8º Congreso Nacional de Mecatrónica
Noviembre 26-27, 2009. Veracruz, Veracruz.

La Identificación del Avance en el Proceso de Negocio Posibilita Garantizar la Seguridad de la Información

Chávez-Velázquez Raúl y Vargas-Soto José Emilio

Universidad Anáhuac México Sur

Abstract

The use given by several software creators to the methods and techniques for design and development cause the result to overlook the triggers of change in the business process and the information in each of its steps. Software applications based on information of the business process are ready to provide the necessary means to make decisions according to the needs of an organization and in expressions that the user is familiar with. This software design, according to the business process must be done and can be used to guarantee the information security.

Resumen

El uso que varios creadores de aplicaciones de negocios dan a los métodos y técnicas utilizados durante las etapas de diseño y desarrollo provocan que el resultado deje de lado la consulta del avance en el proceso de negocio y la información en cada etapa del mismo. Cuando la aplicación provee la información del proceso de negocio el usuario cuenta con una herramienta que le proporciona los elementos necesarios para tomar las decisiones con apego a lo que la organización necesita. Este diseño con apego al proceso de negocio puede aprovecharse para garantizar seguridad a la información.

Palabras clave: Seguridad, ciclo de vida de la información, riesgo.

1. Introducción

El contenido de este documento es un diagnóstico de las aplicaciones de negocio y la asignación de los niveles de seguridad de la información que requieren.

El documento es un artículo que ha sido desarrollado para ser presentado ante el comité evaluador del 8º. Congreso Nacional de Mecatrónica.

Las respuestas que encontrará el lector consisten en: un diagnóstico de las limitaciones en el diseño de aplicaciones de negocios para la asignación sistematizada de los niveles de seguridad de la información y, a manera de conclusión, una alternativa de solución para garantizar la seguridad de la información.

El documento incluye las siguientes secciones:

Introducción – que menciona al destinatario del documento y describe al propio documento y a su contenido.

Tema – proporciona las fuentes de información que indican que el desarrollo del documento es de interés para otras personas y define la cuestión sobre la que trata el artículo.

Datos – con base en fuentes de información primaria y secundaria se identificarán los elementos necesarios para conducir el artículo.

Información – con base en la evidencia extraída de los datos aunada con diversos métodos se construyen elementos que proporcionan la información necesaria para emitir un diagnóstico.

Diagnóstico – descripción de la causa próxima sustentada en la evidencia de la información.

Conclusiones – resumen de resultados ofrecidos por el autor.

Referencias – fuentes primarias y secundarias consultadas.

2. Tema

La seguridad de la información tiene vínculos con el proceso de negocio. El avance en el proceso de negocio define los diferentes niveles de seguridad que la información debe adquirir.

Esta relación entre el proceso de negocio y la seguridad de la información también depende del nivel de seguridad asignado al usuario que participa en el proceso de negocio.

El trabajo con estos tres componentes proporcionan los elementos necesarios para la generación de evidencia que permita emitir un diagnóstico sustentado del manejo de la seguridad de la información.

2.1 La seguridad de la información es un asunto estratégico.

Los incidentes de seguridad de la información pueden provocar desconfianza en los mercados y deben administrarse discretamente para no provocar nuevos incidentes de seguridad [1]. Por lo que la seguridad de la información y en general el uso de las tecnologías de información, es un tema que requiere una alternativa de solución con base en una estrategia [2].

La familiaridad en el uso y el conocimiento de los sistemas de información aparecen como razones significativas de que sea ignorada la efectividad de los sistemas en el soporte estratégico de los procesos de toma de decisión [2].

Algunos de los síntomas encontrados como obstáculos a la aceptación de las herramientas de tecnologías de la información como soporte para la planeación estratégica es la falta de conocimiento y familiaridad del tomador de decisiones con las aplicaciones y métodos que le permitan explotar y manipular la información [2]. Por esta razón es posible considerar que es obligación de las áreas de TI convertir el diálogo tecnológico en diálogo administrativo y humano, de manera que facilite la integración de las valiosas herramientas tecnológicas en el proceso de negocio.

Además las herramientas de TI también son vehículos que facilitan las tareas de transparencia y la reducción de la corrupción [3] cuando cuentan con un diseño adecuado para la seguridad de la información y del proceso de negocio.

En el caso de los servicios de salud en los Estados Unidos de América (EUA), se tiene conciencia que las herramientas de tecnologías de la información causan un gran impacto en la calidad del servicio, el control y reducción de costos y la posibilidad de incrementar la participación del mercado [2].

