INTRODUCCIÓN AL MODELO IBMS

Penagos, Iván.
ingivanpenagos@gmail.com
Universidad Piloto de Colombia

Abstract – ISACA developed a model for the implementation of a program of information security is based on a holistic vision of the company, this model despite being theoretical and have little time for disclosure , the structural components of integrated security information are described in a number of international standards on the subject. In the business model for information security, ISACA has integrated people, technology, processes and the organization itself to view the company as a set of relationships and dynamics that form and not just as the formal organization. This document resumes the model but the reader is invited to consider in detail the proposed model.

Resumen – ISACA desarrollo un modelo para la implementación de un programa de seguridad de la información que está basado en una concepción holística de la empresa, este modelo a pesar de ser teórico y de tener poco tiempo de divulgación, integra los componentes estructurales de la seguridad de la información que están descritos en varios de los estándares internacionales sobre el tema. En el modelo de negocio para la seguridad de la información, ISACA ha integrado a las personas, la tecnología, los procesos y en si mismo a la organización de la empresa vista como el conjunto de interrelaciones y dinámicas que la forman y no únicamente como el organigrama formal. Este documento resume el modelo pero se invita al lector a estudiar con detalle el modelo propuesto.

Índice de Términos – COBIT, CISM, ISACA, modelo IBMS, seguridad de la información.

I. INTRODUCCIÓN

A partir de los trabajo desarrollados por el Instituto para la Protección de Infraestructuras Críticas de Información (*Institute for Critical Information Infrastructure Protection*, ICIIP) en la Universidad de California del Sur (*University of Southern* California) (EE. UU.), ISACA desarrolló un modelo de negocio para la implementación de sistemas de gestión de seguridad de la información. De acuerdo con el anuncio realizado por ISACA el 6 de octubre de 2010, ISACA público un nuevo modelo de negocio comprensivo para la seguridad de la información. De acuerdo con el anuncio de ISACA [1]. Las motivaciones para el desarrollo del modelo de acuerdo con la publicación de ISACA fueron:

"El incumplimiento de la seguridad de información continua asolando a empresas en todo el mundo, a pesar de la utilización de la tecnología más avanzada. Resolver estos problemas requiere mucho más que sólo dispositivos y software. Por tal motivo, para brindar a los profesionales de la seguridad de información una guía completa que aborde los aspectos de personas, el proceso, la organización y la tecnología de la seguridad de información, ISACA emitió hoy los resultados de dos años de investigación y de revisión experta: el Modelo de Negocio para la Seguridad de Información (*BusinessModel for Information Security*, BMIS), disponible como un descargado gratuito en www.isaca.org/bmis. ISACA aclaró que el BMIS (*Business Model for Information Security*), "[puede] utilizarse en empresas de todos tamaños y es compatible con otros marcos de seguridad de información ya existentes. Es independiente de cualquier tecnología en particular y puede aplicarse en todas las industrias, países y sistemas legales y regulatorios. Además, abarca la privacidad y seguridad tradicional de información y proporciona vínculos a riesgos, seguridad física y cumplimiento." [2].

II. EL MODELO IBMS

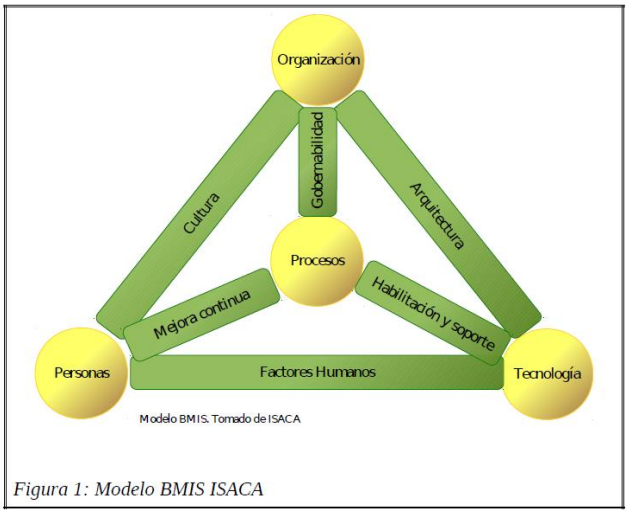

Figura 1: Modelo BMIS ISACA

1) El modelo BMIS de COBIT, conformado por 4 elementos: la organización, los procesos, las personas y la tecnología los cuales se interrelacionan, ca. 2010, Estados Unidos, Modelo de negocio comprensivo para seguridad de la información. Imagen tomado del sitio web de isaca: http://www.isaca.org/Knowledge-Center/PublishingImages/BMIStriangle.jpg

B. La organización

El primer elemento del modelo BMIS es la organización. La organización permite el cumplimiento de los objetivos misionales de la entidad y el logro de los objetivos de la seguridad de la información.

