundamentos de criptología, Introducción a los criptosistemas. Criptología clásica: cifrados y ataques. Secreto perfecto y One-Time Pad. Criptosistemas simétricos: históricos y actuales; modos operativos. Criptosistemas asimétricos; comparaciones de seguridad entre cifradores simétricos y de clave pública. Gestión de claves simétricas y asimétricas. Intercambio seguro de claves. Funciones Hash/MAC/HMAC. Generación de números aleatorios. Ataques. Protocolos especiales.

300 - Gestión estratégica de la seguridad

Organización y estructura del área de seguridad: áreas, funciones y responsabilidades, perfiles, criterios de organización. Técnicas de gestión (estrategia, finanzas, marketing y recursos humanos). Ciclo de vida de los sistemas de seguridad. Gestión de proyectos de seguridad. Tercerización de servicios y gestión de proveedores. Evaluación económica de la seguridad. Métricas y performance. Estrategias, políticas, programas y normas de seguridad. Introducción al análisis y gestión del riesgo.

500 - Seguridad en sistemas operativos y aplicaciones

Instalación y operación segura del sistema operativo. Ciclo de vida del desarrollo de sistemas. Desarrollo y gestión de bases de datos. Controles de los sistemas. Control en la operación y el mantenimiento de las aplicaciones. Aplicaciones distribuidas. Ataques y vulnerabilidades en aplicaciones y sistemas. Buffer Overflows, Format Strings, Race Conditions. Entornos protegidos (sandboxes, chroot). Mecanismos de protección: técnica del canario, segmento no ejecutable. Análisis de logs. HostIDS. Vulnerabilidades en web. Códigos maliciosos.

600 - Seguridad en redes I

Esquemas de seguridad: distribución de claves simétricas. Administración de claves publicas: autoridad certificante y certificados. Administración de claves de sesión compartidas. Seguridad de redes e Internet: Single Sign On, Infraestructura de Clave Publica PKI. Seguridad de WWW; comercio electrónico, gateways de pago, protocolo SET "Secure Electronic Transaction"; seguridad en IP IPSec: Firewalls, SSL. Seguridad en organizaciones: Firma Digital, Factura Electrónica; administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades.

650 - Seguridad en redes II

Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, Intrusión Detection Systems Honeypots; análisis de vulnerabilidades, pruebas de penetración. Desarrollo seguro. Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de control. Ubicación de Firewalls, IDS.

CARLOS ESTEBAN MAS VELEZ
Secretario General

700 - El comportamiento organizacional

Cultura organizacional. Clima organizacional. Comportamiento individual, grupal y organizacional. Dinámica de grupos. Valores y actitudes. Comunicación interpersonal. Motivación. Liderazgo. Trabajo en equipo. Resolución de conflictos. Negociación. Gestión del cambio organizacional. Inteligencias múltiples. El proceso de aprendizaje. Toma de decisiones individuales y grupales.

900 - Marco legal, ética y privacidad.

Introducción al derecho Informático, conceptos y terminología legal. Sistemas legales en Argentina y otros países. Régimen jurídico de protección de la Propiedad Intelectual. Régimen de Firma Digital. Ética y privacidad. Visión jurídica de lo delitos informáticos. Derecho Internacional: legislación transfrontera. Jurisprudencia.

1000 Trabajo final de la Especialización en Seguridad Informática

Al finalizar el primer año el alumno entregará un trabajo final de especialización. El trabajo será individual y consistirá en un análisis crítico de un tema de la carrera. Será expuesto para su aprobación a un jurado designado por el director de la carrera.

800 – Documentación y proyectos de seguridad

Formulación y seguimiento de un proyecto de seguridad en base a un caso de estudio incluyendo el ciclo de vida del os sistemas de seguridad; fase inicial, fase de desarrollo y adquisición, fase de implementación, fase de operación y mantenimiento, fase de disposición.

CARLOS ESTEBAN MAS VELEZ
Secretario General

CUADRO GENERAL DE ASIGNATURAS

Primer cuatrimestre

Asignatura	Carga horaria		Correlatividades
	Teórica	Práctica	
Ejes temáticos de la seguridad	32		-
Criptografía	48	16	Ejes temáticos de la seguridad
Seguridad en sistemas operativos y aplicaciones	44	20	Ejes temáticos de la seguridad
Seguridad en redes I	44	20	Ejes temáticos de la seguridad
Documentación y proyectos de seguridad	16		-

Segundo cuatrimestre

Asignatura	Carga horaria		Correlatividades
	Teórica	Práctica	
Gestión estratégica de la seguridad	48	16	Documentación y proyectos de seguridad
Comportamiento organizacional	32		-
Seguridad en redes II	16	16	Seguridad en redes I Seguridad en sistemas operativos y aplicaciones
Marco legal, ética y privacidad	32		Ejes temáticos de la seguridad
Total	400		

Cabe aclarar, en relación con las materias, que si bien no existe asignación de correlatividades, se propone la estructura organizativa anteriormente descripta para el dictado de ellas, resguardando la coherencia y la profundización y análisis de los conceptos que éstas abordan para permitir la construcción del conocimiento y líneas de investigación del alumnado.

VII. ESTUDIANTES

a) Requisitos de admisión:

Podrán ingresar a la Carrera los postulantes que cumplan con los siguientes requisitos:

- Título de grado: haber aprobado estudios universitarios o de nivel superior no universitario de cuatro años de duración mínima en una universidad pública o privada, nacional o extranjera. Además el postulante deberá superar el proceso de selección, que implica:

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

- Antecedentes: acreditar la posesión de antecedentes académicos y profesionales suficientes a criterio de la universidad, que guarden relación con el área disciplinaria objeto de estudio de la Carrera.
- Examen de admisión: aprobar un examen de admisión donde se evalúan las aptitudes y capacidad lógica, como así también conocimientos de informática y redes.
- Idioma: se exige un acabado dominio de la lectura en idioma inglés. El postulante deberá acreditar ante el Director dicha aptitud o aprobar un examen de comprensión de textos, de acuerdo con lo previsto para cada carrera de posgrado.
- Cartas de recomendación: el aspirante debe presentar dos cartas de recomendación que avalen sus antecedentes académicos y profesionales.
- En la entrevista se evaluará el grado de motivación para el cual el postulante solicita su inscripción, compromiso con la finalización de la carrera, disponibilidad de tiempo, antecedentes y capacidad para abordarla íntegramente.
- Podrán postularse para cursar la carrera:

  a) Los egresados de las carreras que se dictan en la Facultad de Ciencias Económicas, Facultad de Ciencias Exactas y Naturales y Facultad de Ingeniería, UBA

  b) Los egresados de otras universidades que posean títulos afines a los ya señalados.

  c) Los egresados de universidades extranjeras donde se cursen carreras equivalentes en duración y temáticas a las indicadas.

  d) Los egresados de carreras terciarias vinculadas a las áreas temáticas de la carrera, serán evaluados individualmente y la Comisión de maestría establecerá los requisitos previos que correspondan en cada caso.

b) Criterios de selección:

- Dentro de los criterios de selección, primará la calidad del expediente académico y la experiencia profesional. Tendrán prioridad los estudios universitarios de carreras afines a las tres facultades.
- Se tendrá en cuenta la idoneidad de los estudios cursados y las carencias de formación, para establecer su trayectoria curricular, en caso de ser admitidos.
- Por orden de matrícula. Aquellos alumnos que cumpliendo los requisitos de acceso se matriculen entre los 35 primeros serán los que se acepten.

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

c) Vacantes requeridas para el funcionamiento del posgrado:

Para el funcionamiento de la carrera se considerará un mínimo de 15 (quince) alumnos y un máximo de 35 (treinta y cinco).

d) Criterios de regularidad:

La permanencia del alumno en la carrera exige la asistencia del 70% de las clases, la realización de las actividades prácticas y la presentación y aprobación de los trabajos de las asignaturas en tiempo y forma.

- Los alumnos tienen la obligación de cursar todas las materias en la secuencia que se defina desde la Dirección Académica. En caso que por razones debidamente certificadas debiera dejar de cursar una o más materias, deberá solicitar autorización por escrito a la Comisión de la Maestría.
- El sistema de calificaciones será el vigente para el conjunto de la UBA. De no alcanzarse el puntaje suficiente, el alumno podrá, por única vez, rendir una prueba recuperatoria y, en caso de que no volviese a aprobar, no podrá continuar cursando en forma regular la carrera. El alumno en esta situación, podrá solicitar su reincorporación al momento de iniciarse la siguiente cohorte, siendo decisión de la Coordinación Académica y la Comisión de la Maestría, junto con la Secretaría de Posgrado, aceptar o rechazar tal solicitud en función de los méritos académicos del alumno.

e) Requisitos para la graduación

Para acceder al título de la Carrera de Especialización en Seguridad Informática el aspirante deberá:

a) Aprobar las materias y otras actividades establecidas en el diseño curricular o fijado por la Comisión de Maestría que contribuyan a su formación integral y superior en las disciplinas involucradas.

b) Aprobar el trabajo final. Este trabajo será individual y consistirá en un análisis crítico de un tema de la carrera y será expuesto para su aprobación a un profesor designado por el director de la maestría.

VIII. INFRAESTRUCTURA Y EQUIPAMIENTO

Descripción detallada de las instalaciones y equipamientos necesarios para el desarrollo de las actividades académicas del posgrado: espacios físicos, laboratorios (si corresponde), equipamiento, biblioteca y centros de documentación, otros.

Dado que la Carrera se desarrollará en el ámbito de las tres facultades utilizará la infraestructura existente en cada una de ellas.

CARLOS ESTEBAN MAS VÉLEZ
Secretario General

VIII.-MECANISMOS DE AUTOEVALUACION

La Carrera será evaluada periódicamente cada 5 (cinco) años por el Consejo Superior según lo dispuesto en la Resolución (C.S). N 3415/88.

Se contempla el uso de un régimen de encuestas por tema y profesor, que se realizarán una vez terminados los módulos, y materias.

Las encuestas son anónimas y evalúan tanto el tema como la exposición, la claridad del profesor para hacer llegar sus ideas y conocimientos, la previsión que el profesor ha tenido para poder contar con el adecuado soporte teórico y la capacidad de generar interés en la materia.

La evaluación del desempeño docente es interna por medio de talleres en las que se utiliza las encuestas de los alumnos.

Se llevará un archivo estadístico con las conclusiones de cada evaluación.

Se solicitarán informes a los docentes a cargo de las materias respecto de sus apreciaciones de la cursada. Asimismo, se realizarán consultas a especialistas externos en caso que la Comisión de la Maestría considere pertinente.

CARLOS ESTEBAN MAS VELEZ
Secretario General

Anexo 2
Reglamento específico

ARTICULO 1. La conducción de la Carrera de Especialización en Seguridad Informática estará a cargo de una Comisión de Especialización y Maestría conformada seis (6) miembros titulares y tres (3) suplentes. Cada Facultad designará dos miembros titulares y un suplente.
ARTICULO 2. La Comisión nombrará de sus integrantes el Director y los subdirectores que deberán pertenecer respectivamente a cada una de las Facultades que conforman la Carrera de Especialización.
ARTICULO 3 El cargo de Director será ejercido alternativamente por cada una de las Facultades que conforman la Carrera de Especialización.
ARTICULO 4. Los miembros de la Comisión de Especialización y Maestría, director y subdirectores deben ser profesores de las Facultades, reconocidos especialistas en el área. Todas las propuestas de designación deberán ser acompañadas de los "curriculum-vitae" respectivos.
ARTICULO 5. El período de designación de Director y de la Comisión es por dos años. En el caso de la Comisión y subdirectores puede ser prorrogable.
ARTICULO 6. El Director junto con los subdirectores asumirá la responsabilidad de organizar y coordinar el desarrollo de las actividades académicas del Programa.
ARTICULO 7. En caso de acefalía la Comisión seleccionara el nuevo director o subdirector entre los otros dos representantes de la Facultad respectiva
ARTICULO 8. En caso de ausencia temporal del director asumirá el subdirector de más edad.

DE LA SEDE

ARTICULO 9. La sede administrativa y académica de la Maestría y la Carrera será:

a) Durante los dos (2) primeros años ambas sedes estarán en la Facultad de Ciencias Económicas.
b) Para los dos (2) años subsiguientes, la localización de ambas sedes se sorteará entre las Facultades de Ingeniería y de Ciencias Exactas y Naturales.
c) El 5º y el 6º año le corresponderá a la Facultad que no haya sido sede en los años anteriores.
d) Luego se repetirá el ciclo en los años subsiguientes.

CARLOS ESTEBAN MAS VELEZ
Secretario General

ARTICULO 10. El remanente recaudado en concepto de aranceles por la Facultad sede académico administrativa previo descuento de los gastos en honorarios, insumos y gastos administrativos, será repartido en partes iguales entre las tres (3) Facultades organizadoras.

DE LA COMISIÓN DE ESPECIALIZACIÓN Y MAESTRÍA

ARTICULO 11. La Comisión de Especialización y Maestría estará compuesta por seis (6) titulares y tres (3) suplentes. A cada Facultad le corresponden dos titulares y un suplente, quienes serán designados por el Consejo Directivo respectivo.
ARTICULO 12. Serán funciones de la Comisión de Especialización y Maestría:

a) Seleccionar los profesores y tutores.
b) Definir los requisitos previos para el ingreso de los aspirantes.
c) Estudiar los antecedentes de los aspirantes.
d) Proponer al Consejo Directivo de la Facultad sede de la Maestría la aceptación o rechazo, con dictamen fundado, de los aspirantes de la Carrera de Especialización.
e) En caso de ser rechazado el aspirante podrá presentarse nuevamente no antes de UN (1) año a partir de su solicitud anterior.
f) Proponer al Consejo Directivo correspondiente el Consejero de Estudios que servirá de enlace entre el alumno y la Comisión de Especialización y Maestría. El Consejero de Estudios deberá ser elegido entre los profesores de las tres (3) Facultades. El Consejero debe ser de una de las tres (3) Unidades Académicas.
g) Supervisar con el Consejero de Estudios, el progreso de los estudiantes.
h) Definir el plazo máximo durante el cual el aspirante podrá completar su Carrera de Especialización.,
i) Evaluar periódicamente el nivel académico de los cursos, seminarios y programas específicos de la Carrera de Especialización.
j) Emitir opinión fundada sobre los programas analíticos de las diferentes actividades académicas.
k) Los aspectos relacionados con la metodología y evaluación de las actividades de enseñanza y aprendizaje
l) Aprobar informes periódicos y la memoria anual de la Carrera de Especialización que presenta el Director.
m) Determinar los cursos previos de nivelación, que deberán cursar y aprobar los aspirantes de la Carrera de Especialización, y las unidades académicas en las que deberán cumplimentar dichos cursos, en aquellos casos en que los aspirantes no cumplan con los requisitos de la Carrera de Especialización.

CARLOS ESTEBAN MAS VÉLEZ
Secretario Gener

n) Proponer al Consejo Directivo de la Facultad sede de la Carrera de Especialización la aprobación por equivalencia las materias de posgrado que los estudiantes cursen fuera de la Carrera de Especialización. En ningún caso el total de cursos aprobados por equivalencia debe superar el 30% de las materias de la Carrera de Especialización.