Los procesos de negocio, como el de la salud en los EUA, requieren de una estrategia robusta de TI que a su vez sea capaz de soportar la implementación y logro de los objetivos de la estrategia del sector [4].

La percepción de que los sistemas de información son deseables y necesarios para el soporte del proceso estratégico [2] es una realidad y su uso será mejor aceptado al garantizar la seguridad de la información de manera que el usuario la aprecie.

2.2 Con el usuario siempre en mente.

Uno de los retos del profesional de las TI es trabajar para que la seguridad de la información sea de fácil percepción por parte del usuario. Para satisfacer este reto, el profesional de las TI debe mantener en mente la satisfacción de su usuario desde las primeras etapas del diseño de aplicaciones.

Cuando el diseñador de software confronta la realidad y pasa de las etapas de comprender el uso que se hará de la aplicación al proceso de garantizar la seguridad de la información, encuentra que las herramientas, los métodos de diseño y los deseos de su futuro usuario no siempre le permitirán ofrecer una alternativa de solución a prueba de fallas de seguridad.

Así, el diseñador tendrá que acordar conscientemente un nivel adecuado de seguridad que le permita el balance entre la funcionalidad y el rendimiento y mantener la probabilidad de que una amenaza aproveche una vulnerabilidad – riesgo - de nivel aceptable [5].

3. Datos.

3.1 Amenazas.

Además, el profesional de TI debe ser consciente de que las herramientas que provee a la organización ostentan información que, tanto para la organización como para los destinatarios de la misión de ésta, es en muchas ocasiones privada. Por lo que es custodio del activo informático y uno de los servicios que provee es mantenerlo alejado de amenazas ya que los registros de datos son blanco de posibles hackers y/o ladrones de identidad [6].

La seguridad de la información es un tema que adquiere importancia estratégica más allá de la organización e involucra a todos los ciudadanos. Por ejemplo, la cantidad de dólares relacionado con el robo de propiedad intelectual en los países

industrializados es tan grande que atrae a los peores individuos de diversas sociedades [7]. Quizá hasta a la delincuencia organizada. Basta con saber que China y Rusia son reconocidas como líderes en el robo de propiedad intelectual [7].

3.2 Algunas oportunidades.

En el tema de la organización de TI, en los EUA se ha encontrado que la oportunidad laboral del profesional en redes es la de mayor demanda, seguida por los temas de seguridad de la información y soporte al usuario para garantizarle la disponibilidad de los servicios informáticos para acceder a la información [8]. Entre los conocimientos más solicitados están el dominio técnico de la configuración y administración de firewalls marca checkpoint y la administración de redes inalámbricas [8].

Con la demanda de recursos humanos calificados originada tanto en los departamentos de TI como en los proveedores de servicios tercerizados, el profesional de la seguridad de las TI puede ser muy bien pagado, según palabras de Richard Swann, administrador de infraestructura del Institute of Directors [9].

Otras oportunidades pueden provenir de crear los servicios que las diferentes industrias de los países más poderosos necesitan, siempre que sea posible garantizar la seguridad de la información. De manera tal que la estabilidad regional y la calidad de los servicios den la seguridad que se necesita.

3.3 Vulnerabilidades.

Escribir sobre el tema de seguridad de la información pasa de manera obligada por tratar las vulnerabilidades.

Internet y otras tecnologías cada vez llegan a más usuarios con mayor dispersión y esto es una de las causeas de más vulnerabilidades de la infraestructura de TI así como de la aparición de un mayor número de amenazas tanto internas como externas a la organización [10].

La detección de brechas en la seguridad interna de la organización es una tarea cotidiana de las áreas de TI. Estas brechas entre la seguridad deseada y la seguridad provista son vulnerabilidades que facilitan el diagnóstico en la etapa inicial. Si el riesgo se define como la probabilidad de que una amenaza aproveche una vulnerabilidad, es casi evidente que la reducción de las vulnerabilidades es de vital importancia [11].

4. Información – Métodos.

4.1 Saga.

En este artículo se aprovechará este concepto como se encuentra definido y en forma similar a la utilizada por Vargas y Chávez en la administración de proyectos mecatrónicos [12]. En esta ocasión el concepto saga será utilizado para el análisis de procesos de negocios y así simplificar el diseño de aplicaciones y la asignación de la seguridad de la información.

