Universidad de las Ciencias Informáticas

Facultad 3

Título: Propuesta de Norma Técnica para contribuir al desarrollo de software seguro en el Centro de Gobierno Electrónico (CEGEL).

Trabajo de Diploma para optar por el título de

Ingeniero en Ciencias Informáticas.

Autor: Ivian Naivis Albear Lara.

Tutor: Ing. Linnet Acosta De La Cruz.

Ciudad de La Habana, Junio de 2011.

"Año 53 de la Revolución."

El futuro de Cuba tiene que ser necesariamente un futuro de hombres de ciencia, de hombres de pensamiento

Fidel Castro Ruz.

DECLARACIÓN DE AUTORÍA:

Declaro ser autor de la presente tesis y reconozco a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los _____ del mes de _____ del año _____.

Ing. Linnet Acosta De La Cruz	Ivian Naivis Albear Lara.
_____	_____
(Firma del tutor)	(Firma del autor)

DATOS DEL CONTACTO:

Tutora: Ing. Linnet Acosta De La Cruz

Clasificación: Investigación.

Clasificación del área de desarrollo: Gestión de proyectos.

Síntesis de la Tutora: Profesor Instructor Ing. en Ciencias Informáticas en el año 2008, ha tutorado varias tesis desde el curso 2008 – 2010.

Categoría Docente: Instructor

DEDICATORIA:

Dedico este trabajo a mi familia,

en especial a mi mamita y a mi abuela Norma.

A ellas que las adoro con la vida.

A ellas por ser la razón de mi existir.

AGRADECIMIENTOS:

A mi mamá por sobre todas las cosas, por su apoyo incondicional, por ser la guía de mis pasos y la llama que me alumbra en los momentos más oscuros de mi vida, por la confianza que depositó en mí, por ser mi mayor consejera, por ayudarme cada día a ser mejor como persona y como profesional, por enseñarme que la vida está llena de sacrificios y esfuerzos, por su amor inigualable, a ella gracias por existir.

A mi abuelita Norma, por ser otra madre para mí, por defenderme de todos, por su amor incondicional, por su apoyo, por complacerme en la mayoría de mis antojos y ayudarme en lo que necesité y por estar a mi lado en todo momento.

A mi papá, sé que se siente orgulloso de tener una ingeniera en la familia por sus consejos, comprensión y cariño. A mi otra abuela por su ternura. A mis tías, tíos, primos y primas, por ayudarme cuando los necesité, en especial a Yiri por hacer el papel más que de prima, de hermana, y a la familia de Ciudad Habana que durante estos 5 años me acogieron fin de semana tras fin de semana y me brindaron su casa a cambio de nada. A mis abuelos que a pesar que ya no están a ellos les debo mucho. En fin, a toda mi familia que ha estado al tanto en cada momento de mi trayectoria y resultados.

A todos mis vecinos sin dejar de nombrar a Dalgita, Alina, Ana Irma, Mima, Yolanda, Omara, Nidia, a Eddy que ha sido un padre para mí, a mi hermanita Celine por llamarme manita con tanto amor y querer a mi madre como tal; a ella dedico este trabajo para que se forme como yo y mejor.

A mis queridos amigos: La Yiya, Aliuska, Barberán, Lugo (por ser gran parte de mi vida en esta escuela, por soportarme tanto tiempo y por ayudarme muchísimo), Leisy, Rowe, Elizabetha Eichell por ser especial en mi vida. A todos los que alguna vez fueron compañeros de aula y producción, a mis fans de la antigua facultad 4, a los del piquete de los "3m2(Kela, Shaqui, Cervela, Dayan, Pablo y Yaksel), a todos lo que me hicieron reír y compartir momentos muy felices y a los que me llamaban loca cariñosamente.

A mi tutora porque sin ella no hubiese sido posible que todo saliera como tal, por soportarme, por su paciencia, por toda su ayuda durante el desarrollo de este Trabajo de Diploma. A los especialistas que validaron el trabajo en especial a Yanet y a Yurita por ser buenas consejeras y dedicarme su tiempo. Al tribunal y a nuestro líder de la revolución Fidel Castro por confiar en los jóvenes conectados al futuro, y permitirnos crecer como profesionales, en su obra creadora: La Universidad de la Ciencias Informáticas.

Ivian Naivis Albear Lara.

RESUMEN:

Existe una relación directa entre el desarrollo de la seguridad informática y los ataques que atentan contra sus características básicas: la confidencialidad, integridad y disponibilidad de la aplicación.

El avance tecnológico ha devenido en la informatización de los procesos de negocios a través del desarrollo de software que deben cumplir con las necesidades de los clientes, lo que incrementa la importancia de la seguridad de estos sistemas pues manejan en la mayoría de los casos datos sensibles. Es imprescindible ser cuidadosos durante el desarrollo de estas aplicaciones, para evitar vulnerabilidades que pudieran ser aprovechadas por atacantes.

En los proyectos productivos del Centro de Gobierno Electrónico (CEGEL) se detectan defectos en las fases finales del proceso de desarrollo del software, en algunos casos ocasionados por problemas desde las primeras etapas lo que origina retraso en la entrega e insatisfacción del cliente que espera recibir un producto en tiempo y con la seguridad requerida.

En el presente trabajo se propone una norma técnica que abarca 4 momentos fundamentales durante el desarrollo de software, en cada de uno de ellos se proponen reglas que contribuyen a garantizar un nivel mínimo de seguridad en las aplicaciones desarrolladas en el marco del gobierno electrónico en la Facultad 3. Para elaborar la propuesta se estudiaron las normas internacionales relacionadas con la seguridad del software, las resoluciones cubanas, así como todo el basamento teórico necesario para su confección y validación.

Palabras claves: desarrollo de software, norma técnica, seguridad, software.

ÍNDICE:

ÍNDICE DE FIGURAS:

ÍNDICE DE TABLAS:

INTRODUCCIÓN

Durante el desarrollo de software, en muchas ocasiones, no se presta la suficiente atención a un atributo fundamental de los programas informáticos: la seguridad. Generalmente esto sucede debido a la presión por cumplir con el calendario y el presupuesto del proyecto, así como la exigencia de los usuarios por disponer de nuevas funcionalidades. (1)

Es bastante común que en organizaciones que producen software, no exista ninguna incorporación formal de medidas de seguridad al ciclo de desarrollo. La realidad es que en la mayoría de los casos el software se valora fundamentalmente por la funcionalidad que implementa y la calidad del código raramente se considera. (1)

El **proceso de desarrollo de software** "es aquel en que las necesidades del usuario son traducidas en requerimientos de software, estos requerimientos transformados en diseño y el diseño implementado en código, el código es probado, documentado y certificado para su uso operativo". Concretamente "define quién está haciendo qué, cuándo hacerlo y cómo alcanzar un cierto objetivo". (2)

El proceso de desarrollo de software tiene como finalidad la entrega de un producto a un cliente a partir de requisitos definidos previamente, una aplicación o programa que informatice los procesos de ese cliente de modo que los haga más eficientes y eficaces.

La seguridad aún cuando es tan importante para garantizar la protección de los datos ante intrusos o usuarios inexpertos del sistema, no se incluye como un aspecto fundamental a tener en cuenta durante el desarrollo del software o una vez terminado, sin embargo en los últimos años han surgido normas y leyes en diferentes países para garantizar que las aplicaciones una vez desplegadas provean la calidad necesaria a los clientes y la confianza en las empresas desarrolladoras.

La Universidad de las Ciencias Informáticas (UCI) tiene como parte de su misión la informatización del país, y establecerlo como un ente desarrollador de software reconocido internacionalmente. Con el objetivo de obtener mejores resultados durante el proceso de desarrollo de software en la UCI; y cumplir de forma exitosa los compromisos contraídos con los clientes, surgen centros de desarrollo pertenecientes a las respectivas facultades donde fueron creados.

Uno de los centros con que cuenta la Facultad 3 es el Centro de Gobierno Electrónico (CEGEL), en el mismo se desarrollan productos tanto nacionales como internacionales, de alto impacto en la sociedad.

Después de profundizar en los temas de seguridad informática es importante señalar que cada proyecto gestiona la seguridad de sus aplicaciones como estimen conveniente sus miembros. En su estructura interna se aplican las técnicas de seguridad que se consideren necesarias, lo que implica que la seguridad del software se maneja de modo diferente en los productos del centro. En algunos casos se pone en práctica la seguridad reactiva, en otras palabras “la seguridad es sobre la marcha, a medida que van apareciendo los problemas”, y este es el principal conflicto al que se desea dar solución: en la mayoría de los proyectos del centro, como son: Registros y Notarías (RN2 y RN3) en sus fases dos y tres respectivamente, Convenio Integral de Cooperación Cuba-Venezuela (CCV), Sistema de Gestión Fiscal (SGF), Centro de Documentación e Información Judicial (CENDIJ), Grupo de Arquitectura Tecnología y Seguridad (GATS), Tribunales Populares de Cuba (TPC), Calidad y el Portal de la Unión Nacional Jurista de Cuba (UNJC) no tienen en cuenta durante la programación de los módulos establecer mecanismos que aseguren los principios básicos necesarios para la seguridad del software. No presentan un estándar que desde el inicio de la elaboración de los módulos les permita obtener una seguridad en cada etapa de desarrollo. Todos pasan por una etapa de calidad lo mismo dentro del proyecto que cuando concluye el módulo por el grupo de calidad de la facultad, donde solo se comprueba a partir de los Diseños de Casos de Pruebas que la aplicación cumpla con los requisitos funcionales descritos, por tanto este proceso que se lleva a cabo no brinda la seguridad requerida al producto.

A partir de la situación anteriormente descrita se plantea el siguiente **problema de la investigación:** ¿Cómo establecer mecanismos estandarizados para contribuir a garantizar la seguridad durante el proceso de desarrollo de software en los proyectos del Centro de Gobierno Electrónico (CEGEL)?

La investigación determina como **objeto de estudio** el proceso de normalización para el desarrollo de software.

Se define como **objetivo general** proponer una norma técnica para contribuir al desarrollo de software seguro en el Centro de Gobierno Electrónico, y el **campo de acción** se precisa en las normas técnicas para el desarrollo de software seguro en el Centro de Gobierno Electrónico (CEGEL).

Durante la investigación se pretende **defender** la siguiente **idea**: proponiendo una norma técnica que establezca mecanismos seguros durante el proceso de desarrollo de software, se contribuirá a elevar la seguridad del producto final en los proyectos del Centro de Gobierno Electrónico.

Como **objetivos específicos** se establecen:

- Elaborar marco teórico de las normas y leyes existentes para el desarrollo seguro de software tanto internacional como nacionalmente.
- Proponer norma técnica para el desarrollo de software seguro en el Centro de Gobierno Electrónico.
- Validar la norma propuesta.

Para dar cumplimiento a los objetivos mencionados anteriormente se desarrollarán las siguientes **tareas de la investigación:**

- Definición de los aspectos teóricos de la seguridad de la información.
- Análisis de las características y aspectos esenciales de una norma.
- Determinación de las normas y leyes internacionales más importantes definidas para el desarrollo seguro de software.
- Determinación de las normas y leyes cubanas existentes para el desarrollo seguro de software.
- Redacción de norma técnica para el desarrollo seguro de software.
- Validación de la norma técnica propuesta.

Para el desarrollo de esta investigación fueron utilizados métodos teóricos y métodos empíricos.

Dentro de los métodos teóricos se utilizaron:

- Analítico-Sintético: se hace un análisis de las normas para la seguridad en el mundo, Cuba y la UCI, se determinan las características generales así sus relaciones.
- Histórico: se hizo un estudio de la trayectoria de las normas y sus condiciones históricas fundamentales.

Dentro de los métodos empíricos se utilizaron:

- Observación: surgió la idea de elaborar una norma técnica para la seguridad durante el proceso de desarrollo de software a partir de la problemática descrita anteriormente.
- Entrevistas: se realizaron encuestas para comprobar la necesidad de confeccionar la norma.

La estructura del documento está definida de la siguiente manera:

- **En el Capítulo 1. Fundamentación teórica:** Se exponen los conceptos fundamentales relacionados con seguridad, norma técnica y normalización. Se analiza la situación actual de las normas o guías de seguridad que existen tanto en el mundo como en Cuba, así como el estado del tema en la UCI. Se adopta una posición crítica que permita hacer la selección adecuada de aquellos elementos que deben estar presentes en la propuesta.
- **En el Capítulo 2. Propuesta de solución:** Se realiza la descripción y análisis de la solución propuesta; se propone una serie de reglas a tener en cuenta durante el desarrollo de software para que el producto final cumpla con requisitos de seguridad mínimos necesarios.
- **En el Capítulo 3. Validación de la propuesta:** A partir de entrevistas y cuestionarios que se aplicaron a una serie de especialistas en los temas tratados se realizó la validación de la norma propuesta.

Capítulo 1

Fundamentación Teórica

1.1. Introducción

Durante el proceso de desarrollo del software la mayoría de los proyectos, orientados a satisfacer las expectativas del cliente, no tienen un nivel de seguridad óptimo ya sea porque no se hace un análisis de los posibles riesgos que pueden atacar y enfrentar el software, porque se piensa que un software es totalmente seguro si se ejecuta correctamente a partir del diseño o por la ausencia de mecanismos estandarizados que posibiliten determinar medidas de seguridad para aplicarlas durante el desarrollo.

El presente capítulo contiene definiciones y conceptos significativos relacionados con la seguridad del software durante su ciclo de vida. Se hace una investigación de las principales normas utilizadas mundialmente donde se explica el estado actual de las mismas para así aplicar comparativas y realizar una selección adecuada según las características de los proyectos del Centro de Gobierno Electrónico (CEGEL).

1.2. La seguridad durante el proceso de desarrollo del software.

Según la Real Academia Española, define seguridad como “Calidad de seguro”, y a su vez define seguro como “Libre y exento de peligro”. (3)

La seguridad puede dividirse en seguridad reactiva y en seguridad preventiva:

“La **Seguridad Reactiva** se activa una vez ocurrido el evento no deseado, tiene como objetivo estructurar la organización para minimizar las consecuencias de lo ocurrido y permitir enfrentar el presente y futuro de la mejor forma posible, a pesar de lo ocurrido”. (4)

“La **Seguridad Preventiva** reduce la probabilidad de ocurrencia de eventos no deseados y reduce las consecuencias en caso de llegar a ocurrir dicho evento, que puede ocurrir a pesar de las medidas preventivas.” (4)

Sin lugar a dudas la seguridad preventiva como su nombre lo indica, permite prevenir los posibles riesgos por lo tanto sería la más adecuada para los proyectos del CEGEL.