ARTICULO 13. El desarrollo de las distintas actividades académicas y el seguimiento y evaluación del funcionamiento de la Carrera de Especialización será llevada a cabo en reuniones mensuales de la Comisión, donde participarán también el Director y los Subdirectores.

DEL DIRECTOR DE LA CARRERA DE ESPECIALIZACIÓN

ARTICULO 14. Serán funciones del Director de la Carrera de Especialización:

a) Elaboración de informes periódicos y la memoria anual de la Carrera de Especialización.
b) Supervisar el Libro de actas de examen
c) Refrendar las actas de examen conjuntamente con el profesor responsable
d) Resolver problemas de sustitución temporal de docentes

DEL CONSEJERO DE ESTUDIOS

ARTICULO 15. Serán funciones del Consejero de Estudios:

a) Asesorar y orientar al cursante de la Carrera de Especialización en el plan de actividades anuales, que deberá incluir los distintos tipos de actividades señaladas en el programa, y otras tales como eventos científicos, extensión universitaria, etc.
b) Supervisar y evaluar el plan periódicamente
c) Supervisar el cumplimiento de la reglamentación vigente por parte del alumno.

CARLOS ESTEBAN MAS VELEZ
Secretario General

I. INSERCIÓN INSTITUCIONAL DEL POSGRADO

Denominación del posgrado
Maestría en Seguridad Informática

Denominación del Título que otorga
Magister de la Universidad de Buenos Aires en Seguridad Informática

Unidades Académicas de las que depende el posgrado
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería.

Sede/s de desarrollo de las actividades académicas del posgrado
Facultad de Ciencias Económicas, Facultad de Ciencias Exactas y Naturales, Facultad de Ingeniería.

Resoluciones de CD de la/s Unidad/es Académica/s de aprobación del proyecto de posgrado:
El proyecto de posgrado fue aprobado por Resolución (CD) Nº / , Facultad de Ciencias Económicas, por Resolución (CD) Nº / , Facultad de Ciencias Exactas y Naturales, por Resolución (CD) Nº / , Facultad de Ingeniería.

II. FUNDAMENTACIÓN DEL POSGRADO

A) ANTECEDENTES

a) Razones que determinan la necesidad de creación del proyecto de posgrado:

El uso masivo de las TIC (tecnologías de la información y comunicaciones) como medios para generar, almacenar, transferir y procesar información se ha incrementado espectacularmente en los últimos años, y es un elemento indispensable para el funcionamiento de la sociedad actual. La información en todas sus formas y estados se ha convertido en un activo estratégico, al cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad.

La sociedad ha adquirido una gran dependencia respecto del manejo apropiado de la información. Las aplicaciones informáticas son cada vez más importantes, los requerimientos de seguridad son cada vez mayores y esenciales en la operatoria de las organizaciones modernas.

Un componente fundamental en toda clase de actividades es la información. Los recursos informáticos se encuentran permanentemente sujetos a distintas situaciones de riesgo. Múltiples personas en diferentes lugares del mundo, se especializan en realizar toda clase de ataques a la seguridad, para lo cual muchas de las organizaciones no están adecuadamente preparadas.

Asegurar la información de una organización requiere instalar una cultura de seguridad e implementar una adecuada combinación de conceptos, tecnologías, metodologías, estándares, herramientas de gestión y recursos humanos capacitados.

Un profesional en Seguridad Informática debe saber aplicar adecuadamente elementos tecnológicos como técnicas biométricas, técnicas criptográficas, modelos formales de seguridad, arquitectura del computador, sistemas operativos y redes, informática forense, como así también, habilidades y herramientas gerenciales de planeamiento, de continuidad de las operaciones, manejo de incidentes, recursos humanos, auditoria, seguridad física e incluso la adecuada comprensión de los aspectos legales nacionales e internacionales.

Uno de los mayores retos de las organizaciones es garantizar la seguridad de los recursos informáticos y de las personas. Actualmente existen en el mercado regulaciones específicas que imponen entidades de contralor, bancos centrales, bolsas de valores y otros organismos. Estas regulaciones implican que las organizaciones deben respetar normas impuestas, ponerlas en práctica y demostrar que cumplen con las mismas.

La gestión del riesgo es un elemento fundamental en el logro de los propósitos y objetivos de las organizaciones. La explosiva evolución de la tecnología ha creado nuevos factores de riesgo que son prácticamente desconocidos por los niveles de conducción.

En tales circunstancias, se hace evidente la necesidad de participar académicamente en la formación de los recursos humanos para que adquieran la capacidad de asistir a la conducción a conocer en detalle los riesgos, sus características, el efecto en las operaciones y, lo más importante, las formas de afrontarlo y, en lo posible, mitigarlos y/o neutralizarlos.

La gestión de los riesgos informáticos constituye una necesidad ineludible para cualquier organización que quiera administrar y utilizar su información de manera confiable, segura y funcional para el logro de sus objetivos.

Los recursos humanos especializados en Seguridad Informática en nuestro país son escasos y las carreras de grado no contemplan en sus planes de estudio un enfoque integral para solucionar las crecientes necesidades en esta área. Dado este escenario la Maestría en Seguridad Informática es una nueva opción académica que representa el esfuerzo de un grupo de especialistas de la UBA por ofrecer capacitación de alto nivel.

La Maestría es el espacio ideal de convergencia de experiencias, tecnologías y metodologías, en donde los estudiantes puedan prepararse para enfrentar el reto de seguridad que significa vivir en un mundo globalmente interconectado.

Estamos transcurriendo el sexto año de la Maestría. La carrera ha sido acreditada ante la CONEAU (Resolución No. 847/11) y como testimonio del prestigio académico logrado en los años transcurridos, se nos acreditaron premios y distinciones. Así es que en el año 2011 se nos fue otorgado el Premio Sadosky a la INNOVACIÓN EDUCATIVA dentro de la temática RECURSOS HUMANOS en competencia con muchos otros proyectos a nivel nacional. Asimismo, nuestra Maestría ha sido incorporada a la nómina recomendada por varias instituciones que califican la oferta mundial de capacitación. En el año 2012 el ranking de la Eduniversal Evaluation Systems nos ubica entre los “Top 50 Master Programs in the World”.

La experiencia acumulada en estos años ha aportado un aprendizaje en el dictado de los contenidos originalmente propuestos que sugieren una actualización.

Esta Maestría, además de un sólido marco teórico, busca ofrecer a los estudiantes escenarios con casos reales sobre el tema de la seguridad informática y los riesgos a los que se está expuesto, que busquen construir un contexto de aprendizaje práctico alrededor de la vulnerabilidad intrínseca de los sistemas. Se procura establecer un marco de gestión adecuado y coherente de la información crítica de la organización.

Los profesionales en informática deben repensar los conceptos tradicionales en el área de seguridad, para procurar mayores y mejores niveles de aseguramiento de la información.

b) Antecedentes en instituciones nacionales y/o extranjeras de ofertas similares:

A nivel nacional existen en la actualidad dos ofertas que apuntan a objetivos similares pero no con el mismo contenido. Ellas son:

- Posgrado de Especialización en Criptografía y Seguridad Teleinformática en el Instituto Universitario del Ejército – IUE
- Posgrado en Seguridad de la Información en la Universidad del Salvador

Se ha tomado en cuenta, además, el Currículo de Seguridad de la Información presentado en el Congreso Segurinfo 2007 organizado por USUARIA.

A nivel internacional se han evaluado programas de posgrado en diversas universidades de los EE.UU., Europa y Latinoamérica. Finalmente se trabajó sobre varios programas de las universidades de los Estados Unidos por ser los más adelantados en la materia. Los programas más calificados y tomados en cuenta por este grupo de trabajo han sido los siguientes:

- University of Purdue, Indiana, EE.UU.; Cerias (The Center for Education and Research in Information Assurance and Security).
- Norwich University Vermont EE.UU.; Infosec Graduate Program, Master in Science in Information Assurance.
- Kennesaw State University; Georgia, EE.UU. Center for Information Security Education, que ha sido nominado como el National Center of Academic Excellence in Information Assurance Education por la National Security Agency

c) Comparación con otras ofertas existentes en la Universidad: establecer similitudes, diferencias y posibilidades de articulación

No existe en la Universidad de Buenos Aires una oferta comparable con la que contiene esta presentación.

d) Consultas a las que fue sometido el proyecto de posgrado, indicando personas e instituciones (adjuntar documentación pertinente)

Se han realizado numerosas reuniones con la activa participación de los siguientes docentes:

Facultad de Ciencias Económicas:

- Raúl Saroka; Ricardo Rivas; Leopoldo Cansler

Facultad de Ciencias Exactas y Naturales:

- Hugo Scolnik; Graciela Pataro; Rodolfo Baader

Facultad de Ingeniería:

- Alberto Dams; Hugo Pagola; Luis Marrone

Además, se ha consultado a los siguientes expertos del ámbito profesional:

- Juan Pedro Hecht, Julio Ardita, Edgardo Marcelo Ohman,Pablo Kaufer Barbe, Adrián Amigo.

e) Convenios con instituciones

No existen convenios específicos con el posgrado por el momento. La Universidad de Buenos Aires tiene convenios generales de intercambio con otras universidades y cada una de las tres facultades tiene también convenios de intercambio.

B) JUSTIFICACIÓN DE LA MAESTRÍA EN SEGURIDAD INFORMÁTICA.

De acuerdo con el artículo 1º de la Resolución (CS) Nº 5284/12, la Maestría será de tipo Profesional ya que, se vincula específicamente con el fortalecimiento y consolidación de competencias propias de una profesión o un campo de aplicación profesional. A lo largo de su proceso de formación profundiza en competencias vinculadas con marcos teóricos disciplinares o multidisciplinares que amplían y cualifican las capacidades de desempeño que apunte a formar profesionales capaces de participar tanto de la fase de instrumentación como de diseño y decisión.

Este posgrado tiene amplia justificación dentro del siguiente marco de referencia:

- Complejidad del contexto actual de las actividades públicas y privadas
- Universalización de la utilización de las tecnologías informáticas en las organizaciones públicas y privadas.
- Impacto de las TIC en la gestión de las organizaciones.
- Incremento notorio de los problemas de seguridad en materia de la gestión de la información.
- Crecimiento de las formas de delitos mediante el uso de la tecnología.
- Existencia de entes, disposiciones, estándares que exigen a las organizaciones el cumplimiento de normas de seguridad y la generación de responsabilidad emergente para quienes conducen esas organizaciones.
- La escasa oferta en la Republica Argentina de formación universitaria en materia de Seguridad Informática.
- La necesidad de proveer una oferta académica de alto nivel para capacitar a profesionales desde una perspectiva tecnológica, legal, ética y psicosocial.
- La necesidad de mejorar la formación universitaria de los profesionales que buscan dedicarse a la especialidad de la Seguridad Informática.
- La importancia que adquiere la protección de los activos informáticos de las organizaciones y personas, y la información acerca de los individuos.

III OBJETIVOS DEL POSGRADO

- Preparar recursos humanos capacitados en todos los ámbitos relacionados con la Seguridad Informática.
- Generar la capacitación de recursos humanos de excelencia para la docencia de grado y posgrado.
- Promover el desarrollo de la investigación en materia de Seguridad Informática, a partir de la adquisición de rigurosidad científica para el análisis e interpretación del campo disciplinario.

- Crear conciencia de la importancia y los alcances que esta área de conocimiento tiene actualmente en prácticamente todas las actividades de la sociedad, impulsando y fomentando una cultura de Seguridad Informática.
- Formar egresados en los diferentes temas de Seguridad Informática capaces de aplicar sus conocimientos a la sociedad.
- Incorporar el conocimiento de las normas nacionales e internacionales que regulan el área de la Seguridad Informática.
- Adaptar, desarrollar y divulgar por medio de nuestros egresados las mejores prácticas y tendencias internacionales en temas relacionados con Seguridad Informática.
- Formar egresados éticos capaces de generar, aplicar y transmitir los conocimientos adquiridos.

IV PERFIL DEL EGRESADO

El egresado de la Maestría en Seguridad Informática será un profesional con aptitud para promover y aplicar metodologías actualizadas que conduzcan a la práctica de la Seguridad Informática, capaz de discernir entre las ventajas y desventajas asociadas con el diseño y gestión de políticas de seguridad, y de diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos, basado en estándares nacionales e internacionales y aspectos éticos-legales.

Competencias esperadas del egresado de la Maestría en Seguridad Informática:

- Definir e instrumentar un plan integral de Seguridad Informática de la organización.
- Definir estrategias y políticas de Seguridad Informática.
- Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)
- Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.
- Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.
- Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico.
- Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones.
- Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.
- Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática.
- Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas.
- Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática.
- Ejercer la docencia en materia de Seguridad Informática.

V ORGANIZACIÓN DEL POSGRADO

a) INSTITUCIONAL: REGLAMENTO DEL PROYECTO DE POSGRADO.

La Maestría en Seguridad Informática es una Maestría Profesional, estructurada, con una oferta única y común para todos los estudiantes, desarrollada bajo modalidad presencial.

Las actividades programadas dentro del proceso formativo de carácter único podrán desarrollarse en las instalaciones de una o más de las facultades intervinientes.

1. Modalidad de designación de las autoridades del posgrado y funciones.

La carrera de Maestría será dirigida por un Director y dos Subdirectores, y una Comisión de Maestría. El Director y los Subdirectores integran la Comisión de Maestría. La Comisión de Maestría será la encargada de asesorar y colaborar con la gestión de la carrera.
La carrera cuenta también con un Coordinador que es nombrado por el Decano de la Facultad Sede a propuesta de la Comisión de Maestría.

En todos los casos quienes desempeñen esos roles deberán contar con formación de posgrado equivalente o superior a la ofrecida por el posgrado y acorde con los objetivos de éste o, si el caso lo amerita, mérito equivalente demostrado por sus trayectoria académica y/o profesional.

La modalidad de designación de las autoridades y sus funciones figuran en el Reglamento que forma parte del presente.

2. Modalidad de selección y designación de profesores

Podrán ser docentes aquellos que sean profesores de universidades argentinas o extranjeras y/o en su caso expertos de reconocido prestigio en la temática. En todos los casos deberán contar con formación de posgrado equivalente a la ofrecida por la carrera o superior y acorde con los objetivos de ésta o, si el caso lo amerita, una formación equivalente demostrada por sus trayectorias académica y/o profesional y cumplan con los requisitos establecidos en res CS 5918/12.

b) ACADÉMICA: PLAN DE ESTUDIOS. CONTENIDOS MÍNIMOS.

La experiencia acumulada en estos años ha aportado un aprendizaje en el dictado de los contenidos originalmente propuestos que sugieren una actualización de los contenidos curriculares expresado en incorporación de tres nuevas asignaturas, el ajuste de las horas teóricas y de práctica de varias de las materias, el reordenamiento de la secuencia de dictado en algunos casos y cambios de designación de otras asignaturas.

1. Modificación en el orden del dictado de las asignaturas respecto a la organización original:

    a. Se traslada la asignatura Gestión Estratégica de la Seguridad I del segundo cuatrimestre al primero.

b. Se traslada la asignatura Seguridad en Sistemas Operativos y Aplicaciones del primer al segundo cuatrimestre.
c. Se traslada la asignatura Documentación y Proyectos de Seguridad del primer al segundo cuatrimestre.

