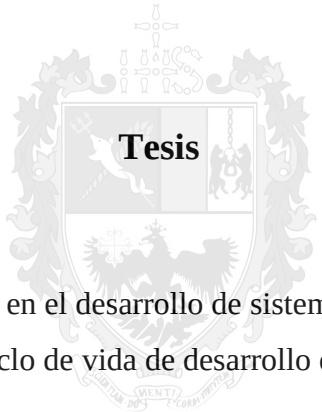
UNIVERSIDAD DEL SALVADOR

Maestría en Auditoría de Sistemas



Tesis

Administración de la seguridad en el desarrollo de sistemas de información dentro de la metodología del ciclo de vida de desarrollo de sistemas CVDS

Director: Daniel Nocella

Alumna: Alice Naranjo Sánchez

Buenos Aires – Argentina

2005

Resumen

El desarrollo de software ha evolucionado de ser una tarea de unos pocos expertos y satisfacer necesidades de grupos reducidos de gran poder económico, a ser una tarea de algunas personas que satisfacen necesidades para pequeñas y medianas empresas e inclusive hasta para unos pocos individuos y ya se habla de la exportación de software en grandes cantidades, a tal punto que es hoy en día un rubro considerable de la Balanza Comercial de muchos países, por lo que se ha mantenido la enorme presión para que estos sistemas sean desarrollados y puestos en producción con el menor costo posible y en el menor tiempo. De allí que la labor de desarrollar software se vaya tornando más compleja cada vez y los productos resultantes dejen mucho que desear.

Pero no sólo esto afecta a la labor del personal de sistemas sino también la rapidez de cambio, en necesidades, en formas de uso, en lenguajes, herramientas, sistemas operativos, esquemas de redes y equipos en donde se ejecutará el software. La tecnología tan cambiante y en constante evolución es otra cosa a la que se deben enfrentar los desarrolladores, por estas razones podemos afirmar que en los últimos años el desarrollo de sistemas ha sobrellevado una carga de presiones y variantes cada vez más diversas.

Los eventos mundiales recientes y los múltiples casos de fraude producidos con ayuda de los SI que se van registrando a diario en las organizaciones, han generado un mayor sentido de urgencia que antes con respecto a la necesidad de tener mayor seguridad en los SI, por eso es importante tener en cuenta que todo desarrollo de SI debe estar basado en una serie de estándares para medir y certificar su calidad y su seguridad.

Se han publicado muchos libros y artículos relacionados con este tema, como el modelado de procesos del negocio, la reingeniería, el desarrollo de sistemas, la calidad, entre otras temáticas. Un número creciente de herramientas automatizadas han surgido para ayudar a definir y aplicar un proceso de desarrollo de software efectivo, pero muy pocos hablan de establecer la seguridad en el desarrollo de sistemas.

Incluir la seguridad en el desarrollo de sistemas usando la metodología del ciclo de vida (CVDS) es una alternativa de seguridad para los SI, por esta razón el trabajo desarrollado presenta un manual que detalla como incorporar la seguridad en todas y cada una de las fases del proceso del CVDS, que incluyen: análisis, diseño, programación, implementación, post-implementación, operación y mantenimiento, cada una de estas fases incluyen aspectos mínimos de seguridad a ser implementados en forma efectiva en el CVDS.

Agradecimientos

A Dios por ser fuente inagotable de fortaleza y mi compañero leal en todos los estudios de la maestría.

A mis padres por el apoyo moral y el ánimo que me dieron para seguir la carrera.

A mi esposo por su cariño, comprensión y entereza al permitir concluir una de las metas más anheladas de mi vida.

A mi Director por la confianza y el apoyo brindado.

A mis profesores por haberme saciado las inquietudes y ansias de saber.

A la Srta. Leonor De Angelis, gracias por todos los consejos y su disposición voluntariosa para guiarme en mi desenvolvimiento universitario

A todo el personal administrativo y del Laboratorio de computación de la Facultad quienes me dieron la asistencia necesaria requerida.

Dedicatoria

Dedico este trabajo a:

Mis padres, que son un ejemplo de tenacidad y superación; fuente de mi inspiración,

Mis hermanos y hermanas a quienes tanto quiero y deseo siempre lo mejor del mundo,

Todas las personas ávidas por conocer el tema de seguridad en el CVDS.

