PRODUCIR SOFTWARE SEGURO ARGENTINO

Romaniz, Susana[*]; Arce, Iván[**]; Gaspoz, Ivana[*]; Castellaro, Marta[*]

[*] Facultad Regional Santa Fe - Universidad Tecnológica Nacional
sromaniz@frsf.utn.edu.ar igaspoz@frsf.utn.edu.ar mcastell@frsf.utn.edu.ar
[**] Programa Seguridad en TIC - Fundación Dr. M. Sadosky Investigación y Desarrollo en TIC
iarce@fundacionsadosky.org.ar

Abstract. Una fuente principal de incidentes que ponen en riesgo la seguridad de la información y el funcionamiento esperado de los sistemas basados en tecnologías de la información y de las comunicaciones es la dificultad de producir software seguro. Concebir a la seguridad del software como un atributo emergente de su proceso de desarrollo es una visión que ha comenzado a lograr consenso entre los actores vinculados directamente con su producción. Disponer de las capacidades necesarias para atender a esta demanda es, ante todo, una decisión estratégica, que no es sencilla de adoptar ni de rápidos resultados. Por ello, la posibilidad de tomar decisiones bien informadas resulta clave para guiar a los responsables de negocio y de tecnología. En este informe se describen proyectos, desarrollados en conjunto entre el sector universitario, empresas y estado, orientados a la atención de la seguridad en los procesos de desarrollo de software.

Keywords: software seguro, proceso de desarrollo de software, medición madurez del proceso

1 Enfoque actual de la seguridad del software

Un aspecto central de la problemática de seguridad en los sistemas de información es la seguridad del software. Hay software "corriendo" por todas partes: controlando el funcionamiento del auto, en el teléfono celular, en el lavarropas, en el banco, en el sistema de distribución eléctrica, en el equipamiento médico y hasta en las computadoras. Los defectos del software con impacto sobre la seguridad pueden ser errores de implementación o fallas de diseño. La Base de Datos Nacional de Vulnerabilidades del Instituto Nacional de Estándares de Tecnología de EEUU (NIST) catalogó más de 50.000 vulnerabilidades de conocimiento público en software comercial durante el período 2001-2012. Se estima que ese número debería multiplicarse por entre 3 y 5 si se desea contabilizar las vulnerabilidades conocidas pero no publicadas, y que sólo el 50% de los problemas de seguridad del software derivan de errores de implementación mientras que el otro 50% se debe a fallas de diseño. El panorama es crítico si además se considera la seguridad del software desarrollado para uso interno o no disponible comercialmente.

Cualquiera sea la medida que se use, está claro que la presencia de problemas de seguridad en el software es muy frecuente y está creciendo. Atender el problema requiere buscar formas de desarrollar software de mayor calidad, con menos fallas que pongan

en riesgo a usuarios y organizaciones que lo usan. La seguridad del software comenzó a prosperar como una disciplina independiente de la seguridad en las computadoras y en las redes. A finales de la década de 1990, los investigadores comenzaron a poner más énfasis en el estudio de la manera en que un programador puede contribuir a la seguridad de un sistema informático o, no intencionalmente, a socavarla. A mediados de la década siguiente, comenzó a surgir el consenso de que la creación de software seguro requiere más que sólo personas inteligentes esforzándose. Para lograr niveles adecuados de seguridad es necesario que ésta esté involucrada en el proceso de desarrollo de software, y resulte una propiedad emergente del producto. Por ende, la seguridad del software también abarca aspectos de negocio, sociales y organizacionales.

2 La evolución reciente del software argentino

Según estadísticas de la Cámara Argentina de Empresas de Software y Servicios Informáticos (CESSI), en el período 2003-2012 las ventas de la industria de software de Argentina crecieron alrededor del 400%, el empleo en el sector aumentó un 376%, mientras que el monto de las exportaciones registró un incremento del 529%. Por su parte, estadísticas de la Cámara de Informática y Comunicaciones de la República Argentina (CICOMRA) muestran un crecimiento similar y la Organización Mundial de Comercio en su reporte del 2009 ubica a la Argentina en la undécima posición del ranking mundial de países con mayor volumen de exportaciones e importaciones de servicios informáticos. Las estadísticas citadas son indicadores del crecimiento acelerado de nuestro país en el desarrollo, uso y exportación de las Tecnologías de Información y Comunicaciones (TIC) en general y del software en particular.

