Modelos y Métodos de Calidad: Fortalecimiento de la Seguridad en los Sistemas de Software

Carlos Salgado, Mario Peralta, Mario Berón
Departamento de Informática Facultad de Ciencias Físico-Matemáticas y Naturales Universidad Nacional de San Luis
Ejército de los Andes 950 – C.P. 5700 – San Luis – Argentina
e-mail: {csalgado, mperalta, mberon}@unsl.edu.ar

RESUMEN

Los avances tecnológicos aportan un nuevo nivel de autonomía a los vehículos, los robots en los almacenes, las cámaras de seguridad y una amplia gama de servicios de Internet. Por lo tanto, los autos, datos personales, métodos de pago electrónico, servicios en la nube y dispositivos personales de empleados serán algunos de los blancos de los *ciberdelincuentes*. La seguridad se ha convertido en un punto crítico para la vida diaria de las personas. Dicho avance, nos lleva a combinar y extender las características deseables o esperables de los recursos humanos para garantizar la seguridad de datos e información de las organizaciones. El incremento en la seguridad, con el uso de modelos de calidad adecuados, con posibilidad de implementar un tablero de control, asegura un adecuado resguardo de toda la información sobre los proyectos en marcha, que es esencial para poder gestionar de manera eficiente.
En este sentido, la presente propuesta consiste en la definición de un modelo que se basa en las mejores características de seguridad de la Norma ISO 25000, tales como Confidencialidad, Integridad, Responsabilidad, Autenticidad y las consideraciones de la ISO 9001 con respecto a las condiciones o características de los recursos humanos de las organizaciones.

Palabras Claves: Seguridad, Ataques al Personal, Métodos de Evaluación, Modelos de Calidad,

CONTEXTO

La presente línea de investigación se enmarca en el Proyecto (PO/16/93) de "Fortalecimiento de la Seguridad de los Sistemas de Software mediante el uso de Métodos, Técnicas y Herramientas de Ingeniería Reversa". Realizado en conjunto con la Universidade do Minho Braga, Portugal. Recientemente aprobado por el Ministerio de Ciencia Tecnología e Innovación Productiva (Mincyt), y por el Proyecto (P031516.) de Investigación: "Ingeniería de Software: Conceptos, Prácticas y Herramientas para el Desarrollo de Software con Calidad". De la Facultad de Ciencias Físico Matemáticas y Naturales, Universidad Nacional de San Luis. Dicho proyecto es la continuación de diferentes proyectos de investigación a través de los cuales se ha logrado un importante vínculo con distintas universidades a nivel nacional e internacional. Además, se encuentra reconocido por el Programa de Incentivos.

1. INTRODUCCIÓN

Las previsiones para 2020 indican que habrá, al menos, 200.000 millones de dispositivos conectados a la red. Y no serán solo computadoras o teléfonos, sino que habrá electrodomésticos, autos, relojes, ropa, entre otros, y serán los blancos para los piratas informáticos. Estas consideraciones ponen de manifiesto la necesidad de modelos, métodos, técnicas y herramientas para poder combatir, o al menos prevenir, dichos ataque. Hoy en día, el acceso a los datos e información está dado desde distintos aparatos o dispositivos electrónicos.
Internet es el medio que permite tener alcance a mayores distancias y diversidad de actores.
Las aplicaciones web son utilizadas en una amplia variedad de áreas, entre ellas, redes sociales, compras, actividad bancaria, sistemas de control, almacenamiento en la nube y demás. Inclusive desde el año 2011, el 75 % de

la distribución de aplicaciones por categorías correspondía a aplicaciones web. Este abrupto crecimiento se debe, entre otras cosas, a la versatilidad que supone un navegador web como cliente ligero, la independencia con el sistema operativo y la posibilidad de mantener o actualizar la aplicación sin la necesidad de interferencia de los usuarios potenciales [1].

Para intentar satisfacer la incesante demanda de sistemas de este tipo, los usuarios ocasionalmente se ven rodeados de software que no fue desarrollado siguiendo un modelo adecuado, que no ha sido codificado siguiendo parámetros de calidad y/o posee un diseño defectuoso, entre otros tantos factores que vuelven a los sistemas poco robustos y con grandes falencias en seguridad [2].

En un contexto de conectividad permanente entre los usuarios, el concepto de "seguridad" se vuelve un factor fundamental [3]. Este motivo, entre otros, es el principal desencadenante de una disciplina que se encuentra en auge en distintos ámbitos de la actualidad, la misma es conocida como: Seguridad Informática.