4.2 Propuesta de saga para el servicio.

Una forma simple para definir una secuencia de sucesos en el proceso de la venta y operación de servicios tercerizados está compuesta por las etapas: T1. Venta, acción de encontrar posibilidades de venta y su logro. T2. Toma operación, ejecución de las labores necesarias para adquirir las responsabilidades del servicio. T3. Estabilidad, continuidad del servicio ofertando los niveles de servicio contractuales. T4. Renovación, ejecución de las labores propias de renovación, renegociación o terminación del contrato. La saga propuesta toma en cuenta todas las etapas del proyecto de servicio como parte de la labor de venta.

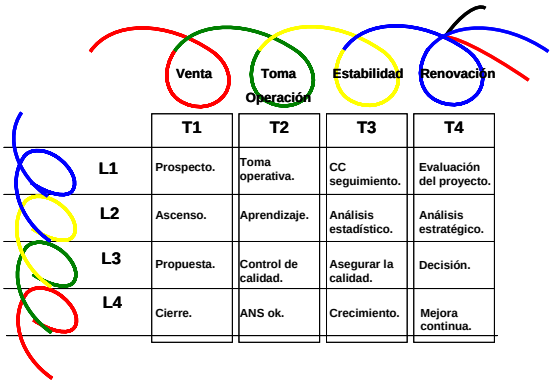

Fig. 1. Propuesta de saga de la venta de servicios.

Los sucesos L1 – L4 mostrados para cada etapa de la saga de venta de servicios son una propuesta de los detonadores que identificarían el avance al siguiente paso.

En el caso de la saga para la etapa de Venta la secuencia es:

L1. Prospecto, a su vez definida, al menos, por tres pasos; 1) identificación de una oportunidad real; 2) conocimiento y empatía con un posible

patrocinador; 3) identificación de la necesidad de servicio.

L2. Ascenso, definida, al menos, por tres pasos; 1) ascenso y conocimiento del (de los) tomadores de decisiones; 2) operacionalización de la necesidad; 3) ubicarse como el posible proveedor predilecto.

L3. Propuesta, oferta de un satisfactor a través de los medios que el beneficiario defina.

L4. Cierre, aceptación contractual o rechazo de la oferta.

4.3 Seguridad de la información durante el proceso de negocio.

La asignación del nivel de seguridad que la información tiene está directamente asociada con el momento que vive en el proceso que la utiliza. Para explicar lo mencionado haré uso de un ejemplo: la información de algunos eventos considerados de seguridad nacional puede ser considerada como secreta hasta un lapso en el que su nivel de seguridad sea reclasificado como público.

En las siguientes secciones se desarrolla el ejemplo de una propuesta de servicio durante la etapa de venta de un satisfactor.

4.4 La propuesta.

Para ejemplificar las transformaciones en el nivel de seguridad de la información se hará uso de la propuesta de una alternativa de solución y su viaje a través de la saga de venta. Las diferentes unidades de información que componen la propuesta serán identificadas a través de su estructura.

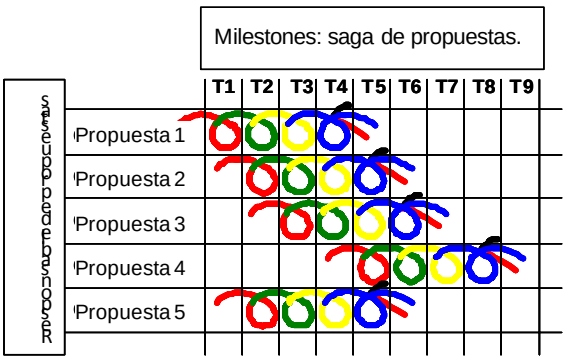

Fig. 2. Cada propuesta tiene su propio ritmo y avance en la saga.

4.5 Supuesto de la estructura de una propuesta de alternativa de solución.

Un supuesto del contenido de una propuesta se muestra en la siguiente figura.

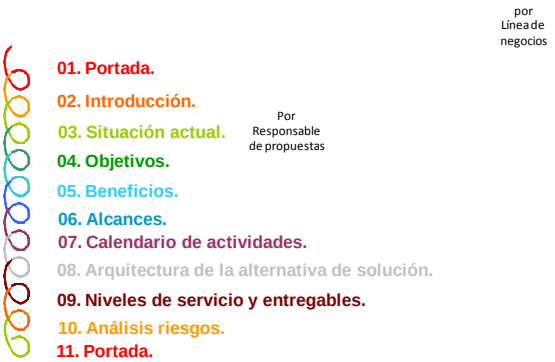

Fig. 3. Estructura supuesta de una propuesta.