Sin embargo, hay evidencias de que este "despegue" del software argentino, tanto del desarrollado y comercializado por el sector SSI como el desarrollo para uso interno del resto del sector productivo, no se ve acompañado por un incremento proporcional en la calidad y la seguridad del software producido. Esto permite vislumbrar un riesgo no sólo técnico sino también de negocios en el corto y mediano plazo asociado directamente con la problemática de seguridad de TIC y con los requerimientos técnicos y regulatorios crecientes del mercado global del software.

3 Antecedentes de las instituciones proponentes del proyecto

El Programa de Seguridad en TIC (STIC) de la Fundación Dr. Manuel Sadosky [1] tiene por objetivo fortalecer tanto las capacidades de los equipos científicos locales que trabajan en temas relacionados con seguridad de TIC, como también las capacidades tecnológicas en seguridad informática de las empresas y el Estado, y fomentar en el proceso una mayor interacción entre los ámbitos académico y productivo.

El Departamento de Ingeniería en Sistemas de Información de la Facultad Regional Santa Fe de la Universidad Nacional Tecnológica (FRSF-UTN) trabaja en la formación de recursos humanos, en investigación y desarrollo, y en transferencia tecnológica en el campo de sistemas de información [2]. Y en lo que se refiere a seguridad en sistemas de información, trabaja desde el año 2007 en el desarrollo tanto de proyectos

de I+D como de transferencia, en los que participan docentes, investigadores y becarios, en el ámbito público y privado [3, 4].

4 Vinculación atendiendo al impacto

La formulación del proyecto "Metodologías para evaluar la madurez de la seguridad del software" surge como una respuesta a la necesidad identificada por sus proponentes del contexto antes descripto. Consiste en observar las actividades vinculadas al proceso de desarrollo de software en el ámbito de empresas localizadas en nuestro país que producen software tanto para consumo interno como terceros, e identificar buenas prácticas relativas a la selección e incorporación de requisitos de seguridad como parte de dicho proceso. *Conscientes del impacto que implica introducir buenas prácticas de este tipo a nivel del negocio, y de la cultura y estructura empresarial, se optó por una metodología orientada a medir la madurez de los procesos de producción de software que atienda a la seguridad en un marco de mejora continua. Al no existir antecedentes en el ámbito local de aplicación de este tipo de metodologías, se adoptó el criterio de formular un proyecto de dos fases*.

En la primera fase, el proyecto se focalizó en la realización de una Prueba Piloto de alcance limitado en cuanto al número de empresas medidas, a fin de *validar tanto la aplicabilidad de la metodología seleccionada como la utilidad de sus resultados*, y la *formación de expertos* en el uso de la metodología. A partir de la experiencia realizada, los resultados obtenidos y las lecciones aprendidas, se formuló la segunda fase, orientada no sólo a *ampliar el número de empresas*, sino también *a involucrar empresas que brindan servicios de consultoría en seguridad de sistemas de información como actores en el uso de la metodología de medición de la madurez*. De esta manera, el impacto esperado y, en parte, verificado, es:

1) obtener datos cuantitativos respecto de las actividades que implementan empresas nacionales en sus procesos de desarrollo de software relacionadas con la atención de la seguridad requerida,

2) actuar como disparador de acciones que interesen a sus responsables máximos y promuevan cambios en la estructura de las áreas de desarrollo de las empresas, y

3) involucrar a empresas que ofrecen servicios de consultoría en seguridad para que hagan extensivos dichos servicios a actividades relacionadas con la producción de software seguro.

4.1 Breve descripción de la metodología adoptada

La metodología emplea un modelo de madurez *Building Security In Maturity Model* (BSIMM) [5], disponible al público bajo licencia "Creative Common Attribution-Share Alike 3.0 License"). Es el resultado de un estudio de iniciativas de seguridad del software del mundo real, iniciado en el año 2009 y actualizado anualmente. Se construyó directamente a partir de datos observados en un número creciente de iniciativas de seguridad del software obtenidos de empresas de diferentes escalas, nichos de mercado y localización geográfica (en particular, empresas de EEUU y Europa).