La noción de seguridad en los Sistemas de Información, se define como un grupo de componentes con características especiales, de los cuales se pueden destacar [4]:

Seguridad: incluye características en concomitancia con la protección del sistema, sus aplicaciones y los recursos compartidos. Incluye la prevención de la adquisición y modificación no autorizada de información, es decir, se intenta cubrir tanto la seguridad del sistema como la de los datos del usuario.

Fiabilidad, disponibilidad y recuperación: indican, respectivamente, la exactitud de la seguridad del sistema y otras funciones del mismo, el soporte a través del tiempo de un sistema seguro y la capacidad de recuperación del mismo luego de haber sufrido un ataque o algún tipo de error/accidente.

Auditabilidad: implica el seguimiento de la continua existencia de seguridad y fiabilidad del sistema, incluyendo la detección de anomalías o un amenazante comportamiento.

Un camino viable para conseguir, como producto final, un sistema que provea mecanismos de seguridad adecuados, es seguir un enfoque correctivo [5]. Esto quiere decir, llevar a cabo la evaluación de la seguridad del software a posteriori de su desarrollo. En este sentido, es preciso hacer referencia a un conjunto de herramientas denominadas: "Herramientas de Análisis de Seguridad de Software".

La seguridad es un atributo de calidad del software y, como parte de un todo, al llevar a cabo un análisis, tradicionalmente se distinguen dos tipos: el *Análisis Dinámico*, donde se diseñan casos de prueba sobre la información base de la especificación, y el *Análisis Estático*, donde las técnicas de evaluación o prueba se diseñan en base a la información derivada del código fuente [6, 7].

Más allá del camino que se tome para realizar sus procedimientos, el fin de las herramientas de análisis de seguridad es encontrar aquellos puntos donde el sistema informático sufre problemas relacionados o, inclusive, identificar aquellas vulnerabilidades que podrían ser potencialmente conflictivas. De acuerdo con el Instituto SANS [8], en el ámbito de aplicaciones web, las herramientas específicas de análisis de seguridad se pueden clasificar, teniendo en cuenta la forma que utilicen para llevar a cabo sus procesos, en al menos cuatro categorías: i) Bloqueo de ataques: basados en la red de datos. ii) Bloqueo de ataques: basados en el servidor de host. iii) Eliminación de vulnerabilidades de seguridad. iv) Soporte seguro para usuarios autorizados.

De esta forma, se puede concluir que existe una gran variedad de posibilidades a la hora de seleccionar una herramienta que ejecute un proceso de análisis de seguridad para aplicaciones Web. Dentro de lo que significa la detección y eliminación de vulnerabilidades de seguridad, con el fin de acotar el alcance de la investigación y, por lo tanto, conseguir un enfoque más preciso, este artículo se centra en la evaluación de los recursos humanos que utilizan las aplicaciones web en las

organizaciones/instituciones.

Desde otro punto de vista, el ataque a través de los empleados es un punto de vulnerabilidad cada vez expuesto debido a las distintas posibilidades de acceso que aportan las nuevas tecnologías. Las organizaciones continuarán mejorando sus posturas de seguridad, implementando las últimas tecnologías de seguridad, trabajando para contratar a personas con talento y experiencia, creando políticas efectivas y permaneciendo vigilantes. Sin embargo, los atacantes probablemente cambien su enfoque y ataquen cada vez más a las empresas a través de sus empleados, dirigiéndose entre otras cosas, a los relativamente inseguros sistemas del hogar de los empleados para acceder a las redes corporativas.

Desde este punto de vista, la norma ISO 9001-2015 [9] trata sobre el recurso humano de una organización. Para que ésta pueda satisfacer a sus clientes con productos de calidad, debe tener un personal de calidad. El recurso humano se considera de calidad cuando:

- es competente en base a cuatro aspectos: educación, formación, habilidades y experiencia;
- está consciente de la importancia de sus actividades en relación con la calidad, y
- está satisfecho.

De acuerdo a la Norma ISO 9001-2015, la organización debe asegurar que su personal es *consciente* de la relevancia e importancia de sus actividades y cómo ellas contribuyen a la consecución de los objetivos de calidad.

Basados en los principios de participación del personal y de la orientación a procesos, tener un personal consciente es una labor de formación y de creación de una cultura organizacional. Que debe garantizar la Alta Dirección de la organización al asegurar que las responsabilidades y autoridades son definidas y comunicadas dentro de la organización.