1.2.1 ¿Qué es la Seguridad de la Información?

El Diccionario de la Real Lengua Española define además diferentes acepciones para la palabra información:

"Comunicación o adquisición de conocimiento que permite ampliar o precisar los que se posean sobre una materia determinada". (3)

"Conocimientos así comunicados o adquiridos". (3)

Existen varios autores que han aportado una definición del término, pero se puede decir que uno de los que más se ha aceptado es el de Miguel Ángel Davara Rodríguez, que plantea: "la información es el resultado del tratamiento de un dato o conjunto de datos orientado y adecuado a un fin determinado". (5)

Los autores de libro "Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas", Emilio del Peso Navarro y Miguel Ángel Ramos González adoptan que "la información simplemente es el conjunto de datos debidamente organizados que brinden conocimiento". (5)

Estos dos últimos conceptos, unidos al término seguridad que se menciona anteriormente, son los adoptados para tratar el tema de la Seguridad de la Información en la presente investigación. Se entiende que la información es el procesamiento de datos o conjunto de datos que aportan conocimiento, y por tanto tienen un valor que es necesario proteger para aquellos que la poseen.

La información de una entidad, empresa, institución, organización o simplemente de las personas, por sí sola posee entonces un valor que estará determinado en la medida del conocimiento que brinda y el interés de esas entidades de cuánto quieren que se sepa de ellos.

Los activos informáticos más importantes para una organización son el hardware, el software y la información. Por tanto, la seguridad de la información se alcanza implantando un conjunto de controles adecuados, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deben ser establecidos, implementados, monitoreados, revisados y mejorados cuándo y dónde sea necesario, para asegurar las características de la seguridad

y que se cumplan los negocios de la organización. (6). Precisamente la aplicación de todos estos elementos es considerada como la gestión de la seguridad de la información. La seguridad informática tiene como objetivo fundamental proteger los activos informáticos mencionados anteriormente.

Para lograr seguridad en las aplicaciones se debe tener en cuenta tres aspectos básicos: la confidencialidad, la integridad y la disponibilidad. Se definen de la siguiente forma:

- Confidencialidad: la aplicación tiene que ser accedida solo por las personas autorizadas.
- Integridad: se refiere a que la aplicación solo puede ser modificada por las personas autorizadas para ello.
- Disponibilidad: plantea que la aplicación tiene que estar disponible para las personas autorizadas en el momento que lo requieran. (5)

Desde el punto de vista de la gestión de la seguridad de la información, las empresas, instituciones, en general toda entidad que posea información, debe establecer acciones que garanticen sus características básicas.

1.2.2 Seguridad durante el proceso de desarrollo de software

El proceso de desarrollo de software tiene como producto final una aplicación, programa o software que gestiona determinados procesos para los que fue diseñado, por tanto maneja información, con determinado valor para sus dueños, entonces trae consigo los problemas para la seguridad de la información.

Debido a los problemas de planificación y presupuesto, la seguridad sólo es tenida en cuenta una vez que los requerimientos funcionales son obtenidos. Por consiguiente, conduce a que la seguridad sea considerada como un concepto que se incorpora tardíamente al sistema; esto conlleva a un diseño pobre e ineficiente de la seguridad, y trae como resultado una implementación inadecuada de la misma. También, la mayoría de las metodologías de diseño y herramientas dedicadas a la seguridad trabajan de esta forma, con ideas de último momento. Por lo tanto, es mandatorio que los conceptos de seguridad formen parte integral en todo el ciclo de vida de desarrollo de software.

Una manera de iniciar o perfeccionar la seguridad en las aplicaciones es pensar en los posibles riegos que puedan atacar y enfrentar el programa informático, para ello se debe antes analizar y mejorar la calidad de la seguridad durante el proceso de desarrollo del software y de esta forma poder lograr

buenos resultados. Eso significa comprobar la seguridad durante la gestión de los requerimientos, análisis y diseño, desarrollo y prueba, independientemente de la metodología de desarrollo que se utilice, y no confiar en la costosa estrategia de esperar hasta que el código esté construido por completo. Por lo general se especula que un software es totalmente seguro si al final este se ejecuta perfectamente, pero esto es una mala práctica del programador.

La seguridad en el software es la mejor forma de hacer seguridad preventiva, hace que la probabilidad de encontrar puertas traseras o fallas de programación en el software sea casi nula y a su vez no pueda haber robo de información.

Las puertas traseras o agujeros, como también se le conoce, en el software son utilizadas de forma directa o indirecta para ganar acceso no autorizado o como punto para atacar a otros ordenadores. Estos agujeros se deben básicamente a descuidos o fallos en la construcción del programa. La mejor forma de evitar descuidos es adoptando estándares y buenas conductas a lo largo del proceso de construcción.

Por ende, es de suma importancia la gestión de la seguridad en las aplicaciones desde el inicio del proyecto hasta su fin, desde que se dan los primeros pasos en la captura de requisitos tratando de entender lo que el cliente desea o necesita, hasta que se le entrega un software con las funcionalidades que satisfacen esas necesidades.

1.2.3 Seguridad durante el proceso de desarrollo de software en Cuba

El desarrollo del software en Cuba se puede considerar incipiente aún, y por ello el gobierno ha trazado desde hace más de una década estrategias que posibiliten elevar la producción y la calidad de este. Uno de los principales impulsos ha sido la creación de la Universidad de las Ciencias Informáticas (UCI), donde se implementan aplicaciones tanto para clientes extranjeros como nacionales.

El Ministerio de la Informática y las Comunicaciones (MIC) el que tiene la responsabilidad de lograr la seguridad en las Tecnologías de la Información y las Comunicaciones (TICs), a través de La Oficina de Seguridad para las Redes Informáticas (OSRI), que tiene por 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.

- Fortalecer la seguridad durante el empleo de las Tecnologías de la Información. Su propósito consiste en implementar un sistema que contribuya al ordenamiento de las actividades asociadas con las redes informáticas y de comunicaciones, mediante el establecimiento de un esquema que garantice niveles aceptables de seguridad. (7)

Las acciones que se llevan a cabo en el MIC no son suficientes para aplicarlas en los proyectos del centro pues se encargan del aseguramiento de las redes informáticas y la información que se trasmite por los medios tecnológicos de comunicación de forma general, no de la seguridad del software durante su desarrollo.

Es la misión estratégica de la empresa Segurmática brindar los servicios de seguridad informática demandados por las entidades radicadas en Cuba, sustituyendo importaciones y garantizando la seguridad del país, brindando los servicios siguientes:

- Suscripción anual a los productos de software antivirus, recuperación de información dañada en discos, confección de Planes de Seguridad Informática, realización de diagnósticos de seguridad a redes de computadoras, adiestramientos de seguridad informática, así como custodia de material informático. (7)

Para lograr el desarrollo en la Industria Cubana del Software (ICSW) se debe tener en cuenta la seguridad del mismo, aspecto fundamental para un buen posicionamiento en el mercado mundial y en el cual no está muy desarrollado aún. Alguna de las acciones que Cuba toma con respecto al tema es la creación de empresas de calidad como: la Empresa de Producción y Desarrollo de Software de Calidad (SOFTCAL), Grupo Nacional de Expertos en Calidad del Software (GNECS), Laboratorio Nacional de Certificación de la Calidad del Software (CALISOFT), las cuales su función principal es la obtención de software de calidad en la región, patentizando con ello la seguridad del mismo.

Se reconoce a partir de las misiones de las entidades dedicadas a la seguridad del software que no se le ha prestado la suficiente atención durante el proceso de desarrollo del mismo, debido que el país no tiene vasta experiencia en esta área y que en los últimos años es cuando se han realizado acciones en este sentido.

1.2.4 Seguridad durante el proceso de desarrollo de software en la UCI

En la Universidad de las Ciencias Informáticas, a pesar de todo el avance tecnológico con el que se cuenta y de todas las aplicaciones de gran impacto que se desarrollan no se había tomado conciencia

de lo importante que es tener en cuenta la seguridad en cada uno de los momentos por los que transita un software antes de ser entregado al cliente. La seguridad del software en la UCI es un aspecto que se ejecuta generalmente de forma reactiva y en muchos casos la seguridad preventiva es obviada, desde el comienzo mismo de la elaboración del software. La UCI cuenta con un grupo de calidad a nivel central (CALISOFT) y además uno en cada centro de desarrollo, donde los procesos de calidad que se llevan a cabo en cada uno de estos grupos no son suficientes para validar que los productos tengan la seguridad mínima requerida.

La identificación de riesgos es una de las medidas menos costosas en tiempo y recursos que se pueden tomar para identificar vulnerabilidades y trabajar en función de ellas para mitigarlas, sin embargo, se hace generalmente dirigida a los riesgos que afectan el desarrollo del proyecto para el cumplimiento de un cronograma y no orientado a identificar problemas de seguridad.

Entre los trabajos que se realizan se encuentra el de la Facultad 2, con un proyecto cuyo objetivo es liberar una herramienta capaz de revisar el código y determinar sus vulnerabilidades, así como las posibles soluciones que pueden ser tomadas para controlarlas y evitar que se conviertan en amenazas.

Pero aún con esta herramienta, si solo se depende de ella para garantizar la seguridad de una aplicación a partir de su código, se corre el riesgo de atrasar el desarrollo de un proyecto pues lo ideal sería no tener que revisar el código bajo la premisa de que este ha transitado por varias fases seguras y por tanto ya es confiable, y en el caso de que no lo sea, las vulnerabilidades serían mínimas. Sería recomendable que las medidas que se tomen para desarrollar software de modo seguro, vayan a la par con el proceso, de modo que este no se atrase, y se obtenga el producto con la calidad y seguridad requeridas para la completa satisfacción del cliente.

1.3. Estudios de Normas

1.3.1 ¿Qué son las normas?

Las normas son “un modelo, un patrón, ejemplo o criterio a seguir. Una norma es una fórmula que tiene valor de regla y tiene por finalidad definir las características que debe poseer un objeto y los productos que han de tener una compatibilidad para ser usados a nivel internacional”. (8)

Las normas permiten establecer disposiciones claras que faciliten la comunicación e intercambio institucional, nacional e internacional entre las empresas, los usuarios y los consumidores, pues son un

patrón necesario de confianza entre cliente y proveedor, es por eso la necesidad de aplicar en los proyectos del Centro de Gobierno Electrónico (CEGEL) de la Facultad 3 una regla a seguir a fin de obtener un mejor ordenamiento de las actividades para la seguridad del producto durante su proceso de desarrollo. Se puede decir además que las normas sirven de guía para regular los procedimientos a seguir en la ejecución de las tareas asignadas.

1.3.2 Normas técnicas

La Real Academia de la Lengua Española define la palabra norma entre sus acepciones como “regla que se debe seguir o que se deben ajustar las conductas, tareas, actividades”. (3)

Define la palabra técnica como adjetivo perteneciente o relativo a las aplicaciones de las ciencias y las artes, o como el conjunto de procedimientos y recursos de que se sirve una ciencia o un arte. (3)

Las normas técnicas son documentos donde se establecen especificaciones técnicas que se basan en la experiencia y el desarrollo tecnológico. Son redactadas por un comité técnico y deben ser consensuadas por consumidores, fabricantes, administración, laboratorios, centros de investigación, todas las partes que se vean afectadas por la aplicación de estas. Su aprobación está dada por un Organismo de Normalización reconocido. (9)

Internacionalmente las normas técnicas más reconocidas son las elaboradas por el Organismo Internacional de Normalización (ISO por sus siglas en inglés) y en Europa el Comité Europeo de Normalización. Los países también pueden tener su propia organización para la redacción de normas, los más reconocidos son:

- España: AENOR, Asociación Española de Normalización y Certificación.
- Francia: AFNOR, Association Francoise de Normalization.
- Alemania: DIN, Deutsches Institut fur Normung.
- Estados Unidos:
    - ANSI, American National Standards Institute.
    - ASTM, American Society for Testing and Materials. (9)

Las normas técnicas generalmente tienen que ser pagadas para aplicarlas, aunque no es obligatoria la implantación. Definen en sí mismas aspectos que deben ser seguidos cuando se quiere obtener determinado resultado. Proveen una garantía al usuario de que un producto cumple con determinadas

condiciones, por ejemplo las normas de seguridad; si un usuario compra un dispositivo que certifica que cumple con determinada norma de seguridad, le brinda confianza al usuario de que el producto obtenido es seguro, por tanto la certificación de una norma por una empresa le acredita un nivel de confianza y garantía de seguridad frente a sus clientes.

1.3.3 ¿Qué es la normalización?

La Real Academia de la Lengua Española define entre sus significados la palabra normalización como

"Acción y efecto de normalizar". (3)

Define entre sus acepciones la palabra normalizar como "Regularizar o poner en orden lo que no lo estaba."

"Tipificar" (ajustar a un tipo o norma). (3)

Según la ISO[1] la Normalización es la actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes y repetidos, con el fin de obtener un nivel de ordenamiento óptimo en un contexto dado, que puede ser tecnológico, político o económico.

Se puede concluir que la normalización es la redacción y aprobación de normas que se establecen a partir de acuerdos para garantizar el acoplamiento y la calidad de los elementos fabricados, la seguridad de funcionamiento y trabajar con responsabilidad social. La normalización es el proceso de elaboración y aplicación de las normas propuestas para distintas actividades científicas, industriales o económicas con el fin de ordenarlas y mejorarlas.

1.3.4 Familias ISO 27000: Seguridad de la Información

La ISO 27000 es la que realmente abarca todo lo relacionado con la seguridad de la información. Esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información (SGSI), una breve descripción del proceso Planificar-Hacer-Chequear-Actualizar (P-H-C-A) respectivamente (Figura 1), términos y definiciones que se emplean en toda la serie 27000.