Su objetivo es ayudar a la comunidad de especialistas en seguridad del software a planificar, ejecutar y medir sus propias iniciativas. BSIMM no es modelo prescriptivo sino un reflejo de lo más avanzado en la seguridad del software, que describe cómo evolucionan, cambian y mejoran a lo largo del tiempo las iniciativas maduras de seguridad del software. Además, es una "vara de medición" de la seguridad del software pensado para ser utilizado por cualquier responsable de la creación y ejecución de una iniciativa de seguridad del software, como una forma de contrastar su propia iniciativa con los datos sobre qué están haciendo otras organizaciones en referencia al modelo.

4.2 Ejecución de la primera fase y participación de las empresas

El objetivo de la primera fase del proyecto fue *adaptar el modelo BSIMM al contexto nacional y desarrollar los recursos locales necesarios para promover el empleo de metodologías que mejoren la calidad de sus productos respecto a la seguridad entre las empresas de la industria del software y organizaciones de distintos sectores productivos que realizan actividades de desarrollo de software para consumo interno*. Se inició en diciembre de 2012 y una duración de 6 meses. El equipo de trabajo se conformó con 4 integrantes de la FRSF-UTN (a cargo de la Dirección del Proyecto), y uno del STIC.

El proyecto se estructuró en 3 Etapas, cuyos objetivos fueron: 1) Desarrollo de los recursos requeridos para la aplicación de la metodología seleccionada en la Prueba Piloto; 2) Ejecución de la Prueba Piloto, aplicando la metodología en empresas de la región centro-litoral; 3) Elaboración de las conclusiones. Las actividades se realizaron con ligeros desfasajes en duración y esfuerzo debido a que se amplió el número de empresas participantes (5 en lugar de las 3 previstas); esto no sólo no impactó significativamente en su ejecución ni en sus resultados, sino que posibilitaron su mejor aprovechamiento, en especial el conocimiento y la experiencia ganados por el equipo de trabajo durante su interacción con las empresas participantes.

Los *principales resultados* de la primera fase fueron:

1) detectar el interés existente en varias de las organizaciones que participaron en las actividades de difusión del proyecto (panel de presentación, divulgación por medios de comunicación y contactos institucionales) y que llevó a que se ampliara el número previsto de empresas participantes;

2) consolidar el equipo de trabajo en cuanto a su experiencia en el uso de la metodología y a su capacidad de definir estrategias para su aplicación y relacionamiento con los entrevistados; y

3) hacer visible la existencia en la región de instituciones abocadas al desarrollo de un enfoque local de las buenas prácticas adoptadas por los fabricantes de software respecto a la seguridad como parte de sus atributos de calidad.

Cabe destacar especialmente que, si bien en la primera fase del proyecto no se previó un mecanismo formal de retroalimentación acerca del impacto sobre la empresa medida derivado de su participación en el proyecto, contactos mantenidos con referentes institucionales y técnicos permitieron identificar, en al menos tres de ellas, *acciones en pro de incorporar en la visión estratégica empresaria la necesidad de adecuar sus procesos de desarrollo de software tendientes a mejorar su calidad respecto de la seguridad*.

4.3 Propuesta de la segunda fase

La segunda fase del proyecto, actualmente en ejecución, tiene como propósito realizar tareas destinadas a *afianzar el desarrollo de recursos humanos locales y de herramientas que faciliten el empleo de metodologías orientadas a mejorar la calidad de los productos de software respecto de la seguridad entre las empresas nacionales productoras de software para consumo interno y de terceros*. En particular, comprende el desarrollo de capacidades en recursos humanos provenientes del mundo académico, de I+D y del campo empresarial en la aplicación de dichas metodologías, a fin de promover su difusión, aplicación y adecuación al contexto nacional. Incluye la realización de un conjunto de mediciones de madurez respecto a la atención de la seguridad en los procesos de desarrollo de software empleados en empresas nacionales del mencionado campo de actividad, y de esta manera *capturar la información requerida para generar la versión 0 de la metodología BSIMM adaptada a la Argentina*.