Para el modelo BMIS la organización es una "red de personas que interactúan usando procesos para canalizar su interacción". Dentro de este primer componente están los empleados y los asociados permanentes de la organización. El

modelo BMIS también considera como parte de la organización a las terceras partes, los vendedores, los consultores, los clientes y los interesados en los servicios o productos de la organización. Como se deduce de esta concepción, el modelo BMIS va más allá del simple organigrama de la entidad o la empresa, la organización es una estructura con relaciones internas y externas que establecen el marco para la efectividad operacional y el último caso el éxito y sostenibilidad de la empresa. El modelo BMIS no define como debe ser la estructura organizacional para la seguridad, pero si aclara que un modelo de implementación de un sistema de seguridad de la información debe considerar a la organización por muchos "modelos tradicionales enfocan la seguridad de la información únicamente en las personas, los procesos y la tecnología, pero no examinan la empresa como un todo" [3].

La organización formal (como parte del componente organización) reporta al responsable de la seguridad de la información acerca de las necesidades que se deben cumplir en términos de la calidad de la información y activos de información que se deben proteger. El conocimiento de las necesidades de la organización a nivel de seguridad de la información es esencial para el responsable de seguridad porque le indica el rumbo que debe seguir el sistema de la gestión de la seguridad de la información para lograr el objetivo más importante: soportar a la función misional enfocándose en los activos de información en lugar de buscar soluciones generales de seguridad.

C. Los procesos

Los procesos son el segundo componente del modelo BMIS. Formalmente dentro del modelo BMIS un proceso es "un conjunto de actividades reales y repetitivas para realizar cierta tarea. Los procesos toman entradas de una o más fuentes (incluyendo otros procesos), manipulan las entradas, utilizan los recursos de acuerdo con las políticas y producen una salida (incluidas salidas para otros procesos)". De acuerdo con las buenas prácticas de estándares como ISO 9001, los procesos deben tener una justificación clara para la naturaleza del negocio, tener responsables, roles y responsabilidades sobre su ejecución, los medios para su realización y las medidas de su desempeño. El proceso es un elemento único a la organización y proporciona los vínculos con todos los demás componentes del modelo BMIS (organización, las personas y la tecnología). Los procesos son elaborados por la organización para lograr sus estrategias, un proceso se conforma de actividades estructuradas que son creadas para lograr resultados particulares mediante tareas individuales o de grupo que se aplican de manera uniforme. Mediante los procesos se pueden explicar las prácticas y los procedimientos tal y como las personas y la organización quieren que se realicen [3].

Dentro de la organización, los procesos son el elemento fundamental que representa los requerimientos que establece la empresa para desarrollar, divulgar, educar y reforzar las prácticas y procedimientos en su operación diaria. A nivel de la seguridad de la información es necesario definir los procedimientos que soportaran el modelo.

D. Las Personas

Dentro del modelo BMIS las personas representan los recursos humanos de la organización, allí se encuentran los empleados, los contratistas, los vendedores y los proveedores de servicios. Es importante anotar que mientras la organización representa la estructura que soporta los procesos de la entidad, las personas son los componentes de esa estructura. Las principales personas dentro del modelo BMIS son los empleados de la empresa o aquellos que son asociados directos de la empresa. Sin embargo en situaciones en donde se utiliza el *outsourcing*, relaciones de múltiples proveedores o servicios gestionados de tecnología, existe un segundo círculo de personas que indirectamente trabajan para la organización. Este segundo círculo también requiere ser considerado dentro del desarrollo del sistema de gestión de seguridad de la información.

Las "Personas" no son únicamente unidades de una persona y no pueden ser estudiadas de manera aislada. Para estudiar como las personas afectan la seguridad y como la seguridad afecta a las personas es necesario estudiar la interacción de las personas como el resto de los elementos del modelo:
Procesos, Tecnología y la Organización. Las personas dentro de la organización tienen sus propias creencias, valores y comportamientos que surgen de su personalidad y experiencias. De igual forma la organización tiene sus creencias, valores y comportamientos y una forma en la que espera que se comporten las personas. Cuando se diseña el sistema de gestión de seguridad de la información es necesario considerar los comportamientos de las personas y de la organización.