[1] *ISO: Organismo Internacional de Normalización*

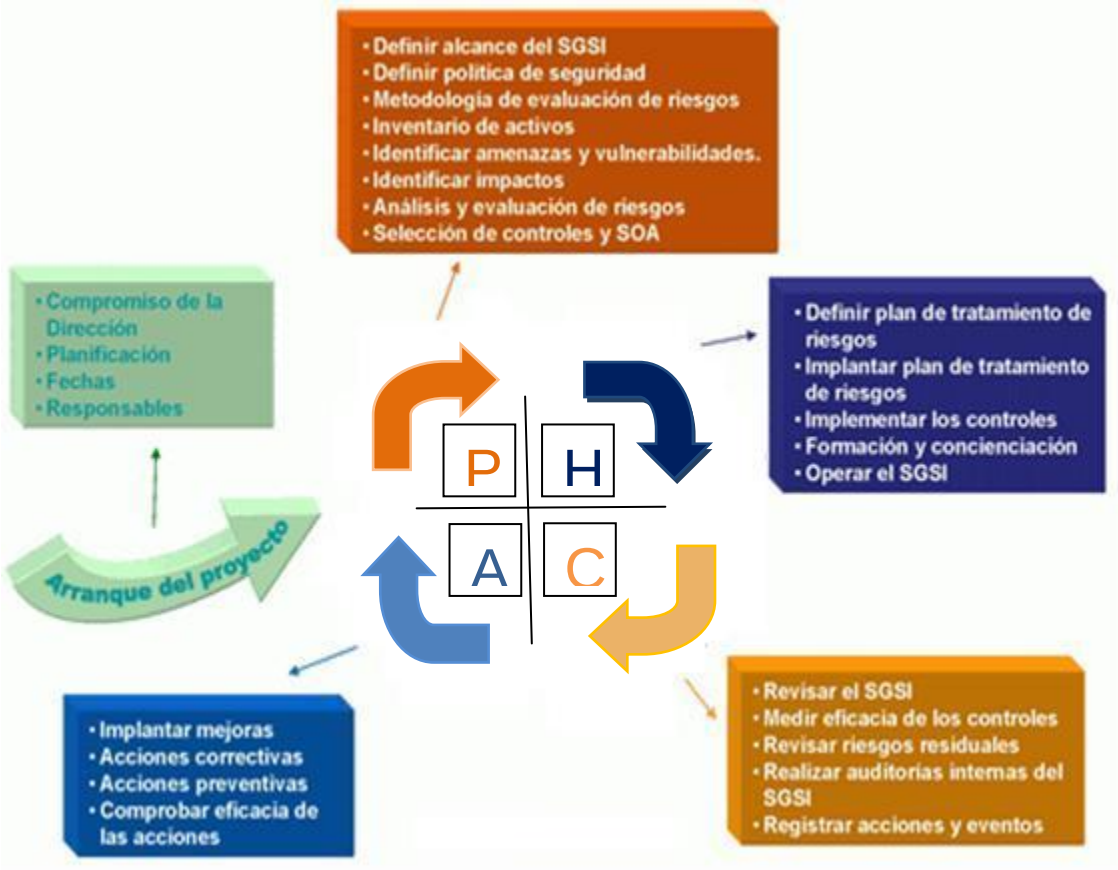

Figura 1. Proceso Planificar-Hacer-Chequear-Actualizar

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares y las normas que incluye son ISO/IEC 27000, a continuación se hace una análisis de la serie 27001 hasta la 27010.

• ISO/IEC 27001:

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Actualmente, este

estándar se encuentra en período de revisión en el subcomité ISO SC27, con fecha prevista de publicación en 2012.

• ISO/IEC 27002:

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

• ISO/IEC 27003:

No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

• ISO/IEC 27004:

No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase Hacer (Implementar y Utilizar) del ciclo.

• ISO/IEC 27005:

No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

• ISO/IEC 27006:

Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de

acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

• ISO/IEC 27007:

En fase de desarrollo, con publicación prevista en 2011. Consistirá en una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

• ISO/IEC 27008:

En fase de desarrollo, con publicación prevista en 2011. Consistirá en una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

• ISO/IEC 27010:

En fase de desarrollo, con publicación prevista en 2012. Es una norma en 2 partes, que consistirá en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales. (10)

1.3.5 Beneficios de las normas ISO

• Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
• Reducción del riesgo de pérdida, robo o corrupción de información.
• Los clientes tienen acceso a la información a través medidas de seguridad.
• Los riesgos y sus controles son continuamente revisados.
• Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
• Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
• Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001).
• Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
• Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
• Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
• Confianza y reglas claras para las personas de la organización.
• Reducción de costes y mejora de los procesos y servicio.
• Aumento de la motivación y satisfacción del personal.
• Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías. (10)

Cada una de estas normas establecen una serie de medidas que al menos buscan mejora continua y sin lugar a duda favorece la calidad de los productos de cualquier empresa y aumenta el porcentaje a pesar que la seguridad al 100 % no existe.

A pesar de los beneficios que brinda esta serie, presentan grandes desventajas para aplicarlas en el Centro de Gobierno Electrónico. Primeramente para adquirirlas hay que pagarlas, además al documentar el por qué la no implementación de cada uno de los controles que desarrolla, una vez definido que no es obligatoria dicha implementación, pueden causar retraso con la entrega del producto, sobrecargando el ritmo habitual del trabajo, por consiguiente se requiere de un esfuerzo adicional, la mayoría no son certificables y no brindan la total transparencia a la organización. Esto provoca desigualdad durante el proceso de seguridad que se lleve a cabo en los proyectos por ende no será un proceso estandarizado como realmente se desea. Destacar que estas normas se centran en la seguridad de la información, y no en la seguridad durante el desarrollo del software.

Sin embargo, teniendo en cuenta los aspectos más destacados e importantes que tiene cada una de ellas por separado, se quiere contruir una norma que recopile toda la informacíón logrando que esté al alcance de todos de forma gratuita, se centrará en la seguridad del código en las aplicaciones brindando la posibilidad de obtener un software con un mínimo de seguridad durante todo su proceso de desarrollo.

1.3.6 Normas en Cuba

Para el tema de las normas en Cuba se cuenta con el sitio “Normas Cubanas Online”. En el mismo solo se encuentran 3 normas referentes al software, y son dirigidas a su calidad como tal. (11) En cuanto a la seguridad durante el desarrollo de software no se encuentra ninguna norma publicada.

No obstante, sí existen resoluciones que contribuyen a garantizar la seguridad de la información, como lo es la Resolución 127/2007, el Reglamento de Seguridad para las Tecnologías de la Información. Aspectos importantes de este reglamento al que se suscriben todas las instituciones pertenecientes al MIC o que utilicen las tecnologías de la información. (12)

En sentido general la resolución aborda los lineamientos por los que deben regirse las organizaciones para lograr la seguridad de las tecnologías, entiéndase también como gestión de la seguridad de la información, pero no se abarca tampoco la seguridad específica que se debe tener en cuenta durante el desarrollo de una aplicación, o a todas las reglas que deben ser seguidas.

1.4. OWASP

El Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. (13)

Es una organización sin ánimos de lucro que no está afiliada a ninguna empresa de tecnología, y su principal objetivo es lograr que las empresas implementen prácticas seguras a partir de identificar los riesgos y los errores más comunes de programación. (14) Se centra fundamentalmente en las aplicaciones web pero muchos de los aspectos que aborda se pueden aplicar en las aplicaciones de escritorio. De todas formas, hoy en día debido al auge de las redes y las tecnologías la mayoría de aplicaciones que se desarrollan son web.

La intención de OWASP no es ni apuntar a una metodología de desarrollo en particular ni proporcionar unas directrices determinadas que se ajusten a una metodología específica. En vez de eso, se presenta un modelo de desarrollo genérico, donde el desarrollador debería seguirlo de acuerdo al proceso que emplee determinada compañía. (15)

El flujo de trabajo del entorno de pruebas OWASP está compuesto por cinco fases y estas compuestas por actividades. (15)

1.4.1 Fase # 1 Antes de comenzado el desarrollo

Antes que el desarrollo de la aplicación haya comenzado es necesario asegurar que:

- Existe un Ciclo de Vida de Desarrollo del Software (SDLC por sus siglas en inglés) adecuado, en el cual la seguridad sea inherente.
- Estén implementadas las políticas y estándares de seguridad adecuados para el equipo de desarrollo.
- Estén desarrolladas las métricas y criterios de medición.

Revisión de Políticas y Estándares.

- Asegurar que las políticas, documentación y estándares adecuados están implementados. La documentación es extremadamente importante, ya que brinda al equipo de desarrollo políticas y directrices a seguir.

- Si la aplicación va a ser desarrollada en JAVA, es esencial que haya un estándar de programación segura en Java. Si la aplicación va a utilizar criptografía, es esencial que haya un estándar de criptografía y así sucesivamente.
- Ninguna política o estándar puede cubrir todas las situaciones con las que se enfrentará un equipo de desarrollo. Documentando las incidencias comunes y predecibles, habrá menos decisiones que afrontar durante el proceso de desarrollo.

Desarrollo de Métricas y Criterios de Medición (Asegurar la Trazabilidad).

- Antes de empezar el desarrollo, es necesario planificar el programa de medición. Definir los criterios que deben ser medidos proporciona visibilidad de los defectos tanto en el proceso como en el producto.
- Es algo esencial definir las métricas antes de comenzar el desarrollo, ya que puede haber necesidad de modificar el proceso de desarrollo para poder capturar los datos necesarios.

1.4.2 Fase #2 Durante la definición de requisitos y el diseño.

Revisión de los Requerimientos de Seguridad.

- Los requisitos de seguridad definen cómo funciona una aplicación desde una perspectiva de la seguridad. Es indispensable que los requisitos de seguridad sean probados y comprobar si hay deficiencias en las definiciones de los mismos. Hay que asegurarse que los requisitos sean lo menos ambiguos posible.

Revisión del Diseño y de la Arquitectura.

- Las aplicaciones deberían tener una arquitectura y un diseño documentado (un modelo, o un documento de texto). Es indispensable comprobar estos elementos para asegurar que el diseño y la arquitectura imponen un nivel de seguridad adecuado.
- Identificar fallos de seguridad en la fase de diseño, no es solo efectivo por los costes a la hora de identificar errores, sino que también puede ser la fase más efectiva para realizar cambios. Por ejemplo, ser capaz de identificar que el diseño precisa realizar decisiones de autorización en varias fases; donde puede ser apropiado considerar un componente de autorización centralizado, es decir, si la aplicación realiza validación de datos en múltiples fases, puede ser conveniente desarrollar un marco de validación centralizado (realizar la validación de entradas en un solo lugar en vez de en cientos, es mucho más sencillo).

Creación y Revisión de modelos UML.

- Una vez completados el diseño y la arquitectura, es necesario construir modelos en Lenguaje Unificado de Modelado (UML por sus siglas en inglés), que describan cómo funciona la aplicación. Estos modelos se emplean para conformar junto a los diseñadores de sistemas una comprensión exacta del funcionamiento del software. Si se descubre alguna vulnerabilidad, debería serle transmitida al arquitecto del sistema para buscar aproximaciones alternativas.

Creación y Revisión de modelos de Amenazas.

- Una vez obtenidas las revisiones del diseño y la arquitectura, y con los modelos UML que explican el funcionamiento del sistema, es hora de abordar un modelado de amenazas. Es preciso analizar el diseño y la arquitectura para asegurarse de que esas amenazas son mitigadas, aceptadas por el negocio, o asignadas a terceros. Cuando las amenazas identificadas no tienen estrategias de mitigación, es necesario revisar el diseño y la arquitectura con los arquitectos de los sistemas para modificar el diseño.

1.4.3 Fase #3 Durante el desarrollo.

El desarrollo es la implementación de un diseño. Sin embargo, en el mundo real, muchas decisiones de diseño son tomadas durante el desarrollo del código. Si la arquitectura y el diseño no son los adecuados, los desarrolladores tendrán que enfrentar muchas decisiones. Si las políticas y estándares son insuficientes, tendrían que afrontar todavía más decisiones.

Inspección de códigos por fases.

- El equipo de seguridad debería realizar una inspección del código por fases con los desarrolladores y, en algunos casos, con los arquitectos del sistema. Pero el propósito de dicha inspección no es realizar exactamente una revisión del código, sino entender el flujo de programación a un alto nivel, su esquema, la lógica y la estructura del código que conforma la aplicación.
- La inspección de código por fases permite además al equipo de revisión de código obtener una comprensión general del código fuente, y facilita a los desarrolladores explicar porque se han desarrollado ciertos elementos de un modo en particular.

Revisiones de Códigos.

- Con una buena comprensión de cómo está estructurado el código y por qué ciertas cosas han sido programadas como lo están en el momento, el probador puede examinar ahora el código real en busca de defectos de seguridad.

1.4.4 Fase #4 Durante el despliegue.

Prueba de Intrusión sobre la Aplicación.

Tras haber comprobado los requisitos, analizado el diseño y realizado la revisión del código, debería asumirse que se han identificado todas las incidencias.

- Las pruebas de penetración de la aplicación después de que haya sido implementada proporcionan una última comprobación para asegurar de que no se ha olvidado nada.

Comprobación de Gestión de Configuraciones.

- La prueba de intrusión de la aplicación debería incluir la comprobación de cómo se implementó su infraestructura. Aunque la aplicación puede ser segura, un pequeño detalle de la configuración podría estar en una etapa de instalación por defecto, y ser vulnerable a explotación.

1.4.5 Fase #5 Durante el mantenimiento.

La seguridad debe de ser preservada durante la operación y el mantenimiento para asegurar la integridad del software.

Ejecución de Revisiones de la Gestión Operativa.

- Debe existir un proceso que detalle cómo es gestionada la sección operativa de la aplicación y su infraestructura.

Ejecución de Comprobaciones Periódicas de Mantenimiento.

- Deberían realizarse comprobaciones de mantenimientos mensuales o trimestrales, sobre la aplicación e infraestructura, para asegurar que no se han introducido nuevos riesgos de seguridad y que el nivel de seguridad sigue intacto.

Verificación del Control de Cambios.

- Después de que cada cambio haya sido aprobado, testeado en el entorno de aseguramiento de la calidad e implementado en el entorno de producción, es vital que como parte del proceso de

gestión de cambios el cambio sea comprobado para asegurar que el nivel de seguridad no haya sido afectado por dicho cambio.

Cuando ya han sido analizadas las actividades a tener en cuenta por cada una de las fases que componen a OWASP se confirma que esta guía facilita identificar los posibles riesgos y vulnerabilidades que pueden presentar las aplicaciones web durante su desarrollo, contribuyendo así a obtener un resultado final seguro aunque no permite su aplicación de forma estandarizada e incluso una de las actividades que propone en la segunda fase es la creación y revisión de modelos UML y se debe tener claro que no en todos los proyectos el lenguaje de modelado que se usa es el UML.

