Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 12, No. 8, Mes Agosto, 2019
ISSN: 2306-2495 | RNPS: 2343
Pág. 42-56
http://seriecientifica.uci.cu

Tipo de artículo: Artículo original
Temática: Soluciones informáticas
Recibido: 01/07/2019 | Aceptado: 20/08/2019 | Publicado: 22/08/2019

Requisitos de Seguridad para el desarrollo de aplicaciones web

Security requirements for the development of web applications

Yisel Niño Benitez[1*], Yoansy López Reyes[2]

[1] Universidad de las Ciencias Informáticas. Carretera de San Antonio de los Baños km 2 ½, Torrens, La Lisa, La Habana, Cuba. ynino@uci.cu.

[2] Universidad de las Ciencias Informáticas. Carretera de San Antonio de los Baños km 2 ½, Torrens, La Lisa, La Habana, Cuba. yoansylr@uci.cu .

[*] Autor para correspondencia: ynino@uci.cu

Resumen

La gestión de la Seguridad Informática desde etapas tempranas del desarrollo de software evita que los mecanismos de seguridad deban ser ajustados dentro de un diseño ya existente, lo que introduce cambios que pueden generar vulnerabilidades en el software, aumentando el coste de desarrollo. Verificar la seguridad de forma temprana y frecuente en el desarrollo de aplicaciones web garantiza la disminución de las vulnerabilidades que pueda presentar el producto. Existen procesos definidos para la gestión y el desarrollo de los requisitos de software, sin embargo, no se gestiona de forma explícita el requisito no funcional Seguridad, ni se consideran tanto las pautas de la norma cubana ISO 25010:2016 para la Seguridad, como los riesgos que puedan estar presentes en el proceso de desarrollo. La presente investigación tiene como objetivo exponer varios elementos sobre el marco teórico de conceptos relacionados con la Seguridad Informática, la Ingeniería de Requisitos y las normas o estándares internacionales que los abordan, a partir de los cuales se elaboró un listado de requisitos de Seguridad teniendo en cuenta estándares y riesgos internacionales con el objetivo de disminuir el número de vulnerabilidades en el desarrollo de aplicaciones web.

Palabras clave: requisito no funcional Seguridad, riesgo, seguridad informática, vulnerabilidad.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 12, No. 8, Mes Agosto, 2019
ISSN: 2306-2495 | RNPS: 2343
Pág. 42-56
http://seriecientifica.uci.cu

Abstract

The management of Computer Security from early stages of software development prevents security mechanisms from being adjusted within an existing design, which introduces changes that can generate vulnerabilities in the software, increasing the cost of development. Check security early and often in the development of web applications ensures the reduction of vulnerabilities that may present the product. There are defined processes for the management and development of software requirements, however, the non-functional Security requirement is not explicitly managed, nor are the guidelines of the Cuban standard ISO 25010: 2016 for Security, as well as the risks that may be present in the development process. The objective of this research is to expose several elements about the theoretical framework of concepts related to Informatic Security, Requirements Engineering and the international norms or standards that address them, from which a list of security requirements was developed taking into account international standards and risks in order to reduce the number of vulnerabilities in the development of web applications.

Keywords: non-functional requirement Security, risk, informatic security, vulnerability.

Introducción

El desarrollo de la Web se manifiesta en una gran cantidad de transformaciones, evolucionando de páginas sencillas con pocas imágenes y contenidos estáticos, a páginas complejas con contenidos dinámicos que provienen de bases de datos. Este progreso ha propiciado la creación de aplicaciones web, las cuales permiten la generación automática de contenido, la construcción de páginas personalizadas según el perfil del usuario, y el desarrollo del comercio electrónico(MARTÍN and MARTÍN 2014; NIÑO BENITEZ and SILEGA MARTÍNEZ 2018). La Seguridad Informática (SI en lo adelante) es el área que se enfoca en "la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente, la información contenida o circulante" (CDI 2017). La SI llega a ser un área de vital importancia dentro de la Ingeniería de Software (IS), ya que como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada.

