MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN – MASI

Diego J. Parada
Docente Facultad de Ingeniería Informática, Universidad Pontificia Bolivariana
Bucaramanga, Santander, Colombia

July A. Calvo
Consultora Junior en Seguridad de la Información, Newnet S.A
Bogotá, D.C., Colombia

Angélica Flórez
Directora Facultad de Ing. Informática, Universidad Pontifica Bolivariana
Bucaramanga, Santander, Colombia

RESUMEN

Actualmente las empresas enfrentan grandes retos para lograr eficacia en sus procesos de negocio; la tecnología es considerada como una de las soluciones reales para suplir las necesidades que se presentan en los procesos organizacionales. Las tecnologías de información permiten tiempos de respuestas adecuados en los procesos que se generen entre las empresas, los clientes y los proveedores. Por ejemplo, debido al crecimiento a nivel mundial de transacciones comerciales en el marco de un mercado global, se hace necesario la utilización de servicios en Internet como: comercio electrónico (ecommerce), Intercambio Electrónico de Datos (EDI – Electronic Data Interchange), B2B (Business to Business), entre otros,.

El Modelo de Arquitectura de Seguridad de la Información – MASI, proporciona a las empresas un marco de acción estratégico el cual establece las directrices en materia de seguridad de la información en los diferentes procesos organizacionales, enmarcado en seis elementos cuyo funcionamiento, al ser correlacionado, permite el conocimiento de las expectativas del negocio planteadas por la Alta Gerencia.

El modelo definido se encuentra compuesto por los siguientes elementos: Negocio, Marco Normativo, Gestión de la Arquitectura de Seguridad de la Información, Acuerdos e Infraestructura de Seguridad de la Información.

Palabras Claves: seguridad de la información, procesos de negocio, arquitecturas de seguridad, gobierno de seguridad de la información, políticas de seguridad de la información, análisis de riesgos.

1. INTRODUCCIÓN

La seguridad informática por no estar concebida dentro de un marco mediador o facilitador, era considerada un entorpecedor para le ejecución de procesos y por ende para el mismo crecimiento del negocio, puesto que solo se sesgaba prohibir cerrando puertos, negando permisos y limitando recursos. A través del tiempo, se ha visto la necesidad de repensar la seguridad informática y dimensionarla en un marco más amplio, lo que conllevó a definir el concepto de seguridad de la información. [1], [2].

La seguridad de la información se visualiza como aquel esquema integrador de las TI, los usuarios y los procesos de negocio, donde se reconoce *la información* como un activo de la organización.

La Arquitectura de Seguridad de la Información define un esquema de acción estratégico en la organización, mediante el cual se establecen las directrices a nivel de seguridad de la información en cada uno de los procesos del negocio.

2. ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN

El Gobierno de Seguridad de la Información (GSI) define que para implementar un esquema de Seguridad de la Información (SI), se deben tener en cuenta seis elementos, que necesariamente representan las intenciones de la Alta Gerencia en la formalización de un programa referente al tema de SI [3]:

1. Alineación Estratégica: objetivos de seguridad alineados con los objetivos del negocio.

2. Administración del Riesgo: dinamizar la forma en cómo se realiza y se da continuidad al análisis y tratamiento del riesgo, de tal manera que se reduzcan los riesgos y el impacto inherente a su materialización.

3. Entrega de Valor: busca que la inversión realizada en SI sea optima, es decir, que sea proporcional al valor del negocio y esta tenga un retorno de inversión.

4. Administración de Recursos: administración efectiva y eficaz de los recursos asignados para la formalización de controles, políticas, roles y responsabilidades además de los presupuestos para SI.

5. Medición del Desempeño: definir indicadores que permitan medir los cambios de estado del negocio antes y después de la implementación de la SI, como soporte y apoyo en los procesos del negocio.

6. Integración: propósito o intención por hacer que los elementos mencionados en los ítems anteriores, converjan en un esfuerzo por asegurar el negocio, es decir, que sus procesos tengan un desempeño transparente antes, durante y después de su ejecución.