1.5. Criterios de expertos

En el presente trabajo se tendrá en cuenta el criterio de especialistas en seguridad informática, es por ello la necesidad de aplicar un método a través del cual se pueda validar lo que se propone en el presente trabajo, como lo es el método Delphi, de esta manera se podrá llegar a un consenso basado en los diferentes criterios de cada uno de los expertos siendo este un proceso repetitivo en busca de mejoras.

1.5.1 Método Delphi

Delphi es un método de investigación sociológica, que aunque pertenece al tipo de entrevista de profundidad en grupo, se aparta de ellas agregando características particulares. Es una técnica grupal de análisis de opinión, parte de un supuesto fundamental y de que el criterio de un individuo particular es menos fiable que el de un grupo de personas en igualdad de condiciones, en general utiliza e investiga la opinión de expertos. (16)

Parisca considera que el Método Delphi “se basa en el principio de la inteligencia colectiva y que trata de lograr un consenso de opiniones expresadas individualmente por un grupo de personas seleccionadas cuidadosamente como expertos calificados en torno al tema, por medio de la iteración sucesiva de un cuestionario retroalimentado de los resultados promedio de la ronda anterior, aplicando cálculos estadísticos”. (16)

Una vez realizado el análisis de las definiciones anteriores para aceptar y validar la norma que se propone en el presente trabajo se realizará una selección de expertos que emitan su criterio, los expertos estarán compuesto por especialistas en el tema de seguridad informática durante el proceso de desarrollo del software en la Universidad de las Ciencias Informáticas, además de ser personas

diestras, con reconocida competencia y con experiencia en el tema que garantice la confiabilidad de los resultados,creativos e interesados en participar.

1.6. Conclusiones parciales

- La información es el activo informático más importante que existe en una organización, posee valor que puede llegar a ser incalculable, por tanto debe ser protegida.
- La Serie ISO 27000-27010 propone aspectos a tener en cuenta o aplicar para la seguridad de la información, pero no abarca específicamente la seguridad durante el desarrollo de software.
- La OWASP es un proyecto dedicado a establecer prácticas seguras a partir de los riesgos identificados más importantes durante el desarrollo de software, pero en el país existe poco escrito o implantado con respecto al tema.
- La existencia de fallas en la seguridad es hoy en día algo inevitable, pero es bueno analizar y mejorar la calidad del software incorporando una serie de medidas de seguridad durante el proceso de desarrollo para reducir el riesgo y poder lograr buenos resultados.
- En Cuba el desarrollo de software es incipiente, impulsado fundamentalmente por la creación de la UCI, y por tanto los trabajos sobre la seguridad durante el proceso de desarrollo de software en CEGEL es incipiente también.
- No se encuentran implementados en la UCI o en el país mecanismos que contribuyan a elevar la seguridad de un software durante su desarrollo de forma estandarizada y una vez terminado el sistema.

Capítulo 2

Propuesta de Norma Técnica

2.1 Introducción

Velar por la seguridad interna en un proyecto productivo, es una tarea que requiere de varios factores y solo es conformada bajo el cumplimiento de un patrón. En el presente capítulo se propone una norma técnica para contribuir a mejorar la seguridad durante el desarrollo de software en los proyectos productivos del CEGEL. Se pretende proporcionar reglas mínimas necesarias para solucionar el problema planteado en la investigación.

2.2 Riesgos más comunes de programación

Es importante definir además de los conceptos teóricos que conforman el ámbito de la seguridad referente al desarrollo de software, cuáles son los riesgos más comunes identificados por la OWASP. En su edición del año 2007 publicaron los 10 errores más comunes de programación, pero en el 2010 se enfocan desde el punto de vista de los riesgos a los que se expone una aplicación web. En su edición de la lista de los 10 riesgos más críticos en el año 2010, se pueden encontrar en: (13)

1. Inyección: las fallas de inyección, tales como el Lenguaje de Consulta Estructurado (SQL por sus siglas en inglés), los Sistemas Operativos (OS por sus siglas en inglés), y el Protocolo Ligero de Acceso a Directorios (LDAP por sus siglas en inglés), ocurren cuando datos no confiables son enviados a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados.
2. Secuencia de Comandos en Sitios Cruzados (XSS por sus siglas en inglés): las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos

en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.

3. Pérdida de Autenticación y Gestión de Sesiones: las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas de forma incorrecta, permitiendo a los atacantes comprometer contraseñas, llaves, token[2] de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.
4. Referencia Directa Insegura a Objetos: una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.
5. Falsificación de Peticiones en Sitios Cruzados (CSRF en sus siglas en inglés): un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la víctima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la víctima.
6. Defectuosa Configuración de Seguridad: una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.
7. Almacenamiento Criptográfico Inseguro: muchas aplicaciones web no protegen adecuadamente los datos sensibles, tales como tarjetas de crédito, y credenciales de autenticación con mecanismos de

[2] *Token: generación y codificación de un número aleatorio tras la autenticación del usuario en la aplicación que se almacena en la sesión del usuario.*

8. Falla de Restricción de Acceso a URL[3]: muchas aplicaciones web verifican los privilegios de acceso a URL antes de generar enlaces o botones protegidos. Sin embargo, las aplicaciones necesitan realizar controles similares cada vez que estas páginas son accedidas, o los atacantes podrán falsificar URL para acceder a estas páginas igualmente.
9. Protección Insuficiente en la Capa de Transporte: las aplicaciones frecuentemente fallan al autenticar, cifrar, y proteger la confidencialidad e integridad de tráfico de red sensible. Cuando esto ocurre, es debido a la utilización de algoritmos débiles, certificados expirados, inválidos, o sencillamente no utilizados correctamente.
10. Redirecciones y reenvíos no validados: las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing[4] o malware[5], o utilizar reenvíos para acceder páginas no autorizadas. (14)

2.3 Análisis de la encuesta aplicada en los proyectos del CEGEL

En el Centro de Gobierno Electrónico (CEGEL) hay un total de 140 profesores de estos 26 no se encuentran vinculados a proyectos productivos para un total de 114 profesores involucrados en el proceso. Se tiene un total de 371 estudiantes, de ellos 8 cumpliendo misión en los Centros de Diagnóstico Integral (CDI) en Venezuela, quedan 363 estudiantes en el centro y actualmente 111 de estos no se les ha asignado proyectos, realmente solo 252 estudiantes están vinculados a la producción para una población de 366 personas.

Para seleccionar la muestra se tienen en cuenta los siguientes datos:

- La población, constituida por 366 personas (profesores, y estudiantes de 3er a 5to año) vinculadas a los proyectos del CEGEL según fuentes estadísticas externas.
- El nivel de confianza, que es de 95% con un grado de error de 5%.

---

[3] *URL: Localizador de Recurso Uniforme.*

[4] *Phishing: es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.*

El término ¨Phishing¨ es conocido como es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas).

[5] *Malware: software malicioso o software malintencionado.*

Y se aplicó la fórmula de la muestra:

$n = (Z^2pqN) / (Ne^2 + Z^2pq)$

n: muestra: es el número representativo del grupo de personas que se quiere estudiar (población) y, por tanto, el número de encuestas que se debe realizar, o el número de personas que se deben encuestar.
N: población: es el grupo de personas que se estudian, las cuales podrían estar conformadas, por ejemplo, por el público objetivo.
Z: nivel de confianza: mide la confiabilidad de los resultados. Lo usual es utilizar un nivel de confianza de 95% (0.96) o de 90% (1.65). Mientras mayor sea el nivel de confianza, mayor confiabilidad tendrán los resultados, pero, por otro lado, mayor será el número de la muestra, es decir, se tendrán que realizar más encuestas.
e: grado de error: mide el porcentaje de error que puede haber en los resultados. Lo usual es utilizar un grado de error de 5 % o de 10 %. Mientras menor margen de error, mayor validez tendrán los resultados, pero, por otro lado, mayor será el número de la muestra y por tanto el número de encuesta también es mayor.
p: probabilidad de ocurrencia: probabilidad de que ocurra el evento. Lo usual es utilizar una probabilidad de ocurrencia del 50 %.
q: probabilidad de no ocurrencia: probabilidad de que no ocurra el evento. Lo usual es utilizar una probabilidad de no ocurrencia del 50 %. La suma de p + q siempre debe dar 100%.

Cálculos para obtener la muestra

- Nivel de confianza (Z) = 1.96
- Grado de error (e) = 0.05
- Universo (N) =366
- Probabilidad de ocurrencia (P) = 0.5
- Probabilidad de no ocurrencia (Q) = 0.5

$n = ((1.96)^2 (0.5) (0.5) (366)) / ((366) (0.05)^2 + (1.96)^2 (0.5) (0.5))$
$n = ((3.84) (0.25) (366)) / ((366) (0.0025) + (3.84) (0.25))$
$n = 351.36 / 0.91 + 0.96$
$n = 351.36 / 1.87$
$n = 187$.

Se aplicó una encuesta (Ver Anexo # 1) a 187 personas (la muestra que se debe tomar) involucradas en el proceso de desarrollo de software, se determinó el conocimiento real, en cuanto a seguridad de software se refiere durante su desarrollo, las tablas que a continuación se muestran representan algunos de los resultados obtenidos, se demostró que más del 50 % de las personas no dominan los aspectos básicos que contribuyen a garantizar la seguridad de las aplicaciones (Figura 2), ni identifican el activo informático más importante, que por su vulnerabilidad requiere de mayor protección.

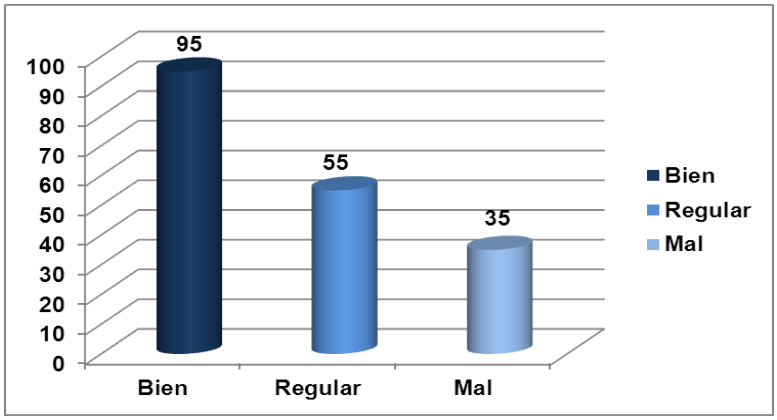

Figura 2. Personas que tienen conocimiento sobre aspectos básicos que contribuyen a garantizar la seguridad en las aplicaciones.

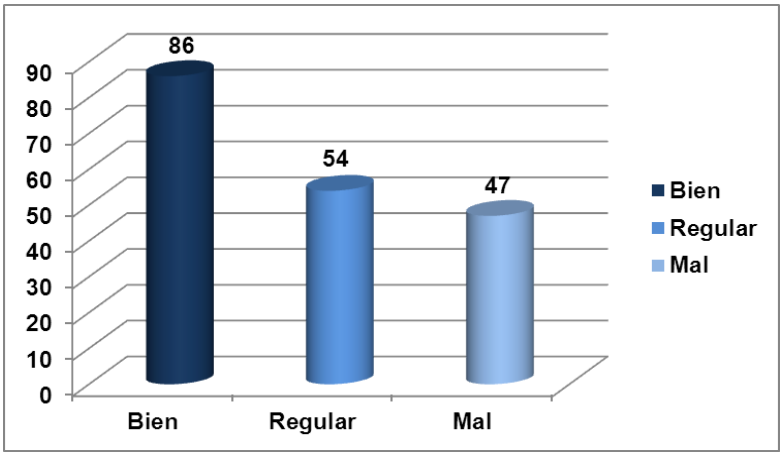

Figura 3. Personas que identifican los activos informático más importantes.

Para la formulación de la norma se tienen en cuenta 3 aspectos fundamentales:

1. Riegos identificados por la OWASP.

2. Insuficiente preparación de estudiantes y profesores en cuanto a gestión de seguridad de la información se refiere, centrado fundamentalmente en la seguridad del código.
3. Inexistencia en el centro de reglas que estandaricen la seguridad del proceso de desarrollo de software para obtener aplicaciones seguras

2.4 Norma para la seguridad durante el proceso de desarrollo de software y su descripción.

En las instituciones, las normas de uso cotidiano generalmente son verbales, no están escritas. Incluso el personal, por falta de esa información o indiferencias a su importancia en caso de que estén presentes en los servicios, las modifican desvirtuando los procedimientos o recomendaciones pautadas.

En consecuencia, las normas deben incluir aquellos aspectos que faciliten el cumplimiento de los objetivos aplicados a la organización a la que sirven, porque le agregan un valor docente importante al generar una utilidad adicional en términos de minimización de riesgos, optimización de las actividades, facilita las comunicaciones y mejora la organización del trabajo.

Entre las metodologías de desarrollo que se utilizan en el Centro de Gobierno Electrónico (CEGEL) se encuentran Scrum, Programación Extrema (Extreme Programming – XP sus siglas en inglés) ambas metodologías ágiles, y además la metodología Proceso Racional Unificado (Rational Unified Process – RUP por sus siglas en inglés) que es sin lugar a dudas una de las más usadas por ser apropiada para proyectos grandes y brindar amplia documentación, aunque también se aplica en proyectos pequeños y su objetivo es asegurar la producción de software de alta calidad que satisfaga la necesidad del usuario final dentro de un tiempo y presupuesto previsible como se persigue en los proyectos del CEGEL.

A partir de un estudio de las metodologías mencionadas y comparaciones entre los flujos de trabajo que se realizan durante las diferentes fases por las que transitan cada una de estas durante el ciclo de vida, se determinaron las disciplinas comunes entre dichas fases además se tuvo en cuenta el siguiente planteamiento: “El ciclo de vida de un proyecto desde la creación científica hasta su introducción en la práctica social consta de cuatro partes principales, aunque no siempre se podrán diseñar en su totalidad, sino que dependerá del tipo de proyecto que se elabore” (17). Para proyectos informáticos, en el presente trabajo se plantea que existen 4 momentos fundamentales donde es necesario ejecutar acciones que contribuyan a obtener un mínimo de seguridad:

1. Inicio del proyecto, gestión de los riesgos de seguridad.
2. Análisis y Diseño.

3. Implementación.
4. Prueba.

Aunque en el alcance de este trabajo se definen los 4 momentos mencionados, el despliegue es fundamental también, pues es donde se instala el software, se capacitan a las personas que lo van a utilizar, e incluso en algunas condiciones se cambia código en la aplicación a partir de las pruebas pilotos que se realizan, sobre todo en el caso del centro donde se desarrolla software a medida, y por tanto una vez que la aplicación se encuentra en despliegue o incluso en la etapa de soporte, pueden realizarse cambios en el código.