Varios autores coinciden en la necesidad de aplicar mecanismos efectivos de IS proporcionando teorías, métodos y herramientas para construir sistemas de software que operen de manera confiable y con la calidad requerida (ISO 2000; NAUR and RANDELL 1968; PRESSMAN and MAXIM 2015; RADATZ *et al.* 1990). Dentro de la IS, un área determinante para el éxito de un proyecto es la Ingeniería de Requisitos (IR), que identifica las características y

propiedades del producto a desarrollar (PRESSMAN and MAXIM 2015; SOMMERVILLE 2011). Los requisitos del sistema se clasifican en Requisitos Funcionales (RF) y Requisitos No Funcionales (RNF) (PRESSMAN and MAXIM 2015). Los RF describen lo que un sistema debe hacer, mientras que los RNF son aquellos que no se refieren directamente a las funciones específicas del sistema, sino a las propiedades emergentes de este como fiabilidad, rendimiento, mantenibilidad, seguridad, portabilidad y estándares a utilizar (SOMMERVILLE 2011). La Norma Cubana (NC) ISO 25010: 2016 (ISO/IEC, NC 2016) relaciona las características de calidad de un producto y sus sub-características que se van a tener en cuenta a la hora de evaluar las propiedades de un producto de software determinado y establece el sistema para la evaluación de la calidad de este.

El RNF de Seguridad se define como grado de protección de los datos, software y/o plataforma tecnológica de posibles pérdidas, actividades no permitidas o uso para propósitos no establecidos previamente (GIL VERA and GIL VERA 2017; LOSAVIO and ESTEVES 2016; VALLE ROJO and OLIVEROS 2014). A diferencia de otros RNF como la fiabilidad y el rendimiento, la seguridad no ha sido completamente integrada dentro del ciclo de vida de desarrollo y todavía es considerada después que el sistema ha sido diseñado (Rosado, Blanco, Sánchez, & Medina, 2009).

En encuestas aplicadas a diferentes roles involucrados en el proceso de desarrollo en la Universidad de las Ciencias Informáticas (UCI), estos conocen que se definen RNF de Seguridad y el 100% de los encuestados lo considera imprescindible para el desarrollo de las aplicaciones seguras. Sin embargo, sobre la gestión de este RNF: solamente el 30% considera la trazabilidad y gestión de la seguridad en todo el ciclo de vida del proceso de desarrollo del producto, el 55% lo propone a partir de la disciplina Requisitos, a pesar de que solo un 10% de estos le da seguimiento hasta la disciplina de Análisis y Diseño, el resto no considera necesario el seguimiento en las disciplinas siguientes. El 95% del total conoce los inconvenientes de no hacer un tratamiento certero de la seguridad en el desarrollo e identifican como aspectos negativos en este sentido: penetración en los sistemas, uso indebido de los servidores y su información, uso indebido de credenciales de autenticación, inyecciones SQL, atraso en el cronograma de entrega del producto por la resolución de No Conformidades (NC) de seguridad en las pruebas de liberación y aumento del costo de desarrollo, imposibilidad de despliegue del producto en determinado entorno por no tener en cuentas las restricciones legales de seguridad del cliente y con ello la pérdida del prestigio de la entidad desarrolladora ante el cliente.

Serie Científica de la Universidad de las Ciencias Informáticas
Vol. 12, No. 8, Mes Agosto, 2019
ISSN: 2306-2495 | RNPS: 2343
Pág. 42-56
http://seriecientifica.uci.cu

La encuesta aplicada ofrece evidencias empíricas que demuestran las insuficiencias en la gestión del RNF de seguridad. Además, se constató el impacto negativo de gestión ineficiente del RNF para el desarrollo de los sistemas en términos de calidad y tiempo. Con el objetivo de aliviar la problemática descrita anteriormente en este artículo se presenta una propuesta de RNF seguridad. Una característica clave de esta propuesta es que plantea el seguimiento del RNF de seguridad desde etapas tempranas lo que contribuirá a disminuir el número de vulnerabilidades en las aplicaciones web.