2. Modificación de la denominación:

   a. del Seminario I a Taller de Trabajo Final de Maestría
   b. del Seminario II a Taller de Trabajo Final de Maestría

3. Modificación de la cantidad de horas (teóricas y prácticas) asignadas a algunas de las asignaturas de acuerdo al siguiente detalle:

a.	Ejes Temáticos de la Seguridad	de 32 a 48 horas
b.	Criptografía I	de 64 a 48 horas
c.	Seguridad en Redes I	de 64 a 48 horas
d.	Gestión Estratégica de la Seguridad I	de 64 a 48 horas
e.	Seguridad en Sistemas Op. y Aplicaciones	de 64 a 48 horas
f.	Documentación y Proyectos de Seguridad	de 16 a 32 horas
g.	Comportamiento Organizacional	de 32 a 24 horas
h.	Criptografía II	de 64 a 48 horas
i.	Informática Forense y Delitos Informáticos	de 32 a 48 horas
j.	Taller de Trabajo Final de Maestría	de 160 a 144 horas

4. No se realizan modificación de horas en las restantes asignaturas

5. Se incorpora en el dictado del primer año la siguiente asignatura:

   a. Taller de Trabajo Final de Integración con 24 horas (segundo cuatrimestre)

6. Se incorporan en el dictado del segundo año las siguientes asignaturas:

   a. Seguridad Física con 16 horas (primer cuatrimestre)
   b. Taller de Desarrollo de Competencias Gerenciales con 16 horas (segundo cuatrimestre)

7. Cambios de correlatividades de acuerdo al cuadro que se expone más abajo.

8. El total de horas del primer año se reduce de 400 a 384 horas.

9. El total de horas de la Maestría se mantiene en 752 horas.

Por lo tanto, el nuevo cuadro de asignaturas queda como sigue:

CUADRO GENERAL DE ASIGNATURAS

Primer Año

Primer cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Ejes Temáticos de la Seguridad	48	-	48	-
Criptografía I	32	16	48	-
Seguridad en Redes I	32	16	48	-

Gestión Estratégica de la Seguridad I	32	16	48	-

Segundo cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Documentación y Proyectos de Seguridad	16	16	32	Gestión Estratégica de la Seguridad I
Seguridad en Sistemas Operativos y Aplicaciones	32	16	48	Ejes Temáticos de la Seguridad
Comportamiento Organizacional	16	8	24	Gestión Estratégica de la Seguridad I
Seguridad en Redes II	16	16	32	Seguridad en Redes I Criptografía I
Marco Legal, Ética y Privacidad	32	-	32	Gestión Estratégica de la Seguridad I
Taller de Trabajo Final de Integración	16	8	24	-
Total Horas Primer Año	**272**	**112**	**384**	-

Segundo Año

Primer cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Seguridad Física	12	4	16	Seguridad en Sistemas Operativos y Aplicaciones
Gestión Estratégica de la Seguridad II	16	16	32	Documentación y Proyectos de Seguridad / Marco Legal, Ética y Privacidad
Criptografía II	32	16	48	Criptografía I / Seguridad en Redes II
Taller de Trabajo Final de Maestría	32	32	64	Aprobación de todas las asignaturas del primer año

Segundo cuatrimestre

Asignatura	Carga horaria			Correlatividades
	Teórica	Práctica	Total	
Auditoria	48	16	64	Gestión Estratégica de la Seguridad II
Informática forense y delitos informáticos	32	16	48	Criptografía II
Taller de Desempeño de. Competencias. Gerenciales.		16	16	Comportamiento Organizacional
Taller de Trabajo Final de Maestría	32	48	80	Propuesta de TF aceptada
Total horas segundo año	**204**	**164**	**368**	-
Carga Horaria Total del Plan de Estudios	**476**	**276**	**752**	-

La propuesta de enseñanza y aprendizaje se estructura en torno al:
- Desarrollo de los aspectos centrales de cada tema mediante exposición, discusión y uso de variadas técnicas que promuevan la apropiación de conocimientos. - Trabajos por proyectos, análisis de casos y resolución de situaciones problemáticas.
- Trabajos de campo.
- Talleres.

CONTENIDOS MÍNIMOS

Ejes temáticos de la seguridad

Hoja de ruta de la maestría. Concepto de seguridad. Servicios básicos de seguridad. Elementos a proteger. Amenazas, riesgos, vulnerabilidades. El factor humano. Revisión de los conocimientos necesarios de matemática discreta sobre los cuales se desarrolla la criptografía contemporánea. Revisión y actualización de los conocimientos necesarios de tecnología de la información: bases de datos; sistemas operativos, redes. Revisión y actualización de los conocimientos necesarios de gestión de las organizaciones: conceptos, técnicas y herramientas. Aspectos éticos y legales. Auditoría y análisis forense.

Criptografía I

Fundamentos de criptología. Introducción a los criptosistemas. Criptología clásica: cifrados y ataques. Secreto perfecto y One-Time Pad. Criptosistemas simétricos: históricos y actuales; modos operativos. Criptosistemas asimétricos; comparaciones de seguridad entre cifradores simétricos y de clave pública. Gestión de claves simétricas y asimétricas. Intercambio seguro de claves. Funciones Hash/ MAC/HMAC. Generación de números aleatorios. Ataques. Protocolos especiales.

Seguridad en redes I

Esquemas de seguridad: distribución de claves simétricas. Administración de claves publicas: autoridad certificante y certificados. Administración de claves de sesión compartidas. Seguridad de redes e Internet: Single Sign On, Infraestructura de Clave Publica PKI. Seguridad de WWW; comercio electrónico, gateways de pago, protocolo SET “Secure Electronic Transaction”; seguridad en IP IPSec: Firewalls, SSL. Seguridad en organizaciones: Firma Digital, Factura Electrónica; administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades.

Gestión estratégica de la seguridad I

Organización y estructura del área de seguridad: áreas, funciones y responsabilidades, perfiles, criterios de organización. Técnicas de gestión (estrategia, finanzas, marketing y recursos humanos). Ciclo de vida de los sistemas de seguridad. Gestión de proyectos de seguridad. Tercerización de servicios y gestión de proveedores. Evaluación económica de la seguridad. Métricas y performance. Estrategias, políticas, programas y normas de seguridad. Introducción al análisis y gestión del riesgo.

Documentación y proyectos de seguridad

Formulación y seguimiento de un proyecto de seguridad en base a un caso de estudio incluyendo el ciclo de vida de los sistemas de seguridad; fase inicial, fase de desarrollo y adquisición, fase de implementación, fase de operación y mantenimiento, fase de disposición.

Seguridad en sistemas operativos y aplicaciones

Instalación y operación segura del sistema operativo. Ciclo de vida del desarrollo de sistemas. Desarrollo y gestión de bases de datos. Controles de los sistemas. Control en la operación y el mantenimiento de las aplicaciones. Aplicaciones distribuidas. Ataques y vulnerabilidades en aplicaciones y sistemas. Buffer Overflows, Format Strings, Race Conditions. Entornos protegidos (sandboxes, chroot). Mecanismos de protección: técnica del canario, segmento no ejecutable. Análisis de logs. HostIDS. Vulnerabilidades en web. Códigos maliciosos.

Comportamiento organizacional

Cultura organizacional. Clima organizacional. Comportamiento individual, grupal y organizacional. Dinámica de grupos. Valores y actitudes. Comunicación interpersonal. Motivación. Liderazgo. Trabajo en equipo. Resolución de conflictos. Negociación. Gestión del cambio organizacional. Inteligencias múltiples. El proceso de aprendizaje. Toma de decisiones individuales y grupales.

Seguridad en redes II

Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, Intrusión Detection Systems Honeypots; análisis de vulnerabilidades, pruebas de penetración. Desarrollo seguro. Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de control. Ubicación de Firewalls, IDS.

Marco legal, ética y privacidad

Introducción al Derecho Informático, conceptos y terminología legal. Sistemas legales en Argentina y otros países. Régimen jurídico de protección de la Propiedad Intelectual. Régimen de Firma Digital. Ética y privacidad. Visión jurídica de los delitos informáticos. Derecho Internacional: legislación transfrontera. Jurisprudencia.

Taller de Trabajo Final de Integración

Tipos de trabajo final (TF). Disposiciones individuales para el desarrollo del TF. Plan de trabajo para el desarrollo del TF. Criterios genéricos y normativos. Consideraciones acerca del plagio. Criterios de estilo de redacción y de citas académicas. Prácticas de redacción. Fuentes de información: búsqueda y selección. Reseñas bibliográficas. Tutorías grupales e individuales.

Seguridad física

Administración y relevamiento de los riesgos. Planeamiento y gerenciamiento de la Seguridad Física. La tecnología y el diseño de procesos de trabajo. Aplicación de diseños. Sistemas de seguridad física.

Gestión estratégica de la seguridad II

Análisis y gestión del riesgo, modelo de valor, mapa de riesgos, evaluación de salvaguardas, informe de insuficiencias, catálogo de elementos, estado de riesgo. Ciclo de vida: análisis y gestión, planificación, implementación de salvaguardas, gestión de configuración y cambios. Relación y complementariedad entre los distintos estándares y/ modelos (frameworks), cumplimiento (compliance), regímenes e instituciones Internacionales y Nacionales: Cobit, Coso, BSI, ISO, ITIL, Basilea II, CMM, SOX, otros.

Criptografía II

Teoría de la información: entropía de Shannon. Entropía condicional. Transinformación. Distancia de unicidad. Algebra abstracta y sus aplicaciones criptográficas. Logaritmo discreto y ataques vinculados. Criptosistema ElGamal y ElGamal generalizado. Campos finitos GF(2^n) en criptosistemas simétricos (AES) y asimétricos (ElGamal). Máquinas de Turing y teoría de la complejidad computacional aplicadas a la criptología. Problemas complejos en campos numéricos. Algebra no conmutativa y aplicaciones criptográficas (GDH-Intercambio Diffie-Hellman generalizado y ZKP-Prueba de conocimiento cero). Curvas elípticas e hiperelípticas. Códigos lineales, problema de la mochila y otros. Ataque de criptoanálisis diferencial a

las redes Feistel. Ataques de colisiones diferenciales a las funciones Hash. Estándar SHA3. Secretos compartidos y protocolos especiales (undeniable signatures, oblivious transfer, electronic cash) Secreto compartido. Elementos de criptografía cuántica, computación cuántica, teoría de información cuántica y sus aplicaciones criptográficas.

Auditoría

Control y auditoría. Normas técnicas. Control y estructura organizativa. Separación de funciones y oposición de intereses. Análisis específico del área de Seguridad Informática. Controles en las entradas al sistema y sus almacenamientos. Transacciones rechazadas y observadas. Concepto de monitoreo. Planificación de las actividades de auditoria. Pruebas de cumplimiento. Evaluación de aplicación de políticas, planes, normas, procedimientos, esquemas, estándares y métricas. Pruebas y técnicas asociadas. Pistas de auditoria. Evaluación del nivel de respuesta ante incidentes. Test de penetración. Test de nivel de divulgación y comprensión de políticas, normas y procedimientos en la organización. Comprobaciones y simulaciones sobre planes de contingencia, continuidad de operaciones y recuperación.

Informática forense y delitos informáticos

Análisis forense: objetivos, principios. Evidencia digital. Metodología de trabajo para el análisis de los datos: identificación de la evidencia digital, preservación del material informático, análisis de datos, presentación del dictamen pericial. Registros temporales. MACtimes. Registros de redes y DNS. File systems con journaling. File System: File System Virtual (VFS). Aspectos internos del File System. Estructura de una partición. Recolección de información volátil y no volátil. Recolección de evidencia de red. Análisis de archivos binarios: análisis estático y análisis dinámico. Consideraciones legales: evidencia y evidencia admisible. Obtención de evidencias. Tipos de evidencia. Características para ser admisible en juicio. Preservación de la cadena de custodia. Informes Periciales.

Taller de Desarrollo de Competencias Gerenciales

Desarrollo de casos y situaciones que permitan adquirir práctica en los siguientes aspectos: comunicaciones interpersonales, negociación, toma de decisiones, trabajo en equipo, liderazgo, motivación y gestión del cambio.

Taller de Trabajo Final de Maestría

Organización de Trabajos Finales de Maestría con orientación académica y con orientación profesional. Importancia del aporte personal y originalidad de los objetivos perseguidos. Desarrollo de un Plan de Trabajo de Maestría. Selección de potenciales Directores de Trabajo Final de Maestría. Estructura de los capítulos y contenidos a incluir en los mismos. Prácticas de redacción. Selección de las fuentes bibliográficas. Referencias y Plagio. Declaración Jurada de origen de los contenidos. Plazos reglamentarios para la presentación de Planes de Trabajo Final de Maestría y del propio Trabajo Final. El proceso de habilitación para la defensa. La defensa del Trabajo Final de Maestría.

VI. ESTUDIANTES

a) Requisitos de admisión:

Podrán ingresar a la Maestría los postulantes que cumplan con los siguientes requisitos:

a) Los graduados de la Universidad de Buenos Aires con título de grado correspondiente a una carrera de CUATRO (4) años de duración como mínimo, de las carreras que se dictan en la Facultad de Ciencias Económicas, Facultad de Ciencias Exactas y Naturales y Facultad de Ingeniería, o
b) Los graduados de otras universidades argentinas con título de grado correspondiente a una carrera de CUATRO (4) años de duración como mínimo, con títulos afines a los señalados en a), o
c) Los graduados de universidades extranjeras que hayan completado, al menos, un plan de estudios de DOS MIL SEISCIENTAS (2.600) horas reloj o hasta una formación equivalente a master de nivel I, de carreras equivalentes en duración y temáticas a las indicadas, o
d) Los egresados de estudios de nivel superior no universitario vinculados a las áreas temáticas de la carrera, de CUATRO (4) años de duración o DOS MIL SEISCIENTAS (2.600) horas reloj como mínimo, serán evaluados individualmente y la Comisión de Maestría establecerá los requisitos previos que correspondan en cada caso, a fin de asegurar que su formación resulte compatible con las exigencias del posgrado al que aspiran.
e) aquellas personas que cuenten con antecedentes de investigación o profesionales relevantes, aun cuando no cumplan con los requisitos reglamentarios citados, podrán ser admitidos excepcionalmente para ingresar a la Maestría con la recomendación de la Comisión de Maestría y con la aprobación del Consejo Directivo de la Unidad Académica Sede de la Maestría o del Consejo Superior.

