Favorecer el desarrollo de actitudes y promover buenas prácticas en Seguridad de la Información. El método de casos como recurso motivacional

Zianni Ernesto E.
Prof. Titular Cátedra de Informática - Facultad de Ciencias Económicas -UNL
ezianni@fce.unl.edu.ar

Nessier Andrea F.
Prof. Adjunta Cátedra de Informática- Facultad de Ciencias Económicas - UNL
anessier@fce.unl.edu.ar

Resumen

Ante la masiva y creciente adhesión en el uso de las Tecnologías de la Información y Comunicación (TICs), y frente a las consecuencias de un uso inadecuado de las mismas, resulta clave inculcar en las nuevas generaciones que la tecnología no puede garantizar por sí sola la seguridad de nuestros ordenadores, la cual depende también del comportamiento de los usuarios.

En ámbitos laborales comienzan a valorar poseer conocimientos que eviten incidentes de seguridad en la operativa de las empresas. Estas generaciones han nacido bajo el "paraguas" de las tecnologías IT, operando con ellas con total naturalidad pero sin ser conscientes de los riesgos inherentes y en este sentido creemos que debe lograrse un entendimiento temprano y conciencia de esta problemática realzando la importancia de las personas frente a la tecnología al momento de preservar la seguridad de la información.

En relación a ello, la educación debe promover el desarrollo de habilidades y competencias para hacer frente al mal uso de las tecnologías informáticas. El presente trabajo describe una estrategia para abordar la problemática de la enseñanza de la seguridad informática con alumnos del ciclo básico de la Universidad; vista como un aspecto esencial del mejoramiento profesional y humano de los usuarios de TICs y como una necesidad emergente en los saberes y formas de actuar de los usuarios en la sociedad actual y futura.

Palabras clave: Seguridad Informática – Uso responsable de TICs – Universidad – Casos

Consideraciones sobre la enseñanza de la Seguridad Informática en la Educación Superior

La inserción de la Informática en el Currículo

La capacidad de pensar reflexivamente es una competencia deseable para cualquier profesional a la hora de tomar decisiones fundadas, y en nuestra asignatura, Informática, ubicada en el ciclo Básico de las carreras de la Facultad de Ciencias Económicas, nos hemos propuesto incentivar el desarrollo de esta competencia, iniciando este desafío en una de las áreas temáticas de mayor relevancia correspondiente a una de las unidades del programa: la Seguridad de la Información.

Desde un punto de vista curricular, una Informática ubicada en el Ciclo Básico de una carrera Universitaria, debe servir de soporte al resto de las asignaturas pero por otro lado la Informática se ha convertido en un instrumento social debido a la masificación del uso de dispositivos electrónicos (computadoras, Tablet, teléfonos celulares) en casi todos los órdenes de la vida económica y social y cuyo impacto hace cada vez más difícil que podamos actuar eficientemente prescindiendo de ellas.

Por tal motivo se comparte la idea de que nuestros alumnos no sean considerados

solamente desde un punto de vista laboral sino que, por el contrario, se observe la pertinencia de una perspectiva social y que nuestras acciones - como docentes en el área de las Tecnologías de la Información - sean llevadas por los alumnos a sus hogares y al medio que los rodea.

Se sabe que los beneficios que aportan las tecnologías son mayores que los riesgos asociados, y por lo tanto el objetivo radica en conocer cuáles son sus riesgos potenciales con el objetivo de minimizarlos mediante el establecimiento de acciones educativas que permitan concientizar y prevenir a los usuarios como punto de partida para la educación en Seguridad Informática.

Este primer nivel de formación debe ser incorporado con un enfoque de sistema, integrando conocimientos, habilidades y conductas dado que todo usuario de un sistema debe recibir una educación en seguridad informática considerando dos aspectos: el uso del sistema y su responsabilidad por contribuir a la seguridad del mismo.

Lo mismo que ocurre en las empresas al implementar Políticas de Seguridad ocurre con los contenidos de esta temática dentro del trayecto educativo: si solo nos limitamos a imponerlos como contenidos obligatorios sin desarrollar una "campaña de sensibilización" frente a la temática, los resultados no serán los deseados.