Materiales y métodos o Metodología computacional

Elementos necesarios de Seguridad informática

La SI tiene el objetivo de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Urbina (URBINA 2016) plantea que la SI es la "disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos a los que está expuesta, tanto físicos como lógicos". Ruiz Larrocha (LARROCHA 2017) la concibe como un conjunto de métodos y técnicas para los propósitos antes mencionados, añadiendo a esto las herramientas necesarias que impiden la ejecución de operaciones no autorizadas de un sistema informático. Para los autores, la SI se enfoca en minimizar los riesgos existentes en el acceso y la utilización malintencionada de la información de los sistemas de software, con el fin de garantizar la integridad, confidencialidad y disponibilidad de la misma, haciendo uso de métodos y herramientas.

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer (AGUILERA LÓPEZ 2010):

- cuáles son los **elementos** que componen el sistema: esta información se obtiene mediante entrevistas con los responsables o directivos de la organización, para lo que previamente hay que realizar un estudio de los riesgos que puedan presentar,
- cuáles son los **peligros** que afectan al sistema, accidentalmente o provocados: estos datos se deducen de los aportados tanto por la organización como por el estudio y prueba del propio sistema,
- cuáles son las **medidas** que deberían adoptarse para conocer, prevenir, impedir, reducir y controlar los riesgos potenciales, definiendo los servicios y mecanismos necesarios para minimizarlos.

La SI se resume, por lo general, en cinco principios/características fundamentales (GARFINKEL *et al.* 1999; ISO/IEC 2013; ISO/IEC, NC 2016):

- **Integridad**: garantiza que los datos no sean modificados desde su creación sin autorización. Se debe asegurar que ningún intruso pueda capturar y modificar los datos en tránsito.
- **Confidencialidad**: avala que la información, almacenada en el sistema informático o transmitida por la red, solamente esté disponible para aquellas personas autorizadas a accederla.
- **Disponibilidad**: garantiza el correcto funcionamiento de los sistemas de información y su disponibilidad en todo momento para los usuarios autorizados.
- **No repudio**: asegura la participación de las partes en una comunicación. El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, el usuario no puede negar dicha acción.
- **Autenticación**: asegura que sólo los individuos autorizados tengan acceso a los recursos.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel. Para lograr este objetivo se necesitan estándares o normas que rijan aspectos imprescindibles a tener en cuenta en la implementación de un sistema de SI.

Estándares y normas de Seguridad informática

La familia de normas **ISO/IEC 27000** constituye un conjunto de estándares que proporciona un marco para la gestión de la seguridad. Contiene buenas prácticas para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización (ARORA 2010). Un SGSI es “esa parte del sistema de gestión general, basada en un enfoque de riesgo comercial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos” (ISO/IEC 2005b). De esta familia a consideración de los autores resaltan:

- **ISO/IEC 27000: 2014 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Generalidades y vocabulario:** proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance y propósito. Aporta las bases de

por qué es importante la implantación de un SGSI, una introducción a estos y una breve descripción de los pasos para su establecimiento, monitorización, mantenimiento y mejora.

- **ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos:** especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI dentro del contexto de la organización. Esta norma tiene un enfoque a procesos.
- **ISO/IEC 27002:2013 Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información:** antigua ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Se diferencia de la anterior (27001) que está enfocada a controles y no a procesos.
- **Modelo de madurez para la gestión de la seguridad informática (ISM3):** tiene como objetivo de la SI el garantizar la consecución de objetivos de negocio. Relaciona directamente los objetivos de negocio de una organización con los objetivos de seguridad de sus productos. Los procesos relacionados con la SI son descritos detalladamente, estableciendo objetivos y métricas que permitan establecer un sistema de calidad enfocado en la mejora continua del proceso, dado que existen criterios para medir la eficacia y eficiencia de los SGSI. El enfoque práctico y de medición, así como la orientación hacia los objetivos de negocio de la organización, es lo que diferencia este modelo del resto de los estándares relacionados con la seguridad de la información(PROENÇA and BORBINHA 2018).
- **OWASP (Open Web Application Security Project)** es una organización enfocada en mejorar la seguridad del software. Su misión es hacer visible la seguridad del software, para que las personas y las organizaciones sean capaces de tomar decisiones al respecto. Proporciona información imparcial y práctica sobre aplicaciones seguras a individuos, corporaciones, universidades, agencias gubernamentales y otras organizaciones en todo el mundo. Emite herramientas de software y documentación basadas en el conocimiento sobre la seguridad de las aplicaciones (OWASP 2017a). Como parte de estas herramientas publica cada cierto tiempo el Top 10 de riesgos más críticos y el Top 10 de controles proactivos a tener en cuenta en las aplicaciones de software. El objetivo de estos programas es crear conciencia sobre la seguridad de la aplicación al describir las áreas de preocupación más importantes en las que los desarrolladores de software deben estar conscientes (OWASP 2016).