Además, el postulante deberá superar el proceso de selección que implica:

- Antecedentes: acreditar la posesión de antecedentes académicos y profesionales suficientes a criterio de la Universidad, que guarden relación con el área disciplinaria objeto de estudio de la Maestría.
- Examen de admisión: aprobar un examen de admisión donde se evalúan las aptitudes y capacidad lógica, como así también conocimientos de informática y redes.
- Idioma: se exige dominio de la lectura en idioma inglés técnico. El postulante deberá acreditar ante el Director o quien el designe dicha aptitud o aprobar un examen de comprensión de textos. Se confeccionará un acta consignando la aprobación firmada por el Director.
- Cartas de recomendación: el aspirante debe presentar dos cartas de recomendación que avalen sus antecedentes académicos y profesionales.
- En la entrevista se evaluará el grado de motivación para el cual el postulante solicita su inscripción, compromiso con la finalización de la maestría, disponibilidad de tiempo, antecedentes y capacidad para abordarla íntegramente.

b) Criterios de selección:

- Dentro de los criterios de selección, primará la calidad del expediente académico y la experiencia profesional. Tendrán prioridad los estudios universitarios de carreras afines a las tres facultades.
- Se tendrá en cuenta la idoneidad de los estudios cursados y las carencias de formación, para establecer su trayectoria curricular, en caso de ser admitidos.
- Por orden de matrícula. Aquellos alumnos que cumpliendo los requisitos de acceso se matriculen entre los 35 primeros serán los que se acepten.

c) Vacantes requeridas para el funcionamiento del posgrado:

Para el funcionamiento de la Maestría se considerará un mínimo de 15 (quince) alumnos y un máximo de 35 (treinta y cinco).

d) Criterios de regularidad y permanencia:

La permanencia del alumno en la Maestría exige la asistencia del 75% de las clases, la realización de las actividades prácticas y la presentación y aprobación de los trabajos de las asignaturas en tiempo y forma.

- Los alumnos tienen la obligación de cursar todas las materias en la secuencia fijada por el plan de estudios.
- El sistema de calificaciones será el vigente para el conjunto de la UBA. De no alcanzarse el puntaje suficiente, el alumno podrá, por única vez, rendir una prueba recuperatoria y, en caso de que no volviese a aprobar, no podrá continuar cursando en forma regular la carrera. El alumno en esta situación, podrá solicitar su reincorporación al momento de iniciarse la siguiente cohorte, siendo decisión de la Comisión de Maestría, junto con la Secretaría de Posgrado, aceptar o rechazar tal solicitud en función de los méritos académicos del alumno.
- El plazo para terminar el posgrado luego de aprobar la última materia son veinticuatro (24) meses. Vencido dicho plazo las autoridades de la Maestría analizarán la situación y, si es necesario, definirán requisitos adicionales para proceder a la readmisión.
- El Trabajo Final de Integración se regirá según el Reglamento específico
- La Tesis o Trabajo Final de Maestría se regirá según el Reglamento especifico.
- La duración teórica a la Maestría es de dos años académicos. Los estudiantes tendrán un plazo máximo de 48 meses desde el ingreso a la carrera para graduarse y un plazo máximo de 24 meses de aprobada la última materia para presentar el Trabajo Final de Maestría.

e) Requisitos para la graduación

Para acceder al título de Magister de la Universidad de Buenos Aires en Seguridad Informática el aspirante deberá:

a) Aprobar las materias y otras actividades establecidas en el diseño curricular o fijado por la Comisión de Maestría que contribuyan a su formación integral y superior en las disciplinas involucradas.

b) Aprobar el Trabajo Final de Integración. Este trabajo de carácter integrador, será individual y consistirá en un análisis crítico de un tema de las materias del primer año y será expuesto para su aprobación ante un jurado.

c) Aprobar la Tesis o el Trabajo Final de Maestría. El maestrando realizará una defensa oral y pública del Trabajo presentado en la que deberá demostrar el dominio y aplicación de métodos científicos y de los conocimientos específicos del campo de la Seguridad Informática.

La Tesis o Trabajo Final de Maestría consistirá en la exposición de una problemática actualizada de un Área temática de Seguridad Informática, que incluya una elaboración del estado de la cuestión, la presentación de los datos empíricos si correspondiere y una exposición fundada de las conclusiones a las que hayan arribado. El mismo será individual y total o parcialmente escrito que podrá adquirir formato de proyecto, obra, estudios de casos, ensayo, informe de trabajo de campo u otras que permitan evidenciar la integración de aprendizajes realizados en el proceso formativo, la profundización de conocimientos en un campo profesional y el manejo de destrezas y perspectivas innovadoras en la profesión. La Tesis o Trabajo Final de Maestría se desarrollará bajo la dirección de un Director de trabajo final de Maestría.

VII.- INFRAESTRUCTURA Y EQUIPAMIENTO

Descripción detallada de las instalaciones y equipamientos necesarios para el desarrollo de las actividades académicas del posgrado: espacios físicos, laboratorios (si corresponde), equipamiento, biblioteca y centros de documentación, otros.

Dado que la Maestría se desarrollará en el ámbito de las tres facultades utilizara la infraestructura existente en cada una de ellas.

VIII.- MECANISMOS DE AUTOEVALUACION

La Maestría será evaluada periódicamente cada 5 (cinco) años por el Consejo Superior según lo dispuesto en la Resolución (CS). Nº 3415/88.

Se contempla el uso de un régimen de encuestas por tema y profesor, que se realizarán una vez terminados los módulos, y materias.

Las encuestas son anónimas y evalúan tanto el tema como la exposición, la claridad del profesor para hacer llegar sus ideas y conocimientos, la previsión que ha tenido para poder contar con el adecuado soporte teórico y la capacidad de generar interés en la materia.

La evaluación del desempeño docente es interna por medio de talleres en las que se utiliza las encuestas de los alumnos.

Se llevará un archivo estadístico con las conclusiones de cada evaluación.

Se solicitarán informes a los docentes a cargo de las materias respecto de sus apreciaciones de la cursada. Asimismo, se realizarán consultas a especialistas

externos en caso que la Comisión de la Maestría considere pertinente. Periódicamente se consultará a los graduados con encuestas que evalúen la pertinencia de los contenidos y las propuestas de cambios

ANEXO 1 - REGLAMENTO ESPECÍFICO

ARTICULO 1. La conducción de la Maestría en Seguridad Informática estará a cargo de una Comisión de Maestría conformada por seis miembros titulares y tres suplentes. Cada Facultad designara dos miembros titulares y un suplente. En todos los casos quienes desempeñen esos roles deberán contar con formación de posgrado equivalente o superior a la ofrecida por el posgrado y acorde con los objetivos de éste o, si el caso lo amerita, mérito equivalente demostrado por sus trayectoria académica y/o profesional.

ARTICULO 2. La Comisión nombrará de sus integrantes el Director y los Subdirectores que deberán pertenecer respectivamente a cada una de las Facultades que conforman la Maestría. Las designaciones serán ratificadas por el Consejo Directivo de la Facultad Sede.

ARTICULO 3. El cargo de Director será ejercido alternativamente por cada una de las Facultades que conforman la Maestría.

ARTICULO 4. Los miembros de la Comisión de Maestría, Director y Subdirectores deben ser profesores de las facultades participantes, reconocidos especialistas en el área. Todas las propuestas de designación deberán ser acompañadas de los curriculum-vitae respectivos. En todos los casos quienes desempeñen esos roles deberán contar con formación de posgrado equivalente o superior a la ofrecida por el posgrado y acorde con los objetivos de éste o, si el caso lo amerita, mérito equivalente demostrado por sus trayectoria académica y/o profesional.

ARTICULO 5. El período de designación de Director, Subdirectores y de la Comisión es por dos años y puede ser prorrogable.

ARTICULO 6. El Director junto con los Subdirectores asumirá la responsabilidad de organizar y coordinar el desarrollo de las actividades académicas del Programa.

ARTICULO 7. En caso de acefalia la Comisión seleccionará el nuevo director o subdirector entre los otros dos representantes de la facultad respectiva y comunicará al Consejo Directivo de la Facultad Sede.

ARTICULO 8. En caso de ausencia temporal del director asumirá el subdirector de más edad.

ARTICULO 9. La carrera cuenta también con un Coordinador que es nombrado por el Decano de la Facultad Sede a propuesta de la Comisión de Maestría. El periodo de designación es por un año y puede ser prorrogable.

DE LA SEDE

ARTICULO 10. La Sede de la Maestría será

a) La sede actual

b) Para los años subsiguientes la Comisión de Maestría resolverá anualmente la relocalización o no de la Facultad sede.

ARTICULO 11. El remanente recaudado en concepto de aranceles por la Facultad Sede previo descuento de los gastos en honorarios, insumos y gastos administrativos, será repartido en partes iguales entre las tres facultades organizadoras.

DE LA COMISIÓN DE MAESTRÍA

ARTICULO 12. La Comisión de Maestría estará compuesta por seis titulares y tres suplentes. A cada facultad le corresponden dos titulares y un suplente, quienes serán designados por el Consejo Directivo respectivo.

ARTICULO 13. Serán funciones de la Comisión de Maestría:
a) Seleccionar los profesores y tutores. La Comisión de Maestría analizará los antecedentes académicos y profesionales y realizará entrevistas con los candidatos quienes deberán presentar una propuesta para la actividad curricular a desarrollar. Elevará las propuestas de nombramiento al Consejo Directivo de la Facultad Sede.
b) Definir los requisitos previos para el ingreso de los aspirantes.
c) Estudiar los antecedentes de los aspirantes.
d) Proponer al Consejo Directivo de la Facultad Sede de la Maestría la aceptación o rechazo, con dictamen fundado, de los aspirantes de la Maestría. En caso de ser rechazado el aspirante podrá presentarse nuevamente no antes de UN (1) año a partir de su solicitud anterior.
e) Proponer al Consejo Directivo correspondiente la designación de un Director de Tesis o Trabajo Final de Maestría para cada maestrando.
f) Supervisar con el Director de Tesis o Trabajo Final de Maestría el progreso de los maestrandos.
g) Proponer al Consejo Directivo correspondiente en la designación del jurado que dictaminará sobre cada Tesis o Trabajo Final de Maestría que se presente
h) Definir el plazo máximo durante el cual el aspirante podrá completar su Maestría, incluida la defensa de su Tesis o Trabajo Final de Maestría en clase oral y pública. Dicho plazo no se podrá prolongar más cuatro años a contar desde la fecha de admisión.
i) Evaluar periódicamente el nivel académico de los cursos, seminarios y programas específicos de la Maestría.
j) Emitir opinión fundada sobre los programas analíticos de las diferentes actividades académicas.
k) Evaluar y emitir opinión sobre los aspectos relacionados con la metodología y evaluación de las actividades de enseñanza y aprendizaje.
l) Aprobar informes periódicos y la memoria anual de la Maestría que presenta el Director.
m) Determinar los cursos previos de nivelación, que deberán cursar y aprobar los aspirantes de la Maestría, y las unidades académicas en las que deberán cumplimentar dichos cursos, en aquellos casos en que los aspirantes no cumplan con los requisitos de la maestría.
n) Proponer al Consejo Directivo de la Facultad sede de la Maestría la aprobación por equivalencia las materias de posgrado que los estudiantes cursen fuera de la Maestría. En ningún caso el total de cursos aprobados por equivalencia debe superar el 30% de las materias de la Maestría.

ARTICULO 14. El desarrollo de las distintas actividades académicas y el seguimiento y evaluación del funcionamiento de la Maestría será llevada a cabo en reuniones mensuales de la Comisión de Maestría.

DEL DIRECTOR DE LA MAESTRIA

ARTICULO 15. Serán funciones del Director de la Maestría:
a) Elaboración de informes periódicos y la memoria anual de la Maestría.
b) Supervisar el Libro de actas de examen
c) Refrendar las actas de examen conjuntamente con el profesor responsable
d) Resolver problemas de sustitucion temporal de docentes
e) Proponer a la Comisión de Maestría candidatos a tutores y profesores de la Carrera
f) Elevar al Consejo Directivo de la Facultad Sede las propuestas de la Comisión de Maestría.
g) Presentar a la Comisión de Maestría las propuestas de informes periódicos y memoria anual de la Maestría.
Las funciones señaladas en los incisos b), c) y d) podrán ser ejercidas también por los Subdirectores.

DEL COORDINADOR ACADÉMICO

ARTICULO 16. Serán funciones del Coordinador Académico:

a) Asistir al Director, Subdirectores y Comisión de Maestría de la Carrera en el cumplimiento de sus funciones.
b) Hacer el seguimiento de la tarea de los docentes y desempeño de los cursantes de la Carrera.
c) Informar a los docentes sobre las normas y procedimientos a aplicar en el dictado de las asignaturas.
d) Informar a los cursantes de los derechos y obligaciones que les competen.
e) Atender el normal desarrollo de las actividades académicas de los alumnos y las cuestiones administrativas que de ellas deriven.
f) Confeccionar los informes académicos y administrativos de acuerdo con las pautas que elabore la Facultad Sede.
g) Confeccionar anualmente y mantener actualizado el cronograma de actividades de la carrera.
h) Asegurar que cada docente haya redactado el programa de la materia según los contenidos mínimos aprobados y teniendo en cuenta los siguientes capítulos:
    Encuadre general.
    Contenidos.
    Bibliografía.
    Métodos de desarrollo de la clase.
    Métodos de evaluación y escala de calificación.
    Pautas de regularidad.
    Cronograma del dictado de clases y de las actividades del curso.
i) Suministrar a la Comisión De Maestría los programas actualizados de las distintas materias que componen el posgrado. Dichos programas serán enviados a la Biblioteca de las Facultades que intervienen para integrar el acervo bibliográfico histórico y permanente.
j) Estar en contacto permanente con los responsables administrativos de la Facultad Sede.
k) Ocuparse de la difusión de toda la información pertinente a los docentes, cursantes y responsables administrativos de la facultad sede.
l) Participar en la elaboración de los programas anuales de admisión de interesados, incluyendo la elaboración de los exámenes de ingreso y todo lo concerniente a la circulación de información desde y hacia los candidatos.
m) Participar en las reuniones periódicas de difusión de la Carrera hacia los interesados que se presenten.

n) Participar en la elaboración de los Reglamentos internos de la Carrera.
o) Mantener informada a la Comisión de Maestría de aquellos aspectos o circunstancias que afecten su funcionamiento.
p) Organizar las reuniones periódicas de las defensas de los trabajos finales de integración de los cursantes y del destino final de la documentación generada.
q) Coordinar las reuniones periódicas de la Comisión de Maestría y llevar el registro de actas respectivo.
r) Llevar un archivo histórico digitalizado y actualizado de todos los documentos que se elaboren en el ámbito de la Carrera, incluyendo entre otros los antecedentes de los docentes y cursantes, registros de las calificaciones y los trabajos finales de integración, tanto los que estén en curso como los concluidos.
s) Toda otra actividad que le sea encomendada por la Comisión de Maestría en el ámbito de su competencia.

DEL DIRECTOR DE TESIS O TRABAJO FINAL DE MAESTRÍA Y PRESENTACION DE TRABAJO FINAL

ARTICULO 17. El Trabajo Final consistirá en la exposición de una problemática actualizada de un Área temática de Seguridad Informática, que incluya una elaboración del estado de la cuestión, la presentación de los datos empíricos si correspondiere y una exposición fundada de las conclusiones a las que hayan arribado. El mismo será individual y total o parcialmente escrito que podrá adquirir formato de proyecto, obra, estudios de casos, ensayo, informe de trabajo de campo u otras que permitan evidenciar la integración de aprendizajes realizados en el proceso formativo, la profundización de conocimientos en un campo profesional y el manejo de destrezas y perspectivas innovadoras en la profesión

ARTICULO 18. Dentro de los DIECIOCHO (18) meses posteriores a su ingreso, el maestrando propondrá su Director de Tesis o Trabajo Final de Maestría. Esa propuesta deberá contar con la conformidad de dicho Director. Cada Director podrá tener a su cargo un máximo de CINCO (5) trabajos finales simultáneamente.

