



## **CARRERA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA Y MAESTRÍA EN SEGURIDAD INFORMÁTICA**

Unidades Académicas de la Universidad de Buenos Aires: Facultades de Ciencias  
Económicas, Ciencias Exactas y Naturales e Ingeniería

### **RAZONES QUE DETERMINAN LA NECESIDAD DE CREACIÓN DEL 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, auditoría, 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.

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.

## **JUSTIFICACIÓN DE LA CARRERA DE ESPECIALIZACION EN SEGURIDAD INFORMÁTICA.**

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 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.

### **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.

### **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.

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.

## **ASIGNATURAS DE LA ESPECIALIZACIÓN**

- Ejes temáticos de la seguridad
- Seguridad en sistemas operativos y aplicaciones
- Seguridad en redes I
- Seguridad en redes II
- Criptografía I
- Documentación y proyectos de seguridad
- Gestión estratégica de la seguridad I
- Comportamiento organizacional
- Marco legal, ética y privacidad

## **ASIGNATURAS ADICIONALES PARA LA MAESTRÍA**

- Criptografía II
- Gestión estratégica de la seguridad II
- Auditoría
- Informática forense y delitos informáticos
- Seminarios I y II

## **CALENDARIO ACADÉMICO PARA EL CUATRIMESTRE 2010**

Preinscripción: 15 de Octubre al 15 de Noviembre de 2009

Reuniones de evaluación de candidatos: **Mes de Noviembre de 2009.**

Inscripción: **15 de Febrero al 10 de Marzo 2010.**

Reuniones de evaluación de candidatos: **a partir de la segunda quincena de febrero 2010.**

Fecha de aceptación: **20 de marzo 2010.**

Inicio de Clases: **30 de Marzo 2010.**

## REQUISITOS PARA EL INGRESO

- Estudios universitarios, o de nivel superior no universitario de cuatro años de duración mínima.
- Antecedentes académicos y/o profesionales vinculados con esta disciplina
- Comprensión de textos escritos en Inglés.
- Presentación y aceptación de la documentación solicitada en el apartado siguiente.
- Aprobar la Entrevista de Admisión.
- Dos cartas de recomendación que avalen antecedentes académicos y/o profesionales.

## DOCUMENTACIÓN A PRESENTAR

- Título original o Certificado de título en trámite en original y fotocopia reducida.
- Documento de identidad.
- Currículum Vitae.
- Foto 4 x 4.
- En el caso de graduados en otros países, presentar adicionalmente Certificado expedido por la Universidad en la que se ha graduado y legalizado por el Consulado Argentino en ese país, que especifique cantidad de años de duración de la carrera. Deberá acompañar asimismo el plan de estudios cursado y aprobado.

## TÍTULOS

**Primer año:** “Especialista en Seguridad Informática”

**Segundo año:** “Magíster en Seguridad Informática”

## METODOLOGÍA DE LA ENSEÑANZA

- Se contemplan Cursos de nivelación y apoyo en Matemáticas, Redes y Sistemas Operativos.
- Asistencia a cursos teórico prácticos.
- Participación en talleres y seminarios.
- Desarrollo de casos de aplicación.
- Actividades prácticas grupales.
- Trabajos de investigación

## TOTAL DE HORAS

**Primer año**, 400 horas totales divididas en:

- 336 hs. presenciales.
- 64 hs. no presenciales destinadas a la elaboración de trabajos prácticos.

**Segundo Año**, 352 horas totales divididas en:

- 162 hs. presenciales
- 30 hs. no presenciales destinadas a la elaboración de trabajos prácticos
- 160 hs. asignadas a la preparación, presentación y defensa oral de la Tesis de Maestría.

**Días y horario de dictado:** cuatrimestres de 16 semanas con tres clases semanales (martes, miércoles de 18:30 a 22 horas y sábados de 10:00 a 13,30 horas).