En el estudio realizado por Katy Anton, Jim Bird y Jim Manico (OWASP, 2016) se describen una lista de conceptos de seguridad que ellos plantean incluir en cada proyecto de desarrollo de software. Los controles especificados en este documento se ordenan de acuerdo a su importancia, siendo el número 1 el más importante (OWASP, 2016). **La verificación de la seguridad temprano y frecuentemente** (Control 1 del Top 10 de Controles Proactivos) propone que desde el proceso de concepción del software se tengan en cuenta los requisitos de seguridad mientras se describen los requisitos del sistema, siempre teniendo en cuenta el resto de los controles propuestos. La gestión temprana de los requisitos de seguridad ayuda a evitar la ocurrencia de riesgos y vulnerabilidades en el proceso de desarrollo del software.

Teniendo en cuenta la criticidad de la SI en las organizaciones y las definiciones de las normas internacionales, se han aprobado estándares y resoluciones adaptadas al contexto nacional cubano.

La Oficina de Seguridad para las Redes Informáticas (OSRI), tiene como objeto social "llevar a cabo la prevención, evaluación, aviso, investigación y respuesta a las acciones, tanto internas como externas, que afecten el normal funcionamiento de las tecnologías de la información del país" ((OSRI), 2018). También se cuenta en Cuba con el centro de Ciberseguridad del Espacio, que es una "estructura especializada que contribuye al fortalecimiento de la seguridad en el ciberespacio cubano, fomentando la cooperación entre todos los factores que inciden en la ciberseguridad a nivel nacional y potenciando la colaboración internacional en esta esfera. Tiene como misión contribuir al fortalecimiento de la seguridad en el ciberespacio cubano y coordinar de manera efectiva la gestión de los eventos cibernéticos que impactan en la ciberseguridad de la nación" (CSC, 2018).

A partir de las vulnerabilidades y debilidades propias de los sistemas informáticos, de las dificultades y limitaciones que se presentan para detectar y neutralizar oportunamente las posibles acciones enemigas en esta esfera, se implementó un basamento legal que establece los requisitos de seguridad en el empleo de las tecnologías de la información a partir de criterios de racionalidad y utilidad, que resulten susceptibles de verificación y tiendan a la disminución de los riesgos en la SI (MINCOM, 2007). Para ello el MINCOM estableció la Resolución 127/2007 que tiene por objetivo "establecer los requisitos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país" (MINCOM, 2007). Además, se cuenta con la traducción normalizada por la Oficina Nacional de Normalización de la NC-ISO/IEC 27001: 2007, elaborada por el Comité Técnico de Normalización NC/CTN 18 de Tecnología de la Información.

Sin embargo, al considerar la SI solo en ciertas etapas del proceso de desarrollo, podrían provocarse conflictos entre las necesidades de seguridad y los RF del sistema. Tener en cuenta la seguridad junto con los RF del sistema a través

de las etapas de desarrollo, ayudaría a limitar los casos de conflicto, identificándolos pronto en el desarrollo del sistema, y encontrando formas de superarlos.

Ingeniería de requisitos, conceptos y estándares

La Ingeniería de Requisitos (IR) es el conjunto de procesos, tareas y técnicas que permiten la definición y gestión de los requisitos de un producto, de un modo sistemático (SOMMERVILLE 2011). Incluye las actividades relacionadas con la determinación de las necesidades o de las condiciones a satisfacer para hacer un software nuevo o modificado. Varios autores consideran que es una colección estructurada de actividades, mediante las cuales se obtienen, validan y mantienen documentados los requisitos del usuario y del sistema (JACOBSON *et al.* 2000; PRESSMAN and MAXIM 2015; SOMMERVILLE 2011).