ARTICULO 19. El Director de Tesis o Trabajo Final de Maestría deberá ser un profesional de sólida formación en el área correspondiente, de acreditada idoneidad y preferentemente con grado académico máximo. El maestrando, junto con la propuesta, deberá adjuntar un “curriculum-vitae” del Director.

ARTICULO 20. El Director de Tesis o Trabajo Final de Maestría será designado por el Consejo Directivo de la Facultad Sede a propuesta de la Comisión de Maestría.

ARTICULO 21. Serán funciones del Director de Tesis o Trabajo Final de Maestría:
a) Establecer las normas dentro de las cuales se desarrollará el trabajo, ajustándose a la normativa general.
b) Elaborar un Plan de Trabajo.
c) Atender y supervisar en forma sistemática el trabajo del maestrando.

ARTICULO 22. Dentro del año de su designación, el Director de Tesis o Trabajo Final de Maestría, juntamente con el maestrando, presentará el Plan para su consideración por la Comisión de Maestría. Dicho Plan debe contener:
a) El tema de investigación sobre el cual tratará el Trabajo Final de Maestría.
b) Lugar de trabajo.
c) Antecedentes existentes sobre el tema.
d) Naturaleza del aporte proyectado.

e) Campo de aplicación de los resultados.
f) Disponibilidad de la infraestructura necesaria y factibilidad de desarrollo del trabajo.
g) Plan de trabajo.

DEL JURADO DE TESIS O TRABAJO FINAL DE MAESTRÍA Y SU DICTAMEN

ARTICULO 23. Se constituirá un Jurado a propuesta de la Comisión Maestría y por designación del Consejo Directivo correspondiente. Dicho Jurado estará formado como mínimo por TRES (3) Profesores preferentemente con título académico máximo con reconocida capacidad en el tema o temas afines. Podrán designarse también hasta DOS (2) miembros suplentes. Podrán formar parte del Jurado, investigadores de reconocida autoridad en el tema, aunque no sean Profesores de las Unidades Académicas, debiendo al menos UNO (1) de éstos ser externo a esta Universidad. El Director de Tesis o Trabajo Final de Maestría no formará parte del Jurado. Los Miembros propuestos para el Jurado dispondrán de un plazo de CINCO (5) días hábiles a partir de recibida la comunicación de su designación para comunicar su aceptación. Los casos de recusación o impugnación a los miembros del Jurado designados se regirán por el Reglamento para la designación de Profesores Regulares.

ARTICULO 24. La designación del Jurado será propuesta dentro de los TREINTA (30) días de presentados los Trabajos de Tesis o Trabajo Final de Maestría a la Comisión de Maestría.

ARTICULO 25. La Comisión de Maestría remitirá al Jurado correspondiente los trabajos presentados por los maestrandos, y dicho Jurado tendrá un plazo no mayor de DOS (2) meses para su estudio, antes de ser convocado.

ARTICULO 26. Respecto a la Tesis o Trabajo Final de Maestría, el Jurado tomará la decisión por mayoría, pudiendo:
a) Aceptar con dictamen fundado.
b) Devolverlo. Dado este caso, el maestrando deberá modificarlo o completarlo para lo cual el Jurado fijará un plazo e informará a la Comisión de Maestría.
c) Rechazarlo con dictamen fundado.

ARTICULO 27. En caso de ser aceptado la Tesis o Trabajo Final de Maestría por el Jurado, el maestrando realizará su exposición en prueba oral y pública, la cual podrá resultar:
a) Aprobada, con dictamen fundado de mayoría y en caso excepcional aprobada con mención especial.
b) Rechazada con dictamen fundado de mayoría.

ARTICULO 28. Las decisiones de los Jurados de Maestrías serán inapelables. Todos los dictámenes deberán asentarse en el Libro de Actas habilitado a tal efecto.

ARTICULO 29. Cuando la Tesis o Trabajo Final de Maestría resulte aprobado, será entregada una copia en formato digital a las Bibliotecas de las tres Facultades, y se guardará en la sede de la Comisión de Maestría.

ARTICULO 30. En todos los casos cuando se menciona facultad correspondiente debe entenderse la facultad en que revista el profesor.

ARTICULO 31. Toda situación no contemplada en este Reglamento deberá ser presentada a la consideración de los Consejos Directivos de las tres Facultades, por la Comisión de Maestría.

ANEXO 2 - REGLAMENTO DEL TRABAJO FINAL DE INTEGRACION

Artículo 1º: De acuerdo a lo dispuesto por el Plan de Estudios de la Maestría en Seguridad Informática el Trabajo Final de Integración de la misma debe ser de carácter individual. El trabajo final de Integración consistirá en el desarrollo y la exposición de una problemática actualizada de un Área temática de Seguridad Informática o un caso práctico de aplicación de tecnología de seguridad informática, que incluya una elaboración del estado de la cuestión, la presentación de los datos empíricos si correspondiere y una exposición fundada de las conclusiones a las que hayan arribado.
El trabajo podrá adquirir el formato de proyecto, estudio de caso, obra o trabajos similares que permitan evidenciar la integración de aprendizajes realizados en el proceso formativo, la profundización de conocimientos en un campo profesional y el manejo de destrezas en la profesión. El Trabajo Final se desarrollará bajo la dirección de un Tutor de Trabajo Final de Integración y, si correspondiese en virtud de la temática, con un Codirector de Trabajo Final de Integración.

Artículo 2º: Para la presentación del Trabajo Final de Integración el estudiante deberá haber cursado y aprobado la totalidad de las asignaturas establecidas en el Plan de Estudios correspondiente al primer año.

Artículo 3º: Al 31 de Octubre de cada año el estudiante deberá tener presentada su Propuesta de Trabajo Final de Integración a la Comisión de Maestría, para su aprobación. Ésta procederá a su evaluación a fin de decidir sobre la aprobación de la propuesta, o, en su caso, la devolverá con observaciones para su revisión y corrección al presentante.

La Propuesta deberá constar de:

1. Resumen (con inclusión de palabras clave)
2. Fundamentación del tema elegido
3. Objetivos y alcance
4. Metodología y plan de actividades.
5. Bibliografía Inicial
6. Propuesta de tutor (con el consentimiento expreso de éste).

Una vez cumplido el punto previo, remitir en formato .pdf al Coordinador Académico a fin de ser considerado por la Comisión de Maestría

Artículo 4º: La Propuesta del Trabajo Final de Integración no debe exceder las cinco (5) páginas, incluyendo carátula, y anexos si correspondiere.

Artículo 5º: Modelo de portada de la Propuesta de Trabajo Final de Integración:

Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Propuesta de Trabajo Final de Integración

Tema
[Denominación del campo temático]

Título
Subtítulo [si corresponde]

Autor/a:
Tutor/a:
Co-tutor/a: [si corresponde]

Año de Presentación
Cohorte del Cursante

Artículo 6º: El plazo máximo para la entrega del Trabajo Final de Integración será de 18(dieciocho) meses, contados a partir de la fecha de aprobación de la última materia del primer año de la Carrera de Maestría. En caso de exceder este tiempo, el Cursante deberá iniciar el trámite de rematriculación al presentar el Trabajo Final como paso previo para llegar a ser considerado.

Artículo 7º: El Trabajo Final de Integración tendrá, como pauta general, una extensión de entre ocho mil (8.000) y diez mil (10.000) palabras, excluido los anexos o apéndices que no sean de propia elaboración.

Artículo 8º: La presentación del Trabajo Final de Integración se hará acorde a lo especificado en el Art. 19º.

Artículo 9º: Los requisitos formales que deberán observarse en la preparación del Trabajo Final de Integración serán los siguientes:

a. Papel: Únicamente papel color blanco únicamente. Tamaño A4 (21 x 29,7 cm).
b. Tipo de letra: Fuente estándar, estilo Arial, tamaño 12. Para las citas, o notas al pie de página, se empleará el tamaño 10. Deberá utilizarse el mismo estilo de fuente en todo el trabajo. No podrá hacerse uso de una fuente de tipo cursiva, excepto en los casos de: palabras extranjeras, términos científicos, título de libros, o cuando sea requerido especialmente por el tutor.
c. Espaciado: Se utilizará un interlineado de 1,5 espacios en todo el texto, salvo cuando sea a continuación de los títulos, donde deberá agregarse un interlineado simple más. En las notas a pie de página, el índice y las citas bibliográficas, se utilizará un interlineado simple.
d. Justificado: Se deberá utilizar el justificado total para todo el texto, notas a pie de página, bibliografía y referencias. En el cuerpo del texto se dejará una sangría de 1,25 cm en la primera línea de cada párrafo.
e. Márgenes: 2,5 cm para los márgenes superior, inferior y derecho; 4 cm para el margen izquierdo (incluye margen el necesario para encuadernación).
f. Impresión: En color negro. Sólo se podrá utilizar color en las figuras y los gráficos. No se podrán incluir correcciones manuales, cintas o líquidos correctores.
g. Numeración: Todas las páginas deberán numerarse en forma correlativa en su parte inferior derecha o central. La página número 1 corresponderá a la Introducción, mientras que las páginas anteriores a ésta podrán numerarse con números romanos en minúsculas. La portada no se numerará. Cada capítulo se

iniciará en una nueva página, conservando siempre la numeración correlativa. No se permitirá una numeración secundaria para los distintos capítulos y secciones.

h. Redacción: En castellano, salvo autorización explícita de la Comisión de Maestría en contrario. Se podrán incluir citas en otras lenguas, pero sólo en notas al pie. La traducción, en tal caso, deberá aparecer en el texto, o bien a continuación de las mismas notas.

i. Encuadernación: El trabajo se presentará prolijamente encuadernado. Podrá ser espiralado, en cuyo caso incluirá una tapa plástica transparente.

j. Acuerdo expreso del Tutor del Trabajo Final de Integración para proceder a su presentación.

k. Una vez cumplido el punto previo, remitir una copia en formato .pdf al Coordinador Académico de la Maestría para ser considerado por la Comisión.

Artículo 10º: La portada deberá contener la siguiente información, en este orden (ver Art. 12º):

a. Universidad de Buenos Aires
b. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería
c. Maestría en Seguridad Informática
d. Título del trabajo
e. Nombre del autor
f. Nombre del Tutor/a y del Co-tutor/a (si lo hubiere)
g. Fecha de presentación y cohorte a la cual pertenece el cursante

Artículo 11º: El orden de los contenidos será el siguiente:

a. Portada: ver Art. 12°

b. Declaración Jurada de origen de los contenidos: Se incluirá, con este título, y en una hoja por separado, el siguiente texto que tendrá el carácter de Declaración Jurada: “Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajo Final de Integración vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”. Al pié de la misma el autor debe firmar en forma manuscrita, en todos los ejemplares impresos entregados, aclarando a continuación sus Nombres y Apellidos y el número de documento personal que lo identifica. Los ejemplares electrónicos entregados incluirán la leyenda “FIRMADO” en lugar de la firma hológrafa.

c. Resumen: Deberá contener no más de doscientas (200) palabras. Incluirá, la descripción de la metodología utilizada y los resultados o conclusiones. Al final del resumen se agregarán como mínimo tres (3) palabras clave.

d. Índice o tabla de contenidos: Un índice completo con sus capítulos y secciones. Se recomienda en la versión digital que cada entrada del índice posea un link al capítulo o sección correspondiente.

e. Numeración de capítulos, secciones, tablas y figuras: Los capítulos y Subcapítulos o secciones deben estar numerados (1, 1.1, 1.2, 2, etc.). Las tablas y las ilustraciones pueden numerarse con la numeración consecutiva desde el comienzo hasta el final del trabajo (Tabla 1, Tabla 2, Tabla 3, etc.) o con numeración por capítulos (Tabla 1.1, 2.1, 3.1, etc.).

f. Prólogo: Podrá tener un prólogo o sección inicial de agradecimientos. No es obligatorio.

g. Nómina de abreviaturas: En caso de ser utilizadas y de no ser expresamente aclaradas en el texto del trabajo.

h. Cuerpo introductorio: En él se presentará brevemente el problema abordado, los objetivos y alcance del trabajo, su estructura, el enfoque que se le ha dado al estudio y la relevancia del trabajo.

i. Cuerpo principal: Deberá estar dividido en capítulos conforme al índice. Se deben desarrollar los objetivos en función del alcance definido en el cuerpo introductorio.

j. Conclusiones: Destacará su contribución específica al tema, no pudiendo ser la misma una mera síntesis de lo anteriormente expuesto. Dejará, además, constancia expresa de su opinión

k. Glosario: Lista de términos especializados utilizados, con el fin de homogeneizar la terminología utilizada en el trabajo.

l. Apéndices / Anexos: Podrán tener Apéndices o Anexos, esto es, secciones relativamente independientes de la obra, que ayuden a su mejor comprensión y permitan conocer los aspectos específicos que —por su longitud o su naturaleza— no resulte conveniente tratarlos dentro del cuerpo principal.

m. Bibliografía específica: Deberá estar dispuesta por orden alfabético o por orden de aparición en el cuerpo y contener todas las referencias hechas en el texto utilizando el sistema numérico, alfabético o combinación de ambos.

   Por ejemplo, para libros:

   [13] Censor Y. and Zenios S., Parallel Optimization Theory and Applications, Oxford University Press, New York, 1997

   Y para trabajos en revistas:

   [8] Bauschke H.H. and Borwein J.M., On projection algorithms for solving convex feasibility problems, SIAM Review, 38, (1996), pp.367-426.

   Para la información obtenida en Internet deberá indicarse la dirección (url) y la fecha precisa de su obtención, por ejemplo:

   [25] IBM creates learning, brain-like, synaptic CPU, http://www.extremetech.com/extreme/93060-ibm-creates-learning-brain-like-synaptic-cpu (consultada el 24/8/2011)

n. Bibliografía General: Se indicará, sin referenciar, aquella bibliografía de respaldo general utilizada como fuente de conocimiento para la elaboración del Trabajo Final presentado.

o. Índices específicos: (temáticos, técnicos, de ilustraciones, gráficos, siglas, etc.).

Se recuerda que esta estructura aquí indicada podrá adaptarse a criterio del autor en caso de trabajos de orientación profesional.

Artículo 12º: Modelo de portada del Trabajo Final de Integración:

Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Trabajo Final de Integración

Título
Subtítulo [si corresponde]

Autor/a:
Tutor/a:
Co-tutor/a: si corresponde

Año de presentación
Cohorte

Artículo 13º: Los Tutores del Trabajo Final de Integración serán docentes de cualquiera de las tres Facultades que integran esta Maestría o que participen en el dictado de alguna de las asignaturas de la Maestría en Seguridad Informática.

Artículo 14º: Entre las funciones de los Tutores del Trabajo Final de Integración están las de: asesorar y orientar al estudiante en la elaboración del Trabajo, supervisar el cumplimiento del Plan previsto por parte del estudiante y aprobar la versión final que será presentada por aquél. Asimismo y a requerimiento de la Comisión de Maestría, generará un breve informe final sobre la labor de su dirigido, destinado exclusivamente a los Jurados del Trabajo Final de Integración.

Artículo 15°: Cada Tutor podrá tener simultáneamente a su cargo hasta un máximo de cinco (5) estudiantes de cada cohorte.