Los seis elementos mencionados y que hacen parte del GSI, establecen las generalidades que orientan a la SI como un apoyo para el normal funcionamiento de los procesos del negocio, y no un entorpecedor de los mismos, como en ocasiones se vislumbra la SI para el negocio. La SI termina siendo una

limitante para el negocio cuando se define sin un orden o un criterio definido como proceso facilitador y enriquecedor de las expectativas del negocio, generando un valor agregado en los procesos del negocio.

Dicho problema deriva una pregunta fundamental y es la preocupación por ¿cómo trabajar de forma ordenada, con sentido de apoyo y facilitador en el normal funcionamiento del negocio?. La respuesta sugiere pensar en un esquema o modelo que garantice la administración (entendida como el proceso de planear, organizar, dirigir y controlar) y la integración mencionada en el GSI, donde existe armonía y equilibrio de los esfuerzos que hace cada elemento del GSI en la materialización de la SI para el negocio; dicho modelo se encuentra enmarcado en lo que se conoce como Arquitectura de Seguridad de la Información.

Desglosando el concepto de Arquitectura de Seguridad de la Información, se define Arquitectura al proceso de diseñar y construir y Seguridad de la Información son las técnicas mediante las cuales se pueda salvaguardar, proteger, resguardar documentos digitales e impresos.

La ASI tiene como propósito el diseñar una estructura lógica que orqueste, es decir, administre (diseñe, organice, direccione y controle) los elementos que conforman el negocio: procesos (know how), actores (Alta Gerencia, proveedores, clientes, usuarios y administradores del sistema) y TI (aplicaciones, dispositivos, infraestructura, entre otros), enmarcados en unos niveles aceptables de seguridad de la información que es transversal a dichos elementos.

Modelos de Arquitectura de Seguridad de la Información
Revisando el estado del arte sobre el tema de ASI, se encuentran los siguientes modelos:

Modelo de Arquitectura de Seguridad por Jan Killmeyer [4]: el autor describe su modelo de ASI con base en la definición de cinco elementos:

1. Organización de la Seguridad e Infraestructura: es el reconocimiento de la necesidad de alinear procesos de negocio con la SI, además declara la existencia de una persona encargada de su ejecución y gestión; dicha persona debe ser parte asesora o miembro de la Alta Gerencia en la organización, con el fin de conocer sus expectativas, logrando la alineación de la agenda de la Alta Gerencia con la del Área de SI.

2. Políticas, Estándares y Procedimientos: elemento conformado por tres conceptos diferentes interrelacionados, el primero de ellos la Política: es definida en términos de los objetivos del negocio y marcan la pauta para el comportamiento de los usuarios; los Estándares son las buenas prácticas en SI; y los Procedimientos definen el paso a paso, la forma como se desarrollan las diversas actividades por las personas encargadas de su ejecución.

3. Líneas base de seguridad y la valoración del riesgo: debido a la gran demanda de esfuerzo en tiempo y dinero en pruebas de vulnerabilidad en los dispositivos, Killmeyer recomienda la definición de tres elementos que permite manejar estas variables; las líneas base como una pauta para la configuración de dispositivos, la educación a los administradores y usuarios en el uso de las políticas de seguridad y la evaluación de los controles, todo ello en un ciclo de realimentación continua.

4. Capacitación y entrenamiento de los usuarios: es el proceso de concienciación de los usuarios por parte de los encargados de la gestión en SI; el objetivo fundamental es dar a conocer a los usuarios de la importancia que tienen las buenas prácticas de SI para el negocio y enseñar la forma como se logran las mismas, al igual que las consecuencias de no acatarlas.

5. Cumplimiento: este elemento es descrito como la etapa final del modelo, en cuanto es el mecanismo de revisión propuesto para observar que lo definido en cada elemento corresponda realmente a la intenciones de la Alta Gerencia y que el trabajo en SI este aportando a su materialización.