Sommerville plantea que "los requisitos para un sistema son la descripción de los servicios proporcionados por el sistema y sus restricciones operativas. Reflejan las necesidades de los clientes de un sistema que ayude a resolver algún problema como el control de un dispositivo, hacer un pedido o encontrar información" (SOMMERVILLE 2011; 2005a).

Sommerville clasifica los requisitos en dos categorías (SOMMERVILLE 2005b):

- **Requisitos del usuario**: son declaraciones, en lenguaje natural y en diagramas, de los servicios que se espera que el sistema proporcione y de las restricciones bajo las cuales debe funcionar.
- **Requisitos del sistema**: establecen con detalle las funciones, servicios y restricciones operativas del sistema. El documento de requisitos del sistema (algunas veces denominado especificación funcional) debe ser preciso. Debe definir exactamente qué es lo que se va a implementar.

Para la Software Engineering Body of Knowledge (SWEBOK) existen dos grandes categorías en las que pueden clasificarse los requisitos (ISO/IEC 2005a), estas son:

- **RF**: especifican acciones que el sistema debe ser capaz de realizar, sin tomar en consideración ningún tipo de restricción física. Especifican el comportamiento de entrada y salida del sistema y surgen de la razón fundamental de la existencia del producto. Indican características y restricciones sobre la funcionalidad del software. Definen el comportamiento interno del sistema.

- **RNF**: son propiedades o cualidades que el producto debe tener, también son conocidos como atributos de calidad. Debe pensarse en estas propiedades como las características que hacen al producto atractivo, usable, rápido o confiable; normalmente están vinculados a RF.

Los RF y los RNF, pueden expresarse en términos del cliente y pueden ser descripciones no técnicas (SEI 2010). Algunas de las categorías de RNF son: apariencia o interfaz externa, usabilidad, rendimiento, soporte, portabilidad, seguridad, privacidad, legales, confiabilidad, ayudas y documentación en línea, y hardware. Estas categorías son relacionadas como características de calidad junto a sus sub-características dentro del modelo de calidad del producto que formaliza la ISO 25010 (ISO/IEC, NC 2016).

Las normas ISO e IEEE que tratan los temas relacionados con la IR, aunque son muy útiles, son considerados estándares con un alto grado de complejidad lo que dificulta su entendimiento debido en su mayor parte a que se encuentran desagregadas en varios documentos que tienden a confundir a los interesados en su implementación y esto implica un aumento en los esfuerzos y costos para preparar la documentación e implantación de los sistemas.

"Los modelos CMMI® (Capability Maturity Model® Integration) son colecciones de buenas prácticas que ayudan a las organizaciones a mejorar sus procesos. Estos modelos son desarrollados por equipos con miembros procedentes de la industria, del gobierno y del Software Engineering Institute (SEI) (…) Las buenas prácticas del modelo se centran en las actividades para desarrollar productos y servicios de calidad con el fin de cumplir las necesidades de clientes y usuarios finales" (SEI 2010).

CMMI define 22 áreas de procesos concentradas en cuatro grandes grupos (SEI 2010): Gestión de procesos, Gestión de proyectos, Ingeniería y Soporte. Las áreas de proceso de Ingeniería cubren las actividades de desarrollo y mantenimiento que se utilizan en las disciplinas ingenieriles y se aplican al desarrollo de cualquier producto (SEI 2010):

- Integración del Producto (PI).
- Desarrollo de Requisitos (RD).
- Solución Técnica (TS).
- Validación (VAL).
- Verificación (VER).

Entre las áreas de Gestión de proyectos se encuentra Administración de Requisitos (REQM, por sus siglas en inglés), importante también en la IR y estrechamente relacionada con las del grupo ingenieril (SEI 2010). El proceso REQM trata directamente la planificación, el monitoreo, las inconsistencias y la trazabilidad de los requisitos. De las áreas de procesos del grupo Ingeniería, es relevante para la investigación el RD por las definiciones hechas para la descripción y el desarrollo de los requisitos.