La información que incluye cada sección se describe a continuación y/o responde a las preguntas enunciadas en cada una.

a) Portada: ¿Qué es este documento? ¿Quién lo envía? ¿A quién está dirigido? Nombre del proyecto.

b) Introducción: ¿Qué es el contenido del documento? ¿Quién es el destinatario del documento? ¿Qué respuestas encontrará el destinatario del documento al leerlo? ¿Cómo está organizado el documento?

c) Antecedentes: ¿Cómo se analizaron los síntomas para emitir un diagnóstico? ¿Cuál es el obstáculo (diagnóstico)? ¿Qué consecuencias y costos ha tenido no resolverlo? ¿Qué se hace actualmente?

d) Objetivos: ¿Cómo sabré si obtuve los resultados esperados? ¿Cómo se medirán los resultados? ¿Cómo se evaluarán los resultados? ¿Cuáles respuestas se dan como alternativa de solución? ¿Se cumplirán los planes del proyecto?

e) Beneficios: ¿Qué ventajas obtengo al resolver el problema con la alternativa propuesta? Es recomendable dar dimensión al impacto económico de los beneficios.

f) Alcances: Limitación del proyecto en: a) Espacio; b) Recursos; c) Responsabilidades;

d) Actividades; e) Entregables. Además debe dejar claro lo que se incluye e indicar lo que se hará con lo que no esté previsto.

g) Plan de trabajo: Secuencia de tareas. Tiempos y recursos involucrados en cada tarea.

h) Alternativa de solución: modelo de infraestructura, modelo de equipo y modelo de procesos.

i) Acuerdos de niveles de servicios y descripción y estructura de entregables. Mecanismos de escalamiento operativo y administrativo.

j) Análisis de riesgos al implementar el proyecto.

k) Precio.

Existe mucha literatura respecto al contenido y organización de una propuesta comercial por lo que versiones similares de estructuras de propuestas pueden encontrarse en revistas y talleres de diverso origen.

Para uso en el artículo se hará referencia únicamente a las grandes secciones de la propuesta, no a los elementos de cada sección. Un análisis más profundo durante el diseño de una aplicación obligaría a identificar y asignar niveles de seguridad a todos los elementos de información.

4.6 Modelo de seguridad.

En las organizaciones la responsabilidad de definir una política de seguridad es de la alta gerencia. Una alternativa para definir dicha política es sustentarla con base en un modelo validado y, en muchas ocasiones, probado. Un ejemplo de modelo de seguridad es el llamado modelo militar, que se describe brevemente a continuación.

La norma de seguridad fundamental del departamento de defensa de los Estados Unidos de América es conocida como *política de seguridad militar*. En esta política la información posee una clasificación y las personas un nivel de autorización. Cuando es necesario determinar si una persona tiene permiso de leer un documento se confronta el nivel de autorización de la persona con la clasificación de seguridad de la información [13].

Los modelos de seguridad son métodos de implementación de la política de seguridad y son validados matemáticamente. Por ejemplo el modelo Bell – LaPadula [13].

Este modelo identifica la asequibilidad de un objeto con base en el nivel de autorización asociado tanto con el sujeto como con el objeto y posteriormente sólo para permitir su lectura, lectura y escritura o solo escritura.

La asequibilidad de la información con base en el modelo utiliza dos propiedades: lectura y escritura.

La propiedad de seguridad para facilitar la lectura especifica que un objeto no puede ser leído si su clasificación es superior a la del sujeto. Esta propiedad es llamada “no lectura hacia arriba”.

La segunda propiedad es denominada estrella y refiere a la asequibilidad para escritura. El sujeto únicamente puede escribir información en un objeto que tiene la misma o superior clasificación. La propiedad es llamada “no escritura abajo”. De esta manera se puede prevenir que un sujeto copie información en un objeto de clasificación inferior.

Con base en este modelo se llevará a cabo un ejercicio para analizar el comportamiento de los niveles de seguridad de la información en un proceso de negocio, la propuesta y la venta tratados en este artículo.

4.7 Implementación.

Se supondrá que las clasificaciones de seguridad son:

Tabla de asignación de nivel de seguridad.				
Clasificación.	**Muy secreto.**	**Secreto.**	**Uso interno.**	**Público.**
Asignación a la persona (ejemplo).			X	
Asignación a la propuesta.	Cada sección de la propuesta cambiará de clasificación con base en el avance de la saga de venta.			