E. La tecnología

La tecnología es el elemento más común de un sistema de gestión de seguridad de la información, comparativamente es el elemento de mayor complejidad y de mayor especialización dentro del modelo BMIS. La tecnología proporciona a los responsables de la seguridad muchas de las herramientas que se deben usar para el cumplimiento de la misión y la estrategia de la organización como un todo, incluida la protección de los parámetros fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad. Sin embargo la tecnología no lo es todo en cuanto a seguridad de la información, con frecuencia se considera que la inversión en tecnología resolverá los problemas de seguridad de la información y no siempre es así [3].

III. GOBERNALIDAD

La gobernabilidad de acuerdo con la definición de ISACA es: "Conjunto de responsabilidades y practicas ejecutadas por el comité directivo y ejecutivo con la meta de proveer direccionamiento estratégico, asegurar que se cumplen los objetivos, garantizar que los riesgos son gestionados apropiadamente y verificando que los recursos de la empresa son usados con responsabilidad"

Cualquier acción a nivel de gobernabilidad tiene que estar plenamente justificada particularmente todas aquellas que modifican procesos de la empresa. La gobernabilidad incluye pero no está limitada a:

- Políticas

- Estándares, guías y documentación normativa
- Reglas de responsabilidad
- Reglas para adjudicación y para priorizar la asignación de recursos
- Métricas
- Leyes

La gobernabilidad actúa como conector entre los elementos de organización y procesos y representa la acción de poner en práctica los procedimientos dentro del modelo BMIS. Esto significa gestionar los procesos mientras que se aplican las directrices del nivel directivo. Mientras que la organización y los procesos representan lo que se "debe hacer" y "como hacerlo" la gobernabilidad es un catalizador que hace que los dos elementos interactúen. Las leyes y regulaciones se representan a nivel de procesos mediante procedimientos e instrucciones. La gobernabilidad se ve afectada por otros dos elementos de interconexión del modelo que son: La cultura y la Arquitectura. Por ejemplo si el elemento tecnológico es inadecuado para resolver las necesidades de seguridad de la organización, la arquitectura sufrirá presiones que distorsionan el modelo obligando a cambios en las estrategias de gobernabilidad lo que conducirá a cambios en los procedimientos y las instrucciones lo que afectará directamente los procesos de la organización.
Todas las actividades de la gobernabilidad deben ser explicitas y deben ser parte del diseño y estrategia de la organización.

Algunos de los marcos de referencia que se usan para implementar la gobernabilidad incluyen:

• COBIT 4.1
• Principios de gobierno corporativo de la OECD
• Normas de la serie ISO 27000
• Buenas prácticas de ITIL
• El *framework* de gestión de riesgos corporativos de COSO
• El conjunto de controles de seguridad de NIST SP 800-53

Cultura

La cultura es el integrador dinámico que conecta a las personas y la organización. La cultura se puede definir como "patrón de comportamientos, creencias, suposiciones, actitudes y formas de hacer las cosas".

- La cultura organizacional se forma con el tiempo mediante el diseño de una estrategia organizacional y el comportamiento de las personas en su trabajo
- La cultura organizacional depende de la cultura individual la cual es variada y heterogénea.

El desarrollo de una cultura de la seguridad de la información no es una tarea fácil ni rápida, es un objetivo de largo plazo que debe ser considerado por cada persona dentro de la empresa. Las personas son el elemento consciente de la estrategia de seguridad de la información y en ese sentido todas las personas que forman la organización desde los niveles directivos y ejecutivos, los niveles operativos e inclusive las terceras partes que mantienen relación con la empresa tienen la habilidad de mejorar o debilitar la seguridad de la información. Si las personas se comportan teniendo en mente la seguridad de la información e incorporando las prácticas de la seguridad de la información en sus actividades diarias, existe mayor probabilidad de que los activos de información de la empresa estén protegidos adecuadamente.