A partir de la importancia que se le confiere a la identificación temprana de los requisitos de seguridad y su seguimiento durante el ciclo de vida del proyecto, y teniendo en cuenta que la actividad productiva de la UCI está certificada con el nivel 2 de madurez de CMMI y se encuentra en el proceso de definición de los materiales para la certificación del nivel 3 se decide utilizar el modelo CMMI. Especialmente, las definiciones realizadas por la universidad de las áreas de procesos REQM y RD para la definición de los requisitos de seguridad, tomando como apoyo las definiciones de la ISO 25010 para el atributo de calidad seguridad. Para el análisis de la trazabilidad bidireccional de los requisitos se utilizará el subproceso definido por la universidad para el nivel 2 de CMMI. La trazabilidad ayuda a determinar si todos los requisitos fuente se han tratado totalmente y si todos los requisitos de nivel más bajo se pueden tracear hacia una fuente válida. Se hace además necesaria a la hora de evaluar el impacto de los cambios de los requisitos sobre las actividades del proyecto y los productos de trabajo resultantes.

Resultados y discusión

Requisitos de Seguridad para aplicaciones web

El alcance específico de la seguridad debe estar claramente definido por los interesados en términos de los activos a los que se aplica la seguridad y las consecuencias contra las que se evalúa la seguridad.

Teniendo en cuenta los resultados de encuestas aplicadas a diversos roles inmersos en el desarrollo de software pertenecientes a varias áreas de la UCI, a lo planteado por la Norma Ramal (NR) 2-1 Requisitos de la Calidad para Sistemas Informáticos y Productos de Software (CALISOFT 2018), los Diez riesgos más críticos en Aplicaciones Web de OWASP (OWASP 2017b), y el Estándar de Verificación de Seguridad en Aplicaciones de OWASP (OWASP *et al.* 2017) se identificaron un conjunto de requisitos de seguridad que deben gestionarse en el desarrollo de aplicaciones web en la UCI. Los requisitos fueron agrupados de acuerdo a los principales objetivos de seguridad o sub-características analizadas en la investigación. Para la validación de los mismos se utilizó la técnica de grupo focal.Como resultado de la aplicación de esta técnica se obtuvo como resultado un total de 37 requisitos.

Integridad:

- RNFS 1: utilizar marcos de trabajo que automáticamente previenen los ataques XSS (Cross-Site Scripting o inyección de código malicioso).
- RNFS 2: validar los datos que se reciben y velar por la integridad de los datos que se devuelven.
- RNFS 3: prevenir los ataques CSRF (del inglés Cross-Site Request Forgery o falsificación de petición en sitios cruzados).
- RNFS 4: evitar las inyecciones de código.
- RNFS 5: utilizar LIMIT y otros controles SQL para evitar la fuga masiva de datos en caso de inyecciones SQL.
- RNFS 6: realizar validaciones para la entrada de datos al servidor utilizando “listas blancas”.
- RNFS 7: cifrar los datos sensibles que sean almacenados.

Confidencialidad:

- RNFS 8: proteger las conexiones autenticadas o que involucren funciones o información relevante.
- RNFS 9: no mostrar referencias hacia objetos internos de la aplicación.
- RNFS 10: no se deben mostrar mensajes con información que ayude a recopilar información sobre el producto o las configuraciones del servidor.
- RNFS 11: evitar la elevación de privilegios en las cuentas de usuarios.
- RNFS 12: todos los elementos de la infraestructura deben ser revisados para asegurarse de que no contienen ninguna vulnerabilidad conocida, así como las herramientas administrativas usadas para el mantenimiento de los diferentes componentes.
- RNFS 13: no almacenar datos sensibles de manera innecesaria.
- RNFS 14: deshabilitar el almacenamiento en caché de datos sensibles.

Disponibilidad:

- RNFS 15: realizar estudio sobre las posibles vulnerabilidades que se puedan presentar en la tecnología a utilizar en el desarrollo.
- RNFS 16: utilizar tecnologías seguras para el desarrollo.
- RNFS 17: cumplir los requisitos exclusivos de los límites de negocio de las aplicaciones.
- RNFS 18: controlar el receptor de escucha de las Bases de Datos.