Objetivo de la Norma

Establecer un estándar que contribuya a garantizar la seguridad durante el proceso de desarrollo de software en los proyectos del Centro de Gobierno Electrónico.

Alcance de la Norma

La norma está dirigida a los proyectos productivos del Centro de Gobierno Electrónico.

Propósito

Definir las reglas a seguir para contribuir a elevar la seguridad durante el proceso de desarrollo de software en CEGEL.

Reglas definidas

2.4.1 Inicio del Proyecto

Durante el inicio del proyecto se realizarán las siguientes actividades:

- Identifique los riesgos de seguridad durante el análisis de riesgos.
- Establezca el plan de mitigación de estos riesgos.
- Determine los estándares de seguridad a emplear (se debe incluir el plan de riesgos de seguridad con su consecuente plan de mitigación de riesgos).
- Es conveniente determinar el tratamiento que se le va a dar a los usuarios del sistema.
- Se recomienda definir herramientas a utilizar por cada una de las fases de desarrollo de software para garantizar su seguridad.

Descripción de las actividades:

Identificar los riesgos de seguridad durante el análisis de riesgos.

Se realizará en la fase inicial del proyecto una reunión con todos los miembros para identificar los posibles riesgos, en dependencia de las actividades realizadas, la experiencia de cada uno de los miembros del equipo y las tareas planificadas. Los riesgos identificados serán priorizados en dependencia del impacto que tengan en el proyecto. Se harán reuniones periódicas para ir gestionando los riesgos así como ir identificando los nuevos. Para dar cumplimiento se identifican los activos informáticos con los que cuenta el proyecto.

Tabla 1. Identificación de Activos Informáticos

No.	Descripción	Tipo	Ubicación
1			
2			

No.: en ese campo se enumeran cada uno de los activos identificados

Descripción: se escribe el nombre detallado de cada activo identificado.

Tipo: se clasifica el activo informático atendiendo al tipo (Software (SW), Hardware (HW), Personal Informático (PI)).

Ubicación: lugar donde se encuentra ubicado el activo informático.

Luego, se tiene en cuenta los aspectos básicos de la seguridad de la información al mismo tiempo el costo, el dominio y la imagen, por nombrar algunos, se obtiene la importancia total de dichos activos para determinado proyecto.

Tabla 2. Importancia de Activos Informáticos

No	Dom	Valoración por Aspectos						Importancia
		Función	Costo	Imagen	Confid.	Integrid.	Disponib.	Wi
1	D1							
2	D1							

No: enumerar los activos

Dom. : dominio al que pertenece cada activo (D1, D2, así sucesivamente).

Función: valor entre 1 (mínimo) y 10 (máximo) que se le asigna al activo para representar cuán importante es su funcionamiento.
Costo: valor entre 1 (mínimo) y 10 (máximo) que se le asigna al activo para representar su costo en caso de deterioro o pérdida.
Imagen: valor entre 1 (mínimo) y 10 (máximo) que se le asigna para representar la imagen del proyecto en caso que se deteriore o se pierda dicho activo.
Confidencialidad (Confid.): poner un el valor entre 1 (mínimo) y 10 (máximo) de cuán confidencial se considera es el activo.
Integridad (Integrid.): poner un el valor entre 1 (mínimo) y 10 (máximo) de cuán integral se considera es el activo.
Disponibilidad (Disponib.): poner un el valor entre 1 (mínimo) y 10 (máximo) de cuán disponible se considera es el activo.
Wi o Valor: representa la importancia de cada activo que se obtiene con valor promedio de cada uno de los aspectos valorados en los activos. La importancia total sería la sumatoria de Wi.

De esta manera se pasa a identificar las amenazas para el proyecto y una vez que estén listados se determina entonces cómo influyen estos riesgos en cada uno de los activos.

Tabla 3. Valoración de las amenazas en los Activos Informáticos

		Bienes informáticos		
No.	**Amenazas**	**1**	**2**	**3**
1				
2				

No: se enumeran los riesgos identificados
Amenazas: se nombra el riesgo identificado
Bienes informáticos: se marca en cuál o cuáles de los activos representados por la enumeración que le corresponde se ve afectado con el riesgo identificado.

Establecer el plan de mitigación de estos riesgos.

A partir del análisis de riesgo elaborado, se establecen las medidas de seguridad y procedimientos, de acuerdo al peso estimado para cada bien informático y de esta manera enfrentar a cada uno de los ataques o posibles ataques que perjudican el desarrollo del proyecto con éxito, es decir, en el plan de mitigación de riesgos se debe reflejar la solución a seguir para dar respuesta al riesgo.

Determinar los estándares de seguridad a emplear.

- Estándar de programación (se definirán las directrices de programación segura en dependencia del lenguaje de programación definido para el desarrollo del proyecto).
- Estándar de criptografía. Todos los datos que sean de importancia para el sistema o más específicamente para los usuarios del sistema deberán ser transmitidos o salvados usando herramientas criptográficas. El equipo de desarrollo definirá los sistemas criptográficos a emplear sin inventar el nuevo algoritmo de encriptación, sino usar herramientas probadas.
- Personal especializado en la seguridad de la información: Se seleccionará el especialista en el proyecto que tendrá como objetivo fundamental asegurar que se apliquen procesos seguros, y revisar por cada una de las fases de los proyectos que se cumplan los preceptos establecidos en la norma. Será responsable además de preparar en cuanto a seguridad se refiere al administrador de configuración, quien tendrá en cuenta cada vez que se haga algún cambio en la configuración del sistema el impacto que tiene este en la seguridad del mismo.
- Cada proyecto elaborará y pondrá en práctica su plan de seguridad informática, que incluye el cronograma de revisión de estado de la seguridad.

Definir el tratamiento que se le va a dar a los usuarios del sistema

Definir los roles y privilegios de los usuarios, el alcance que van a tener los usuarios en el sistema para determinar luego el acceso de cada uno.

Definir herramientas a utilizar por cada una de las fases de desarrollo de software para garantizar su seguridad

Es recomendable hacer un estudio de las herramientas existentes para aumentar el nivel de seguridad durante las diferentes fases por la que transita el software y de esta manera determinar cuál es la mejor en dependencia de las necesidades y características del proyecto.

- No deben faltar en los servidores fundamentales del proyecto o en las computadoras donde se guarde información sensible (esencialmente el repositorio) sistemas detectores de intrusos.
- En caso de emplearse sistemas operativos Windows el cortafuego estará activado sin excepciones. En caso de utilizarse sistemas operativos libres asegurar la configuración correcta de sus correspondientes cortafuegos.

2.4.2 Análisis y Diseño

En este momento es donde se diseña el sistema, se definen las clases que se implementarán. Se debe cumplir con las siguientes actividades a desarrollar:

- Identifique los requisitos de seguridad.
- Las interfaces del sistema deben cumplir con los principios de seguridad de programación segura “Mínimo Privilegio” y “Separación de Privilegios” y los sistemas tendrán establecidos mecanismos de autenticación.
- El analista principal será el responsable de revisar durante esta fase junto al especialista de seguridad del proyecto, de que se apliquen las actividades establecidas por la norma, de que los miembros del proyecto que inciden directamente estén preparados en los riesgos de seguridad a los que la aplicación está expuesta en el momento.
- El marco de validación será centralizado.
- Al completar el diseño y la arquitectura de la aplicación se deben revisar nuevamente.

Requisitos de seguridad

Es práctica común definir los requisitos que debe cumplir el sistema para responder las necesidades de los clientes, y no identificar cuáles son los requisitos de seguridad que lo caracterizan. Se tendrán en cuenta los siguientes mecanismos de seguridad:

- Gestión de Usuarios (reinicio de contraseñas, entre otros).

  La gestión de usuarios será para tener un control sobre los usuarios actuales, velar por la seguridad, que no acceda ningún usuario que ya no es miembro del proyecto a la aplicación o a la información confidencial que se maneje en el mismo

- Autenticación

La autenticación es la verificación de que el usuario que trata de identificarse es válido, usualmente se implementa con una contraseña en el momento de iniciar una sesión. Existen cuatro tipos de técnicas que permiten realizar la autenticación de la entidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas (autenticación de varios factores)

- Algo que solamente el individuo conoce: la contraseña.
- Algo que la persona posee: una tarjeta magnética.
- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales.
- Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

- Autorización

La autorización es el procedimiento para determinar si el usuario o proceso previamente identificado y autenticado tiene permitido el acceso a los recursos.

Esta técnica se implementa a través de uno de los modelos de control de acceso: Control de Acceso Obligatorio (MAC), Control de Acceso Discrecional (DAC) o el modelo de Control de Acceso basado en Roles (RBAC).

- Confidencialidad de los datos

Solo podrán acceder a los datos que se manejan en la aplicación personas autorizadas.

- Integridad

Se refiere a que los datos que se manejan en la aplicación solo podrán ser modificados por las personas autorizadas para ello.

- Disponibilidad

Plantea que los datos que se manejan en la aplicación tienen que estar disponibles para las personas autorizadas en el momento que lo requieran.

- Gestión de Sesiones

El propósito de esta acción es ofrecer a los usuarios la posibilidad de salvar y restaurar sus sesiones. Una sesión es una colección de aplicaciones, todas ellas tienen un estado interno. Este estado puede ser el nombre de un fichero abierto, una imagen visualizada o el marcador de un juego.

- Seguridad de Transporte

Se debe velar para que personas ajenas al proyecto no accedan a los datos de la aplicación, y que la información confidencial que viaje por la red o se lleve de un lugar a otro esté segura de forma tal que solo pueda ser accedida por personas autorizadas.

- Privacidad

Este punto también se refiere a mantener todos los datos protegidos de las personas que no estén autorizadas a manejar dicha información, las contraseñas deben mantenerse en secreto, se les debe dar uso personal.

Interfaces del sistema

- Mínimo Privilegio y Separación de Privilegio**.**

Para que estén presentes ambos principios de seguridad en las interfaces del sistema se deben otorgar los permisos estrictamente necesarios para efectuar las acciones que se requieran, ni más ni menos de lo solicitado. Estos principios son vitales para alcanzar el objetivo de integridad, al requerir que a un usuario no se le otorguen mayores privilegios que los necesarios para efectuar su trabajo.

- Autenticación

En caso que la interfaz sea un sitio web, se debe garantizar que a partir de una URL obtenida de otro usuario se redireccione a la interfaz de autenticación en el sistema.

Validación

Para la validación de los datos de entrada del sistema, se realizará en un único componente, en un único lugar y de esta manera garantizar que sea de forma centralizada.

Diseño y arquitectura

Una vez finalizado el diseño y la arquitectura de las interfaces del sistema, las revisiones permiten encontrar vulnerabilidades que puede tener el sistema a partir de los riegos y requisitos de seguridad previamente identificados. El arquitecto del proyecto debe jugar un papel fundamental durante esta actividad junto al analista.

2.4.3 Implementación

Para la Autenticación se debe tener en cuenta que:

- Las aplicaciones web harán uso del protocolo HTTPS.
- Las variables se pasarán por el Método Post.

- Se emplearán Listas de Control de Acceso.

Para la implementación de la Base de Datos se debe cumplir con los siguientes puntos:

- Nombre los objetos de las bases de datos siguiendo una codificación.
- Debe tener en cuenta para la seguridad los nombres de las tablas, vistas y procedimientos almacenados.
- El nombre de las llaves debe tener también una codificación.
- Los nombres de los campos no deben hacer referencia a la tabla a la que pertenecen.
- Se deben normalizar los nombres de las variables a utilizar.
- Las transacciones deben estar restringidas en la aplicación “solo lectura”.
- Los datos serán validados si cumplen con las reglas establecidas.
- La confirmación de las transacciones así como su cancelación contribuye a evitar problemas de inconsistencia o de integridad de los datos.
- Las excepciones deberán ser estandarizadas.

Aplique modelo de control de acceso basado en roles (RBAC en sus siglas en inglés) para la definición de los usuarios en el sistema.

Debe restringirse en las aplicaciones el uso de llamadas al sistema operativo, en el caso de que sea imprescindible se deben probar la seguridad del mismo antes de la liberación de la aplicación a los clientes.

Autenticación

- Protocolos HTTPS

El protocolo de Transferencia de Hiper-Texto (HTTPS siglas en inglés) es la versión segura del protocolo de Transferencia de Hiper-Texto (HTTP por sus siglas en inglés). Es recomendable usar este protocolo en las aplicaciones web, básicamente permite que la web codifique la sesión con certificado digital**.** De este modo, el usuario tiene ciertas garantías de que la información enviada desde dicha página no podrá ser interceptada y utilizada por terceros.

- Las variables

Las variables se pasarán por el Método Post, ya que un usuario con intenciones maliciosas puede emplear el Método Get en beneficio propio y para perjuicio de la institución.

- Listas de Control de Acceso

Se emplearán Listas de Control de Acceso para garantizar que solo se brindan los permisos necesarios ya que el control de acceso incluye autenticar la identidad de los usuarios o grupos y autorizar el acceso a datos o recursos. Es necesario se establezcan estas listas para proteger la confidencialidad, integridad y disponibilidad de los objetos, y por extensión de la información que contienen, con esto se logra que los usuarios autorizados accedan solo a los recursos que ellos requieren para realizar sus tareas.

Base de Datos

- Nomenclatura en la base de datos

Se recomienda nombrar los objetos de bases de datos siguiendo una codificación. Desde el punto de vista de la seguridad garantiza que aun cuando la aplicación o software no tenga implementado el uso de procedimientos almacenados o alguna otra alternativa que evite las inyecciones SQL, al menos dificulte al atacante acertar con el nombre de las tablas, vistas o procedimientos.

En cuanto a las llaves de las bases de datos es importante que el nombre de las mismas tenga una codificación para garantizar que sea homogéneo el nombramiento en todos los proyectos.