Arquitectura

La arquitectura comunica la organización y la tecnología. Con frecuencia la arquitectura se equipara a la infraestructura cuando se habla de seguridad o tecnología, es importante aclarar que la arquitectura incluye mucho más que aspectos que únicamente la tecnología. En muchos aspectos la arquitectura es análoga a lo que representan los componentes de seguridad y salubridad de un edificio (accesos, diseños, sistemas de protección, sistemas de evacuación, áreas comunes, sistemas de soporte vital como agua, energía).
Para la norma ISO/IEC 42010:2007 (*Systems and software engineering — Architecture description* is an international standard for architecture descriptions of systems and software.) la arquitectura es "la organización fundamental de un sistema que comprende sus componentes, sus interrelaciones, su ambiente y los principios que gobiernan su diseño y evolución"

Existen diversas aproximaciones para el establecimiento de la arquitectura de seguridad. Si una arquitectura empresarial incluye los objetivos de seguridad de la organización inherentemente fija el entorno para la arquitectura de la seguridad, sin embargo separar los elementos de la arquitectura general no permite la integración lo que va en contravía del modelo BMIS. Mientras que existen varias tendencias a nivel de arquitectura empresarial, los más comunes son *The Open Group Architecture Framework* (TOGAF) y el *zachman enterprise* framework27 y su modelo derivado *herwood Applied Business Security Architecture (SABSA) security framework.* Para el caso del modelo BMIS se adoptó el modelo de zachman enterprise framework27 en tres elementos básicos:

• Contextual
• Conceptual
• Lógico

1. Componente Contexto
   Es el nivel más alto del modelo de zachman y define las relaciones de una estructura como su entorno. En términos de una construcción sería equivalente a un diagrama del edificio con sus vías de acceso, estacionamientos, zonas verdes, etc. La misma noción se aplica a la seguridad de la información la cual reside en un contexto organizacional, el contexto de arquitectura describe la relación con los demás componentes de la empresa, sus relaciones con las áreas financieras, de recursos humanos, legal, mercadeo y de operaciones.

Al nivel del componente de contexto, la arquitectura existe para garantizar que las políticas de seguridad cumplen con las leyes y regulaciones del país, la industria y los sectores específicos a los que pertenece la empresa, incluidas las expectativas de los clientes y los proveedores, en este nivel también se encontraran los estándares que se usan como buenas prácticas.

2. Componente Conceptual
   El componente conceptual garantiza que la tecnología (física y lógica) no solamente soportará sino que habilitará activamente los objetivos de la seguridad. En este nivel se encontrarán un conjunto de actividades que se interrelacionan operativamente y componentes de tecnología que trabajan para lograr los objetivos de seguridad. Siguiendo la analogía de una construcción, el componente conceptual mostraría la interrelación de sistemas dentro del edificio.

3. Componente lógico
   El componente lógico especifica detalladamente el diseño de los componentes de seguridad utilizando tecnología para garantizar que se logran los objetivos de seguridad definidos, ser resistente a ataques y soportar los posibles daños.

Habilitación y soporte

Bajo el término habilitación el modelo BMIS agrupa las funciones necesarias para el aprovisionamiento de servicios de tecnología para la empresa. Bajo el término soporte se agrupan las funciones necesarias para garantizar que los servicios de tecnología operan correctamente. En términos prácticos se puede decir que un sistema de gestión de servicios de tecnología bajo norma ISO 20000 o ITIL brinda el soporte necesario para la existencia de la habilitación y soporte.

La habilitación y soporte comunican a los procesos y la tecnología, la tecnología habilita la ejecución de los procesos y los procesos a su vez permiten la entrega y operación de la tecnología.

La habilitación y soporte es el catalizador que permite demostrar la necesidad de un balance correcto entre los procesos y la tecnología y los impactos que tiene la selección de la tecnología en los procesos del negocio.

La habilitación y soporte debe tener en cuenta los siguientes elementos para un correcto funcionamiento.

• Procesos balanceados y rápida adaptación a los cambios
• Apego a los propios estándares
• Uso de controles apropiados
• Fuerte enfoque en la seguridad
• Reconocimiento del cumplimiento de requerimientos

Dentro de la habilitación y soporte se debe reconocer que la tecnología se debe seleccionar, evaluar, implementar y controlar. Dentro de los mismos principios de la habilitación y soporte los procesos deben ser diseñados, desarrollados, implementados y utilizados. El principal problema de las organizaciones no es la ausencia de tecnología, muchas veces los procesos son insuficientes para la tecnología existente y en otras ocasiones la tecnología dentro de la organización es inadecuada para los procesos existentes. La tarea de la habilitación y soporte es balancear la tecnología y los procesos.