- RNFS 19: garantizar que el servidor no envíe directrices o cabeceras de seguridad a los clientes o que se encuentren configurados con valores inseguros.
- RNFS 20: actualizar las configuraciones apropiadas de la tecnología usada de acuerdo a las advertencias de seguridad y seguir un proceso de gestión de parches.
- RNFS 21: utilizar una herramienta para mantener un inventario y control de versiones de los componentes
- RNFS 22: utilizar componentes únicamente de orígenes oficiales y utilizando los canales seguros.
- RNFS 23: analizar riesgos y vulnerabilidades del entorno de despliegue del cliente atendiendo a sus características.

No repudio:

- RNFS 24: cifrar todos los datos en tránsito utilizando protocolos seguros.
- RNFS 25: identificar o firmar de forma única los mensajes intercambiados.
- RNFS 26: almacenar los mensajes intercambiados en ficheros logs para su posterior consulta.

Autenticación o Autenticidad:

- RNFS 27: no mantener contraseñas creadas por defecto, débiles o muy conocidas especialmente en el caso de los administradores del sistema.
- RNFS 28: definir mecanismos de autenticación personalizado para todos los usuarios del sistema.
- RNFS 29: no se deben utilizar cuentas suministradas por defecto.
- RNFS 30: no permitir ataques de fuerza bruta y/o ataques automatizados.
- RNFS 31: utilizar controles contra contraseñas débiles.
- RNFS 32: alinear la política de longitud, complejidad y rotación de las contraseñas establecidas.
- RNFS 33: limitar el tiempo de respuesta de cada intento fallido de inicio de sesión.
- RNFS 34: controlar el ciclo de vida de las contraseñas.
- RNFS 35: un usuario estándar (no administrador) no debe tener acceso a modificar sus privilegios en la aplicación o los de otro usuario con su mismo rol.
- RNFS 36: cerrar automáticamente la sesión de un usuario cuando ha estado inactivo durante un cierto lapso de tiempo.

- RNFS 37: destruir el identificador de sesión luego de salir o cerrar el sistema.

Con la identificación de los requisitos expuestos en la investigación, se pretende que el uso de estos contribuya a elevar el conocimiento en materia de SI y la calidad en el desarrollo de aplicaciones web, gracias a la tipificación de riesgos y/o vulnerabilidades que pueden estar presentes tanto en el entorno del cliente como en el equipo de desarrollo.

Conclusiones

En el presente trabajo se hace una revisión de conceptos relevantes sobre SI. Este análisis permitió arribar a las siguientes conclusiones: la SI se enfoca en minimizar los riesgos existentes en el acceso y utilización mal intencionada de la información de los sistemas de software. La SI es un tema que recibe la atención de la industria de software lo que se puede evidenciar con la presencia de varios documentos tales como la familia de normas ISO/IEC 27000, diferentes materiales estandarizados de OWASP y la Resolución 127:2007 del MINCOM que ofrecen definiciones precisas para la identificación temprana de los requisitos de seguridad. A partir de las definiciones hechas en las áreas de procesos de REQM y RD del modelo CMMI para la UCI, se realizaron las modificaciones necesarias para lograr una correcta gestión del RNF de Seguridad. La correcta interpretación de las sub-características de seguridad definidas en la ISO 25010 y los riesgos más críticos propuestos por OWASP en el año 2017, favorecieron la identificación de una lista de RNF de Seguridad que contribuye a disminuir las vulnerabilidades en los desarrollos de aplicaciones web.

Referencias

AGUILERA LÓPEZ, P. *Seguridad informática*. México, 2010. p.

ARORA, V. Comparing different information security standards: COBIT v s. ISO 27001 *Qatar: Carnegia Mellon University*, 2010.

CALISOFT, C. N. D. C. D. S. *Norma Ramal – Requisitos de la Calidad para Sistemas Informáticos y Productos de Software*, 2018. [2018]. Disponible en: http://subcomite7.cubava.cu/2017/02/10/norma-ramal-requisitos-de-la-calidad-para-sistemas-informaticos-y-productos-de-software/

CDI. *Centro de Delitos Informáticos*. *Centro de Delitos Informáticos*, 2017.