- Las transacciones

Las transacciones deben estar restringidas en la aplicación solo lectura, esto permite que no sean modificados los nomencladores de la BD, en caso que ocurra alguna inyección SQL, la transacción existe pero no se realizará hasta tanto se ejecute por lo tanto solo podrán actualizar la base de datos aquellas personas que evidentemente tengan el permiso asignado, y podrán realizar funcionalidades de aceptar u actualizar para brindar mayor seguridad.

- Validación de los datos

Para que los datos sean válidos se debe verificar que cumpla con lo siguiente: se le pide confirmación de actualización al usuario, si se confirma es entonces cuando se actualiza en la base de datos. Una vez terminada la transacción se vuelve a la pantalla anterior para que el usuario introduzca nuevos datos si lo desea, o se pasa a otra forma con otras opciones según defina el equipo de desarrollo. Es fundamental dejar establecida la validación de datos y la restricción en cuanto a las transacciones y cuáles son las funcionalidades o usuarios que pueden ejecutarlas.

- Excepciones

Las excepciones deberán ser estandarizadas de modo que no informen al usuario final de detalles innecesarios que puedan propiciar ataques al sistema desde la base de datos. Se debe considerar de la misma forma para toda la aplicación.

Modelo de control de acceso

Es recomendable aplicar Modelo de Control de Acceso Basado en Roles (RBAC) para la definición de los usuarios en el sistema, en este modelo a los usuarios le son asignados uno o varios roles, mientras que los permisos y privilegios se le asignan a estos roles. Por tanto, la política de control de acceso basado en roles regulan el acceso de los usuarios a la información en término de sus actividades y funciones de trabajo (roles).

2.4.4 Prueba

- Se realizarán pruebas de intrusión y pruebas de stress.
- Se realizarán auditorías de seguridad y revisiones.
- Se harán evaluaciones de los procesos para determinar el cumplimiento de la norma de seguridad establecida.

Pruebas de intrusión y pruebas de stress

Se hará uso de herramientas o métodos que atenten contra la aplicación desde el punto de vista del atacante, para revisar el comportamiento frente a situaciones inesperadas, antes de liberar el sistema o subsistemas en Calidad.

Auditorías y Revisiones

Las auditorías son procesos formales que se llevan a cabo en los proyectos productivos para medir los criterios previamente establecidos por la dirección general de calidad y se emite una evaluación en cada una de las áreas y en general.

Se les realizará a los proyectos auditorías de seguridad en 4 momentos fundamentales:

1. Iniciado el proyecto, antes de iniciar la implementación de los requisitos.
2. Liberaciones de módulos.
3. Al finalizar el proyecto, justo antes de la fase de despliegue.
4. Durante la etapa de soporte.

Las revisiones al igual que las auditorías son chequeos a los proyectos, pero solo en algunas áreas específicas y con un menor grado de formalidad.

Evaluaciones

El personal de calidad conjuntamente con el jefe del proyecto serán los encargados de evaluar en un período determinado el cumplimiento de la norma establecida.

2.5 Conclusiones Parciales

- Existen riesgos de seguridad durante la implementación de software a los cuales se encuentran expuestos los proyectos del CEGEL.
- La encuesta realizada a los miembros de los proyectos productivos del Centro, arrojó entre sus resultados que los mismos no definen los aspectos de la seguridad durante el desarrollo de software de igual forma o correctamente.
- La norma propuesta puntualiza que la seguridad durante el proceso de desarrollo de software se puede precisar en 4 momentos fundamentales: Inicio del proyecto, Análisis y Diseño, Implementación y Prueba.
- Por cada uno de los momentos definidos se proponen reglas a seguir para contribuir a garantizar la seguridad durante el proceso de desarrollo de software.

Capítulo 3

Validación de la solución propuesta

3.1 Método de Validación. Delphi

Para la validación de la propuesta presentada en el Capítulo 2, se utilizó Criterio de un Panel de Expertos haciendo uso de las técnicas que propone el método Delphi. Este panel está integrado por especialistas en seguridad informática y/o desarrollo de software.

El método Delphi consiste en la selección de un grupo de expertos a los que se les pregunta su opinión sobre cuestiones referidas a acontecimientos futuros. Las estimaciones de los expertos se realizan en sucesivas rondas, anónimas, con el objetivo de lograr un consenso basado en la discusión entre expertos, pero con la máxima autonomía por parte de los participantes. Por lo tanto, la capacidad de predicción del Delphi se basa en la utilización sistemática de un juicio intuitivo emitido por un grupo de expertos.

El Delphi es uno de los métodos para realizar pronósticos más confiables, constituye un procedimiento para confeccionar un cuadro de la evolución de situaciones complejas, a través de la elaboración estadística de las opiniones de un grupo de expertos en el tema tratado. Permite rebasar el marco de las condiciones actuales más señaladas de un fenómeno y alcanzar una imagen integral y más amplia de su posible evolución, reflejando las valoraciones individuales de los expertos que pueden estar basadas en un análisis lógico, como en su experiencia intuitiva. (18)

En esta técnica se realiza una selección del grupo de expertos que participará en el proceso de evaluación, teniendo en cuenta que ningún experto conoce la identidad y las respuestas individuales de los otros que componen el grupo. Se debe hacer una buena elección de los expertos, para que el resultado sea el mejor.

En el presente capítulo se hará una breve descripción de cómo se realizó la validación del trabajo a partir de un proceso de elección de expertos y los resultados obtenidos.

Se tuvieron en cuenta los siguientes aspectos:

- Elección de expertos.
- Elaboración del cuestionario, para validación de la propuesta.
- Desarrollo práctico y explotación de resultados.

3.2 Elección de Expertos.

Se entiende por experto, tanto al individuo en sí como a un grupo de personas u organizaciones capaces de ofrecer valoraciones conclusivas de un problema en cuestión y hacer recomendaciones respecto a sus momentos fundamentales con un máximo de competencia. La autenticidad de la valoración de los criterios de expertos puede ser determinada solamente, sobre la base de la solución práctica del problema y el análisis de los resultados. (18)

Por experto se considera la persona capaz de ofrecer valoraciones concluyentes sobre la seguridad informática y específicamente del conocimiento que posea de la seguridad durante el proceso de desarrollo de software.

Para el procedimiento de la elección de los expertos se debe llevar a cabo los siguientes pasos:

3.2.1 Determinar las áreas de conocimiento que deben dominar los expertos.

Los expertos a consultar para la validación de la propuesta realizada en el Capítulo 2 deben poseer un elevado conocimiento en temas relacionados con la norma a evaluar, tales como:

- Normas y estándares nacionales e internacionales de seguridad del software.
- Actividades durante el proceso de desarrollo de software.
- Seguridad durante el proceso de desarrollo de software.

3.2.2 Confeccionar el listado de expertos candidatos.

Para la determinación de la cantidad de expertos, no existe una norma generalizada que determine un número óptimo. Se recomienda como mínimo 7 expertos y un máximo de 30. En este trabajo se decidió contar con un número de 7 expertos para la confección del panel, teniendo en cuenta el nivel de complejidad y profundidad del contenido.

1 Subdirector de Investigación y Postgrado del Centro de Gobierno Electrónico.
1 Asesor de Planificación y Control del Centro de Gobierno Electrónico.

1 Jefa de Departamento de Gestión Gubernamental.

1 Administrador y Diseñador de Bases de Datos.

1 Analistas.

1 Desarrollador.

1 Jefe de proyecto.

La confección del listado de expertos (Anexo 2) se realizó teniendo en cuenta las posibilidades reales de participación de los candidatos, pues todos son graduados de nivel superior y tienen experiencia en la docencia y en el proceso productivo de la Universidad.

3.2.3 Confirmar la participación de los candidatos.

Una vez confirmado el listado se invitó personalmente a cada experto para participar en la evaluación. Al ser confirmada su participación, se estableció el listado final de los expertos (Anexo 2), en este caso los 7 candidatos estuvieron de acuerdo en participar, informando a cada especialista su inclusión en la norma a evaluar y las instrucciones necesarias para contestar las preguntas. De esta forma culmina el proceso de selección.

3.2.4 Determinar coeficiente de experticia de los expertos.

Las características de los expertos influyen decisivamente en la confiabilidad de los resultados obtenidos. Estas características son: calificación técnica, capacidad de emitir una decisión al respecto, conocimientos específicos sobre el tema a evaluar, disposición a participar, entre otros. (20) (21)

Para la selección de los expertos es útil emplear la valoración por competencias. Este método consiste en calcular el coeficiente de competencia (k) del experto a partir de la autovaloración del experto sobre su conocimiento o información sobre el tema (kc) y el coeficiente de argumentación o valoración (ka) mediante la siguiente ecuación. (21)

El coeficiente de conocimiento (Kc) se obtiene de un análisis de la tabla (Ver Tabla 4) perteneciente pregunta 1 y 2, en dependencia de la disciplina a evaluar (seguridad informática y desarrollo de software), del cuestionario de autovaloración aplicado a los expertos (Ver Anexo 3) calculado sobre la valoración del propio experto en una escala del 0 al 10 y multiplicado por 0,1; de esta forma, la evaluación “0” indica que el experto no tiene absolutamente ningún conocimiento de la problemática correspondiente, mientras que la evaluación “10” significa que el experto tiene pleno conocimiento de

la problemática tratada. Entre estas dos evaluaciones extremas hay nueve intermedias. El experto deberá marcar con una cruz en la casilla que estime pertinente.

Tabla 4.Coeficiente de Conocimiento

0	1	2	3	4	5	6	7	8	9	10

Para el coeficiente de argumentación se ofrece otra tabla (Tabla 5), perteneciente a las pregunta 3 y 4 en dependencia de la disciplina a evaluar del cuestionario (Anexo 3), los resultados se transforman en valores numéricos a partir de la escala de puntuación de las fuentes de argumentación (Tabla 6).

Tabla 5. Coeficiente de Argumentación

No.	Fuente de Argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
		Alto	Medio	Bajo
1	Análisis realizado por usted.			
2	Su experiencia obtenida.			
3	Trabajo de autores nacionales.			
4	Trabajo de autores extranjeros.			
5	Su propio conocimiento del estado del problema en el extranjero.			
6	Su intuición.			

Tabla 6. Escala de Puntuación de las Fuentes de Argumentación

Fuentes de Argumentación	Grado de Influencia		
	Alto	Medio	Bajo
1. Análisis teórico realizado por usted.	0.3	0.2	0.1
2. Su propia experiencia en el problema.	0.5	0.4	0.2

3. Trabajos de autores nacionales.	0.05	0.05	0.05
4. Trabajos de autores extranjeros.	0.05	0.05	0.05
5. Su propio conocimiento del problema.	0.05	0.05	0.05
6. Su intuición.	0.05	0.05	0.05
Totales	**1.0**	**0.8**	**0.5**

El coeficiente de experticia se calcula por la siguiente fórmula:

k = (kc + ka)/2.

El código de interpretación de los coeficientes de competencias es como sigue:

- Si 0,8 < k < 1,0 coeficiente de competencia alto.
- Si 0,5 < k < 0,8 coeficiente de competencia medio.
- Si k < 0,5 coeficiente de competencia bajo.

Es recomendable incluir en el grupo a los expertos de coeficiente de competencia alto y medio. En la encuesta de autovaloración (Anexo 3) aplicada a los expertos, se determinó su coeficiente de competencias, los resultados se reflejan a continuación (Ver Tabla 7 y Tabla 8):

Tabla 7. Coeficiente de competencia de los expertos en el tema de seguridad informática

Expertos	Kc	Ka	K	Nivel
1	0.6	0.5	0.55	MEDIO
2	0.8	0.8	0.8	ALTO
3	0.7	1	0.85	ALTO
4	0.7	0.8	0.75	MEDIO
5	0.8	0.8	0.8	ALTO
6	0.8	0.9	0.85	ALTO
7	0.6	0.9	0.75	MEDIO

Tabla 8. Coeficiente de competencia de los expertos en el tema de proceso de desarrollo de SW

Expertos	Kc	Ka	K	Nivel
1	0.7	0.5	0.6	MEDIO

2	0.8	0.9	0.85	ALTO
3	0.8	1	0.9	ALTO
4	0.7	0.8	0.75	MEDIO
5	0.9	0.9	0.9	ALTO
6	0.8	0.8	0.8	ALTO
7	0.7	1	0.85	ALTO

3.3 Elaboración de los cuestionarios.

Para la elaboración del cuestionario se tuvieron en cuenta los objetivos que debería cumplir la norma propuesta para su implantación en los proyectos del CEGEL y que sirviera de guía para la evaluación por parte de los expertos. La encuesta establece una serie de preguntas de enfoque investigativo, que facilita a los expertos interactuar entre sí, evitando los roces sociales no deseados y de esta forma eliminar el efecto líder que pueden causar algunos expertos. La encuesta además permite ver la posibilidad real de poder aplicar la propuesta según las características actuales de los proyectos productivos del CEGEL.

Para realizar la validación de la norma propuesta se utilizó el Cuestionario de Validación (Ver Anexo 4), el mismo está compuesto por 8 preguntas en su mayoría de tipo cualitativas que brindan valores de ____Sí, ____No. La aplicación de la encuesta facilita que los expertos brinden su criterio exacto acerca los atributos identificados (Pi) donde 0<i<10:

P1: Necesidad de existencia de la norma para elevar la seguridad del software.

P2: Nivel de completitud de las reglas.

P3: Posibilidad de aplicación de la propuesta en los proyectos del centro correspondiente.

P4: Integración con el proceso de desarrollo de software.

P5: Correcta definición de las reglas que conforman la norma propuesta.

Los atributos son la base de la encuesta (Anexo 4) que se aplicó de forma anónima a cada integrante del panel además de varias preguntas, para obtener la posibilidad real de aplicar la propuesta y la calidad de la norma también se brindó la opción de modificar aspectos que los especialistas consideraran necesarios y de exponer sus criterios a favor y/o en contra de las reglas definidas.

3.4 Desarrollo práctico y explotación de resultados.

A partir de la respuesta de los cuestionarios realizados a los expertos, se procedió al cómputo y análisis de estos para una correcta explotación de los resultados. Para procesar los datos se hizo uso de la herramienta SPSS (Ver características en Anexo 5) y se pasó a construir la matriz de rango que a continuación se presenta. (Ver Tabla 9)

Nota 1: Se da una puntuación de 0/1 si la respuesta de los especialistas es negativa o positiva respectivamente.

Nota 2: En la P5 se dará una puntuación de 2/3/4 para baja/media/alta respectivamente.