Artículo 16º: El Director de la Maestría propondrá los integrantes para conformar el jurado que evaluará los Trabajos Finales de Integración y la elevará a la aprobación de la Comisión de Maestría.

Artículo 17º: Los Miembros propuestos para el Jurado dispondrán de un plazo de cinco (5) días hábiles, contados a partir de recibida la comunicación de su designación, para comunicar su aceptación. Estará formado por profesores de la Carrera o Maestría.

Artículo 18º: El Tribunal podrá - decidir:

1) la aprobación del Trabajo Final de Integración, y la calificación tal como fuera presentada, o

2) la devolución del mismo a los efectos de su corrección o

3) el rechazo del mismo y la sanción a su autor según lo estipulado en el Art. 23 y conexos.

Artículo 19°: El Director de la Carrera fijará la fecha y lugar de reunión del jurado para la exposición oral de los Trabajos Finales de Integración. La presentación final del trabajo se realizará en un acto público, en una exposición no mayor de 30 minutos sobre los aspectos fundamentales del trabajo. El cursante deberá concurrir con 4 (CUATRO) ejemplares impresos y firmados en su Declaración Jurada (Art. 11º b) y 3 (TRES) ejemplares impresos de la exposición de defensa, junto con un disco compacto con la versión digital de la exposición (en formatos Word y PDF). Las versiones impresas del Trabajo Final de Integración deben coincidir en un todo con la versión digital entregada.

Concluida la exposición, el aspirante procederá a contestar las preguntas que pudiere formular el jurado.

Artículo 20º: La calificación del Trabajo Final de Integración se hará según la escala de 0 a 10, requiriéndose un mínimo de cuatro (4) puntos para su aprobación. En caso de la obtención de diez (10) puntos, el Jurado podrá añadir la recomendación de publicación, la cual no implicará ningún compromiso por parte de la Universidad, sino sólo un reconocimiento académico.

Artículo 21º De la evaluación del Trabajo Final de Integración **y su exposición oral**

En la evaluación de los trabajos se considerarán los siguientes aspectos:

a) Pertinencia y vigencia en relación con los objetivos del estudio y de la revisión realizada de la literatura vinculada con dichos objetivos.

b) La claridad formal del lenguaje, la corrección gramatical y la coherencia del estilo.

c) Claridad expositiva en la presentación oral y nivel de conocimientos demostrados.

d) El contenido de las conclusiones del trabajo

Artículo 22º Citas de trabajo de terceros.

El documento no debe contener frases textuales de documentos de terceros sin estar citadas y referenciadas. La cita es obligatoria ya que permite distinguir el trabajo del alumno de las ideas tomadas de terceros.

Al usar y citar información de una fuente externa en el trabajo, corresponde resumirla o escribirla con palabras propias. Al insertar un fragmento de texto literal del documento ajeno de hasta tres o cuatro líneas, es obligatorio indicarlo entre comillas y/o con letra cursiva. Si es necesario incluir un fragmento literal largo, debe copiarse el texto en un párrafo aparte, utilizando una sangría más marcada a derecha e izquierda y seleccionando un tipo de caracteres más pequeños. La referencia debe estar identificada claramente en la lista de referencias.

Artículo 23º Definición de Plagio.

A los fines del presente Reglamento se define como Plagio lo siguiente:

- Copiar y presentar ideas (palabras, gráficos, algoritmos o productos intelectuales) de otros como propios, ya sea en forma literal o directa o por medio de paráfrasis.
- Presentar como nueva y original una idea o producto derivado de una fuente preexistente.
- Usar la producción (literaria, gráfica o algorítmica) de terceros sin acreditar la fuente, por más reducida que sea esa producción.

Dicho en otras palabras, el Plagio es un acto de fraude. Involucra el robo del trabajo de otro y mentir ulteriormente acerca de él.

Artículo 24º Comprobación de Plagio.

El Plagio, según lo definido en el Art. 22., de comprobarse y cualquiera sea su extensión, generará el rechazo del trabajo presentado y su autor será sancionado acorde a lo aquí estipulado.

Artículo 25º Clasificación y sanciones para casos de Plagio.

A los fines del presente Reglamento el Plagio será clasificado como falta leve, falta grave o falta muy grave, apreciado según criterios de razonabilidad por parte del Jurado encargado de entender sobre el mismo. En todos los casos, el trabajo presentado recibirá la calificación de 0 (CERO) Puntos.

Falta leve: se deberá presentar una obra nueva con otro tutor y cotutor si corresponde y un tema nuevo en el plazo de 6 (SEIS) meses contados a partir de la fecha de reprobación.

Falta grave: se procederá a la suspensión del cursante por el término de 1(UN) año contado a partir de la fecha de reprobación. Durante ese lapso no podrá cursar materias ni rendir exámenes de Posgrado. Una vez cumplido dicho plazo, se deberá presentar una obra nueva con otro tutor y cotutor si corresponde y un tema nuevo en el plazo de 6 (SEIS) meses.

Falta muy grave: se procederá a la suspensión del cursante por el término de 2(DOS) años contados a partir de la fecha de reprobación. Durante ese lapso no podrá cursar materias ni rendir exámenes de Posgrado. Una vez cumplido dicho plazo, se deberá presentar una obra nueva con otro tutor y cotutor si corresponde y un tema nuevo en el plazo de 6 (SEIS) meses.

Artículo 26º El alumno de posgrado podrá deducir recurso de reconsideración contra la decisión adoptada por el Jurado, debiendo ser presentada, en forma escrita y de manera fundada, ante las Autoridades del Posgrado dentro de los 5 (CINCO) días de haberse notificado fehacientemente de la resolución de rechazo.

ANEXO 3 - REGLAMENTO DE TESIS O TRABAJO FINAL DE MAESTRÍA

Título 1: Condiciones Generales

Artículo 1º: De acuerdo a lo dispuesto por el Reglamento General de la Universidad de Buenos Aires, la Tesis o Trabajo Final de Maestría deberá ser de carácter individual, inédito y constituir un valor agregado en el área del conocimiento de la temática propia de la Maestría.

La Tesis o Trabajo Final de Maestría podrá ser de índole académica o profesional y consistirá en el desarrollo y la exposición de una problemática actualizada de un área temática de Seguridad Informática o un caso práctico de aplicación de tecnología de seguridad informática, que incluya una elaboración del estado de la cuestión, la presentación de los datos empíricos si correspondiere y una exposición fundada de las conclusiones a las que hayan arribado y deberá presentar un enfoque o aporte original del tema. Este último aspecto será ineludible y definitorio al momento de evaluarse el trabajo de final de maestría, al igual que el estricto ajuste a los aspectos formales del documento presentado y que quedan enunciados en el presente Reglamento.

En particular se definen:

a) Tesis o Trabajo Final de Maestría con orientación académica: Trabajo sobre un campo disciplinar o interdisciplinar, individual y escrito con formato de monografía que evidencia el estudio crítico de información relevante respecto del tema o problema específico y el manejo conceptual y metodológico propio de la actividad de investigación. La Tesis o Trabajo Final de Maestría se desarrollará bajo la dirección de un Director y, si correspondiese en virtud de la temática, con un Codirector.
b) Trabajo Final de Maestría con orientación profesional: Trabajo individual y escrito que podrá adquirir formato de proyecto, estudio de caso, obra o trabajos similares que permitan evidenciar la integración de aprendizajes realizados en el proceso formativo, la profundización de conocimientos en un campo profesional y el manejo de destrezas y perspectivas innovadoras en la

profesión. El trabajo final de maestría se desarrollará bajo la dirección de un Director y, si correspondiese en virtud de la temática, con un Codirector.

En todos aquellos aspectos que no estén específica y taxativamente estipulados en el presente Reglamento, se deberá dar cumplimiento a lo que indique la Facultad Sede de la Maestría. Sin embargo, en caso de discrepancias, se dará por válido lo estipulado en el presente Reglamento.

Artículo 2º: Para la presentación del trabajo final de maestría, el maestrando deberá haber cursado y aprobado la totalidad de las asignaturas y los seminarios establecidos en el Plan de Estudios de la carrera de Maestría. Asimismo debe haber aprobado previamente el Trabajo Final de Integración.

Título 2: Del Plan de Tesis o Trabajo Final de Maestría

Artículo 3º: Dicho Plan deberá constar de:

1. Resumen
    1.1. Palabras clave
2. Fundamentación del tema elegido
    2.1. Antecedentes del tema
    2.2. Estado actual del tema
    2.3. Planteo del problema
    2.4. Alcances y limitaciones de la propuesta
    2.5. Aportes teóricos y/o prácticos al campo temático
3. Objetivos y alcance
    3.1. General
    3.2. Específicos o particulares.
4. Hipótesis del trabajo
5. Metodología y plan de actividades.
6. Bibliografía Inicial
7. Propuesta de director de Tesis o Trabajo Final de Maestría (con el consentimiento de éste).

Esta estructura podrá variar para el caso de trabajo final de maestría de orientación profesional y se adaptarán en ese último caso al criterio del autor y anuencia del Director. Una vez cumplido el punto previo, remitir en formato .pdf al Coordinador Académico a fin de ser considerado por la Comisión de Maestría

Artículo 4º: El Plan de Tesis o Trabajo Final de Maestría no debe exceder las VEINTE (20) páginas, incluyendo carátula, y anexos si correspondiere, por la índole de la investigación. Para notas y citas referenciales puede emplearse cualquiera de los estilos en uso, pero en todos los casos, se empleará un solo criterio (ver artículo 9).

Artículo 5º: Modelo de portada del Plan de Tesis o Trabajo Final de Maestría:

Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Plan de Trabajo Final de Maestría (o Tesis)

Tema
[Denominación del campo temático]

Título
Subtítulo [si corresponde]

Autor/a:
Director/a
Co-director/a: [si corresponde]

Año de Presentación
Cohorte del Maestrando

Título 3º: Del Tesis o Trabajo Final de Maestría

Artículo 6º: El plazo máximo para la entrega de la Tesis o el Trabajo Final de Maestría será de 24(veinticuatro) meses, contados a partir de la fecha de aprobación de la última materia. Este plazo regirá para todos los Cursantes que hayan ingresado a la Maestría en el 2013 y años ulteriores. En caso de exceder este tiempo, el Cursante deberá iniciar el trámite de rematriculación al presentar el Tesis o Trabajo Final de Maestría como paso previo para llegar a ser considerada.

Artículo 7º: El documento final de la Tesis o Trabajo Final de Maestría tendrá, como pauta general, una extensión mínima de diez mil (10.000) palabras y una extensión máxima de 80 páginas, sin considerar los anexos y/o apéndices que no sean de su propia elaboración. En carácter de excepción, y a indicación del Director del trabajo final de maestría, el número de páginas podrá ser menor. Esta situación deberá ser informada a la Comisión del Posgrado con antelación a la presentación del trabajo final de maestría.

Artículo 8º: La presentación de la Tesis o Trabajo Final de Maestría se hará acorde a lo especificado en el Art. 19º.

Artículo 9º: La Tesis o Trabajo Final de Maestría debe ser presentada según los siguientes requisitos formales:

l. Papel: Únicamente papel blanco. Tamaño A4 (21 x 29,7 cm).

m. Tipo de letra: Fuente estándar, estilo Arial, tamaño 12. Para las citas, o notas al pie de página, se empleará el tamaño 10. Deberá utilizarse el mismo estilo de fuente en todo el trabajo final de maestría. No podrá utilizarse una fuente de tipo cursiva, excepto en los casos de: palabras extranjeras, términos científicos, título de libros o cuando sea requerido especialmente por el Director.

n. Espaciado: Se utilizará un interlineado de 1,5 espacio en todo el texto, salvo a continuación de los títulos donde deberá agregarse un interlineado simple más. En las notas a pie de página, el índice y las citas bibliográficas, se utilizará un interlineado simple.

o. Justificado: Se deberá utilizar el justificado total para todo el texto, notas a pie de página, bibliografía y referencias. En el cuerpo del texto se dejará una sangría de 1,25 cm en la primera línea de cada párrafo.

p. Márgenes: 2,5 cm para los márgenes superior, inferior y derecho; 4 cm para el margen izquierdo (incluye margen para encuadernación).

q. Impresión: En color negro, se podrá utilizar color en las figuras y los gráficos. No se podrán incluir correcciones manuales, cintas o líquidos correctores.

r. Numeración: Todas las páginas deberán numerarse en forma correlativa en su parte inferior derecha o central. La página número 1 corresponderá a la Introducción, mientras que las páginas anteriores a ésta podrán numerarse con números romanos en minúsculas. La portada no se incluye en la numeración. Se deberá iniciar cada capítulo en una nueva página y seguir la numeración en forma consecutiva; no se podrá utilizar una numeración secundaria para los distintos capítulos y secciones.

s. Redacción: En castellano, salvo autorización explícita de la Comisión. Se podrán incluir citas en otras lenguas, pero sólo en notas al pie. La traducción deberá aparecer en el texto o en las mismas notas.

t. Encuadernación: El trabajo deberá presentarse prolijamente encuadernado. Podrá ser espiralado, en cuyo caso incluirá una tapa plástica transparente.

u. Acuerdo expreso del Director para proceder a su presentación.

v. Una vez cumplido el punto previo, remitir una copia en formato .pdf al Coordinador Académico de la Maestría para ser considerado por la Comisión.

Artículo 10º: La **portada** deberá contener la siguiente información, en este orden:

h. Universidad de Buenos Aires
i. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería
j. Maestría en Seguridad Informática
k. Tesis o Trabajo Final de Maestría

l. Título del trabajo final de maestría
m. Nombre del autor
n. Nombre del Director y del Co-director (si lo hubiere)
o. Fecha de presentación y cohorte del cursante.

Artículo 11º: El orden de los contenidos será el siguiente:

p. Portada: Ver Art(s) 10º y 12º

q. Declaración Jurada de origen de los contenidos: Se incluirá, con este título, y en una hoja por separado, el siguiente texto que tendrá el carácter de Declaración Jurada: "Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis o Trabajo Final de Maestría vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual". Al pié de la misma el autor debe firmar en forma manuscrita, en todos los ejemplares impresos entregados, aclarando a continuación sus Nombres y Apellidos y el número de documento personal que lo identifica. Los ejemplares electrónicos entregados incluirán la leyenda "FIRMADO" en lugar de la firma hológrafa.

r. Resumen: Deberá contener no más de doscientas (200) palabras. Incluirá, la descripción de la metodología utilizada y los resultados o conclusiones. Al final del resumen se agregarán como mínimo tres (3) palabras clave.

s. Índice o tabla de contenidos: Un índice completo con sus capítulos y secciones. Se recomienda en la versión digital que cada entrada del índice posea un link al capítulo o sección correspondiente.

t. Numeración de capítulos, secciones, tablas y figuras: Los capítulos y Subcapítulos o secciones deben estar numerados (1, 1.1, 1.2, 2, etc.). Las tablas y las ilustraciones pueden numerarse con la numeración consecutiva desde el comienzo hasta el final del trabajo (Tabla 1, Tabla 2, Tabla 3, etc.) o con numeración por capítulos (Tabla 1.1, 2.1, 3.1, etc.).

u. Prólogo: Podrá tener un prólogo o sección inicial de agradecimientos. No es obligatorio.

v. Nómina de abreviaturas: En caso de ser utilizadas y de no ser expresamente aclaradas en el texto del trabajo.

w. Cuerpo introductorio: En él se presentará brevemente el problema abordado, los objetivos y alcance e hipótesis del trabajo, su estructura, el enfoque que se le ha dado al estudio y la relevancia de la investigación.

x. Cuerpo principal: Deberá estar dividido en capítulos conforme al índice. Se deben desarrollar los objetivos en función del alcance definido en el cuerpo introductorio.

y. Conclusiones: Se explicará cómo se justifican en el desarrollo la o las hipótesis planteadas en el Cuerpo Introductorio, sintetizando los hallazgos y su relación con las mismas no pudiendo ser las mismas una mera síntesis de lo anteriormente expuesto. Dejará, además, constancia expresa de su opinión

z. Glosario: Lista de términos especializados utilizados, con el fin de homogeneizar la terminología utilizada en el trabajo.

aa. Apéndices / Anexos: Podrá tener Apéndices o Anexos, esto es, secciones relativamente independientes de una obra, que ayudan a su mejor comprensión y permiten conocer los aspectos específicos que —por su longitud o su naturaleza— no resulta conveniente tratarlos dentro del cuerpo principal.

a. Bibliografía: Deberá estar dispuesta por orden alfabético o por orden de aparición en el cuerpo y contener todas las referencias hechas en el texto utilizando el sistema numérico, alfabético o combinación de ambos.