Asimismo consideramos la necesidad de plantear el tema de la Seguridad Informática en varias etapas, y desde esa perspectiva reconocemos el trabajo que se realiza desde los establecimientos educativos desde muy corta edad (nivel inicial, primario y secundario) en temas como el cyberbullying, grooming y sexting.

Pero creemos que la seguridad informática debe abordar, en los últimos años del estadío escolar, aspectos vinculados a la protección de datos e información, para continuar el abordaje de estos temas en el ciclo básico de las carreras Universitarias con alumnos que aún están transcurriendo una etapa de inserción a la vida universitaria, recontextualizando sus métodos de estudio y sus modos de afiliación, de manera de lograr:

- Evidenciar la vigencia de la problemática y desarrollar un entendimiento temprano de su incidencia como pieza fundamental en el entramado empresarial y su relación con el resto de las actividades de las personas, para posibilitar abordar en el ciclo superior temáticas tales como políticas de seguridad, planes de contingencia, normas y estándares de seguridad, análisis de riesgos, registros de auditoría, trazabilidad de acciones, etc., que no hacen más que fortalecer la vinculación entre la seguridad y la continuidad del negocio.

- Poner de manifiesto que los usuarios representan el eslabón más débil de la cadena de seguridad y que el perfil de las amenazas ha ido cambiando. La técnica de ataque más perfeccionada en los últimos tiempos se basa en acceder a información a partir de las personas vinculadas al sistema, valiéndose de engaños, y la tecnología no puede protegernos de eso.

- Promover formas de actuación frente a determinadas manifestaciones que podrían generar el mal uso de las tecnologías informáticas y las redes. Con los alumnos que recibimos en la Universidad, "hemos podido comprobar el impacto que genera una falsa sensación de seguridad a partir de una sobrevaloración de las soluciones técnicas y medidas automatizadas en detrimento de una 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" (Zianni, Nessier, 2014:129), y la **única manera de evitarlo es la formación.**

Los alumnos que recibimos: sus hábitos y preferencias en el uso de Tecnología

Sabemos que los adolescentes tienden a transgredir normas existentes en distintos

ámbitos de la vida, como propio proceso de autoafirmación y esta actitud se extiende al campo de la seguridad de la Información ya que comprobamos que gran parte de los alumnos que recibimos en la Universidad tienen poca conciencia sobre las medidas de seguridad en el mundo digital, por lo cual creemos ampliamente justificada nuestra preocupación por encontrar una estrategia de intervención para sensibilizar, elevar la motivación y favorecer el desarrollo de actitudes hacia una cultura de la seguridad de la información en virtud de la creciente relevancia social del tema de la Seguridad en el uso de las Tecnologías de la Información en la vida cotidiana de las personas y organizaciones. Por otro lado, dentro de las áreas de actuación futura de los alumnos, la protección de la información es un territorio donde la capacidad de actuar responsablemente es cada vez más apreciada por los empleadores.

Por la ubicación de nuestra asignatura en el currículo, el aprendizaje se ve seriamente influenciado por la dificultad de asociar los conceptos teóricos que se explican en el aula con la vida real de una organización como consecuencia de la falta de experiencia laboral de nuestros alumnos. Esto acrecienta la actitud pasiva hacia el aprendizaje a la que están acostumbradas e imponen una metodología centrada en la figura del profesor y en su forma de exponer y presentar los contenidos.

Las **redes sociales** son parte de los hábitos cotidianos de navegación de nuestros alumnos, convirtiéndose la mayoría de las veces en el principal motivo para conectarse a Internet. Asimismo no pueden negarse los beneficios que pueden aportar en el campo de la educación para la creación y distribución de contenidos por parte del alumnado.

El mercado laboral no ha quedado al margen de esta tendencia y 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, por lo cual ciertas conductas, lenguajes, opiniones, fotos, y hasta faltas de ortografía, pueden traducirse en valoraciones negativas que obstaculicen el acceso a los puestos de trabajo ofrecidos. Nuestras opiniones reflejan nuestra forma de pensar y debemos asegurarnos que estén en consonancia con la manera en que deseamos ser valorados. Por lo tanto, los alumnos deben comprender que muchas veces los límites entre la información profesional/laboral y la personal no siempre son claros y que aunque configuremos que dicha información "sólo quede disponible para mis 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 Tablet, desde los cuales se tiene acceso directo al email, a los perfiles de las redes sociales, al chat como así también se realizan operaciones bancarias y por lo general no incluyen medidas de protección.