Tabla 9. Criterio de los expertos

Especialistas / Preguntas	E1	E2	E3	E4	E5	E6	E7
P1	1	1	1	1	1	1	1
P2	1	0	1	1	0	1	1
P3	1	1	1	1	1	1	1
P4	1	1	0	1	1	1	0
P5	4	4	3	4	4	3	4

Con los resultados obtenidos de la tabla anterior se determinó el grado de concordancia de los expertos, se hizo uso del coeficiente de Kendall (W). En la Tabla 10 se reflejan los resultados:

Tabla 10. Criterios de los expertos

Prueba W de Kendall

Rangos

	Rango promedio
P1	2,79
P2	2,21
P3	2,79
P4	2,21
P5	5,00

Estadísticos de contraste

N	7
W de Kendall[a]	,793
Chi-cuadrado	22,213
gl	4
Sig. asintót.	,000

a. Coeficiente de concordancia de Kendall

Esta tabla muestra el número de casos válidos (N), el valor del estadístico W (W de Kendall), su transformación en Chi-cuadrado (X^2), sus grados de libertad (gl) y el nivel crítico (Sig. asintót.).

El coeficiente W de Kendall es una medida de la concordancia de los especialistas y por definición del Método Delphi, el resultado debe moverse en un rango de 0 a 1 y debe ser siempre W > 0,5 mientras más se acerque el coeficiente a 1, mayor será el grado de concordancia entre los expertos. En el estudio realizado resultó ser un aproximado de W= 0.7, por tanto la propuesta resultó ser aceptada y con un nivel de concordancia alto con respecto a los criterios que fueron evaluados.

La tabla muestra que el valor del nivel crítico (0,000) es menor que 0,05, por tanto se puede rechazar la hipótesis de concordancia nula y concluir que entre las puntuaciones de las variables estudiadas existe asociación significativa.

A partir de los criterios emitidos por los especialistas sobre la propuesta de la norma para el desarrollo de software seguro en los proyectos del Centro de Gobierno Electrónico se obtienen los siguientes datos:

- El 100% de los especialistas están de acuerdo que la existencia de la norma es necesaria para contribuir a elevar la seguridad del software por cada uno de los momentos definidos durante todo el ciclo de vida del mismo (Figura 4).

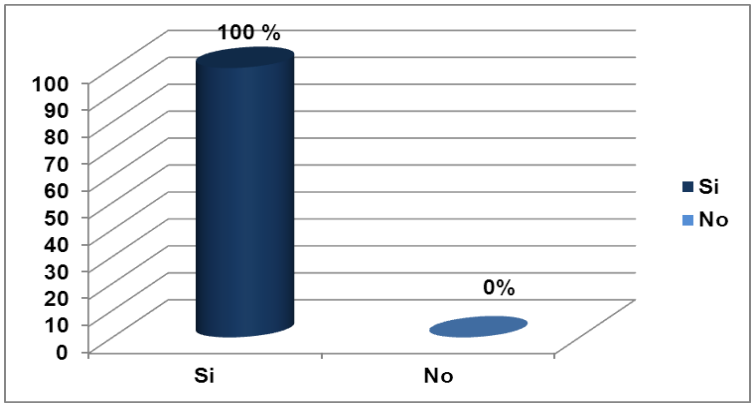

Figura 4. Importancia de la norma

- El 71.46% de los especialistas consideran que las reglas definidas en la norma son las necesarias para lograr seguridad en el software (Figura 5).

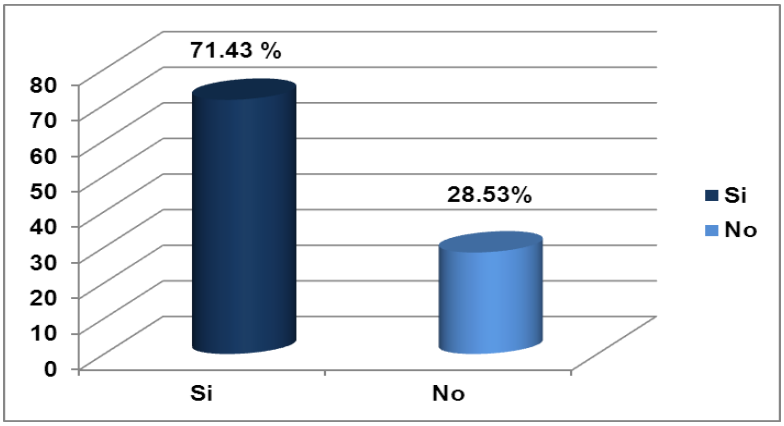

Figura 5. Reglas necesarias para la seguridad

- El 100% de los especialistas consideran que la norma puede ser aplicada a los proyectos del centro para lograr mayor organización en el equipo de desarrollo y seguridad del software (Figura 6).

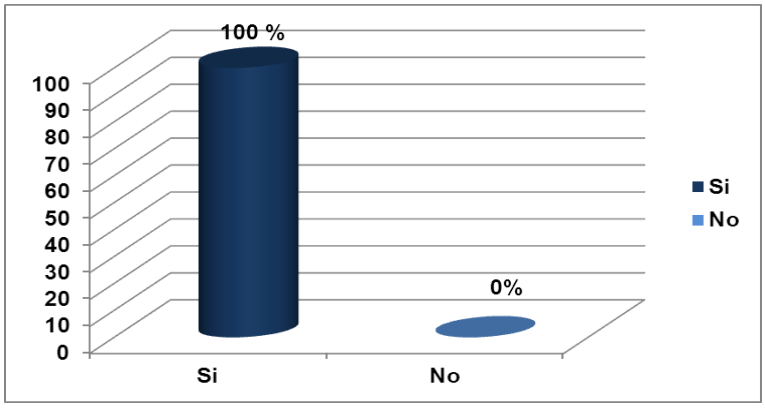

Figura 6. Posibilidad de aplicar la norma

- Solo el 28.54% de los especialistas consideran que las reglas que conforman la norma no engloban las fases fundamentales del proceso de desarrollo del software (Figura 7).

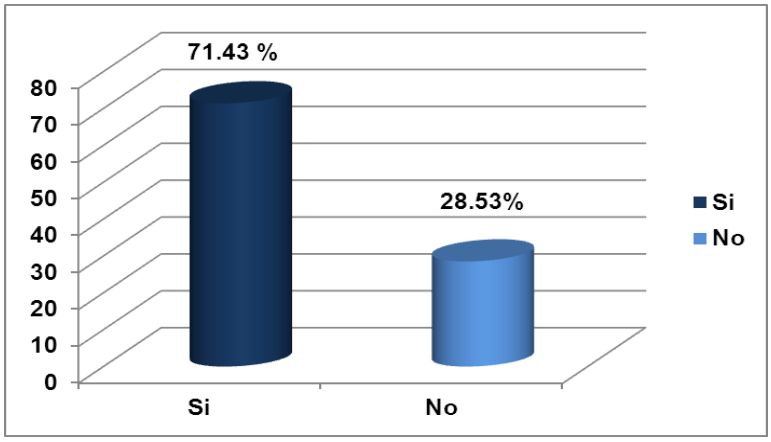

Figura 7. Momentos que engloba la norma

- El 100% de los especialistas valoran entre alta y media la correcta definición de la propuesta para desarrollar software seguro (Figura 8).

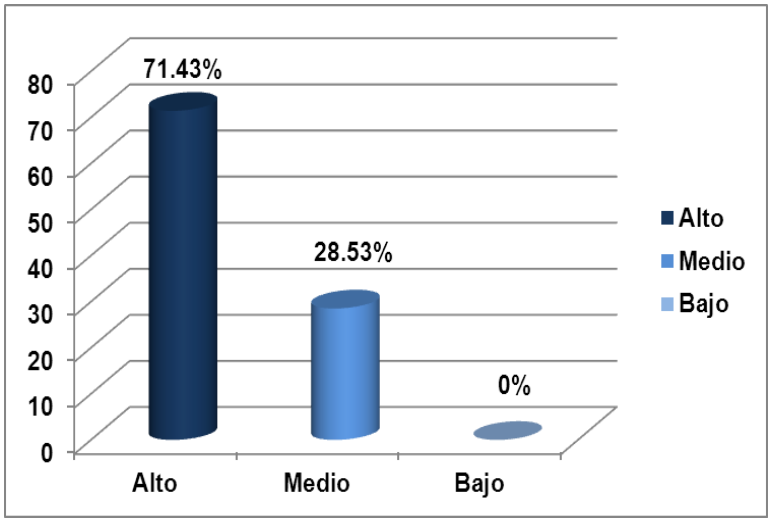

Figura 8. Valoración de la correcta definición de la norma

Con todo el análisis anteriormente realizado queda demostrada la aceptación por parte de los especialistas de la norma que se propone en el presente trabajo de diploma, para contribuir a elevar el nivel de seguridad en los productos que se desarrollan en el CEGEL.

Por tanto, por los resultados obtenidos en esta primera ronda realizada para valorar y validar la norma propuesta, se concluye de forma satisfactoria la aplicación del método Delphi sin necesidad de proceder a una segunda ronda de entrevistas.

3.5 Conclusiones Parciales.

- Las personas seleccionadas que conformaron el panel de expertos cumplen con el conocimiento adecuado para la validación de la propuesta.
- El criterio de los especialistas arrojó un alto coeficiente de concordancia y permitió observar el grado de aceptación que tiene la propuesta.
- La propuesta tiene una alta probabilidad de éxito al ponerla en marcha en los proyectos del centro.

Conclusiones generales

- El estudio realizado sobre las normas y leyes existentes sobre la seguridad de la información o durante el desarrollo de software, permite plantear que las normas internacionales o guías referentes al tema no suplen completamente las necesidades de seguridad mínimas en el CEGEL.
- En Cuba y en la UCI los trabajos realizados para contribuir a garantizar la seguridad durante el desarrollo de software son incipientes.
- La norma técnica propuesta establece reglas a ser seguidas durante momentos fundamentales del proceso de desarrollo de software, que contribuirá a la obtención de aplicaciones seguras a partir de establecer directrices que estandaricen el trabajo.
- La aplicación del método Delphi para validar la norma técnica propuesta arrojó como resultados que presenta concordancia, fue aceptada por los especialistas y tiene alto grado de probabilidad de éxito al ser aplicada.

Recomendaciones

- Aplicar la norma propuesta a los proyectos del CEGEL para contribuir a la mejora de la seguridad en el proceso de desarrollo.
- Realizar una selección entre los proyectos del CEGEL y aplicar una prueba piloto de la propuesta, de esta forma se podrá determinar cuán eficiente es la norma de manera práctica, como solución a la problemática existente.
- Continuar desarrollando reglas a la propuesta realizada para complementarla a partir de los cambios frecuentes en las tecnologías de desarrollo de software.
- Incluir además de los momentos definidos, reglas durante el Despliegue.
- Proponer la norma a una entidad cubana certificadora de normas para su aprobación oficial.

Referencias bibliográficas

1. **de los Reyes, Daniel.** Security Art Work. *Security Art Work.* [Online] Octubre 23, 2009. [Cited: Noviembre 21, 2010.] http://www.securityartwork.es/2009/10/23/incorporando-la-seguridad-al-proceso-de-desarrollo-de-software/.

2. **Jacaboson, i, Booch, G and Rumbaugh, J.** *El Proceso Unificado de Desarrollo de Software.* s.l. : Addison Wesley, 2000.

3. Real Academia de la Lengua Española. *Sitio de La Real Academia Española.* [Online] [Cited: Noviembre 15, 2010.] http://www.rae.es..

4. Creacionistas.com. [Online] Creacionistas.com. Capacitadores de TI, S.A., 2009. [Cited: Noviembre 15, 2010.] http://capacitadoresdeti.com/consultorias/soluciones-varias/seguridadti..

5. **Navarro , Emilio del Peso and Ramos, Miguel Angel.** *Confidencialidad y Seguridad de la Información la LORTAD y sus implicaciones socioeconómicas.* Madrid : Dias de Santos, 1994.

6. *Norma Técnica Peruana NTP-ISO/IEC 17799.* Lima, Perú : s.n., 2007.

7. **desoft s.a.** Ministerio de la Informática y las Comunicaciones. *Ministerio de la Informática y las Comunicaciones.* [Online] 2010. [Cited: Enero 15, 2011.] http://www.mic.gov.cu/sitiomic/servlet/hmicmision..

8. Gestión de Calidad y Evaluación en Bibliotecas. *Gestión de Calidad y Evaluación en Bibliotecas.* [Online] Diciembre 5, 2011. [Cited: Enero 9, 2011.] http://biblionormas.blogspot.com/2006/12/conceptos-normas-y-normalizacin.html.

9. Biblioteca Universidad Zaragoza. *Biblioteca de la Universidad de Zaragoza.* [Online] biblioteca.unizar.es, 2010. [Cited: Enero 9, 2011.] http://biblioteca.unizar.es/buscar/normas.php#que..

10. *Código de prácticas para la administración de la seguridad de la información.* s.l. : Norma ISO-IEC 17799.

11. **DISAIC, NConline Consultoría Informacional.** NORMAS CUBANAS ONLINE. *NORMAS CUBANAS ONLINE.El Sitio Oficial de las Normas Cubanas.* [Online] DISAIC, 2010. http://www.nconline.cubaindustria.cu/nc%20con%20bd1/BuscarNormas/ResultadoBusqueda.asp..

12. *Ministerio de la Informática y las Comunicaciones. Resolución No. 127/2007.* Ciudad de La Habana : s.n., 2007.

13. **Creative Commons Attribution Share-Alike.** *OWASP Top 10-2010 Los diez riesgos más importantes en aplicaciones Web.* 2010.

14. OWASP. *The Open Web Application Security Project.* [Online] OWASP, 2010. [Cited: Enero 9, 2011.] http://www.owasp.org/index.php/OWASP:About..

15. Guía de pruebas de OWASP (OWASP Testing Guide). *OWASP, la comunidad libre y abierta sobre seguridad en aplicaciones.* [Online] 2008. [Cited: Enero 9, 2011.] http://www.owasp.org..

16. **Bravo Estévez, María de Lourdes and Gallaste, Arrieta .** El método Delphi. Su implementación en una estrategia didáctica. *El método Delphi. Su implementación en una estrategia didáctica.* [Online] [Cited: Enero 13, 2011.] http://www.rieoei.org/deloslectores/804Bravo.PDF.