Modelo de Arquitectura de Seguridad por Jeimy Cano [5]: este es un modelo sustentado en la definición de tres elementos:

1. Estructuras: reconocimiento de los procesos fundamentales que precisan la esencia que componen la SI, entre estos se encuentran: la Información (reconocida como un activo), las Estrategias del Negocio (procesos que generan valor en la organización en su operación), los Fundamentos de la SI (basados en los principios de confidencialidad, integridad y disponibilidad como características de la información), y por último, la Administración de Riesgos (implementación de alguna metodología para descubrir vulnerabilidades y las estrategias para tratarlas y mitigar las amenazas).

2. Procesos: llevar a cabo la implementación de las buenas prácticas de seguridad; propuesta basada en la norma internacional ISO 27002.

3. Acuerdos: define la relevancia de establecer el canal de comunicación entre el área de SI y la Alta Gerencia. Entre los aspectos a tener en cuenta se encuentran: establecimiento de prioridades con la Alta Gerencia, competencias y habilidades requeridas en el área de SI, establecimiento y materialización del nivel de compromiso de la Alta Gerencia en los proyectos definidos en el Área de SI, la definición y operacionalización de los acuerdos de nivel de servicio, niveles de inversión en infraestructura de SI. Por último, se propone compartir y alinear la agenda interna de la Alta Gerencia, con la agenda interna del área de SI.

Modelo Arquitectura Empresarial [6]: los autores del modelo pertenecientes a IBM proponen dividirlo en cuatro dominios para hacerlo manejable (fundamentados en el hecho del continuo crecimiento y expansión del negocio):

1. Dominio Procesos: procedimientos, herramientas y reglas que apoyan las actividades del negocio.

2. Dominio Información y Conocimiento: trazabilidad en la trasformación de datos en información, hasta llegar al conocimiento en todos los niveles del negocio.

3. Dominio Infraestructura: la conformación de la plataforma tecnológica (Sw, Hw y servicios) y de comunicaciones

(redes e interconectividad) que apoya la ejecución de los procesos de negocio.

4. Dominio Organización: definición de roles y responsabilidades de los usuarios del negocio así como de las relaciones de los interesados.

Si bien este modelo no habla sobre SI, si es una perspectiva interesante que pretende esquematizar la administración y organización del negocio, y se convierte en un referente a tener en cuenta en el proceso de formalización de una ASI.

Arquitectura de Seguridad de Sistemas de Información por el SANS Institute [7]: SANS es una de las instituciones más prestigiosas a nivel mundial en el tema de SI, cuenta con un modelo denominado "Information Systems Security Architecture: A Novel Approach to Layered Protection" cuya autor es George Farah, quien con base en la definición de cinco fases muestra cómo se desarrolla una arquitectura de seguridad para un sistema de información mediante el establecimiento de algunas directrices:

1. *Fase 1. Realización de Evaluaciones de la Seguridad:* el fin de dicha fase es encontrar vulnerabilidades al sistema de información, independiente de que se hayan aplicado o no controles. Esta fase se realiza mediante cinco procesos: primero, se realizan entrevistas con los dueños de los procesos; el segundo es la realización de un inventario de activos; el tercero es la implementación de un Análisis del Impacto del Negocio (BIA - Bussiness Impact Analysis); el cuarto es la identificación de amenazas sobre el inventario de activos; el quinto es la implementación de un Análisis de Riesgos (AR - Analysis Risk).

2. *Fase 2. Formulación del Diseño de los Objetivos de la Arquitectura de Seguridad*: tiene su fundamento en los resultados de la Fase 1, de tal manera que se definan con un alto nivel de acierto los objetivos de la ASI, para ello se tiene en cuenta la definición de la arquitectura lógica y física del sistema de información.

3. *Fase 3. Construcción de Políticas y Procedimientos:* teniendo los resultados de las dos fases anteriores, se procede a concebir una política apropiada para el negocio a través de su conocimiento, esta debe ser definida en su estructura teniendo en cuenta el marco de la Política Corporativa, y en esencia debe guiar a los usuarios internos y externos sobre la forma en la cual se debe utilizar el sistema de información.

4. *Fase 4. Implementación del Diseño de los Objetivos de la Arquitectura de Seguridad:* habiendo seguido secuencia en el cumplimiento de las fases, se establecen los plazos, la financiación y los recursos necesarios para implementar la ASI.

