Modelo BMIS (Business Model for Information Security) de ISACA

Hernandez Divantoque, Claudia Alejandra
claus1056@gmail.com
Universidad Piloto de Colombia

Resumen—En este documento se presenta el modelo BMIS desarrollado por ISACA, se explica cada una de las partes que lo conforman y como se comportan todas en conjunto. Adicionalmente indica como se refleja cada componente al momento de implementar o diseñar un programa de seguridad de la información para el negocio

Abstract— In this paper the model developed by ISACA BMIS is presented, explained each of the parties thereto and behave like all together. Additionally indicate how each component when implementing or designing an security program information for the business is reflected.

Índice de Términos— Gestión, modelo, negocio, Seguridad de la información.

I. Introducción

ÉSTE DOCUMENTO BRINDA UNA INTRODUCCIÓN AL MODELO BMIS PARA LA SEGURIDAD DE LA INFORMACIÓN ELABORADO POR ISACA. ISACA es una empresa líder en el mundo proveedor de conocimientos, certificaciones y educación de la seguridad que sirven de garantía en sistemas de información, esta entidad desarrollo trabajos durante dos años en la Universidad de California Sur, creando un modelo de negocio que permite la implementación de sistemas de gestión de seguridad de la información, *Business Model for Information Security* o más conocido como BMIS. Este modelo está basado en la concepción de que las partes de la organización en conjunto se comportan diferente a la suma de de cada uno de ellas, es decir, permite implementar la seguridad de la información teniendo en cuenta todos y cada uno de los componentes de la organización. Es un modelo en el que ISACA "*ha integrado las personas, la tecnología, los procesos y en sí 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*" [1]. Según ISACA esta modelo puede ser empleado en empresas de cualquier tamaño y es compatible con cualquier otro marco de seguridad de la información que ya existe. Cada uno de los cuatro componentes nombrados será descrito de tal forma que pueda entenderse y saber en qué parte de la organización está representado. Este es un modelo muy completo ya que en su estructura no deja escapar ninguna de las partes de la organización y representa su interacción de tal forma que al querer implementar un sistema para la seguridad información no queden espacios que permitan ser víctima de ataques por parte de hackers o de personas que quieran infiltrar el objetivo del negocio.

II. Descripción de las partes del modelo

A. Elementos

El modelo está compuesto por cuatro elementos: la organización, los procesos, la tecnología y las personas, estos elementos interactúan entres si por medio de unas interconexiones, a se relacionan cada uno de los elementos.

1) La Organización es el primer elemento del modelo, en este se permite lograr los objetivos del negocio que a su vez brinda la información que permite alcanzar los objetivos de la seguridad de la información. Este elemento reúne todas las personas que integran el negocio tanto personal de trabajo como directivos los cuales se pueden identificar como organización informal y formal respectivamente, las terceras partes como los vendedores, los consultores, los clientes e interesado en los productos o servicios de la organización. La organización forma es quien debe

informar al responsable de la seguridad de la información cuales son las necesidades que se deben cumplir en cuanto a calidad de la información y que activos de información se deben proteger, este elemento le ayuda a los encargados de la seguridad a tomar las decisiones y el camino más eficiente para implantar un buen sistema de seguridad de tal forma que vaya de la mano con los objetivos misionales que tenga la organización.

2) Los Procesos: Este elemento es *"un conjunto de actividades reales y repetitivas para realizar ciertas tareas*" [2]. En los procesos hay unas entradas de varias fuentes que utilizan recursos y dan unas salidas, para que estos tengan algún beneficio en el negocio deben: estar alineados con las políticas y satisfacer los requerimientos del mismo, deben estar documentados, para asegurar eficacia y eficiencia deben ser monitoreados o revisados periódicamente y sin duda deben ser comunicados al personal de forma adecuada. Con base en lo anterior se puede deducir que en este elemento se ve la relación entre los otros 3 elementos del modelo. Los procesos deben ser creados por las directivas de tal forma que puedan llevar a la organización a cumplir su estrategia de negocio, así mismo en seguridad de la información se deben tener claros los procesos que soportan el objetivo de la organización.

3) La Tecnología: Es una herramienta en los procesos que sirven para la misión y estrategia de la organización, está conformada por herramientas aplicaciones y la infraestructura, es el elemento que más relación tiene con la gestión de la seguridad de la información.

4) Las Personas: Este representa el recurso humano dentro del modelo en los negocios, las personas son un conjunto dentro de la organización, estas no deben tratarse de manera aislada son un conjunto ya que interactúan entre si. Para diseño del sistema de gestión de seguridad de la información se necesita entender las creencias, valores y comportamientos tanto de las personas como de la misma organización.