Abreviaturas

AAA	American Accounting Association
AICPA	American Institute of Certified Public Accountants
ANSI	American Nacional Standard
COBIT	Control Objectives for information and related technology
COSO	Committee of Sponsoring Organizations for the Treadway Commission
CPD	Centro de procesamiento de datos
CVDS	Ciclo de Vida de Desarrollo de Sistemas
FEI	Financial Executive Institute
IEEE	Institute of Electric and Electronic Engineering
IIA	Institute of Internal Auditors
IMA	Institute of Management Accountants
ISO	Internacional Standard Organization
ISACA	Information System Audit and Control Association
NIST	National Institute of Standards and Technology
PAD	Área de procesamiento de datos
PED	Procesamiento Electrónico de Datos
SDLC	Software Development Life Cycle
SI	Sistemas de información
SIC	Sistemas de información computarizados
TI/IT	Tecnologías de la Información

Índice General

Lista de Figuras

Lista de Tablas

INTRODUCCIÓN

El desarrollo de sistemas es una tarea que siempre está en constante actualización y por consiguiente se proyecta con más fuerza hacia el perfeccionamiento en la forma de hacer desarrollos, por esa razón un tema en vigencia como lo es la metodología CVDS tan usada en todo desarrollo de software necesita un modelo de seguridad que delinee los aspectos más importantes de seguridad a plasmar desde el análisis hasta su operación y mantenimiento; es decir durante la construcción misma de los sistemas, más no al final de ella, porque quizás resulte mucho más costoso y difícil de aplicar.

La construcción masiva de sistemas, o lo que diría la producción y exportación de los mismos en forma comercial, hace necesario que se elaboren este tipo de propuestas, relacionadas al establecimiento de la seguridad en el proceso del CVDS.

Se ha establecido, tanto teórica como prácticamente, que los costos de seguridad son altos porque en su mayoría se aplican en la fase de implementación del CVDS únicamente y éstos a su vez pueden generar problemas al interactuar en una aplicación particular al no haber sido establecidos en todo su proceso de desarrollo y al desconocer detalles de cada fase y su integración.

El trabajo desarrollado tiene como propósito elaborar un manual de seguridad basado en las fases de la metodología del ciclo de vida integrando elementos claves de seguridad desde el inicio de su arquitectura.

A continuación describo la motivación, los objetivos, alcance, hipótesis, aportes específicos, beneficios, la organización del presente documento y la audiencia a la cual le debería ser útil este documento.

Motivación

La idea de emplear cada una de las fases en la esquematización de la seguridad no es nueva para mí; siempre fue una preocupación latente, teniendo en cuenta lo que pude palpar como Analista de Sistemas en muchas empresas, donde los Analistas, un poco

más antiguos parecían engañar a los usuarios en las pruebas de sistemas para lograr su aceptación porque no habían alcanzado a desarrollar todo y porque los tiempos eran tan apremiantes que tenían que cumplir con esa fase que se les vino encima y luego podían terminar de afinar. Entonces me preguntaba: ¿Qué garantiza que el sistema funcionaría correctamente una vez que esté en Producción?

Justificativos

Hoy en día la economía global depende más de sistemas automatizados que en épocas pasadas; esto ha llevado a los equipos de desarrollo a enfrentarse con una nueva década de procesos y estándares de calidad., sin embargo, ¿cómo explicamos la alta incidencia de problemas en los proyectos de sistemas? Conozco muchas empresas en que los proyectos de sistemas han fracasado. ¿Por qué existen tantos proyectos de sistemas con retrasos, presupuestos sobregirados, con problemas de calidad y que presentan fallas en la operación? Hagamos un análisis de conciencia y hablemos claro, esto es usual, nunca se cumplen los tiempos, peor el presupuesto y no digamos de la calidad y las fallas en la operación. ¿Cómo podemos tener una producción o una economía de calidad, cuando nuestras actividades diarias dependen de la calidad del sistema y ésta no tiene enfoques mínimos de seguridad en su desarrollo? La respuesta es al unísono simplemente hay desconfianza de los sistemas.