5. *Fase 5: Integración de las prácticas de seguridad para mantener el estado de seguridad:* se propende por el mantenimiento de un entorno de trabajo seguro, basado en la aplicación exitosa de las fases del modelo; se logra estableciendo el personal idóneo y con las capacidades necesarias para la evaluación y actualización de la arquitectura de seguridad del sistema de información; como consecuencia se realiza:

   a. Gestión de cambios de los elementos o dispositivos que conforman la arquitectura lógica o física

   b. Gestión de Proyectos de TI, donde se clarifique la definición de los requisitos y etapas en la ejecución de proyectos que realimenten el estado de la arquitectura o su redefinición.

3. MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN - MASI

MASI es una propuesta estratégica para la administración de la SI con base en los modelos consultados, la investigación realizada en el tema y la experiencia de los autores. Por lo anterior, MASI es la propuesta que los autores someten a consideración, para la incorporación de la seguridad de la información en los procesos de negocio en las organizaciones.

MASI es una estructura lógica conformada por cinco elementos (ver figura 1): Negocio, Normativa, Gestión de la ASI, Acuerdos e Infraestructura de SI, cada uno de estos elementos es un proceso desarrollado mediante la asignación de actividades y tareas en SI pensadas y alineadas con los objetivos del negocio.

Figura 1. Elementos de MASI

Negocio

El objetivo de este elemento de MASI radica en la definición de estrategias de seguridad de la información alineadas con los objetivos organizacionales mediante el conocimiento detallado del negocio, para lograrlo se debe realizar un estudio y análisis de la siguiente documentación: la misión, la visión, el plan estratégico, las metas organizacionales, el cuadro de mando integral.

Procedimiento de para el desarrollo del elemento de Negocio

- Identificar los elementos de estrategia de negocio que se han definido en la organización, dentro de los cuales se pueden encontrar:
    - Balance Score Card
    - Misión
    - Visión
- Realizar un análisis de la información encontrada en la organización.
- Efectuar una reunión entre la Alta Gerencia y los encargados de la seguridad de la información para resolver inquietudes acerca de las estrategias del negocio.
- Identificar las metas del negocio.
- Definir las metas de la arquitectura.
- Realizar una tabla que permita visualizar en que puntos las metas de la arquitectura apoyan las metas del negocio.

Normativa

Se enfoca en la definición de las directrices regulatorias organizacionales y de seguridad de la información, por tal razón involucra desde la normativa corporativa hasta lo normativa de seguridad de la información que se defina.

La normativa corporativa puede estar enmarcada en: el código de ética, código de buen gobierno, reglamento interno de trabajo, normativa antifraude, acuerdos entre las partes. La normativa de seguridad podrá contener al menos: políticas, normativas y procedimientos. Desde la normativa corporativa se deben incluir elementos que refuercen y propendan por el cumplimiento de la normativa de seguridad de la información de tal forma que la seguridad sea entendida por los involucrados (empleados, contratistas, proveedores) como una directriz estratégica para el negocio.

Procedimiento para el desarrollo del elemento de normativa

- Identificar la normativa corporativa dentro de la cual se puede encontrar:
    - Código de ética
    - Código de buen gobierno
    - Reglamento interno de trabajo
    - Manual de responsabilidades
- Realizar un análisis de la normativa encontrada en la organización.
- Efectuar una reunión entre la Alta Gerencia y los encargados de la seguridad de la información para resolver inquietudes acerca de la normativa identificada
- Desarrollar la normativa de seguridad
- Modificar la normativa corporativa para que apoye el cumplimiento de la normativa de seguridad.
- Formalizar la normativa de seguridad y los cambios a la normativa corporativa.

Gestión de la Arquitectura de Seguridad

La Gestión de la Arquitectura se realiza teniendo en cuenta cinco elementos que son: Análisis de riesgo, monitorización, entrenamiento, actualización, mantenimiento. Estos elementos desarrollados en conjunto son la base para la adaptación de la metodología a las estrategias del negocio.

