Experiencias en la enseñanza de Seguridad Informática

Sznek Jorge Eduardo
Departamento de Ciencias de la Computación, Universidad Nacional del Comahue,
Buenos Aires 1400, Neuquén, Argentina
jsznek@uncoma.edu.ar

Resumen:

La dinámica de los cambios tecnológicos ofrece desafíos permanentes para los docentes universitarios de carreras vinculadas a las TIC´s.
La Seguridad Informática es una de las áreas que más evolucionó en los últimos años, en relación directa con el aumento en el uso de las computadoras y las redes de computadoras y de los delitos relacionados con ellas, especialmente delitos cuyo objetivo final es la apropiación de datos en tránsito o contenidos en medios masivos de almacenamiento.
La evolución de la Seguridad Informática se expresa en la propagación de trabajos de investigación, congresos y otros eventos científicos, y en el desarrollo de metodologías, técnicas, procedimientos y herramientas específicas para la protección de la información.
Por tales razones resulta natural considerar a la *Seguridad Informática* como una especialidad en si misma, con aspectos propios y particulares, y por lo tanto digna de ser desarrollada académicamente en una materia específica.
En este trabajo se describen la génesis y evolución de la materia S*eguridad Informática*, entre los años 1999 y 2007, planteada como materia optativa en la currícula de la carrera de Licenciatura en Ciencias de la Computación que se dicta en la Universidad Nacional del Comahue.
Asimismo se destacan las estrategias didácticas implementadas para su dictado y se muestra lo importante que resulta aglutinar en una sola materia específica conceptos vistos en otras materias de la carrera.
Finalmente se enumeran los principales logros obtenidos y se plantean las perspectivas a futuro para la continuidad de esta oferta académica.

Palabras Claves

Area Sistemas, Laboratorio Virtual, Plataforma de Educación a distancia, Redes, Seguridad Informática, Sistemas Operativos, TIC´s.

Introducción

Desde mediados de la década de 1980 la disciplina de *Seguridad Informática* no ha cesado de expandirse y abarcar nuevos y mayores aspectos.
En noviembre del año 1988 hizo su aparición un programa bautizado como "*worm de internet*" [1], que infectó miles de computadoras a través de explotar debilidades existentes en utilitarios de sistemas basados en BSD Unix y de aprovechar potencialidades de la interconexión en red entre diferentes computadoras. Este acontecimiento, que provocó la interrupción de Internet durante varios días, fue el principal impulsor y disparador de varias líneas de investigación en Seguridad Informática: explotación de las debilidades de los sistemas, código malicioso, herramientas para filtrado de flujos de datos, políticas y procedimientos para el intercambio de información, etc.
Desde entonces, la Seguridad Informática no ha cesado de evolucionar, adquiriendo múltiples y variadas facetas.
Una posible definición de la Seguridad Informática puede ser la siguiente: "*un compendio de técnicas, herramientas, especialidades, disciplinas, protocolos, medidas,*

metodologías y normativas que van desde lo más básico de la seguridad física necesaria para proteger a los sistemas informáticos, hasta temas complejos de protocolos criptográficos avanzados, pasando por las políticas y planes de seguridad, legislación, etc" [2]. En otras palabras, puede verse como un conjunto de temáticas interrelacionadas que, integradas, conforman un perfil apropiado para un especialista en Seguridad Informática.

La Licenciatura de Ciencias de la Computación en la Universidad Nacional del Comahue

En el año 1986 la Universidad Nacional del Comahue (UNCo) firmó un convenio con la Universidad Nacional del Sur para el dictado de los tres primeros años de la Licenciatura en Ciencias de la Computación. Esa responsabilidad recayó en un primer momento en el Departamento de Matemática y Estadística, en el cual existía el Área de Informática. En 1989 se crea en la UNCo el título intermedio de Analista en Computación. En 1994 se comienza a dictar el cuarto año de la Licenciatura mediante una ampliación del convenio.