Mejoramiento continuo (lo emergente)

El mejoramiento continuo conecta los procesos y las personas para permitir que se logre un aprendizaje continuo de la seguridad de la información.

Los procesos de aprendizaje son críticos en la seguridad de la información ya que asisten en la comprensión de los requerimientos que dan forma efectiva a las estrategias de seguridad de la información que encajan en los comportamientos de la empresa como un todo. El mejoramiento continuo ayuda a la personalización, mejoramiento y difusión de los procedimientos y reglas de seguridad para llevar la seguridad de la información de la teoría a la práctica.

El modelo BMIS es claro al afirmar “(Lo) emergente, como tal, no siempre es signo de mejoramiento en términos de seguridad, en la medida en que nuevas formas espontáneas de hacer las cosas emergen dentro de la organización estas pueden ser positivas o negativas. Por ejemplo un comportamiento habitual que es considerado en las políticas y estándares puede evolucionar con el tiempo (para mejorar o deteriorar).

Factores humanos

“Los factores humanos conectan las personas y la tecnología. La relación entre personas y tecnología surge del hecho de que las debilidades en la seguridad pueden ocurrir debido a la forma como la gente usa la tecnología y como entienden la necesidad de apegarse a los conceptos de seguridad. De manera similar la tecnología es el elemento que puede mejorar notablemente la calidad del trabajo y la forma en que las personas cumplen sus tareas.

El modelo BMIS expone que para entender cómo el factor humano afecta a los demás componentes del modelo es necesario diagnosticar los problemas y deficiencias en la interacción humana y los sistemas de seguridad actuales, para llevar a cabo el diagnóstico de esta situación, BMIS, propone varios enfoques:

1. Diseño de equipos: Los cambios en la naturaleza física de los equipos y el trabajo de las personas (ejemplo uso de autenticación biométrica).
2. Diseño de tareas: Enfocarse más en los cambios en los procedimientos que en cambiar los dispositivos.

Esto puede implicar asignar parte o todo un trabajo a otros colaboradores o a componentes automatizados.

3. Diseño del medio ambiente: Implementar cambios como mejoramiento de iluminación, temperatura, reducir ruido en los entornos en donde se desarrollan las tareas.
4. Entrenar a las personas: preparar a los empleados para afrontar los retos que encontraran en sus ambientes de trabajo enseñándoles y practicando las destrezas necesarias para las tareas físicas e intelectuales.
5. Selección de personal: Esta técnica reconoce que los individuos son diferentes en sus dimensiones físicas y mentales que son relevantes para el desarrollo apropiado de sus funciones. Ya que el desempeño se puede mejorar mediante la selección de los mejores operadores que poseen las mejores destrezas para el trabajo particular, esta selección optimizará la ejecución de los procesos.

IV. CONCLUSIONES

Como lo explica ISACA "Mientras que el modelo (BMIS) integra todos los componentes y actividades dentro de un programa de seguridad (de la información), la aplicación práctica que seguir una serie de fases. Esta implementación en fases asegurará que las medidas y soluciones de seguridad existentes serán completamente adoptadas dentro del modelo y que la inversión se protegerá".

La utilización del modelo no implica la reinvención del negocio, las medidas existentes dentro de la organización son positivas y deben ser acogidas dentro del modelo de la seguridad de la información.

A la fecha BMIS es un concepto nuevo que no ha sido ampliamente divulgado, sin embargo ISACA está planificando y desarrollando casos de estudio reales que puedan ser publicados para que sirvan como apoyo a la implementación del modelo.

Para poder iniciar una implementación de un programa de seguridad basado en BMIS es necesario:
Fuerte integración del programa actual de seguridad de la información.
Análisis de los controles actuales de seguridad de la información.
Alinear las normas, procedimientos y estándares en uso con el modelo.
Identificar con claridad las fortalezas y debilidades existentes en la seguridad de la información.

REFERENCIAS

[1] http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Issues-Comprehensive-Business-Model-for-Information-Security-Spanish.aspx

[2] http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Issues-Comprehensive-Business-Model-for-Information-Security-Spanish.aspx

[3] Modelo BMIS, traducción Ing. Juan Carlos Alarcón