A continuación se describe cada elemento que conforma la Gestión de la ASI:

Análisis de riesgo: mediante el análisis de riesgo se obtiene el conocimiento referente a:

- Las amenazas y vulnerabilidades que atentan contra los activos de información.
- Los controles existentes para la mitigación de los riesgos.
- Probabilidad e impacto de la materialización de los riesgos.

Se debe tener en cuenta que el análisis de riesgo proporciona información referente a las necesidades de inversión de las organizaciones, enfocando los esfuerzos en la mitigación de los riesgos existentes a través de la definición de los planes de tratamiento.

Monitorización: la monitorización permite la evaluación de los componentes de la ASI, el fin es determinar si la ejecución de los mismos está apoyando o no las estrategias del negocio, para ello se basa en tres tipos de monitorización: monitorización técnica, monitorización personal y monitorización operacional.

- **Monitorización técnica:** la monitorización técnica está enfocada en la ejecución de procedimientos de gestión de vulnerabilidades.
- **Monitorización de personal:** se identifica el nivel de sensibilización de las personas involucradas (empleados, contratistas, proveedores) respecto a seguridad de la información.
- **Monitorización operacional:** hace referencia a la monitorización de los procesos; se requiere de la definición de un procedimiento de gestión de incidentes que permita la identificación de las fallas y la documentación de las soluciones, de tal forma que esto permita la mejora continua y el aprendizaje, procesos que realimentan la ASI.

Actualización: consiste en el proceso de mejoramiento de los elementos de la arquitectura, teniendo en cuenta los resultados de la monitorización y las posibles auditorias que se realicen al MASI.

Mantenimiento: el proceso de mantenimiento consiste en la implementación de las mejoras identificadas en la etapa de monitorización.

Entrenamiento: como resultado del análisis de riesgos, de la monitorización y de las auditorias, surgen diferentes vulnerabilidades que deben ser tratadas a través de la realización de campañas que estén enfocadas en cambios a nivel cultural. Para ello se puede tener en cuenta la realización de: propaganda, cursos de capacitación, concursos, entre otras actividades.

Procedimiento para el desarrollo del elemento de Gestión de la Arquitectura.

- Definir la metodología de gestión de riesgos.
- Realizar una reunión con la Alta Gerencia para la aprobación de la metodología.
- Aplicar la metodología de gestión de riesgos.
- Definir los procedimientos de gestión de incidentes y gestión de vulnerabilidades técnicas.
- Definir las actividades a desarrollar para la actualización de la documentación de la arquitectura.
- Realizar la priorización de la implementación de las oportunidades de mejora identificadas.
- Definir el proceso de gestión de la cultura de seguridad de la información

Infraestructura tecnológica de seguridad de la información
La definición de la infraestructura de seguridad se basa en el concepto de defensa en profundidad, tomando como referentes el Modelo de Defensa en Profundidad de Microsoft [8] y el Modelo SAFE de Cisco [9]. En el modelo SAFE de Cisco se define que la infraestructura de seguridad debe contemplar seis elementos que son: identificación, aseguramiento, segregación, resistencia, correlación y monitoreo, los cuales están enfocados en garantizar tanto la visibilidad como el control de la infraestructura; por otra parte, Microsoft define que la infraestructura de defensa en profundidad debe garantizar seguridad a nivel de: datos, aplicación, equipos de cómputo, red interna y perímetro.

Unificando los dos modelos, MASI establece los elementos de control definidos por el modelo SAFE de Cisco para garantizar la visibilidad, y el control deben ser definidos en cada uno de los niveles que define el modelo de defensa en profundidad de Microsoft.

Procedimiento para el desarrollo del elemento de infraestructura Tecnológica de seguridad.

- Identificar la plataforma tecnológica actual.
- Identificar los elementos de seguridad informática disponibles en la red.
- Evaluar las características de los elementos de seguridad frente los requerimientos de seguridad necesarios para establecer mecanismos de defensa en profundidad.
- Una vez realizado el análisis se procede a identificar las oportunidades de mejora.
- Realizar el diagrama de la infraestructura propuesta.