Se inició en diciembre de 2013, con una duración prevista de 15 meses, y suma dos nuevos integrantes, uno por cada una de las instituciones. Además, prevé incorporar al equipo tres nuevos integrantes con experiencia en ingeniería de la seguridad y/o ingeniería del software, seleccionados de entre los propuestos por empresas proveedoras de productos y consultoría en seguridad informática que manifiesten su interés de participar en el proyecto. La ejecución de esta segunda fase del proyecto presenta el desafío de identificar empresas interesadas en atravesar un proceso de medición de las buenas práctica que aplican en sus procesos de desarrollo de software, así como el de detectar empresas que se desenvuelven en el campo de la seguridad informáticas que vean en los resultado de este proyecto un nuevo nicho de negocio.

5 Aspectos destacables y acciones a considerar

Se enumeran un conjunto de aspectos que se consideraron importantes destacar a propósito del proyecto en sí mismo y de acciones orientadas a propiciar los objetivos del mismo. En cuanto a lo específico del proyecto, se destacan las siguientes conclusiones:

1) El empleo de la metodología adoptada ha demostrado ser hasta el momento una eficaz vía para promover entre las empresas involucradas la visibilidad de factores claves y encarar planes de mejora continua en cuanto a la calidad de sus productos de software respecto de la seguridad;

2) La realización de las Mediciones de Madurez no demandan un esfuerzo significativo por parte de las empresas participantes, a la par que el retorno recibido vía el Informe de Evaluación de Madurez fue muy positivamente valorado por la mayoría de las ellas.

3) Resultó clave en la predisposición de las empresas para conocer las características del Proyecto y su posterior participación en el mismo, experiencias previas en otras actividades de Vinculación Tecnológica con algunas de las instituciones a cargo del Proyecto;

4) Tomando como referencia la primera fase del Proyecto, y considerando el número de empresas que asistieron a su presentación pública, el número de empresas

participantes representó un porcentaje significativo, la mayoría de las cuales manifestaron su interés de manera casi inmediata;

5) En cuanto a la evolución del equipo a cargo del Proyecto, respecto a su integración, aprendizaje y experiencia logrados, se han logrado resultados muy importantes, atiendo especialmente al hecho que está integrado por diferentes perfiles de especialización.

En cuanto a la identificación de acciones orientadas a propiciar los objetivos del proyecto, se destacaron los siguientes requerimientos que están siendo atendidos actualmente:

1) Revisar algunos criterios de selección de las empresas candidatas, en particular respecto a la necesidad de que la empresa cuente con un rol (formal o informal) de responsable de seguridad;

2) Lograr una mayor integración de los instrumentos dan soporte al conjunto de las actividades vinculadas con la realización de una Medición BSIMM, y comenzar a formalizar su proceso de ejecución;

3) Ajustar la planificación de las Mediciones en base al esfuerzo y tiempo identificados durante la ejecución de la primera fase;

4) Formalizar una estrategia de retroalimentación empresa-equipo a los fines de dimensionar el impacto a corto, mediano y largo plazo.

6 Conclusiones y futuro previsto

Como se describió al inicio, concebir a la seguridad del software como un atributo emergente de su proceso de desarrollo es una visión que está logrando consenso entre los actores vinculados con su producción. Pero lograr los cambios requeridos en las organizaciones no es proceso rápido ni sencillo. Por ello entendemos que impactará positivamente el hecho de contar con información que ayude a todos los actores (usuarios –personas, y organizaciones públicas y privadas–, instituciones educativas y científicas, fabricantes y proveedores de software, y entes regulatorios) interesados en estos cambios a conocer cuál es el grado real en la adopción de buenas prácticas y así tomar decisiones bien informadas. Esto permitirá definir líneas de I+D y contenidos curriculares nuevos que desarrollen las capacidades locales necesarias para atender los requerimientos emergentes en pos de facilitar la producción nacional de software seguro.

Referencias

1. http://www.fundacionsadosky.org.ar/es/Programas-Proyectos/seguridad-en-tic
2. http://www.frsf.utn.edu.ar/institucional/departamentos/sistemas y http://gistic.frsf.utn.edu.ar
3. Romaniz, S. "Gestión de un Programa de Concientización acerca de la Seguridad de la Información". 3rd Intern. Symposiym on Innovation and Technology ISIT 2012. Perú. 2012.
4. Castellaro, M. y otros. "Qué hay respecto a atender a la seguridad durante el desarrollo de sistemas de información?" 1er. Congreso Nacional de Ingeniería Informática / Sistemas de Información CoNaIISI 2013. Argentina. 2013.
5. http://www.bsimm.com