De manera que la información de los contactos, los correos, las conversaciones de chat, los mensajes de texto, las fotos, etc. son susceptibles de ser "atacadas". Los dispositivos móviles permiten conciliar la vida personal con el entorno laboral y si eso lo vinculamos con la creciente aparición de amenazas para sistemas Android (principalmente) y para plataformas sociales, pone de manifiesto la obligación de aumentar los esfuerzos en la educación de los alumnos.

Otra amenaza muy difundida para el robo de identidad es el **Phishing**. En la misma se requiere de una participación activa por parte del usuario ya que es él mismo quien brinda información sensible en sitios que no son apropiados para hacerlo.

La mejor forma para evitar este fraude es estar prevenidos y capacitados sobre cómo operan los sitios que intentan capturar nuestros datos y muchas veces lo consiguen.

Estas situaciones mencionadas como ejemplo, posibilitarían 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 administrar 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, cuales son las medidas de prevención básicas cuando accedemos a Internet desde una máquina pública, cómo salvaguardar información, aplicaciones de seguridad específicas para dispositivos móviles, entre otros.

La estrategia que nos ha dado buenos resultados

Fundamentos y actividades

En la teoría del constructivismo el aprendizaje es una actividad social en la cual los alumnos al relacionarse, dialogar, observar y/o escuchar a otro, aprenden y ponen en juego competencias necesarias no solo para su transitar Universitario sino también para la vida laboral. (Rosas, Sebastián, 2001).

Desde nuestro lugar como docentes, sabemos que el recurso quizás más utilizado para promover el aprendizaje de esas competencias es el trabajo en grupo. Pero, como ya hemos destacado, en los cursos del ciclo básico, ya sea por la cantidad de alumnos como por una tradición educativa de centrar el aprendizaje en la figura del profesor, lograr una participación fluida de los alumnos no resulta una tarea fácil.

Tal como se menciona en el artículo publicado en la Revista Iberoamericana de Educación "Formación Docente en Seguridad TIC: cuestiones pendientes" (Zianni, Nessier, 2014:132), la propuesta metodológica que ha madurado en estos últimos años desde su implementación para abordar el tema de la Seguridad de la Información se basa en una selección adecuada de noticias de actualidad que continuamente encontramos en revistas y diarios de difusión masiva (intrusiones a sistemas, robo de información, falencias detectadas en plataformas sociales, etc.) que al vincularse a situaciones que les resultan familiares a los alumnos, y a partir de los disparadores adecuados, despiertan el interés personal de los estudiantes y los invita a reflexionar, apuntando al primer objetivo que perseguimos a esta altura de la carrera: **concientizar** al alumno sobre la problemática, buscando modificar percepciones y analizando el **¿por qué?** y el **¿para qué?** tener buenas prácticas de seguridad de la información.

A partir de allí la estrategia estimula el pensamiento, la búsqueda de razones y propuesta de soluciones, dando lugar a la etapa de la **capacitación**, que se encargará del **¿cómo?** proteger la información.

Desde ya que el papel desempeñado por los estudiantes condiciona la clase de actividades mentales comprometidas en la práctica educativa y tal como plantea Berlyne (1960) favorecer la curiosidad de los alumnos haciéndoles preguntas en lugar de presentarles información sobre los hechos nos ha garantizado aumentar el interés en aprender más sobre el tema.

Las acciones que proponemos se encuadran dentro de la estrategia del método de casos, a partir de situaciones reales de ataques a la seguridad en internet, sobre las que se debate para elaborar conclusiones y una especie de guía de recomendaciones.

Los casos que se seleccionen deben proporcionar datos concretos para reflexionar, analizar y debatir en grupo, suscitando polémica a partir de posiciones encontradas y de esta forma favorecer un aprendizaje activo y colaborativo, centrado en un diálogo democrático.