Supondremos que durante el ejercicio a desarrollar la clasificación de la persona no cambia, es la misma tanto para lectura como para escritura y revisaremos una idea del cambio de clasificación que sufrirán las diferentes secciones de una propuesta. Para mayor facilidad se propone la matriz de la figura 4.

Al hacer el cruce de la característica como usuario interno en la facultad de lectura, el sujeto puede leer información con su nivel de seguridad e inferiores, por lo que los cambios en su posibilidad de

acceder y leer las diferentes secciones de la propuesta se muestra en la matriz de la figura 5.

Un ejercicio similar podría desarrollarse para la posibilidad del sujeto por escribir en las diferentes secciones de la propuesta.

También es posible desarrollar un ejercicio similar si otra política de seguridad y otro modelo de seguridad son elegidos.

5. Diagnóstico.

Como primer paso se identificaron los diferentes sucesos de un fenómeno. El fenómeno puede ser un proceso de negocio. Al identificar los sucesos de un proceso de negocio es posible tener claridad de las situaciones que provocan un cambio de estado en el proceso y, por lo tanto, un cambio de estado en la información que el proceso utiliza.

El análisis de la estructura de la información y sus cambios de nivel de seguridad durante el desarrollo de un proceso de negocio proveen la información necesaria para que el administrador de la seguridad de la información cree los cuadros y perfiles necesarios de los diferentes usuarios de la información.

Al combinar los procesos de negocio, los niveles de seguridad de las distintas piezas de información y armonizarlo con la seguridad del posible usuario hará posible definir los perfiles y sistematizar la seguridad de la información, siempre que se encuentre asociada con el momento vigente del proceso de negocio.

Sin embargo el proceso de negocio y los detonadores no son fuentes tradicionales del diseño de aplicaciones para la automatización de empresas. Este diseño de aplicaciones con soporte en el proceso de negocio permitiría enlazar el perfil del usuario con la posibilidad de acceder a la información únicamente con base en el flujo operativo de la organización y sin requerir la asignación discrecional de atributos de seguridad de la información.

El problema determinado es que:

La ausencia de la identificación de detonadores de cambio en el proceso de negocio como parte del diseño de aplicaciones limita las posibilidades de garantizar la seguridad de la información.

Ya que sin la identificación de dichos detonadores con base en el modelado del proceso de negocio el diseño de las aplicaciones carece del apego necesario al flujo de la información y sus cambios en requerimientos de seguridad, por lo que los aplicativos se convierten en interfaces aisladas de consulta y reporte de volúmenes de datos almacenados con ayuda de algunas pantallas.

Las consecuencias del diseño tradicional de software se traducen en la imposibilidad del usuario de explotar la información con base en el seguimiento del flujo del proceso de negocio por lo que cada ocasión que requiere la información que le permita el análisis del negocio y no cuenta con el reporte o pantalla que se lo facilite, el usuario se frustra y, en el mejor de los casos, solicita y consigue una adecuación de su sistema.

6. Conclusión.

Es posible entrelazar los niveles de seguridad de la información con la saga del proceso de negocio, de manera tal que facilite su automatización. Esta labor tomada en cuenta durante el diseño de aplicaciones también permitirá que los usuarios de aplicaciones estén facultados para explotar la información con base en sus necesidades de negocio.

El ejercicio desarrollado a través del ejemplo del proceso de venta y su propuesta no está limitado a la política de seguridad ni al modelo de seguridad elegidos, por lo que el desarrollo de mejores aplicativos que garanticen de forma automatizada la seguridad de la información es viable.

Referencias

[1] Cobanoglu C., DeMicco F. *"To Be Secure or Not to Be. Isn't This the Question? A Critical Look at Hotel's Network Security"*, *International Journal of Hospitality & Tourism Administration*. The Haworth Press, Inc., Vol. 8, No. 1, 43 – 59, 2007.

[2] Yap G., Platonova E., Musa P. "*Use of Information Systems in Air Force Medical Treatment Facilities in Strategic Planning and Decision-Making"*, *Journal of Medical Systems*. Springer Science and Business Media B. V., Vol. I, No. 30, 9 – 16, 2006.