## CUERPO DOCENTE

- Altmark, Daniel
- Baader, Rodolfo
- Cansler, Leopoldo
- Dams, Alberto
- Hecht, Pedro
- Marrone, Luis
- Pagola, Hugo
- Pataro, Graciela
- Rivas, Ricardo
- Saroka, Raúl
- Schvartstein, Leonardo
- Scolnik, Hugo
- Profesores y Especialistas invitados de relevancia en la temática de seguridad.

### Organizado en forma conjunta por:

Facultades de Ingeniería, de Ciencias Económicas y de Ciencias Exactas y Naturales de la Universidad de Buenos Aires.

**Sede:** La sede Administrativa y Académica del posgrado es la Facultad de Ciencias Económicas (Córdoba 2122 - CABA) y el **dictado de las clases** se realizará en el edificio de la calle Tucumán 3035 - CABA.

**Página web:** <http://www.econ.uba.ar/posgrado>

## COMISION DE COORDINACION

Por la Facultad de Ciencias Económicas: Dres. Raúl Saroka ([rsaroka@econ.uba.ar](mailto:rsaroka@econ.uba.ar)) y Ricardo Rivas ([cesti@econ.uba.ar](mailto:cesti@econ.uba.ar))

Por la Facultad de Ciencias Exactas y Naturales: Dr. Hugo Scolnik ([hugo@dc.uba.ar](mailto:hugo@dc.uba.ar)) y Lic. Graciela Pataro ([gpataro@dc.uba.ar](mailto:gpataro@dc.uba.ar))

Por la Facultad de Ingeniería: Ings. Alberto Dams ([adams@fi.uba.ar](mailto:adams@fi.uba.ar)) y Hugo Pagola ([hpagola@fi.uba.ar](mailto:hpagola@fi.uba.ar))

## **ANEXO I**

### **PLAN DE ESTUDIOS. CONTENIDOS MÍNIMOS. CARRERA DE ESPECIALIZACIÓN**

#### **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.

#### **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.

#### **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.

#### **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.

#### **Seguridad en redes I**

Esquemas de Seguridad: distribución de claves simétricas. Administración de claves públicas: autoridad certificante y certificados. Administración de claves de sesión compartidas. Seguridad de redes e Internet: Single Sign On, Infraestructura de Clave Pública 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.

#### **Seguridad en redes II**

Problemas, amenazas, ataques, defensa y prevención: amenazas pasivas, ataques y códigos maliciosos; defensa y prevención, Intrusion 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.

### **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.

### **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 transfronteriza. Jurisprudencia.

### **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.

### **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 maestría.

## ANEXO II

### PLAN DE ESTUDIOS. CONTENIDOS MÍNIMOS. MAESTRIA

#### **Criptografía II**

Cifradores de bloque en detalle. Criptoanálisis diferencial y lineal. Cifradores de flujo en detalle y números pseudoaleatorios, LFSR. FCSR, NLFSR. Introducción a los generadores pseudoaleatorios caóticos. Ataques de colisiones diferenciales a las funciones Hash. Ataques al RSA: métodos exponenciales y subexponenciales. Ataque al logaritmo discreto: métodos exponenciales y subexponenciales. Contenedores criptográficos portátiles. Protocolos especiales (undeniable signatures, oblivious transfer, electronic cash, etc.). Pruebas de conocimiento cero (ZKP). Criptografía cuántica.

#### **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.

#### **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.

#### **Auditoria**

Control y auditoria. 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.

#### **Seminario I**

Actividades que garanticen el objetivo de realización de la Tesis. Dichas actividades tienen su punto de apoyo en el tema de tesis el cual, trabajado a lo largo de la cursada, irá tomando forma mediante la investigación y análisis realizados. El objetivo es que el maestrando tenga el apoyo necesario para presentar su proyecto y posterior trabajo de tesis.

#### **Seminario II**

Actividades que garanticen el objetivo de realización de la Tesis. Dichas actividades tienen su punto de apoyo en el tema de tesis el cual, trabajado a lo largo de la cursada, irá tomando forma mediante la investigación y análisis realizados. El objetivo es que el maestrando tenga el apoyo necesario para su trabajo de tesis, y que también, obtenga una sólida base respecto a la metodología de investigación.