A partir de 1997 se dicta en forma completa la carrera Licenciatura en Ciencias de la Computación en la Universidad Nacional del Comahue. Este logro fue resultado directo del Proyecto FOMEC 493/96 que permitió el doble objetivo de formar recursos humanos propios y dar respuesta a una demanda del medio.

Contenidos de Seguridad Informática en las materias

A medida que se avanza en la currícula de la carrera, cada una de las materias aporta, directa o indirectamente conceptos de Seguridad Informática. A modo de ejemplo se puede mencionar que la materia de 2do. año *Elementos de Programación* incluye el tema de ocultamiento de la información, en su unidad 3, Abstracción de Datos.

Ya más explícitamente aparecen contenidos de Seguridad Informática en los programas de las materias *Organización de Computadoras*, *Teoría y Diseño de Bases de Datos*, *Sistemas Operativos*, y *Redes y Teleprocesamiento*, entre las principales.

Durante el año 1998 se realizó una investigación acerca de las ofertas académicas en Seguridad Informática existentes en diversas universidades del mundo, encontrando materias enfocadas principalmente a la criptografía y a la seguridad en redes. Algunas pocas universidades ya incluían temas más generales como Evaluación de Sistemas Seguros, Código Malicioso, Control de Acceso, etc.

Frente a este panorama y explotando la posibilidad de proponer materias optativas como complementarias a las materias obligatorias de la currícula, es que a fines del año 1998 surgió la iniciativa de dictar una materia dirigida a los alumnos del 5to. Año de la Licenciatura en Ciencias de la Computación.

La materia se designó *Seguridad Informática I*, y se fundamentó en el objetivo de suministrar a los alumnos el conjunto de conceptos básicos que definen a esta disciplina de las Ciencias de la Computación, teniendo en cuenta su creciente importancia día tras día.

Otra motivación para implementar la materia fue que los conceptos de Seguridad Informática se encontraban embebidos en todas las áreas de las Ciencias de la Computación, sin estudiarse en profundidad en ninguna de ellas.

Además se contempló que temas tan importantes como *Evaluación y Gestión de la Seguridad* o *Administración de la Seguridad* formen parte de los contenidos curriculares de la nueva materia, de modo que al culminar sus estudios de grado, los alumnos adquieran conocimientos integrales sobre Seguridad Informática que amalgamen cada uno de los tópicos estudiados en las respectivas materias.

Finalmente se consideró que la inclusión de esos temas en una materia específica iba a resultar de gran importancia en la formación de los futuros profesionales en Ciencias de la Computación que fueran egresando de la UNCo.

Materia Seguridad Informática I

Desde lo programático, la materia implementada se dividió en 3 partes, a saber:

1) Conceptos básicos,
2) Seguridad de Cómputo
3) Seguridad de las Comunicaciones.

Cada una de estas partes, a su vez, se dividió en capítulos que desarrollaban más específicamente los diferentes temas.

De este modo, la primera parte incluía los capítulos:

1) Introducción
2) Evolución histórica de la seguridad informática

La segunda parte incluía los capítulos:

3) Control de acceso
4) Código malicioso
5) Planeamiento y administración de sistemas seguros
6) El Libro Naranja

Y la tercera parte incluía los capítulos:

7) Criptografía
8) Comunicaciones y seguridad de redes
9) Seguridad en Internet
10) Herramientas de seguridad

Como se puede observar, el programa era lo suficientemente amplio y abarcativo dando lugar a la discusión de temas muy actuales al momento del cursado (por ejemplo, código malicioso), pero también muy específico para permitir fijar conceptos básicos como ser los referidos a Control de Acceso (contraseñas, permisos, etc).

La bibliografía inicial se basó en [3], [4] y una serie de papers, artículos y otras publicaciones académicas y científicas.

