FORMACIÓN DOCENTE EN SEGURIDAD TIC: CUESTIONES PENDIENTES

Ernesto E. Zianni*, Andrea F. Nessier**

SÍNTESIS: El uso masivo de las tecnologías de la información y la comunicación (TIC) ha traído consigo una consecuencia sobre la que los sistemas educativos no pueden mantenerse al margen: la cuestión de la seguridad informática. En el presente trabajo se fundamenta la necesidad de incorporar esa temática no solo en la formación docente sino también en los últimos tramos de la educación media, teniendo en cuenta que muchos estudiantes se incorporan al mercado laboral apenas finalizada esa etapa educativa.

Dicha formación, para constituirse en una verdadera herramienta, debería llevarse adelante en dos instancias: la toma de conciencia y la capacitación. En este sentido, se describe en este artículo una experiencia desarrollada con estudiantes del ciclo básico universitario, en la que se les provee la información adecuada para que adviertan que la seguridad informática se vincula con la mayor parte de sus actividades, no solo estudiantiles o laborales, sino también personales.

Palabras clave: seguridad TIC; formación docente; mercado laboral.

FORMAÇÃO DOCENTE EM SEGURANÇA TICS: PENDÊNCIAS

SÍNTESE: O uso massivo das tecnologias da informação e da comunicação (TICs) trouxe consigo como consequência que os sistemas educativos não podem se manter à margem: a questão da segurança informática. No presente trabalho fundamenta-se a necessidade de incorporar essa temática não somente na formação docente como também na última etapa da educação média, tendo em conta que muitos estudantes se incorporam ao mercado de trabalho assim que finaliza essa etapa educativa.

Esta formação, para constituir-se numa verdadeira ferramenta, deveria ser levada adiante em dois níveis: a tomada de consciência e a capacitação. Neste sentido, menciona-se neste artigo uma experiência desenvolvida com estudantes do ciclo básico universitário, na qual se lhes provê da informação adequada para que percebam que a segurança informática

* Docente Titular del Área Informática de la Facultad de Ciencias Económicas, Universidad Nacional del Litoral, Santa Fe, Argentina.

** Docente Adjunta del Área Informática de la Facultad de Ciencias Económicas, Universidad Nacional del Litoral, Santa Fe, Argentina.

Artículo recibido: 27/02/14; evaluado: 06/03/14 - 12/05/14; aceptado: 19/05/14

está vinculada à maior parte de suas atividades, não só estudantis ou trabalhistas, como também pessoais.

Palavras-chave: segurança TICs; formação docente; mercado de trabalho.

TEACHER TRAINING IN ICT SECURITY: OUTSTANDING ISSUES

ABSTRACT: The massive use of information and communication technologies (ICT) has brought about a result to which educational systems cannot stand on the sidelines: the question of computer security. The present work is based upon the need to incorporate this theme not only in the teacher training but also in the last stages of secondary education, taking into account that many students are early incorporated into the labour market after that educational stage.

Such training, to become a real tool, should be pursued in two instances: awareness and training.

In this sense, it's mentioned in this article an experience developed with students of the basic university cycle, which provides them with the appropriate information to warn that the computer security is linked with the greater part of its activities not only student or labour but also personal.

Keywords: ICT; security; teacher training; labour market.

1. INTRODUCCIÓN

Los currículos actuales de la educación secundaria en Argentina no incluyen la informática entre sus asignaturas, con excepción de los bachilleres especializados. En lugar de esto, los docentes de los trayectos de tecnologías de información y comunicación (TIC) están siendo «reubicados» con el fin de conformar «parejas pedagógicas» con los profesores de otras asignaturas, de modo tal que hagan su aporte en la utilización de TIC para la enseñanza de la disciplina de que se trate. Esta situación contrasta con las iniciativas de otros países que, por ejemplo, buscan incorporar la enseñanza de la programación incluso desde el nivel primario.

Como docentes del área de las TIC en el ciclo básico de las carreras universitarias, entendemos que la informática debe cruzar transversalmente los currículos –en ambos niveles de formación–, y ser utilizada en las demás asignaturas. Pero su uso no debe limitarse a contribuir a la enseñanza de otras materias, pues como disciplina tiene contenidos propios que requieren de un espacio curricular específico, además de docentes identificados con dicha área.

La incorporación de las tecnologías informáticas ha significado un adelanto incuestionable, pero también su uso inadecuado ha introducido manifestaciones inapropiadas para la sociedad. En este aspecto, resulta clave

inculcar en los jóvenes que la tecnología no garantiza por sí sola la seguridad de nuestros ordenadores, sino que depende también del comportamiento de los usuarios.

Hemos comprobado el impacto que genera en los alumnos universitarios una falsa sensación de seguridad, que proviene de una sobrevaloración de las soluciones técnicas y medidas automatizadas, en detrimento de la participación activa de los usuarios, cuyos comportamientos son los que en muchos casos gatillan los riesgos, de manera consciente o inconsciente, por acción o por omisión.