17. **Urda, B. M. O.** *Gerencia de Proyectos de Ciencia e Innovación Tecnológica. Folleto curso de postgrado. CITMA.* Ciudad de la Habana, cuba : s.n., 1998.

18. **González-Santos, MsC. Odalys.** EL FUTURO DE LA BIBLIOTECA UNIVERSITARIA CUBANA. *EL FUTURO DE LA BIBLIOTECA UNIVERSITARIA CUBANA.* [Online] Octobre 2010. [Cited: Mayo 7, 2011.] http://www.dict.uh.cu/.../Los%20estudios%20de%20futuro.%20Surgimiento,%20desarrollo%20y%20evolución%20conceptual.doc.

19. **Caseres, E.** El método Delphi.Características. *El método Delphi.Características.* [Online] 2006. [Cited: Abril 28, 2011.] http://www.codesyntax.com. .

20. **FEBLES, A. CRIS, CUJAE 2003.** *FEBLES, A. CRIS, CUJAE.* 2003.p 136. 2003 .

21. **DELPHY., CRITERIO DE EXPERTOS: MÉTODO.** *CRITERIO DE EXPERTOS: MÉTODO DELPHY.* 2006.

22. CubaMinrex. Ministerio de Relaciones Exteriores de Cuba. *CubaMinrex. Ministerio de Relaciones Exteriores de Cuba.* [Online] [Cited: Enero 9, 2011.] http://www.cubaminrex.cu.

23. **Rodríguez Batista, María Lilia.** *Propuesta de Procedimiento para el Aseguramiento de la Calidad de Software en los proyectos productivos.* Ciudad de la Habana : s.n., 2007.

24. Instituto Nacional de Normalización. INN. *Instituto Nacional de Normalización. INN.* [Online] 2010. [Cited: Enero 9, 2011.] http://www3.inn.cl/cdocumentacion/portada/index.php.

25. Scribd. *Scribd.* [Online] 2010. [Cited: Abril 25, 2011.] http://es.scribd.com.

26. **Hernández León, Rolando Alfredo and Coello González, Sayda.** *EL PARADIGMA CUANTITATIVO DE LA INVESTIGACIÓN CIENTÍFICA.* Ciudad de la Habana : Editorial Universitaria (EDIUNIV), 2002. ISBN:959-16-0343-6.

Glosario de términos

UCI: Universidad de las Ciencias Informáticas

CEGEL: Centro de Gobierno Electrónico.

SW: Software.

HW: Hardware.

SI: Seguridad Informática.

RUP: Proceso Racional Unificado.

XP: Programación Extrema.

ICSW: La Industria Cubana del Software.

MIC: Ministerio de la Informática y las Comunicaciones.

TICs: Tecnologías de la Información y las Comunicaciones.

OSRI: La Oficina de Seguridad para las Redes Informáticas.

SOFTCAL: La Empresa de Producción y Desarrollo de Software de Calidad.

GNECS: Grupo Nacional de Expertos en Calidad del Software.

CALISOFT: Laboratorio Nacional de Certificación de la Calidad del Software.

OWAPS: Proyecto de Seguridad de Aplicaciones Web Abiertas.

ISO: Organismo Internacional de Normalización.

INN: Instituto Nacional de Normalización.

UML: Lenguaje Unificado de Modelado.

XSS: Secuencia de Comandos en Sitios Cruzados.

SQL: Lenguaje de Consulta Estructurado.

HTTP: Transferencia de Hiper-Texto.

SPSS: Paquete Estadístico para las Ciencias Sociales.

Anexos

Anexo # 1: Encuesta para determinar el conocimiento que tienen sobre seguridad durante el proceso de desarrollo de software las personas involucradas en este.

Entrevista a aplicar en los proyectos del Centro de Gobierno Electrónico (CEGEL)

IMPORTANTE LEER ANTES DE RESPONDER LA ENCUESTA

Esta encuesta tiene como objetivo fundamental determinar el conocimiento que tienen sobre seguridad durante el proceso de desarrollo de software, aquellas personas involucradas en este. Necesitamos que primero responda las preguntas generales, y luego en dependencia de su rol, las que correspondan. Le agradeceremos por brindarnos 5 minutos de su tiempo al responder esta encuesta.

Preguntas:

1. Seleccione con una (X) cuál o cuáles son los aspectos básicos que se garantizan con la seguridad informática:

__Autenticación ___Integridad __Autorización __Proporcionalidad __Confidencialidad __Disponibilidad __Ninguno

2. Seleccione cuáles son los activos informáticos más importantes en su proyecto:

__Mesas __Sillas __Software __Materiales de Oficina __Datos __Hardware __Ninguno

   - ¿A cuál de ellos está dirigida la máxima seguridad? ¿Por qué?

3. Seleccione la metodología de desarrollo que se usa en su proyecto:

__XP __AUP __SCRUM __RUP __Otras

4. Selecciona cuál es su rol en el proyecto:

   __Jefe de proyecto __Jefe de módulos __Analista __Diseñador __Desarrollador __Probador __Arquitecto

5. Proponga al menos 3 aspectos que usted considere no deben faltar para garantizar la seguridad durante el desarrollo del software en el área que usted se desempeña (en dependencia de su rol).

   RESPONDA LAS SEGUIENTES PREGUNTAS EN DEPENDENCIA DE SU ROL

Si es Jefe de Proyecto:

1. ¿Existe un plan de seguridad en su proyecto?

   __Sí __No __No sé

2. ¿Quién es el máximo responsable de que exista? Marque con una (X)

   __Jefe de módulo __Analista __Diseñador __Desarrollador __Probador __J´ de proyecto __Arquitecto __Ninguno

3. ¿Se definieron en su proyecto directrices para la programación segura antes de iniciar el desarrollo?

   __Sí __No

   a) En caso positivo escriba brevemente dos directrices

Si es Analista:

1. ¿En el análisis de riesgos, identifica usted riesgos de seguridad?

   __Si __No __No sé

a) Escriba 2 ejemplos de riesgos de seguridad

2. ¿En la captura de requisitos identifica usted requisitos de seguridad?

   __Si __No __No sé

a) En caso positivo ponga al menos 2 ejemplos e indique si son funcionales o no funcionales.

3. ¿Pone en práctica el plan de mitigación de riesgos una vez identificados los mismos?

   __Si __No __No sé

4. ¿Conoce usted los principios de seguridad de la programación?

   __Si __No __No sé

a) En caso positivo identifíquelos marcando con una (X)

   __Eslabón más débil __ Confidencialidad __Proporcionalidad __Disponibilidad __Dinamismo __Mínimo Privilegio __Integridad __ Participación Universal __ Ninguno

b) ¿Las interfaces del sistema cumplen con dos de estos principios?

__Si __No __No sé

c) En caso positivo diga cuáles son.

Si es Desarrollador:

1. ¿Cuál protocolo utilizarías en las aplicaciones web para garantizar una autenticación segura?

   __FTP __HTTP __HTTPS __Ninguno __Otro:

2. ¿Cómo se garantiza que solo se brinden los permisos necesarios a un usuario determinado?

   __Disponibilidad __Autenticación __Integridad __Autorización __Identificación

   __Control de Acceso __Confidencialidad __Ninguno

3. ¿Se utiliza alguna codificación para nombrar los objetos o las llaves de la BD en su proyecto?

   __Sí __No __No sé

4. ¿Se normalizan las variables en su proyecto?

   __Sí __No __No sé

   a) ¿Por qué?

5. Escriba dos ejemplos de validación de los datos en su proyecto.

Si es Probador:

1. ¿Cómo se realizan las pruebas de funcionalidad de tu proyecto?

   __Con la aplicación online __Con los Casos de pruebas __Los dos __Ninguna

2. ¿Se hace uso de las planillas para plantear las No conformidades Detectadas?

   __Sí __No __No sé

3. ¿Se realizan auditorías de seguridad en el proyecto?

   __Sí __ No __No sé

   a) En caso positivo diga en cuáles momentos.

4. ¿Se realizan en su proyecto pruebas de stress?

   __Sí __No

a) En caso positivo explique brevemente en qué funciona.

5. ¿Se realizan en su proyecto pruebas de intrusión?

__Sí __No

a) En caso positivo explique brevemente en qué funciona.

Si es Arquitecto:

1. ¿Qué estilos arquitectónicos usas en tu proyecto?

__Estilos de Flujo de Datos ___Estilos de llamada y retorno __Estilos de código móvil __Estilos heterogéneos ___Estilos Peer-to-Peer

2. ¿La arquitectura es una descripción de los subsistemas y los componentes de un sistema informático y las relaciones entre ellos?

__Sí __No __No sé

3. ¿En las aplicaciones de escritorio es la arquitectura la encargada de gestionar la seguridad y los permisos del sistema?

__ Si __No __No sé

4. ¿Permite el diseño arquitectónico de su proyecto visualizar la interacción entre las entidades del negocio?

__Si __No __No sé

5. El diseño arquitectónico de su proyecto describe claramente cómo se construirá la aplicación de software.

__Si __No __No sé

6. Si tiene algún elemento que aportar sobre la seguridad del proceso de desarrollo de software a través de la arquitectura, por favor escríbalo a continuación.

Anexo # 2: Listado de expertos

No	Nombre	Labor que realizan
E1	Yurisleidys Leiva Zuñiga	Jefa de Departamento de Gestión Gubernamental

E2	Omar A. García Pérez	Desarrollador
E3	Jorge Y. Jorrín Perdomo	Subdirector de Investigación y Postgrado del Centro de Gobierno Electrónico
E4	Darián González Ochoa	Asesor de Planificación y Control del Centro de Gobierno Electrónico
E5	Yanet Pérez Valcárcel	Jefe de proyecto
E6	Reinaldo Rodríguez Veitía	Administrador y Diseñador de Bases de Datos
E7	Yuriesky Duarte Correa	Analista

Anexo # 3: Encuesta de autovaloración de los expertos.

Compañero(a)

Se desea someter a valoración de un grupo de expertos, la propuesta de una norma técnica para el desarrollo de software seguro en los proyectos del Centro de Gobierno Electrónico (CEGEL) de la Facultad 3. Para ello se necesita conocer el grado de dominio que usted posee en temas relacionados con la seguridad informática y el proceso de desarrollo de software. Es por ello que se desea dedique un minuto de su tiempo y responda las preguntas que a continuación se presentan.

1. Marque con una cruz (X) el grado de conocimiento que usted tiene sobre el tema de seguridad informática (0= conocimiento nulo; 10=conocimiento muy avanzado por lo que puede considerarse especialista en el tema).

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

2. Marque con una cruz (X) el grado de conocimiento que usted tiene sobre la temática del proceso de desarrollo de software (0= conocimiento nulo; 10=conocimiento muy avanzado por lo que puede considerarse especialista en el tema).

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

3. Marque con una cruz (X) el nivel de influencia que ha tenido cada una de las fuentes indicadas a continuación, en su conocimiento sobre la seguridad informática.

No.	Fuente de Argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
		Alto	Medio	Bajo
1	Análisis realizado por usted.			
2	Su experiencia obtenida.			
3	Trabajo de autores nacionales.			
4	Trabajo de autores extranjeros.			
5	Su propio conocimiento del estado del problema en el extranjero.			
6	Su intuición.			

4. Marque con una cruz (X) el nivel de influencia que ha tenido cada una de las fuentes indicadas a continuación en su conocimiento sobre el desarrollo de software.

No.	Fuente de Argumentación	Grado de influencia de cada una de las fuentes en sus criterios		
		Alto	Medio	Bajo
1	Análisis realizado por usted.			
2	Su experiencia obtenida.			
3	Trabajo de autores nacionales.			
4	Trabajo de autores extranjeros.			
5	Su propio conocimiento del estado del problema en el extranjero.			

6	Su intuición.			

Anexo # 4: Encuesta de validación de los expertos.

Compañero(a)

La presente encuesta forma parte de la aplicación del Método de Valoración de Especialistas. A partir del siguiente cuestionario se pretende validar la propuesta de una norma técnica para el desarrollo de software seguro en los proyectos productivos del Centro de Gobierno Electrónico (CEGEL) perteneciente a la Facultad 3. Con este fin se solicita su valiosa colaboración, y le aseguramos, que sus opiniones se tendrán en cuenta para la aplicación de la Norma, la propuesta se encuentra adjunta a esta encuesta. Para su análisis y mejor comprensión de la norma se le informa que en la misma se definieron las reglas a seguir durante 4 momentos fundamentales identificados; cada una de ellas con una descripción detallada de las funciones que realizan. Usted debe calificar las siguientes afirmaciones según el grado de factibilidad que le brinden a la norma. Para la mejor comprensión de sus criterios se dividieron los mismos en 2 rangos: Si/No desde la 1ra a la 4ta pregunta, para la quinta se evaluó en 3 rangos y las restantes son preguntas abiertas para la mejora de la propuesta.

Preguntas	**Criterios de Expertos**	
	Si	**No**
1. Considera usted necesaria la existencia de la norma para contribuir a elevar la seguridad del software por cada momento definido, una vez culminado y puesto en explotación.		
2. Cree usted que las reglas definidas son las necesarias para la seguridad del software		
3. La norma puede ser aplicada a los proyectos del centro para lograr mayor organización en el equipo de desarrollo y seguridad del software.		
4. Considera usted que las reglas definidas		

encierra las fases fundamentales del proceso desarrollo de software.		

5. En qué medida considera usted la correcta definición de las reglas que conforma la norma.

   ___Alta _____Media _____Baja

   a) Si cree preciso adicionar o eliminar alguna regla, menciónela o explíquela brevemente.

6. ¿Cuáles elementos usted expondría a favor de la propuesta y cuáles en contra?
7. Elabore un comentario general sobre la norma que está siendo evaluada, que aporte elementos para mejorarla.

   _____

8. Describa la norma propuesta con una sola palabra:

   _____.

   Le agradecemos por su valiosa colaboración y estamos seguros que sus sugerencias contribuirán a perfeccionar la norma propuesta.

   Muchas gracias por su atención y le pedimos disculpas por las molestias ocasionadas.

Anexo # 5: Tabla simplificada de las características del SPSS.

Característica	SPSS
Amigabilidad con el usuario	Excelente
Calidad de gráficos	Bueno
Variedad análisis estadísticos	Bueno
Documentación	Excelente
Soporte técnico	Bueno
Sistemas Operativos	Microsoft Windows, Apple Mac o Linux.