Acuerdos
Este elemento establece el medio o el canal de comunicación que garantice la integración del área de seguridad (proceso de seguridad) y la Alta Gerencia (expectativas del negocio), a fin de alinear los esfuerzos operacionales, tácticos y estratégicos del negocio. Este elemento se definió tomando como referencia el modelo del doctor Jeimy Cano referenciado en la etapa inicial del artículo.

Procedimiento para el desarrollo del elemento de acuerdos

- Definir un canal de comunicación entre los encargados de la seguridad de la información y la Alta Gerencia.
- Realizar actividades de seguimiento continuo de las actividades desarrolladas por el área de seguridad a fin de identificar oportunidades de mejora.
- Definir un procedimiento de revisión continuo entre la Alta Gerencia y los encargados de la seguridad de la información.

4. CONCLUSIONES

Para lograr el buen funcionamiento de MASI, es fundamental el conocimiento del negocio, debido a que de ello depende que todas las decisiones tomadas en la definición y funcionamiento del modelo estén alineadas con las estrategias de negocio.

La gestión de MASI permite el mejoramiento continuo de los diferentes elementos que lo componen, por tanto es indispensable que las actividades definidas en el mismo se ejecuten de forma organizada.

La Arquitectura de Seguridad de la información es un esquema administrativo interdisciplinario, por tal razón debe estar en constante realimentación, ello le permitirá evolucionar de la mano del crecimiento organizacional y su entorno de negocio, garantizando así una ASI acorde a las necesidades organizacionales.

Como en todo proceso de cambio organizacional, la implementación de MASI en las organizaciones depende en gran medida del apoyo de la Alta Gerencia.

5. TRABAJO FUTURO

Desarrollar la guía metodológica de implementación de cada uno de los elementos del modelo.

Definir una estrategia que permita mostrar a la Alta Gerencia el retorno de inversión referente a la implementación de MASI en las organizaciones.

Desarrollar el esquema que permita medir la eficacia de MASI.

Desarrollar la guía de implementación de cada uno de los elementos del modelo.

BIBLIIOGRAFÍA

[1] RAMIÓ, Jorge. Estado del Arte de la Formación Profesional en Seguridad Informática en Iberoamérica: Estrategias y Tendencias. En IV Jornada Nacional de Seguridad Bogotá – Colombia (24 – 25 de junio de 2004).

[2] HUERTAS, Juan. Validez de la seguridad informática en el tiempo: …un enfoque documental seguro en el tiempo… En IV Jornada Nacional de Seguridad Bogotá – Colombia (24 – 25 de junio de 2004).

[3] Gobierno de Seguridad de la Información, Capitulo 1, Curso de preparación CISM 2008.

[4] KILLMEYER, Jan. Information Security Architecture: An Integrated Approach to Security in the Organization. 2ª edición. Estados Unidos: Auerbach, 2006. 393p

[5] CANO, Jeimy. Arquitecturas de Seguridad Informática: Entre la administración y el gobierno de la Seguridad de la Información. En: SEMINARIO DE ACTUALIZACION EN SEGUIDAD INFORMATICA. (2008: Bucaramanga). Documento Modulo I Seminario de Actualización en Seguridad Informática. Bucaramanga: Facultad de Ingeniería Informática, 2008, p 28.

[6] IYER, Bala. GOTTLIEB, Richard. The Four-Domain Architecture: An approach to support enterprise architecture design. Julio 21 de 2004.Disponible en Web: http://www.research.ibm.com/journal/sj/433/iyer.html

[7] SysAdmin Audit, Networking and Security Institute. Information Systems Security Architecture: A Novel Approach to Layered Protection. Estados Unidos. SANS, 2004

[8]MORA, Cristian. "Implementación de Sistemas de Información Seguros" [San Pedro Sula, Honduras]: Julio de 2005. Disponible en Web: www.iimv.org/actividades2/05Tecnolog/Microsoft.ppt.

[9]Cisco. Cisco SAFE Solution Overview. Cisco, Estados Unidos. 2009.