Por otro lado, el personal debe ser *competente*. Entendiendo competencia como un "conjunto de comportamientos observables que están causalmente relacionados con un desempeño bueno o excelente en un trabajo concreto y en una organización concreta" [10].

La norma ISO 9001 considera que una persona es competente cuando cumple los requisitos de educación, formación, habilidades y experiencia que la organización determina para cada puesto de trabajo. Donde:

- Educación: Estudios mínimos requeridos para un determinado puesto.
- Formación específica: Son todos aquellos conocimientos adicionales que necesarios para desempeñar las actividades de un puesto, por ejemplo, especialización en determinadas herramientas informáticas.
- Habilidades especiales de tipo práctico. Por ejemplo, la habilidad que debe tener un vendedor. Estas habilidades, específicas para cada puesto, facilitan el desempeño del mismo.
- Experiencia mínima, que el trabajador debe tener en el puesto o en puestos similares y que incluye un período de prácticas mínimo en la empresa.

Estas competencias son de tipo umbral, es decir, las mínimas que debe tener una persona para realizar su trabajo con éxito, pero no van a diferenciar a los trabajadores con desempeño excelente de los que tienen un desempeño normal.

En cuanto a la *satisfacción,* un personal satisfecho es aquel personal motivado, que siente que tiene cubiertas sus necesidades personales, que se siente a gusto con el trabajo que desempeña y estima que tiene estabilidad en él. Tiene la tranquilidad suficiente como para dedicar todos sus esfuerzos físicos, psíquicos e intelectuales a desarrollar su trabajo sin que tensiones o preocupaciones ajenas a las actividades propias del puesto lo distraigan.

Un elemento que contribuye a una buena productividad y a la satisfacción del empleado es el mantenimiento del área de trabajo en condiciones cómodas y saludables. En la Norma ISO 9001-2015 se define que el ambiente de trabajo está relacionado con aquellas condiciones en las cuales se realiza el trabajo incluyendo los factores físicos, ambientales o de cualquier otro tipo. En este punto, la norma establece que la organización debe determinar y gestionar el ambiente de

trabajo necesario para lograr la conformidad con los requisitos del producto. En este sentido es importante el estudio de los aspectos ergonómicos y de seguridad e higiene en el área de trabajo.

De ahí que las organizaciones deben intentar controlarlos y crear condiciones lo más cómodas y seguras posibles para que el trabajador pueda ser eficiente sin que se vea afectado por estos elementos. Realizar un trabajo en condiciones incómodas o inseguras crea en el trabajador un sentimiento de descontento pues le hace pensar que la empresa no se preocupa por cómo realiza su trabajo.

Desde este punto de vista, al contar con un modelo y/o método se debe procurar prevenir o anticiparse para lograr mantener los procesos organizacionales funcionando de forma segura y sistemática para garantizar la satisfacción y trabajo de calidad del personal de las organizaciones. Ese es el actual desafío que presenta el nuevo paradigma de negocio y las bondades de las TIC.

En base a ellos se analizan los beneficios de definir un modelo y/o método de calidad que permita establecer las pautas y pasos a seguir a la hora de analizar la existencia de vulnerabilidades de seguridad en las aplicaciones web, las cuales son el nexo entre los empleados y su trabajo. Tal vez considerar los nuevos paradigmas de trabajo a distancia y lo que conlleva al acceso a los recursos de la empresa/organización de manera remota.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Los principales ejes de esta línea de I+D están asociados a:

- Estudio de modelos conceptuales aplicados a la calidad de productos software.
- Estudio de normas de calidad aplicadas a productos software.
- Estudio de estándares y metodologías aplicadas a la construcción de Modelos de Calidad de productos.
- Construcción de modelos de calidad de productos software aplicables a diferentes ámbitos.
- Hacer una investigación profunda sobre las vulnerabilidades de seguridad que afectan a los sistemas de Información.
- Investigar el estado del arte de los patrones/estilos arquitectónicos de sistemas de información, y de los protocolos utilizados en su desarrollo.
- Integrar las investigaciones realizadas en ambos proyectos con el fin de crear un conjunto de herramientas que faciliten a los distintos actores en ciclo de desarrollo de software poder interactuar en pos de la seguridad de los sistemas, recursos de la organización.
- Análisis de los distintos protocolos de seguridad. Pensando en la definición de reglas, normas, protocolos, guías que permitan desarrollos escalables y seguros, brindando soporte en la integración de subsistemas que posiblemente estén ubicados en diferentes posiciones geográficas, posean diferentes sistemas operativos y utilicen diferentes protocolos de software y hardware.