Características del cursado

El cuadro 1 refleja las características generales de la materia a lo largo del período al que hace referencia este trabajo:

Año	Inscriptos	Aprobaron	Régimen	Requisitos
1999	10	8	Promoción Directa	▪ Desarrollar y exponer 3 monografías ▪ Presentar 1 trabajo final
2000	7	5	Promoción Directa	▪ Desarrollar y exponer 3 monografías ▪ Presentar 1 trabajo final
2001	11	11	Promoción Directa	▪ Desarrollar y exponer 3 monografías ▪ Presentar 1 trabajo final
2002	19	15	Examen Final	▪ Desarrollar y exponer 2 monografías ▪ Rendir 2 parciales múltiple choice
2003	13	11	Examen Final	▪ Desarrollar y exponer 2 monografías ▪ Rendir 2 parciales múltiple choice
2004	12	7	Promoción Directa	▪ Desarrollar y exponer 2 monografías ▪ Realizar 5 TP en linux ▪ Rendir 2 parciales múltiple choice
2005	5	5	Promoción Directa	▪ Desarrollar y exponer 2 monografías ▪ Realizar 5 TP en linux ▪ Rendir 2 parciales múltiple choice
2006	8	5	Promoción Directa	▪ Desarrollar y exponer 2 monografías ▪ Realizar 5 TP en linux ▪ Rendir 2 parciales múltiple choice
2007	8	7	Promoción Directa	▪ Desarrollar y exponer 2 monografías ▪ Realizar 5 TP en linux ▪ Rendir 2 parciales múltiple Choice

Cuadro 1: características grales. del dictado

El cursado consistió en el dictado de clases teórico-prácticas, con 12 horas semanales durante 16 semanas. A partir de 2004 se incorporó el uso de un Laboratorio para el desarrollo de las clases prácticas.

En los siguientes párrafos se hace mención a algunos aspectos particulares dignos de destacar que complementan el cuadro anterior:

- Las monografías fueron individuales, con una extensión no superior a las 10 páginas y debían consistir en la profundización de temas vistos en las clases teóricas.
- Las exposiciones debían reflejar los conceptos desarrollados en las respectivas monografías y demostrar el grado de comprensión de los mismos por parte de los alumnos.
- El trabajo final era individual, basado en una investigación bibliográfica sobre un tema asignado por la cátedra, con una extensión no mayor a 25 páginas y una estructura que debía incluir una sección de resumen, otra de desarrollo, las conclusiones y las referencias bibliográficas.
- Los aspectos que se tuvieron en cuenta en la evaluación del trabajo final fueron:
  - Grado de organización del trabajo;
  - Nivel de profundidad en el tratamiento del tema;
  - Conclusiones;
  - Bibliografía utilizada.
- En el año 2001 se asignó a cada alumno una serie de programas de seguridad. El trabajo final consistió en que cada alumno debía evaluar el conjunto de programas asignado, escribiendo un informe sobre cada uno de ellos. Para esto debían instalarlos y ejecutarlos, analizando su accionar y la eficiencia con que la llevaban adelante. Todos estos programas fueron de características shareware o freeware, y abarcaron temas de control de acceso, criptografía, control de integridad, seguridad en comunicaciones, administración de contraseñas, etc. Esto fue el primer paso dado hacia la incorporación de laboratorios prácticos.
- En el año 2002 se redujo el número de monografías y exposiciones a 2, planteándose además para ser hechas en grupos de 2 ó 3 miembros, poniendo a prueba la habilidad de los alumnos para exponer sus trabajos también en grupo.
- Los parciales, con una modalidad de múltiple choice, abarcaron los temas vistos en la teoría y los temas desarrollados en las monografías. Más adelante, al incorporar los TP, también se incluyeron preguntas sobre estos.
- A partir del año 2002, se aplica un criterio más amplio en la asignación de temas para monografías: esto es que algunos temas no se habían visto en clase, otros apenas se habían mencionado y otros se habían visto un poco más en profundidad; en este último caso, la monografía debía enfocar el tema desde otra óptica y profundizar lo estudiado en clase.
- En el año 2004 se incorporan trabajos prácticos en máquina bajo plataforma linux, asignándose 2 TP para la segunda parte y 3 TP para la tercera parte. La primera parte, al tratarse de conceptos introductorios y aspectos históricos, no incluyó TP en máquina.
- A partir de 2004 se comenzó a utilizar la Plataforma de Educación a Distancia del Comahue (PEDCO) [5] como herramienta de intercambio entre docentes y alumnos.
- A partir del año 2005 los TP se desarrollaron en la plataforma ADIOS [6] en el Laboratorio, facilitando que los alumnos pudiesen realizar sus trabajos prácticos sin necesidad de montar una infraestructura en linux, ya que ADIOS es una distribución en formato *Live CD* basada en Fedora con soporte para LIDS (*Linux Intrusion Detection System*), SELinux (*NSA Security Enhanced Linux*), y máquinas virtuales UML (*User Mode Linux*).
- Los TP desarrollados en ADIOS abarcaron los siguientes tópicos:
  - Seguridad de archivos y administración de usuarios: creación de usuarios y