Las actividades que se han venido estructurando son:

- Presentación y descripción de situaciones problemáticas referidas a incidentes de seguridad informática para establecer la preocupación existente por la temática.
- Indagar de qué manera perciben nuestros alumnos los peligros de Internet

Caso 1: Noticias de actualidad que pongan en evidencia la preocupación existente en el tema de Seguridad Informática.

Figura 1. Recuperado de http://www.telam.com.ar/notas/201410/83157-ciberseguridad-empresas-kaspersky-ataque.html

Caso 2: incidente de seguridad de gran repercusión que respalda que todos podemos ser blanco de las amenazas.

Figura 2. Recuperado de http://www.infobae.com/2012/12/28/688836-como-se-filtro-el-video-florencia-pena

Muchos usuarios tienen la percepción que tecnologías como el antivirus y el firewall son suficientes para protegerse contra cualquier amenaza. Noticias como ésta presentan datos relevantes que muestran que la realidad es que muchas empresas sufren fallas o ataques a sus sistemas y que los usuarios deben asumir que pueden ser víctimas de diferentes amenazas, incluso sin saberlo.

Este reconocimiento constituye el primer paso de madurez para adquirir una correcta cultura de seguridad a través de la formación y la información en el ámbito personal, profesional y educativo

- A qué considera "problemas de seguridad informática" en una empresa? ¿Cuáles serían las consecuencias en cada uno de los problemas planteados?
- ¿Conocen a alguna empresa que haya sufrido intrusiones en su sistema?
- ¿Han intentado acceder al sitio web de una empresa y no pudieron? ¿Qué error les reportó? ¿a qué puede deberse?
- ¿Cómo podrían continuar sus actividades las empresas que vieron alterados sus datos?

Este tipo de casos de amplia difusión mediática permite respaldar el concepto de que todos podemos ser el blanco de una amenaza informática y sufrir un incidente sobre la información que almacenamos puede ser grave, tanto en términos hogareños como corporativos.

Las computadoras no solo son herramientas de uso cotidiano para las empresas, sino también para las familias y por lo tanto la adopción de medidas de prevención y buenas prácticas para garantizar la seguridad son fundamentales.

- ¿Es posible infiltrar una computadora en particular?
- ¿A distancia puede hacerse?
- ¿Qué función tienen los antivirus en estos casos?
- ¿Y qué pueden hacer una vez que infiltran las máquinas?
- ¿Cuál es la finalidad?
- ¿Esto es un delito para el Derecho argentino?

Caso 3: Noticias de actualidad con la cual se identifiquen como usuarios actuales

Figura 3. Recuperado de http://www.lanacion.com.ar/1715664-investigadores-argentinos-descubren-una-falla-de-seguridad-en-facebook

La lectura de una noticia referida a la seguridad en Facebook, red social seguramente utilizada por la mayoria de los alumnos, permitiría presentar una serie de interrogantes a modo de disparadores, para los cuales probablemente recibiríamos mayor cantidad y variedad de respuestas que podríamos canalizar hacia nuestros objetivos en la temática de la seguridad, como por ejemplo:

- ¿Facebook es una red social pública o privada?
- ¿Hemos leído las condiciones de servicio y la política de uso de datos de la red social, a las cuales hemos dado nuestra conformidad al registrarnos en la misma?
- ¿les han llegado invitaciones tales como "quien ha visitado tu perfil"; "descubre quien mira tu perfil" o "entérate de quien te ha borrado en Facebook"? ¿han respondido a dichas invitaciones? ¿Cómo se generan las mismas?
- ¿se pueden intercambiar en Facebook pequeñas aplicaciones de terceros?
- ¿sabemos si dichas aplicaciones desarrollan algún otro tipo de actividad oculta?
- ¿Mi nivel de privacidad en Facebook es configurable? ¿Qué opciones de seguridad en Facebook conocen y utilizan? ¿Por qué?
- ¿Qué inconvenientes les ocasionaría que sus datos personales se hagan públicos?