La única manera de contrarrestar esto es mediante la formación. En este sentido, es preciso desarrollar un entendimiento temprano y una suficiente conciencia de esta problemática, quitándole el tinte tecnológico y realzando la importancia del papel que juegan las personas al momento de preservar la seguridad de la información. Por tanto, la escuela debe constituirse en el primer peldaño de esa formación.

Al educar a los alumnos en esta temática, es importante diferenciar los distintos niveles escolares. En el caso de los menores, sabemos que la responsabilidad sobre las buenas prácticas no recae solo en los educadores sino también en los padres, y reconocemos que las instituciones educativas se han comprometido seriamente, a través acciones preventivas y de concientización, para evitar y combatir situaciones de *cyberbullying, sexting* y *grooming,* entre otras.

Ahora bien, en esta oportunidad proponemos reflexionar sobre la necesidad actual de educar a los jóvenes que se encuentran en el último tramo de la escuela secundaria, con posibilidades de insertarse a corto plazo en el mercado laboral, en las buenas conductas y prácticas en el uso de las tecnologías informáticas, desde una perspectiva más cercana al mundo del trabajo, para permitirles adquirir competencias vinculadas a la protección de datos, navegación segura y aspectos legales del uso de las TIC.

Es necesario que los alumnos del último año de la escuela media, quizás próximos a ocupar puestos de trabajo que seguramente demandarán el uso de sistemas informáticos, estén conscientes de que los usuarios representan el eslabón más débil de la cadena de seguridad. Para ello, el aspecto educativo es esencial, dado que por mucho que se planifiquen los diferentes aspectos de la seguridad, es preciso confiar en las personas.

2. ÁREAS DE VACANCIA EN LA FORMACIÓN DOCENTE EN TIC

Las redes sociales forman parte de los hábitos cotidianos de navegación de los alumnos, siendo la mayoría de las veces el principal motivo por el que se conectan a internet, y es innegable el beneficio que ellas pueden aportar en el campo de la educación, para la creación y distribución de contenidos por parte de los estudiantes.

El mercado laboral no ha quedado al margen de esta tendencia; hay estudios que demuestran que las empresas, como parte del proceso de selección de nuevos empleados, investigan en las redes sociales los perfiles de los candidatos, y que ciertas conductas, lenguajes, opiniones, fotos y hasta características como escribir con faltas de ortografía, pueden devenir en valoraciones negativas que obstaculicen el acceso al puesto de trabajo en cuestión. Esto es así porque nuestras opiniones reflejan nuestra forma de pensar; por lo tanto, debemos asegurarnos que estén en consonancia con la manera en que deseamos ser valorados. Así, los alumnos deben comprender que los límites entre la información profesional o laboral y la información personal no siempre son claros, y que configurar dicha información para que esté disponible «solo para amigos», no significa que estará segura.

Por otro lado, las amenazas de seguridad dejaron de ser exclusivas para las computadoras y se han trasladado a los teléfonos celulares y *tablets,* desde los cuales se tiene acceso directo al correo electrónico, las redes sociales y el *chat,* sin contar con que también se realizan operaciones bancarias que, por lo general, no incluyen medidas de protección. De manera que la información de los contactos, los correos, las conversaciones, los mensajes de texto, las fotos, etc., son susceptibles de ser «atacadas». Además, los dispositivos móviles permiten conciliar la vida personal con el entorno laboral, y si vinculamos esto con la creciente aparición de amenazas para sistemas Android (principalmente) y plataformas sociales, se acentúa la necesidad de aumentar los esfuerzos en la educación de los alumnos.

Otra amenaza muy difundida para el robo de identidad es el *phishing,* que requiere de una participación activa por parte del usuario, ya que es él mismo quien brinda información sensible a sitios que no son apropiados para ello. La mejor forma de evitar este fraude es estar prevenidos y capacitados sobre cómo operan los sitios que intentan capturar nuestros datos (y muchas veces lo consiguen).

Estas tres situaciones, mencionadas como ejemplo, brindan la posibilidad de abordar con los estudiantes contenidos referidos a cómo detectar sitios *web* fraudulentos; cómo identificar un sitio *web* seguro para ingresar datos confidenciales; cómo cifrar archivos y mensajes; cómo admi-

nistrar filtros de correo electrónico para disminuir los correos no deseados; cómo administrar nuestras claves de acceso a los distintos servicios; cómo borrar nuestras *huellas* cuando navegamos; cuáles son las medidas básicas de prevención básicas que debemos tomar al acceder a internet desde una máquina pública; cómo salvaguardar información; cuáles son las aplicaciones de seguridad específicas para dispositivos móviles, etcétera.

Sin duda que los docentes, con independencia de su orientación, se han ido capacitando para incorporar las TIC en sus actividades escolares, tanto en el uso de plataformas virtuales, búsquedas en internet, herramientas ofimáticas y aplicaciones específicas, o en su defecto han conformado «parejas pedagógicas» con docentes de formación más tecnológica. No obstante, respecto de la seguridad de la información, entendemos que nos encontraríamos con dificultades, incluso en los casos de docentes formados en herramientas como las mencionadas, por lo cual se impondría diagramar un plan de formación específico, no con el objetivo de que los docentes sean expertos en seguridad informática sino brindándoles la capacitación adecuada para que en su quehacer cotidiano puedan tomar decisiones apropiadas en este aspecto.