grupos, asignación de permisos de acceso a directorios, análisis de la fortaleza de las contraseñas y uso de *OpenLDAP* [7] para la validación centralizada de los usuarios.
- Backups y logs: realización de copias de respaldo y recuperación de datos; utilización de los registros del sistema para analizar los eventos que van ocurriendo.
- Servicios, Sniffing y SSH: utilización de herramientas de sniffing para intentar capturar tráfico y detectar contraseñas en sesiones FTP.
- Autenticación con PKI: creación y uso de autoridades de certificación y certificados digitales en sesiones SSL.
- Filtrado: utilización de la herramienta *squid* [8]; implementación de filtrado en firewalls.

Objetivos perseguidos

Seguridad Informática se orientó a alumnos que, a punto de concluir su carrera, tuvieran un interés especial por temas de infraestructura tecnológica, con un fuerte acento en redes y sistemas operativos.

Es por ello que los principales objetivos que se planteó la cátedra con respecto a los alumnos, fueron los siguientes:

- Que adquirieran habilidad en la redacción de papers y publicaciones de carácter académico, desarrollando así su capacidad analítica.
- Que desarrollaran capacidad de síntesis.
- Que fueran capaces de expresarse frente a un auditorio, a través de la exposición de algún tema (en el ejercicio profesional, este tipo de práctica puede resultar habitual al tener que efectuar presentaciones frente a colegas, clientes, superiores, etc.)
- Que fueran capaces de analizar críticamente bibliografía actualizada.
- Que pudieran aplicar los conocimientos adquiridos en sus ámbitos de desempeño laboral.
- Que adquirieran habilidades en el manejo de diversas herramientas de seguridad.

Estrategias didácticas

Para lograr dichos objetivos se aplicaron los siguientes aspectos didácticos:

- Dictado de clases expositivas con una fuerte dosis de interactividad. Esto consistió en ir planteando situaciones y/o interrogantes de los temas estudiados a los efectos de generar debates.
- Producción de monografías: se pensó en que era una adecuada oportunidad para que los alumnos se entrenaran en la escritura de informes con una estructura predeterminada, al estilo de los trabajos que se presentan en eventos científicos y/o académicos.
- Exposiciones: se fundamentó en la posibilidad de entrenar a los alumnos en la presentación de un tema frente a un auditorio, haciendo uso de diapositivas y con un tiempo acotado.
- Laboratorios: como se explicó antes, estos consistieron de trabajos prácticos en ADIOS. La principal motivación del uso de este ambiente fue la posibilidad de recrear situaciones reales pudiendo hacer uso de las herramientas provistas por el ambiente y experimentar sin poner en riesgo equipamiento físico. Se han probado cuestiones tales como husmeo y captura de tráfico (sniffing), fuerza bruta para averiguar contraseñas, uso de certificados digitales para sesiones SSL, filtrado de paquetes mediante el uso de firewalls (iptables), etc.
- Uso de plataforma de educación a distancia: resultó todo un hallazgo para los alumnos poder acceder al sitio de la materia con las novedades, informaciones y materiales para las clases, además de poder recibir y enviar comunicaciones al resto de los integrantes del curso, tanto docentes como alumnos.
- Encuesta a alumnos: como una metodología de mejora continua, año tras año se ha

implementado desde la cátedra una encuesta dirigida a los alumnos con el objeto de recabar inquietudes sobre los diferentes aspectos del cursado.