Por ejemplo, para libros:

[13] Censor Y. and Zenios S., Parallel Optimization Theory and Applications, Oxford University Press, New York, 1997

Y para trabajos en revistas:

[8] Bauschke H.H. and Borwein J.M., On projection algorithms for solving convex feasibility problems, SIAM Review, 38, (1996), pp.367-426.

La información obtenida en Internet deberá señalar la fecha precisa de su obtención, por ejemplo:

[25] IBM creates learning, brain-like, synaptic CPU, http://www.extremetech.com/extreme/93060-ibm-creates-learning-brain-like-synaptic-cpu (consultada el 24/8/2011)

b. Bibliografía General: Se indicará, sin referenciar, aquella bibliografía de respaldo general utilizada como fuente de conocimiento para la elaboración de La trabajo final de maestría presentada.

c. Índices específicos: (temáticos, técnicos, de ilustraciones, gráficos, siglas, etc.).

Se recuerda que la estructura aquí indicada podrá adaptarse a criterio del autor en caso de trabajo final de maestría de orientación profesional.

Artículo 12º: Modelo de portada del Documento Final de la Tesis o Trabajo Final de Maestría:

Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Trabajo Final de Maestría (o Tesis)

Título

Subtítulo [si corresponde]

Autor:
Director/a
Co-director/a: si corresponde

Año de presentación
Cohorte

Título 4: De los Directores de la Tesis o Trabajo Final de Maestría

Artículo 13º: Los Directores de la Tesis o Trabajo Final de Maestría deberán ser, o haber sido, profesores universitarios, o poseer título académico equivalente o superior, (salvo excepción expresamente autorizada por la Comisión del Posgrado). También podrán ser profesionales o investigadores de reconocido prestigio en la especialidad pertinente al tema de Tesis o Trabajo Final de Maestría que deba dirigir con la autorización expresa de la Comisión y el Consejo Directivo de la Facultad sede de la Maestría.

Artículo 14º: Entre las funciones de los Directores están las de: asesorar y orientar al maestrando en la elaboración de la trabajo final de maestría, supervisar el cumplimiento del Plan previsto por parte del maestrando y participar, con voz pero sin voto, en el Jurado del trabajo final del maestrando por él dirigido. Asimismo y a requerimiento de la Comisión de Maestría, generará un breve informe final sobre la labor de su dirigido, destinado exclusivamente a los Jurados del trabajo final de maestría.

Artículo 15°: Cada Director de Tesis o Trabajo Final de Maestría podrá tener a su cargo un máximo de 5 (CINCO) cursantes simultáneamente.

Título 5: Del Jurado de la Tesis o Trabajo Final de Maestría, su defensa.

Artículo 16º: La Comisión del Posgrado propondrá al Consejo Directivo de la Facultad sede de la Maestría un Jurado compuesto por tres (3) profesores de reconocida competencia en el tema o en temas afines. Podrán designarse también hasta dos (3) miembros suplentes. Este jurado deberá estar integrado por al menos un miembro externo a la institución. No podrán participar en el jurado personas que hayan trabajado junto al candidato, o a su Director, en los dos años que precedan la presentación del trabajo final de maestría. Los jurados externos deberán ser profesores afines a la especialidad del tema del Tesis o Trabajo Final de Maestría o expertos de reconocida trayectoria nacional o internacional que le otorguen rango equivalente a juicio de la Comisión, o investigadores de prestigio en especialidades afines a dicha temática.
El Director podrá sugerir candidatos a actuar como miembros externos del jurado. El postulante no debe participar en esta instancia.
El postulante tendrá derecho a impugnar parcial o totalmente el Jurado, dentro de los diez días hábiles de conocida su designación, aduciendo fundamentos precisos que puedan ser ratificados por el Director del trabajo final de maestría, quien dejará constancia escrita adjunta al pedido de su opinión. La actuación será considerada y

evaluada por La Comisión del Posgrado, que decidirá sobre su procedencia o rechazo, haciendo constar su dictamen en Actas. Su decisión será inapelable.
Si se hace lugar a la impugnación, dispondrá, en la misma Acta, la realización de nuevas propuestas para formalizar la pertinente designación.

Artículo 17º: Los Miembros propuestos para el Jurado dispondrán de un plazo de cinco (5) días hábiles a partir de recibida la comunicación de su designación para comunicar su aceptación.
La designación del Jurado será propuesta dentro de los treinta (30) días de presentadas la Tesis o Trabajo Final de Maestría a la Comisión de Maestría.
La Comisión de Maestría remitirá al Jurado l Tesis o Trabajo Final de Maestría correspondiente y dicho Jurado tendrá un plazo no mayor de dos (2) meses para su estudio, antes de ser convocado.
Artículo 18º: El Jurado podrá proponer, con dictamen fundado:

1) la aprobación de la Tesis o Trabajo Final de Maestría, tal como fuera presentada., o

2) la devolución del mismo al presentante, a los efectos de su corrección, que deberá concretarse en un período no superior a un año, o

3) el rechazo del mismo.

La decisión del Jurado se tomará por simple mayoría y se asentará en Actas. El autor, con aval del Director, tendrá derecho a solicitar por escrito la reconsideración del dictamen del Jurado, en casos de devolución o rechazo. La Comisión de Maestría decidirá si se hace lugar, o no, a dicha solicitud y la comunicará por escrito. También esta decisión, con los respectivos fundamentos, deberá asentarse en el libro de Actas. La misma será inapelable.
En todos los casos, la opinión deberá estar fundamentada y acompañada, cuando fuera pertinente, de indicaciones acerca de los errores, omisiones o defectos encontrados en el trabajo final de maestría.

Título 6: La defensa pública de la Tesis o Trabajo Final de Maestría
Artículo 19°:

a) La Comisión de Maestría fijará la fecha y lugar de realización de la misma y los medios de difusión del acto para conocimiento de los posibles interesados en asistir.

b) Apenas se resuelva que la Tesis o Trabajo Final de Maestría sea defendida, el interesado hará entrega de 4 (CUATRO) ejemplares impresos de la misma al Coordinador Académico de la Maestría, firmados en la Declaración Jurada (Art. 11º b), de los cuales tres ejemplares serán destinados a los Jurados y el restante a la biblioteca de la Facultad Sede. Los ejemplares impresos deben coincidir en un todo con el ejemplar electrónico acompañante (en formatos Word y PDF), en un CD que se entrega junto con dichos ejemplares impresos.

c) La defensa del trabajo se realizará en un acto público, en una exposición no mayor de 30 minutos salvo expresa indicación del Jurado, sobre los aspectos fundamentales del trabajo. La plantilla, fuentes y demás detalles de la presentación quedan a criterio del postulante. Sólo los miembros del Jurado podrán formular preguntas al expositor. En esa oportunidad y antes de comenzar, el Cursante hará entrega de 3 (tres) ejemplares impresos de las placas proyectadas a los Jurados.

Artículo 20°: Una vez finalizada la exposición y la sesión de preguntas, el Jurado deliberará en privado y labrará un acta emitiendo dictamen, en conjunto, o por separado, dejando su opinión sobre:

a) Pertinencia y vigencia en relación con los objetivos del estudio.

b) Pertinencia y vigencia de la revisión de la literatura en relación con los objetivos del estudio.

c) La claridad formal del lenguaje, la corrección gramatical y la coherencia del estilo.

d) Claridad expositiva en la presentación oral y nivel de conocimientos demostrados.

e) El contenido de las conclusiones del trabajo final de maestría

Título 7: De la calificación de la Tesis o Trabajo Final de Maestría

Artículo 21º: La calificación del Tesis o Trabajo Final de Maestría se hará según la escala de 0 a 10, requiriéndose un mínimo de cuatro (4) puntos para su aprobación. En caso de la obtención de diez (10) puntos, el Jurado podrá añadir la recomendación de publicación, la cual no implicará ningún compromiso por parte de la Universidad, sino sólo un reconocimiento académico.

Artículo 22º: Citas de trabajos de terceros.
El documento no debe contener frases textuales de documentos de terceros sin estar citadas y referenciadas. La cita es obligatoria ya que permite distinguir el trabajo del alumno de las ideas tomadas de terceros.
Al usar y citar información de una fuente externa en el trabajo, corresponde resumirla o escribirla con palabras propias. Al insertar un fragmento de texto literal del documento ajeno de hasta tres o cuatro líneas, es obligatorio indicarlo entre comillas y/o con letra cursiva. Si es necesario incluir un fragmento literal largo, debe copiarse el texto en un párrafo aparte, utilizando una sangría más marcada a derecha e izquierda y seleccionando un tipo de caracteres más pequeños. La referencia debe estar identificada claramente en la lista de referencias.

Artículo 23º Definición de Plagio

A los fines del presente Reglamento se define como Plagio lo siguiente:

- Copiar y presentar ideas (palabras, gráficos, algoritmos o productos intelectuales) de otros como propios, ya sea en forma literal o directa o por medio de paráfrasis.
- Presentar como nueva y original una idea o producto derivado de una fuente preexistente.
- Usar la producción (literaria, gráfica o algorítmica) de terceros sin acreditar la fuente, por más reducida que sea esa producción.

Dicho en otras palabras, el Plagio es un acto de fraude. Involucra el robo del trabajo de otro y mentir ulteriormente acerca de él.

Artículo 24º Comprobación de Plagio.

El Plagio, según lo definido en el Art. 23., de comprobarse y cualquiera sea su extensión, generará el rechazo del trabajo presentado y su autor será sancionado acorde a lo aquí estipulado.

Artículo 25º Clasificación y sanciones para casos de Plagio.

A los fines del presente Reglamento el Plagio será clasificado como falta leve, falta grave o falta muy grave, apreciado según criterios de razonabilidad por parte del Jurado encargado de entender sobre el mismo. En todos los casos, el trabajo presentado recibirá la calificación de 0 (CERO) Puntos.

Falta leve: se deberá presentar una obra nueva con otro director y codirector si corresponde y un tema nuevo en el plazo de 6 (SEIS) meses contados a partir de la fecha de reprobación.

Falta grave: se procederá a la suspensión del cursante por el término de 1(UN) año contado a partir de la fecha de reprobación. Durante ese lapso no podrá cursar materias ni rendir exámenes de Posgrado. Una vez cumplido dicho plazo, se deberá presentar una obra nueva con otro director y codirector si corresponde y un tema nuevo en el plazo de 6 (SEIS) meses.

Falta muy grave: se procederá a la suspensión del cursante por el término de 2(DOS) años contados a partir de la fecha de reprobación. Durante ese lapso no podrá cursar materias ni rendir exámenes de Posgrado. Una vez cumplido dicho plazo, se deberá presentar una obra nueva con otro director y codirector si corresponde y un tema nuevo en el plazo de 6 (SEIS) meses.

Artículo 26º El alumno de posgrado podrá deducir recurso de reconsideración contra la decisión adoptada por el Jurado, debiendo ser presentada, en forma escrita y de manera fundada, ante las Autoridades del Posgrado dentro de los 5 (CINCO) días de haberse notificado fehacientemente de la resolución de rechazo.

ANEXO H - CONTENIDOS MINIMOS vs COMPETENCIAS Detallado

Trabajo Final de Especialización en Evaluación Universitaria (2023)