3. UNA ESTRATEGIA QUE HA DADO BUENOS RESULTADOS

Consideramos que las escuelas están en condiciones de trabajar la seguridad de la información dándole un *enfoque organizacional* y vinculado al mundo del trabajo, a partir de la gran cantidad de información confidencial que mantienen en sus registros, tanto de docentes como de alumnos, y el aumento en la conectividad de sus equipos. Simplemente utilizando a la propia institución como ejemplo de las consecuencias que ocasionaría una intrusión en sus sistemas, puede justificarse que cada integrante de la comunidad educativa con acceso al sistema de información de la institución reciba una formación en el área de seguridad, desde dos aspectos: el uso del sistema y su responsabilidad para contribuir a la seguridad del mismo.

Los docentes del área de tecnología de escuelas secundarias, al igual que el resto de los profesores de todos los niveles educativos, deben tener una formación que incluya, además del conocimiento en lo disciplinar, otros saberes, habilidades y actitudes profesionales para estimular y motivar el aprendizaje de los alumnos.

La necesidad de *seducir* al alumno captando su atención para hacer óptimo el proceso de enseñanza / aprendizaje se hace más notoria cuando se trata de conocimientos que serán requeridos para desempeñarse

en el mercado laboral, dado que los estudiantes sienten esa etapa como muy lejana, a pesar de que muchos de ellos, por elección o necesidad, accederán a un puesto de trabajo apenas egresen de la escuela media.

La propuesta metodológica que ha madurado en los últimos años para abordar el tema de la seguridad en la información consiste en una selección de noticias de actualidad de revistas y diarios de difusión masiva, referidas a intrusiones a sistemas, robo de información, falencias detectadas en plataformas sociales, etc., que les resulten familiares a los alumnos. Así, y a partir de los disparadores adecuados, se despierta el interés personal de los estudiantes y se los invita a reflexionar, apuntando al primer objetivo que debe perseguirse en este estadio educativo: *concientizar* al alumno sobre la problemática, buscando modificar percepciones y analizando *por qué* y *para qué* es necesario tener buenas prácticas de seguridad de la información.

A partir de allí, la estrategia estimula el pensamiento, la búsqueda de razones y la propuesta de soluciones, dando lugar a la etapa de *capacitación*, que se refiere a *cómo* proteger la información. De esta manera se favorece la comprensión del tema, conformando un entorno de aprendizaje constructivista que nos ha garantizado el cumplimiento de los objetivos propuestos y permitido estructurar la enseñanza de los contenidos con alumnos de un ciclo básico. Debido a la naturaleza de este artículo, no abordamos en detalle la estrategia utilizada.

4. CONCLUSIONES

Vivimos inmersos en un ecosistema digital (*e-mail,* dispositivos móviles, redes sociales, compras por internet, etc.) que nos reporta grandes beneficios en tareas habituales, tanto laborales como sociales, pero que al mismo tiempo nos expone a una cantidad de creciente riesgos, lo cual torna imprescindible que el usuario promedio desarrolle algunas habilidades que le permitan adquirir una conducta adecuada y segura al momento de utilizar las TIC.

La falta de conocimiento constituye una de las vulnerabilidades que los intrusos han sabido explotar, y dada la incidencia del factor humano en los problemas de seguridad, el aspecto educativo es esencial para conservar el control.

Esta educación no debe basarse solo en explicaciones técnicas, sino que debe integrar conocimientos, habilidades y conductas para generar conciencia del impacto de las amenazas sobre las organizaciones, la sociedad

y las personas. Además, si solo nos limitamos a imponer estos contenidos –que no vislumbramos que puedan transversalizarse– como obligatorios, sin desarrollar una campaña de sensibilización frente a la temática, los resultados no serán los deseados. El punto de partida de este proceso, entonces, debe ser la escuela; y la formación de los educadores, el primer paso.

BIBLIOGRAFÍA

FAERMAN, Juan (2009). *Faceboom. El nuevo fenómeno de masas Facebook.* Ediciones B.

RAMIÓ AGUIRRE, Jorge (2004). «Formación en seguridad informática: El reto educacional de esta década». Universidad Politécnica de Madrid, España. Disponible en: www.criptored.upm.es/guiateoria/gt_m001i.htm.

RODRÍGUEZ CUERVO, Alejandro (2010). «La seguridad informática. Una necesidad en la docencia universitaria». *Revista Iplac,* n.° 1. Disponible en: www.revista.iplac.rimed.cu/index.php?option=com_content&view=article&id=108:la-seguridad-informca&catid=17&Itemid=213.

SALAZAR PEÑA, Mikel (2006). «¿Cómo afectará la convergencia de educación a la seguridad?» *Revista Dintel,* n.° 3. Disponible en: www.revistadintel.es/Revista1/Num3suplemento/tribuna/Mikel.pdf.