Uno de los principales pilares de la materia fue la permanente revisión y renovación de los contenidos en concordancia con la dinámica de los cambios tecnológicos. A modo de ejemplos se puede citar que:

- En el curso del año 2000 se trató "el problema del año 2000" desde el punto de vista de la Seguridad Informática.
- Los contenidos del capítulo 6, El Libro Naranja, se fueron reduciendo en forma paulatina y, simultáneamente, añadiendo conceptos de otros sistemas de evaluación tales como ITSEC (Information Technology Security Evaluation Criteria) y CC (Common Criteria).
- A partir de 2004 se dio un fuerte impulso en el temario a Gestión de la Seguridad, tomando como referencia la norma ISO/IEC 17799 [9].
- También en 2004 se incluyó en el temario el análisis de AES (Advanced Encryption Standard) como estándar criptográfico de clave privada en reemplazo de DES (Data Encryption Standard).
- En 2005 se agregó al temario el estudio de Computación Forense aplicada al análisis de eventos de seguridad.
- En ese mismo año se añadió el estudio de *honeypots* y *honeynets* [10] como herramientas facilitadoras de la detección de intrusiones.

Resultados observados

Del análisis de la experiencia realizada durante los años 1999 a 2007, se desprenden los siguientes resultados:

- Según el cuadro 1, casi el 80% de los alumnos han superado exitosamente la materia. El 20% restante, en su mayoría corresponden a alumnos que han abandonado sus estudios.
- Creciente interés por parte de los alumnos que debían elegir sus materias optativas (de hecho, se recibieron innumerables consultas sobre los requisitos necesarios para cursarla, lo que evidenció lo acertado de la iniciativa de ofertar esta materia y proporcionó estímulos a la cátedra para revisar y renovar los contenidos y metodologías empleados).
- Aceptación de los planteos de la materia, tanto en la metodología de evaluación como en los temas desarrollados, aspectos que surgen del análisis de los resultados de las encuestas anuales.
- Compromiso de los alumnos con sus compañeros en presenciar las exposiciones, participando activamente de las mismas.
- Muchos de los alumnos que cursaron *Seguridad Informática* luego continuaron con *Sistemas Distribuidos* como segunda materia optativa, completando así una "especialización" en el área Sistemas del Departamento de Ciencias de la Computación.
- Varios de los alumnos posteriormente desarrollaron su tesis de grado en temas de Seguridad Informática o en Redes de Computadoras. Un listado de las tesis en Seguridad Informática es el siguiente:
  - Control de Acceso Basado en Roles. Alumnos: Cassolini, R. – Domínguez, G.
  - Criptografía. Alumnos: Rozas, C. – Bianchini, G.
  - Ataques TCP/IP. Alumno: Hanzich, M.
  - Infraestructura de Clave Pública y Firma Digital. Alumnos: Dolan, C. – Croceri, N.
  - Seguridad en Mensajería Instantánea. Alumno: Sagripanti, M.
  - Autenticación por reconocimiento de voz. Alumnos: Santos, V. – Martín, D.
  - Autenticación por reconocimiento facial. Alumnos: Rozzisi, M. – Forquera, J.
  - Implementación de una Honeynet virtual para el estudio del comportamiento de intrusos. Alumno: Fernández, H.
  - Control de Acceso basado en roles para

web. Alumno: Salcedo, M.