Codigo Asignatura	Contenidos mínimos	Definir e instrumentar un plan integral de Seguridad Informática de la organización	Definir estrategias y políticas de Seguridad Informática	Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)	Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.	Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.	Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico	Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones	Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.	Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática	Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas	Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática	Ejercer la docencia en materia de Seguridad Informática.	TOTAL
	Numero asignado a la Competencia	1	2	3	4	5	6	7	8	9	10	11	12	
CRIPT1	Fundamentos de criptología.	1	1	1	1	1	1	1	1	0,5	1	1	1	11,5
CRIPT1	Introducción a los criptosistemas.	1	1	1	1	1	1	1	1	0,5	1	1	1	11,5
CRIPT1	Criptología clásica: cifrados y ataques.									0,5			1	1,5
CRIPT1	Secreto perfecto y One-Time Pad.	1	1	1	1	1	1	0,5	1	0,5	1	1	1	11
CRIPT1	Criptosistemas simétricos: históricos y actuales; modos operativos.	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	6,5
CRIPT1	Criptosistemas asimétricos; comparaciones de seguridad entre cifradores simétricos y de clave pública.	1	1	1	1	1	1	0,5	1	0,5	1	1	1	11
CRIPT1	Gestión de claves simétricas y asimétricas.	1	1	1	1	1	1	0,5	1	0,5	1	1	1	11
CRIPT1	Intercambio seguro de claves.	1	1	1	1	1	1	0,5	1	0,5	1	1	1	11
CRIPT1	Funciones Hash/ MAC/HMAC.	1	1	1	1	1	1	0,5	1	0,5	1	1	1	11
CRIPT1	Generación de números aleatorios.	1	1	1	1	1	1	0,5	1	0,5	1	1	1	11
	TOTALES CRIPT1	8,5	8,5	8,5	8,5	8,5	8,5	5,5	8,5	5	8,5	8,5	10	
CRIPT2	Teoría de la información: entropía de Shannon. Entropía condicional.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Transinformación.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Distancia de unicidad.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Algebra abstracta y sus aplicaciones criptográficas.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Logaritmo discreto y ataques vinculados.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Criptosistema ElGamal y ElGamal generalizado.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Campos finitos GF(2n) en criptosistemas simétricos (AES) y asimétricos (ElGamal).	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Máquinas de Turing y teoría de la complejidad computacional aplicadas a la criptología.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Problemas complejos en campos numéricos.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Algebra no conmutativa y aplicaciones criptográficas (GDH-Intercambio Diffie-Hellman generalizado y ZKP-Prueba de conocimiento cero).	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Curvas elípticas e hiperelípticas.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Códigos lineales, problema de la mochila y otros.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Ataque de criptoanálisis diferencial a las redes Feistel.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Ataques de colisiones diferenciales a las funciones Hash.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Estándar SHA3.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Secretos compartidos y protocolos especiales (undeniable signatures, oblivious transfer, electronic cash).	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
CRIPT2	Elementos de criptografía cuántica, computación cuántica, teoría de información cuántica y sus aplicaciones criptográficas.	1	1	1	1	1	1	1	1	0,2	1	0,2	1	10,4
	TOTALES CRIPT2	17	17	17	17	17	17	17	17	3,4	17	3,4	17	
RED1	Esquemas de seguridad: distribución de claves simétricas.						1					1	1	3
RED1	Administración de claves publicas: autoridad certificante y certificados.						1	1				1	1	4
RED1	Administración de claves de sesión compartidas.						1					1	1	3
RED1	Seguridad de redes e Internet: Single Sign On, Infraestructura de Clave Publica PKI.				1	1	1	1				1	1	6
RED1	Seguridad de WWW; comercio electrónico, gateways de pago, protocolo SET “Secure Electronic Transaction”; seguridad en IP IPSec: Firewalls, SSL.				1	1	1	1				1	1	6
RED1	Seguridad en organizaciones: Firma Digital, Factura Electrónica; administración de identidades: identidades y cuentas directorio corporativo; gestión de identidades.	1	1	1	1	1	1	1	1	1	1	1	1	12
	TOTALES RED1	1	1	1	3	3	6	4	1	1	1	6	6	
RED2	Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, Intrusión Detection Systems Honeypots; análisis de vulnerabilidades, pruebas de penetración	1	1	1	1	1	1	1	1	1	1	1	1	12
RED2	Desarrollo seguro.													0
RED2	Seguridad en Organizaciones: modelos de alta disponibilidad y seguridad; dominios de seguridad, monitoreo de seguridad; puntos de control.	1	1	1	1	1	1	1	1	1	1	1	1	12
RED2	Ubicación de Firewalls, IDS	1	1	1	1	1	1	1					1	8
	TOTALES RED2	3	3	3	3	3	3	3	2	2	2	2	3	
GEST1	Organización y estructura del área de seguridad: áreas, funciones y responsabilidades, perfiles, criterios de organización.	1	1	1	1	1			1		1	1		8
GEST1	Técnicas de gestión (estrategia, finanzas, marketing y recursos humanos).	1	1	1	1	1			1		1	1		8
GEST1	Ciclo de vida de los sistemas de seguridad.	1	1	1	1	1			1		1	1		8
GEST1	Gestión de proyectos de seguridad.	1		1										2
GEST1	Tercerización de servicios y gestión de proveedores.	1	1	1	1	1			1		1	1		8
GEST1	Evaluación económica de la seguridad.	1	1	1	1	1			1		1	1		8
GEST1	Métricas y performance.	1	1	1	1	1			1		1	1		8
GEST1	Estrategias, políticas, programas y normas de seguridad.	1	1	1	1	1			1		1	1		8
GEST1	Introducción al análisis y gestión del riesgo.	1	1	1	1	1			1		1	1		8
	TOTALES GEST1	8	7	8	7	7	0	0	7	0	7	7	0	

Codigo Asignatura	Contenidos mínimos	Definir e instrumentar un plan integral de Seguridad Informática de la organización	Definir estrategias y políticas de Seguridad Informática	Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)	Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.	Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.	Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico	Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones	Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.	Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática	Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas	Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática	Ejercer la docencia en materia de Seguridad Informática.	TOTAL
	Numero asignado a la Competencia	1	2	3	4	5	6	7	8	9	10	11	12	
GEST2	Análisis y gestión del riesgo: mapa de riesgos, evaluación de salvaguardas, informe de insuficiencias, catálogo de elementos, estado de riesgo.	1	1	1	1	1	1	1	1	1	1	1	1	12
GEST2	Ciclo de vida: análisis y gestión, planificación, implementación de salvaguardas, gestión de configuración y cambios				1				1	1	1	1	1	6
GEST2	Relación y complementariedad entre los distintos estándares y/ modelos (frameworks), cumplimientos (compliance), regímenes e instituciones Internacionales y Nacionales: Cobit, Coso, BSI, ISO, ITIL, Basilea II, CMM, SOX, otros.	1	1	1	1	1			1	1	1	1	1	10
	TOTALES GEST2	2	2	2	3	2	1	1	3	3	3	3	3	
DyPS	Formulación y seguimiento de un proyecto de seguridad en base a un caso de estudio incluyendo el ciclo de vida de los sistemas de seguridad; fase inicial, fase de desarrollo y adquisición, fase de implementación, fase de operación y mantenimiento, fase de disposición.	1	1	1	1	1	1	1	1	1	1	1	1	12
	TOTALES DyPS	1	1	1	1	1	1	1	1	1	1	1	1	
SSOyA	Ciclo de vida del desarrollo de sistemas.	1	1	1			1				1		1	6
SSOyA	Desarrollo y gestión de bases de datos.	1	1	1		1	1						1	6
SSOyA	Controles de los sistemas.	1	1	1	1	1	1				1	1	1	9
SSOyA	Control en la operación y el mantenimiento de las aplicaciones.	1	1	1	1	1	1				1	1	1	9
SSOyA	Aplicaciones distribuidas.			1		1	1				1	1	1	6
SSOyA	Ataques y vulnerabilidades en aplicaciones y sistemas.	1		1	1	1	1	1			1	1	1	9
SSOyA	Buffer Overflows, Format Strings, Race Conditions.			1	1			1					1	4
SSOyA	Entornos protegidos (sandboxes, chroot).			1	1			1					1	4
SSOyA	Mecanismos de protección: técnica del canario, segmento no ejecutable.			1	1			1					1	4
SSOyA	Análisis de logs.	1		1	1			1					1	5
SSOyA	HostIDS.	1		1	1			1					1	5
SSOyA	Vulnerabilidades en web.	1	1	1	1			1					1	6
SSOyA	Códigos maliciosos.	1	1	1	1			1					1	6
	TOTALES SSOyA	9	6	13	10	5	6	8	0	0	5	4	13	
SF	Administración y relevamiento de los riesgos.		1	1	1				1					4
SF	Planeamiento y gerenciamiento de la Seguridad Física.	1								1				2
SF	La tecnología y el diseño de procesos de trabajo.					1		1						2
SF	Aplicación de diseños.			1	1	1	1	1				1		6
SF	Sistemas de seguridad física.	1	1	1	1	1			1					6
	TOTALES SF	2	2	3	3	3	1	2	2	1	0	1	0	
AUDIT	Control y auditoría.	1	1	1	1	1	1	1			1	1	1	10
AUDIT	Normas técnicas.	1	1	1	1	1	1		1	1	1	1	1	11
AUDIT	Control y estructura organizativa.	1				1	1	1	1				1	6
AUDIT	Separación de funciones y oposición de intereses.	1	1	1	1	1	1	1	1	1	1	1	1	12
AUDIT	Análisis específico del área de Seguridad Informática.	1	1		1				1	1	1	1	1	8
AUDIT	Controles en las entradas al sistema y sus almacenamientos.	1					1	1	1					4
AUDIT	Transacciones rechazadas y observadas.						1	1					1	3
AUDIT	Concepto de monitoreo.		1		1			1	1		1	1	1	7
AUDIT	Planificación de las actividades de auditoria.	1	1	1	1	1		1		1	1	1	1	10
AUDIT	Pruebas de cumplimiento.	1	1	1	1	1		1				1	1	8
AUDIT	Evaluación de aplicación de políticas, planes, normas, procedimientos, esquemas, estándares y métricas.	1		1	1			1	1		1	1	1	8
AUDIT	Pruebas y técnicas asociadas.	1	1			1		1		1		1	1	7
AUDIT	Pistas de auditoria.						1	1						2
AUDIT	Evaluación del nivel de respuesta ante incidentes.		1	1		1		1	1		1	1		7
AUDIT	Test de penetración.							1						1
AUDIT	Test de nivel de divulgación y comprensión de políticas, normas y procedimientos en la organización.		1	1	1	1		1	1	1	1	1	1	10
AUDIT	Comprobaciones y simulaciones sobre planes de contingencia, continuidad de operaciones y recuperación	1	1	1	1	1		1		1		1	1	9
	TOTALES AUDIT	1	3	3	2	3	1	5	2	2	2	3	2	
IF	Análisis forense: objetivos, principios.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Evidencia digital.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Metodología de trabajo para el análisis de los datos: identificación de la evidencia digital, preservación del material informático, análisis de datos, presentación del dictamen pericial	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Registros temporales.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	MACtimes.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Registros de redes y DNS.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	File systems con journaling.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	File System: File System Virtual (VFS).	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Aspectos internos del File System.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Estructura de una partición.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Recolección de información volátil y no volátil.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Recolección de evidencia de red.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Análisis de archivos binarios: análisis estático y análisis dinámico.	1	1	1	1	1	1	1	1	1	1	1	1	12

Codigo Asignatura	Contenidos mínimos	Definir e instrumentar un plan integral de Seguridad Informática de la organización	Definir estrategias y políticas de Seguridad Informática	Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)	Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.	Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.	Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico	Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones	Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.	Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática	Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas	Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática	Ejercer la docencia en materia de Seguridad Informática.	TOTAL
	Numero asignado a la Competencia	1	2	3	4	5	6	7	8	9	10	11	12	
IF	Consideraciones legales: evidencia y evidencia admisible.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Obtención de evidencias.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Tipos de evidencia.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Características para ser admisible en juicio.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Preservación de la cadena de custodia.	1	1	1	1	1	1	1	1	1	1	1	1	12
IF	Informes Periciales.	1	1	1	1	1	1	1	1	1	1	1	1	12
	TOTALES IF	19	19	19	19	19	19	19	19	19	19	19	19	
CO	Cultura organizacional.	1	1	1	1	1				1		1	1	8
CO	Clima organizacional.	1	1	1		1				1		1	1	7
CO	Comportamiento individual, grupal y organizacional.	1	1	1		1			1	1		1		7
CO	Dinámica de grupos.	1	1						1	1				4
CO	Valores y actitudes.	1	1	1	1	1	1	1	1	1	1	1	1	12
CO	Comunicación interpersonal.	1	1	1	1	1	1	1	1	1	1	1	1	12
CO	Motivación.	1	1	1		1			1	1		1	1	8
CO	Liderazgo.	1	1	1		1			1	1	1	1	1	9
CO	Trabajo en equipo.	1	1	1	1	1	1	1	1	1	1	1	1	12
CO	Resolución de conflictos.	1	1	1	1	1		1	1	1	1	1	1	11
CO	Negociación.	1	1	1	1	1		1	1	1	1	1	1	11
CO	Gestión del cambio organizacional.	1	1	1		1	1	1	1	1	1	1		10
CO	Inteligencias múltiples.	1	1		1		1		1	1		1		7
CO	El proceso de aprendizaje.						1		1	1			1	4
CO	Toma de decisiones individuales y grupales.	1	1	1	1	1	1		1	1		1	1	10
	TOTALES CO	14	14	12	8	12	7	6	13	15	7	13	11	
MLEP	Introducción al Derecho Informático, conceptos y terminología legal.	1	1	1						1				4
MLEP	Sistemas legales en Argentina y otros países.	1	1	1		1		1	1	1	1	1	1	10
MLEP	Régimen jurídico de protección de la Propiedad Intelectual.	1	1	1	1	1		1	1	1		1	1	10
MLEP	Régimen de Firma Digital.	1	1	1	1	1		1	1	1		1	1	10
MLEP	Ética y privacidad.	1	1	1	1	1	1	1	1	1	1	1	1	12
MLEP	Visión jurídica de los delitos informáticos.	1	1		1	1	1	1	1	1		1		9
MLEP	Derecho Internacional: legislación transfrontera.	1		1	1	1		1	1	1		1	1	9
MLEP	Jurisprudencia.	1	1	1	1	1	1	1	1	1	1	1		11
	TOTALES MLEP	8	7	7	6	7	3	7	7	8	3	7	5	
TDCG	Desarrollo de casos y situaciones que permitan adquirir práctica en los siguientes aspectos: comunicaciones interpersonales, negociación, toma de decisiones, trabajo en equipo, liderazgo, motivación y gestión del cambio.	1	1	1		1	1		1	1		1		8
	TOTALES TDCG	1	1	1		1	1		1	1		1		8
TTFM	Prácticas de redacción.	1	1	1		1	1	1	1			1	1	9
TTFM	Selección de las fuentes bibliográficas. // Fuentes de información: búsqueda y selección.	1	1	1	1	1	1	1	1	1			1	10
TTFM	Referencias y Plagio	1	1	1		1	1	1	1				1	8
	TOTALES TTFM	3	3	3	1	3	3	3	3	1		1	3	

ANEXO I

GRILLA DE COMPETENCIAS DEL PERFIL DEL EGRESADO Y ASIGNATURAS QUE LAS CUBREN EN LA CURRICULA

Trabajo Final de Especialización en Evaluación Universitaria (2023)

		ASIGNATURAS QUE LAS CUBREN											
Nro	**COMPETENCIAS**	**CRIPT 1 y 2**	**RED 1 y 2**	**GEST 1 y 2**	**D y PS**	**SSOyA**	**SF**	**AUDIT**	**CO**	**MLEP**	**IF**	**TDCG**	**TTFM**
1	Definir e instrumentar un plan integral de Seguridad Informática de la organización	X	X	X	X	X	X	X	X	X	X	X	X
2	Definir estrategias y políticas de Seguridad Informática	X	X	X	X	X	X	X	X	X	X	X	X
3	Elaborar los planes, programas, procedimientos y normas (seguridad, recuperación de desastres, continuidad de negocios, etc.)	X	X	X	X	X	X	X	X	X	X	X	X
4	Identificar las amenazas y las vulnerabilidades a la que están sujetos organizaciones e individuos, y sugerir y aplicar las medidas de protección adecuadas a cada situación.	X	X	X	X	X	X	X	X	X	X		X
5	Analizar y evaluar los riesgos inherentes al uso de las TIC, su impacto en la estructura organizativa y asesorar en la toma de las decisiones pertinentes.	X	X	X	X	X	X	X	X	X	X	X	X
6	Participar en el diseño de sistemas a efectos de que se consideren los criterios de seguridad apropiados y con sentido económico	X	X	X	X		X	X	X	X	X	X	X
7	Evaluar herramientas y recursos para limitar riesgos, mitigar los efectos de acciones hostiles y poder recuperar la capacidad de operación de las organizaciones	X	X	X	X	X	X	X	X	X	X		X
8	Fortalecer el grado de control interno de las organizaciones mediante la educación y concientización de la problemática de la Seguridad Informática.	X	X	X	X		X	X	X	X	X	X	X
9	Comprender y gestionar tanto los aspectos tecnológicos, humanos, legales y éticos que inciden en la Seguridad Informática	X	X	X	X		X	X	X	X	X	X	X
10	Asumir la responsabilidad máxima en materia de Seguridad Informática en las organizaciones públicas y privadas	X	X	X	X	X		X	X	X	X		
11	Ejercer el asesoramiento y la consultoría en organizaciones públicas y privadas en materia de Seguridad Informática	X	X	X	X	X	X	X	X	X	X	X	X
12	Ejercer la docencia en materia de Seguridad Informática.	X	X	X	X	X		X	X	X	X		X