Tal vez suene ilógico pero, a pesar de los avances que ha dado la tecnología, aún existen procesos de desarrollo de sistemas informales, parciales y en algunos casos no confiables.

El reemplazo de plataformas y tecnologías obsoletas, la compra de sistemas completamente nuevos, las modificaciones de todos o de casi todos los programas que forman un sistema, entre otras razones, llevan a desarrollar proyectos en calendarios sumamente ajustados; esto ocasiona que se omitan muchos pasos importantes en el ciclo de vida de desarrollo, entre éstos, la seguridad. Diría yo que ella nunca es o ha sido considerada.

Es importante entonces tener un proceso de planificación del ciclo de vida de la seguridad de los sistemas de información en una organización. Un proceso que incluya una fase de análisis, que cuente con la generación de especificaciones correctas del

aplicativo a elaborar, que dichas especificaciones describan con claridad, sin ambigüedades, en forma consistente y compacta, el comportamiento del sistema; que el diseño de esos requerimientos esté enmarcado en el entorno claro de lo que se desea desarrollar; la programación aplique el esquema establecido en su enfoque; las pruebas certifiquen lo que el sistema debe hacer en un ambiente de seguridad previamente determinado, la implementación satisfaga las exigencias de control mínimas y la post-implementación así como la operación y el mantenimiento permitan retroalimentar al personal de seguridad respecto a los esquemas que se deben mantener para mejorar el ambiente operativo del aplicativo.

El concepto de seguridad debe aplicarse en todas nuestras actividades, sin embargo a pesar de lo acontecido, en muchos países este tema sigue siendo una utopía, algo irrealizable o difícil de implantar, principalmente por su costo, no caben ideas creativas que puedan reducir la inversión y maximizar los beneficios. Por esto hablar de seguridad es para mí una responsabilidad de todos, lograr difundir su importancia también lo es, más aún en un área que quizás poco se ha trabajado, cual es el enfoque de la administración de seguridad en el desarrollo de sistemas de información bajo la metodología del ciclo de vida de desarrollo de sistemas CVDS.

Objetivos

Ante la creciente importancia del uso de la seguridad y de la carencia de manuales establecidos para la aplicación de la misma en todas las fases en forma detallada e integrada, se propone como objetivo específico de este trabajo el siguiente:

Establecer un manual de seguridad para aplicarlo en cada una de las fases del desarrollo de sistemas bajo la metodología del CVDS.

Para hacer realidad este objetivo se plantean los siguientes objetivos particulares:

- Determinar una manera secuencial e integrada para aplicar la seguridad en los sistemas de información

- Desarrollar a través del manual, un marco de referencia para la aplicación de la seguridad en los Sistemas de información teniendo como base los estándares internacionales relativos a seguridad
- Contribuir al fortalecimiento de la seguridad de los sistemas de información en las empresas

Alcance

Este trabajo limita su alcance a:

a) En relación con la arquitectura de software, no se especifica lenguaje particular alguno, de allí su independencia con cualquier lenguaje de programación.
b) En cuanto a plataforma, el trabajo no particulariza plataforma alguna y por consiguiente tiene independencia de hardware o arquitectura de red particular.
c) El trabajo incluye la generación de especificaciones de seguridad para cada fase de la metodología del CVDS incluyendo el desarrollo y la programación, no la compra de software a terceros.
c) El trabajo establece especificaciones de seguridad concretas para cada fase de la metodología del CVDS sin ahondar en detalles específicos de configuraciones de seguridad relativos a plataforma de hardware, software o red.

Hipótesis

El trabajo descansa sobre una hipótesis fundamental que considera un análisis previo:

En la actualidad las empresas demandan una solución rápida de las necesidades de sistemas de información, exigiendo un óptimo servicio, calidad en los sistemas realizados, alta funcionalidad y todo esto a un costo muy bajo.

Para el departamento de sistemas es difícil alcanzar todo esto en corto tiempo y por esa razón, tratan de reducir su trabajo y dar resultados priorizando la programación de las aplicaciones y dejando como punto exclusivo para implementar la seguridad, la fase de implementación, la que en muchas oportunidades no es planificada ni desarrollada

adecuadamente. Surgen pues posteriormente, los huecos o fallas de seguridad, que hacen que todos tengan acceso a todo y se produzcan las vulnerabilidades de los sistemas.