Caso 4: recepción de un mensaje que solicita el suministro de información sensible

Figura4: suplantación de identidad que direcciona a un sitio fraudulento

Casos de esta naturaleza, de tanta difusión en los últimos tiempos basados en la recepción de un mensaje desde un supuesto contacto del usuario (por lo general una entidad bancaria), que busca influir en él a partir de una situación creíble, nos enfrenta al planteo de diversos interrogantes que nos permitan indagar si los alumnos pueden identificar un correo falso y a partir de allí delinear una manera de actuar frente a estas situaciones:

- ¿cómo sé que dicha entidad es realmente quien envía el mensaje? ¿tengo formas de analizar el remitente del mensaje?
- ¿A qué dirección web ingreso al utilizar el enlace que me proveen en el mensaje?
- ¿pueden solicitarme datos privados a través de un email?
- Una vez que ingrese a la página que me solicitan en el mensaje: ¿tengo formas de verificar que estoy en la página oficial de la entidad?
- ¿Qué mecanismos de seguridad me ofrecen este tipo de sitios al momento de ingresar mis datos?

Caso 5: noticia de actualidad con la cual se identifiquen como futuros profesionales

Figura 5: Recuperado de http://www.infobae.com/2009/03/09/435674-a-partir-hoy-afip-y-anses-aceptaran-la-firma-digital

En este caso, la lectura de una noticia en el área de la seguridad Informática referida a un organismo directamente vinculado a la futura actividad profesional de los actuales alumnos entendemos que los predispone favorablemente para poder analizar aspectos tales como:

- ¿Qué es y para qué sirve la firma digital?
- ¿Qué beneficios conlleva su utilización? ¿Cuáles son los requisitos para poder utilizarla?
- ¿Podemos equipararla a la firma hológrafa? ¿Cuál es el marco legal?

A modo de conclusión

Vivimos dentro de un ecosistema digital (email, 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 gran cantidad de riesgos crecientes, lo cual torna imprescindible que el usuario promedio necesite desarrollar algunas habilidades que permitan adquirir una conducta al momento de utilizar las Tecnologías de la Información y Comunicación.

La falta de conocimiento es 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 tenerlo controlado**, dado que por mucho que se planifiquen los diferentes aspectos de la seguridad informática, es preciso confiar en las personas.

Esta educación no debe basarse específicamente en explicaciones técnicas sino en integrar conocimientos, habilidades y conductas para concientizar del impacto que tienen para las organizaciones, la sociedad y las personas, las diferentes amenazas informáticas que existen en la actualidad.

Para que el aprendizaje sea constructivo y significativo, como decía Ausubel (1978), la motivación es una condición esencial y el docente debe lograr un contexto adecuado que genere actitudes positivas hacia el aprendizaje.

Vimos la necesidad de buscar enfoques alternativos que acerquen a los alumnos a las realidades que deben enfrentar como usuarios y profesionales, y comprobamos que la utilización de sucesos que atraigan la atención, vinculados al campo de la seguridad informática, genera el estímulo necesario que permite romper con los esquemas tradicionales de la "clase magistral" y constituye un instrumento pedagógico que facilita que el alumnado reflexione y se implique en el tema.

Referencias bibliográficas

Ausubel (1978). *Educational Psychology.* New York: Holt.

Berlyne, D. E. (1960). *Conflict, arousal and Curiosity*. New York: Mc Graw Hill.

Coll, C., Onrubia, J. (1999). *Evaluación de los aprendizajes y atención a la diversidad.* En Coll, C. (coord.) Psicología de la instrucción. La enseñanza y el aprendizaje en la Educación Secundaria. Barcelona: ICE/Horsori.

Laevers, F., Heylen, L., Daniels, D. (2004). *Ervaringsgericht werken met 6- tot 12 jarigen in het basisonderwijs.* CEGO, Leuven. Traducción financiada por la Asociación Flamenca de Cooperación al Desarrollo y Asistencia Técnica PROMEBAZ. *La práctica experiencial en*

la educación básica. Recuperado de: http://www.vvob.org.ec/sitio/sites/default/files/2008_promebaz_la_practica_expereincial_en_la_educacion_basica.pdf.

Rosas, R., Sebastian, C. Piaget, Vigotsky y Maturana (2001). *Constructivismo a tres voces.* Buenos Aires, Argentina: Ed. Aique.

Zianni, E., Nessier, A. (2014). *Formación docente en seguridad TIC: cuestiones pendientes*. Revista Iberoamericana de Educación. Monográfico número 65. Mayo-Agosto 2014. Recuperado de: http://www.rieoei.org/