3. RESULTADOS OBTENIDOS/ESPERADOS

Según lo establece la Norma 25010 [11], la seguridad se define como la "Capacidad de protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos", y, considerando las subcaracterísticas esperables o deseables para un producto software en cuanto a seguridad, el modelo que se propone en esta línea de investigación consiste de las siguientes características:

- *Confidencialidad*. Capacidad de protección contra el acceso de datos e información no autorizados, ya sea accidental o deliberadamente.
- *Integridad*. Capacidad del sistema o componente para prevenir accesos o modificaciones no autorizados a datos o programas de ordenador.
- *No repudio*. Capacidad de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no

puedan ser repudiados posteriormente.

- *Responsabilidad*. Capacidad de rastrear de forma inequívoca las acciones de una entidad.
- *Autenticidad*. Capacidad de demostrar la identidad de un sujeto o un recurso.

Además de estas características, se considera de suma importancia la subcaracterística: ***ataques a través de los empleados***, la cual tiene que ver con lo que se refiere al personal dentro de una organización. Las organizaciones continuarán mejorando sus posturas de seguridad, implementando las últimas tecnologías de seguridad, trabajando para contratar a personas con talento y experiencia, creando políticas efectivas y permaneciendo vigilantes. Sin embargo, los atacantes probablemente cambien su enfoque y ataquen cada vez más a las empresas a través de sus empleados, dirigiéndose entre otras cosas, a los relativamente inseguros sistemas del hogar de los empleados para acceder a las redes corporativas. Por lo tanto, otra arista más a considerar es la seguridad aplicada fuera de la organización.

Es por ello que se está trabajando en la definición del modelo mencionado. El objetivo es proveer una herramienta que permita prevenir en gran medida los distintos ciberataques a los que los usuarios de las nuevas tecnologías están expuestos en la actualidad.

4. FORMACION DE RECURSOS HUMANOS

El equipo de profesionales de la UNSL que forman parte de la línea de investigación de este trabajo llevan adelante diferentes trabajos finales integradores de Ingeniería en Informática, Ingeniería en Computación, Licenciatura en Ciencias de la Computación. Además, en el marco de esta línea de investigación, se está desarrollando una tesis para la Maestría en Calidad de Software dictada por la Universidad de San Luis bajo Resolución ME N° 1589/13. En el ámbito de dicho proyecto se propone la investigación sobre modelos y métodos de calidad que fortalezcan el desarrollo de software.

5. BIBLIOGRAFÍA

[1] R. CHOPRA. Web Engineering. PHI Learning Pvt. Ltd., 2016.

[2] P. E. Black. Software assurance metrics and tool evaluation. In Software Engineering Research and Practice, pages 829–835, 2005.

[3] C. Vulnerabilities. Exposures,"the standard for information security vulnerability names". Common Vulnerabilities and Exposures: The Standard for Information Security Vulnerability Names. url: http://cve. mitre. org, 2007.

[4] J. Song, G. Hu, and Q. Xu. Operating system security and host vulnerability evaluation. In Management and Service Science, 2009. MASS'09. International Conference on, pages 1–4. IEEE, 2009.

[5] P. G. Neumann. Computer system security evaluation. In National Computer Conference, 1978.

[6] M. Ishrat, M. Saxena, and D. M. Alamgir. Comparison of static and dynamic analysis for runtime monitoring. International Journal of Computer Science & Communication Networks, 2:615–617, 2011.

[7] C. Artho and A. Biere. Combined static and dynamic analysis. In Proc. AIOOL '05, ENTCS, pages 98–115. Elsevier Science, 2005.

[8] I. SANS. Seguridad 101: Los tipos de malware. https://www.sans.org/critical-security-controls/, 2017.

[9] ISO ORG. (Septiembre de 2015). *ISO 9001:2015*. Recuperado el octubre de 2016, de http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm

[10] Pereda, S., Berrocal, F., Sanz, P. (2003), Los perfiles de exigencias en la ocupación del profesional de recursos humanos, Psicología desde el Caribe, Universidad del Norte, Nº 12

[11] ISO/IEC 25010:2011. Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models."