[3] Kumar R., Best M. "*Impact and Sustainability of E-Government Services in Developing Countries: Lessons Learned from Tamil Nadu, India"*, *The Information Society*. Taylor & Francis LLC., No. 22, 1 – 12, 2006.

[4] Kolodner R., Cohn S., Friedman Ch. *"Health Information Technology: Strategic Initiatives, Real Progress"*, *HEALTH A F FA I R S ~ We b Ex c l u s i v e*. Project HOPE–The People-to-People Health Foundation, Inc., 391 – 395, 2008.

[5] Lathrop S., Gates C., Darrell M., Hill J. *"Risk Assessment of a Power Plant: Evaluating the Security of a Supervisory Control and Data Acquisition System"*, *ASHRAE Transactions*. American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., Vol. 112, Part 2, 671 – 679, 2006.

[6] Sharpe V. *"Privacy and Security for Electronic Health Records"*, *Hastings Center Report*. Hastings Center, Vol. 35, No. 6, 49-49, 2005.

[7] Liebesfeld J. *"Intellectual Property Theft as Blood Sport"*, *Security*. ABI/Inform Global, Vol. 45, No. 3, 106-106, 2008.

[8] ACM**.** *"IT Hiring Up"*, *Communications of the ACM*. Association of Computing Machinery, Vol. 48, No. 2, 9-9, 2005.

[9] Flinders K**.** *"Firms falling short on security skills"*, *Computer Weekly*. ProQuest Computing, Jun 12, 50-50, 2007.

[10] Cannoy S., Palvia P., Schilhavy R**.** *"A Research Framework for Information Systems Security"*, *Journal of Information Privacy & Security*. ABI/INFORM Global, Vol. 2, No. 2, 3-29, 2006.

[11] Kondakci, S**.** *"Dependency Analysis of Risks in Information Security"*, *International Review on Computers and Software*. Praise H'orlhy Prize S.r.l., Vol. 3, No. 1, 11-19, 2008.

[12] Vargas J., Chávez R. *"Enseñanza de la Administración y Desarrollo de Proyectos Mecatrónicos"*, XI Congreso Mexicano de Robótica, Asociación Mexicana de Robótica, 5 páginas, Celaya, Guanajuato, México 2009.

[13] Hansche S., Berti J., Hare C. *"Official (ISC)^2 guide to the CISSP exam"*, Auerbach Publications, Estados Unidos de América, 1ª. Ed., 2003.

	Asignación de seguridad del una propuesta de servicios tercerizados.															
	Fase de venta.															
	Prospecto				Ascenso				Propuesta				Cierre			
	GS	S	I	P	GS	S	I	P	GS	S	I	P	GS	S	I	P
Portada.		X				X					X					X
Introducción.		PNE				X				X						X
Situación actual.	PNE					X				X					X	
Objetivos.	PNE					X				X						X
Beneficios.	PNE				PNE					X					X	
Alcances.	PNE					PNE				X						X
Plan de trabajo.	PNE					PNE				X						X
Alternativa de solución.	PNE				PNE					X					X	
Acuerdo de niveles de servicio y entregables.	PNE				PNE					X					X	
Análisis de riesgos.	PNE				PNE					X					X	
Precio.	PNE				PNE				X						X	

GS - Gran Secreto (Top Secret).
S - Secreto.
I - uso Interno.
P - información Pública.

PNE - Posiblemente No Existe la información.

*** El nivel de seguridad asignado se identifica por una X o el identificador PNE.**

Fig. 4. Clasificación de seguridad.

	Propuesta de sercicios tercerizados: autorización de LECTURA para una persona con clasificación de usuario INTERNO.															
	Fase de venta.															
	Prospecto				Ascenso				Propuesta				Cierre			
	GS	S	I	P	GS	S	I	P	GS	S	I	P	GS	S	I	P
Portada.			ND				ND				X				X	
Introducción.			ND				ND				ND				X	
Situación actual.			ND				ND				ND				X	
Objetivos.			ND				ND				ND				X	
Beneficios.			ND				ND				ND				X	
Alcances.			ND				ND				ND				X	
Plan de trabajo.			ND				ND				ND				X	
Alternativa de solución.			ND				ND				ND				X	
Acuerdo de niveles de servicio y entregables.			ND				ND				ND				X	
Análisis de riesgos.			ND				ND				ND				X	
Precio.			ND				ND				ND				X	

ND - No Disponible.

*** El nivel de seguridad asignado se identifica por una X o el identificador ND.**

Fig. 5. Cambios a la clasificación de seguridad.