- Satisfacción de los alumnos que pudieron aplicar rápidamente los conceptos estudiados en sus ámbitos de desempeño laboral.

Otros aspectos

- Se impulsó la publicación de monografías en CRIPTORED [11], sitio dedicado a establecer una red académica en Seguridad Informática, lo que representó un estímulo para los alumnos al ver sus trabajos en Internet y que los mismos sean leídos y consultados por miles de personas.
- Otro logro adicional, en especial para el Departamento de Ciencias de la Computación fue que, a raíz de la inclusión en CRIPTORED del docente a cargo de la materia, se establecieron contactos con otras universidades públicas del país y se colaboró en la formulación de materias específicas; al respecto se puede mencionar a:
  - UBA: colaboración con el Lic. Rodolfo Baader en la materia optativa *Seguridad de la Información* de la carrera de Licenciatura en Ciencias de la Computación.
  - UTN regional San Francisco: colaboración con el Ing. Mauro Graziozi en la materia optativa *Seguridad de la Información* de la carrera de Ingeniería en Sistemas de Información.

Perspectivas

Considerando la experiencia altamente exitosa, se plantea la perspectiva de cómo continuar evolucionando. Al respecto es posible optar por los siguientes posibles caminos:

1) Continuar básicamente con la misma modalidad, actualizando año tras año los contenidos y las herramientas usadas en los laboratorios.

2) Reformular el plan de la materia dirigiendo los contenidos hacia temas más específicos como ser Gestión de la Seguridad, Criptografía, Seguridad en Redes, etc.
   Esta estrategia apunta a crear nuevas materias optativas complementarias de *Seguridad Informática* y fuertemente ligadas a una especialización de los egresados en temas de TIC´s.

Adicionalmente, se debe continuar promoviendo la realización de tesis de grado y estimular la producción de trabajos académicos, integrando a los alumnos en los diferentes proyectos que encara el Departamento de Ciencias de la Computación.

Conclusiones

Varios son los puntos que se pueden mencionar a modo de conclusiones:

- La aceptación de la materia fue muy buena, más aún considerando que en diferentes años hubo oferta de otras materias optativas, las que en muchos casos no pudieron siquiera dictarse por no contar con alumnos interesados.
- Muchos de los alumnos que cursaron *Seguridad Informática* optaron por esta rama de la computación para su desempeño profesional.
- La materia fue especialmente útil para "cerrar el círculo" entre todas las demás materias de la carrera en donde se trataron temas inherentes a la seguridad informática.
- La continuidad en el tiempo permitió ir modificando los contenidos adaptándolos a temas de mayor vigencia o que representaban avances tecnológicos.
- Las estrategias didácticas y los recursos empleados en el dictado de la materia demostraron ser correctos, con una muy buena aceptación por parte del alumnado.

Como conclusión general, se puede afirmar que el dictado de Seguridad Informática resultó un acierto del Departamento de Ciencias de la Computación, apostando con ello a la

producción de profesionales con una adecuada formación y conocimiento de los temas tecnológicos de actualidad.

Bibliografía

[1] The Internet Worm Program: An Analysis. Eugene H. Spafford, Purdue Technical Report CSD-TR-823, November 1988.
[2] Formación en seguridad informática: El reto educacional de esta década. Jorge Ramió Aguirre, Asociación Colombiana de Ingenieros de Sistemas (ACIS), 2006.
[3] Computer Security Basics. D. Russel and G. Gangemi, O'Reilly and Associates.1991,
[4] Trusted Computer System Evaluation Criteria ("Orange Book"). Department of Defense, USA.
[5] http://pedco.uncoma.edu.ar/
[6] http://os.cqu.edu.au/adios/
[7] http://www.openldap.org/doc/admin23/quickstart.html
[8] http://www.squid-cache.org/
[9] http://www.iso.org/iso/catalogue_detail?csnumber=33441
[10] The Honeynet Proyect: www.**honeynet**.org/
[11] http://www.criptored.upm.es