Es por esta razón que considero importante incluir la seguridad desde el inicio del desarrollo de un sistema.

La pregunta que me hago es ¿Todas las empresas toman en cuenta la seguridad a la hora de desarrollar sistemas de información transaccionales y/u operacionales? y me respondo: " Si las empresas tomaran en cuenta el tema de seguridad desde el inicio del desarrollo de los sistemas de información y contaran con un manual de seguridad que explique lo que se debe hacer en cada una de las fases de desarrollo de un sistema y lo aplicasen, tendrían la base fundamental para una administración de seguridad razonable de los sistemas ".

Aporte

Entre los aportes que ofrece el trabajo se tienen:

1. El análisis de riesgos en cada fase
2. El desarrollo de los controles a manera de políticas que mitigan esos riesgos
3. La especificación funcional de los requerimientos de seguridad

Todos los cuales se unen en un manual que integra definiciones detalladas de seguridad en el desarrollo de sistemas.

Pero los aportes principales de este trabajo en un contexto global, se dan en cuatro áreas: Social, tecnológica, económica y académica.

1.- Social

Podremos apreciar que el principal aporte de nuestro trabajo radica en el campo social, pues es nuestra sociedad la que demanda una mejor atención de la gerencia a los servicios de información que poseen las empresas.

Así mismo la sociedad, se verá beneficiada de la optimización y eficiencia de los servicios de Sistemas de Información que manejen el esquema propuesto como resultado de nuestro estudio.

Las estrategias competitivas de las empresas planteadas bajo un sistema óptimamente controlado ofrecerán nuevas alternativas, oportunidades y/o servicios a nuestra sociedad.

2.- Tecnológica

Se definirán ambientes administrativos y de control de la tecnología que interactúen en el desarrollo de sistemas de información, estableciendo ambientes de control interno en el área de Sistemas.

3.- Económica

Este trabajo permitirá a las empresas alcanzar una alta rentabilidad como producto del costo de oportunidad de tener sistemas de información razonablemente seguros.

Por medio de la implementación del manual de seguridad, producto resultante de este trabajo, las empresas tendrán una mejor relación costo-beneficio de los sistemas de información a desarrollar.

4.- Académica

Este trabajo puede ser usado como referencia básica del entorno global de Sistemas de Información, Auditoría de Sistemas, Control Interno, Administración de Sistemas y Control de Gestión.

Así mismo servirá como material de ayuda a la formación de personas especializadas en Auditoría y Seguridad de Sistemas de Información.

Pero su principal aporte académico radica en las estrategias administrativas que se plantean para el control de los sistemas de información.

Beneficios

Algunos de los beneficios que se espera obtener de este trabajo son:

1. Garantizar la seguridad razonable de una aplicación desarrollada bajo estos preceptos
2. Los programadores podrán crear aplicaciones basadas en el enfoque de seguridad
3. Facilitar el desarrollo de sistemas razonablemente seguros para el auge de la exportación y crecimiento de la industria del software.
4. El modelo de seguridad del CVDS propone mitigar los riesgos identificados en cada una de las fases
5. El aseguramiento de la calidad del software, aún cuando no sea un aspecto puntualmente desarrollado en este trabajo, está vinculado a él.

Organización

El trabajo se organiza en cuatro partes, donde la primera nos lleva por un recorrido de la evolución histórica de la seguridad dando fundamentos generacionales que sustentan la profundización en el tema, así mismo hace un análisis de los riesgos y los controles existentes en la actualidad que afectan a los SI, la segunda parte da el marco teórico de donde parte el desarrollo propuesto, la tercera parte describe las normativas y/o estándares internacionales vinculados al tema de seguridad y la cuarta parte desarrolla el manual de seguridad del CVDS recorriendo una a una sus fases y recomendando la implementación de los controles correspondientes a través de políticas concretas.

Audiencia

Este trabajo desarrolla un manual que pretende ser considerado como un documento de referencia o una guía para todos aquellos interesados seriamente en el tema de seguridad, está dirigido a los Gerentes, Jefes y Administradores de sistemas; Contralores, Jefes de Seguridad y oficiales; programadores, analistas y todo el personal