GARFINKEL, S.; G. SPAFFORD, *et al. Seguridad y comercio en el Web*. McGraw-Hill, 1999. p. 9701021428

GIL VERA, V. D. and J. C. GIL VERA Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas *Scientia et technica*, 2017, 22(2).

ISO. *ISO 9000:2000 Sistemas de gestión de la calidad — Conceptos y vocabulario*. 2000. p.

ISO/IEC. *Ingeniería de Software - Guía del Cuerpo de Conocimiento de Ingeniería de Software (SWEBOK)*, 2005a. First edition: 210.

---. *ISO/IEC 27001 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*, Switzerland, 2005b.

--- ISO/IEC 27002: 2013 Information technology — Security techniques — Code of practice for information security management, 2013.

ISO/IEC, N. INGENIERÍA DE SOFTWARE Y SISTEMAS – REQUISITOS DE LA CALIDAD Y EVALUACIÓN DE SOFTWARE (SQuaRE) – MODELOS DE LA CALIDAD DE SOFTWARE Y SISTEMAS

(ISO/IEC 25010: 2011, IDT), 2016.

JACOBSON, I.; G. BOOCH, *et al. El proceso unificado de desarrollo de software/The unified software development process*. Pearson Educación, 2000. p. 8478290362

LARROCHA, E. R. *Nuevas tendencias en los sistemas de información*. Editorial Centro de Estudios Ramón Areces S. A., 2017. 332 p. 978-84-9961-269-0

LOSAVIO, F. and Y. ESTEVES. *Modelado del Negocio como Técnica Centrada en la Calidad del Software para el Análisis del Dominio del Aprendizaje Electrónico*. IV Simposio Científico y Tecnológico en Computación/SCTC 2016/ISBN: 978-980-12-8407-9. Universidad Central de Venezuela, Caracas, Venezuela, 2016. p.

MARTÍN, A. R. and M. J. R. MARTÍN. *Aplicaciones web*. Ediciones Paraninfo, SA, 2014. p. 8428398755

NAUR, P. and B. RANDELL Software Engineering: Report of a conference sponsored by the NATO Science Committee, Garmisch, Germany, 7th-11th October 1968, 1968.

NIÑO BENITEZ, Y. and N. SILEGA MARTÍNEZ Requisitos de Seguridad para aplicaciones web *Revista Cubana de Ciencias Informáticas*, 2018, 12: 205-221.

OWASP. *OWASP*. *OWASP*, 2017a.

---. *OWASP Top 10 - 2017 Los diez riesgos más críticos en Aplicaciones Web*, 2017b.

--- OWASP Top 10 controles proactivos 2016, 2016: 28.

OWASP; J. MANICO, *et al.* Estándar de Verificación de Seguridad en Aplicaciones 3.0.1, 2017.

PRESSMAN, R. S. and B. R. MAXIM. *Ingeniería de Software. Un enfoque práctico*. 8th. 2015. p. 978-0-07-802212-8

PROENÇA, D. and J. BORBINHA. *Information Security Management Systems-A Maturity Model Based on ISO/IEC 27001*. International Conference on Business Information Systems, Springer, 2018. 102-114 p.

RADATZ, J.; A. GERACI, *et al*. IEEE standard glossary of software engineering terminology *IEEE Std*, 1990, 610121990(121990): 3.

SEI. *CMMI® para Desarrollo, Version 1.3*, Carnegie Mellon University., 2010.

SOMMERVILLE, I. *Ingeniería de software*. 9na. Addison-Wesley, 2011. p. 978-607-32-0603-7

---. *Ingeniería del software*. Pearson Educación, 2005a. p. 8478290745

---. *Ingeniería del software. 7ma Edición*. United Kingdom, Pearson Education, 2005b. p.

URBINA, G. B. *Introducción a la seguridad informática*. Grupo Editorial Patria, 2016. p. 6077444715

VALLE ROJO, S. D. and A. OLIVEROS Elicitación y especificación de requerimientos no funcionales para aplicaciones web, 2014.