Los cuatro elementos están ubicados de tal forma que interactúen entre sí (figura1), con base en esto "*Si una de las partes del modelo es modificada, no es considerada o no es gestionada adecuadamente, es posible que el equilibrio del modelo esté en riesgo*."[3],

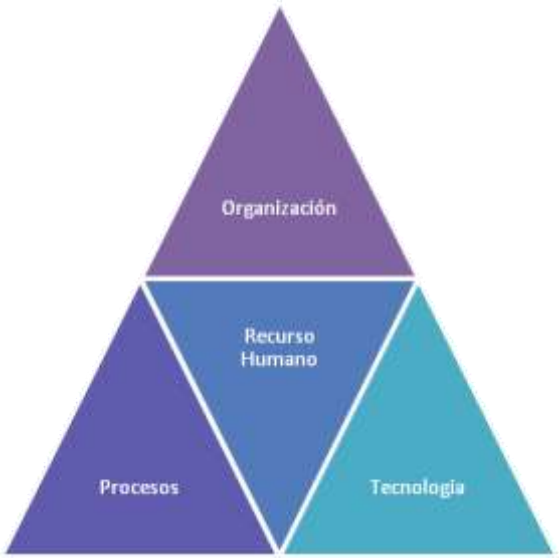

Fig1. Elementos del modelo BMIS. [4]

B. Conexiones

Los cuatro elementos del modelo se relacionan por medio de interconexiones dinámicas, las seis interconexiones son:

1) Gobernabilidad: Esta conexión establece la relación entre la organización y lo procesos, es la forma en que los alto directivos y ejecutivos, estipulan responsabilidades y actividades encaminadas a asegurar y a cumplir los objetivos del negocio, es decir, el gobierno establece límites sobre los que opera el negocio. Herramientas como políticas, estándares, guías, documentación normativa, reglas, métricas y leyes apoyan esta interconexión. Adicionalmente se apoya en marcos de referencia como: COBIT 4.1, Normas de la serie ISO 27000, ITIL y el framework de gestión de riesgo corporativo COSO, que son usados para implementar gobernabilidad. "*El gobierno se encarga de asegurar que se determinen y definan los objetivos, de garantizar que los riesgos se gestionen adecuadamente y de verificar que los recursos de la empresa se utilicen con responsabilidad*" [3], esto indica que definitivamente esta conexión es la principal, pues relaciona lo que deber hacerse en el negocio y como se debe hacer.

2) Cultura: Conecta a las personas y la organización, para el modelo es un "*patrón de comportamiento, creencias, suposiciones, actitudes*

y formas de hacer las cosas"[5], debido a que esto es propio de cada persona que conforma la organización, se hace más difícil la tarea de generar una cultura generalizada de seguridad de la información, se debe tener presente que se generan dos tipos de cultura organizacional: la que se da con el tiempo dependiendo de la estrategia organizacional y el comportamiento de las personas en sus funciones laborales y la que depende de la cultura individual que la hace variada y diferente. Es necesario integrar a todas y cada una de las personas al proceso de seguridad de tal forma que colaboren y lo hagan propio para así proteger al máximo los activos de información que posea la empresa.

3) Arquitectura: Esta conexión se relaciona con la organización y la tecnología, este intenta revisar la relación de los componentes de tal forma que puedan aplicarse o relacionarse de la mejor forma con la tecnología. Existen unos modelos de arquitectura empresarial tales como: TOGAT (The Open Group Architecture Framework, zachman Enterprise framework 27 y SABSA. El modelo BMIS de ISACA se basa en la arquitectura propuesta por zachman la cual se apoya en tres elementos, el contextual: esto es el entorno donde se encuentra la organización por lo tanto se deben tener en cuenta las leyes y regulaciones de un país, la industria, las expectativas de los clientes y proveedores, de tal forma que las políticas de seguridad se encajen con cada uno de ellos. El conceptual: muestra la relación operativa de los componentes y la tecnología. El lógico: siendo redundantes, esta es la lógica para el diseño de componentes de seguridad y así garantizar la resistencia a ataques o para soportar daños.

	Why	How	What	Who	Where	When
Contextual	Goal List	Process List	Material List	Organisational Unit & Role List	Geographical Locations List	Event List
Conceptual	Goal Relationship	Process Model	Entity Relationship Model	Organisational Unit & Role Relationship Model	Locations Model	Event Model
Logical	Rules Diagram	Process Diagram	Data Model Diagram	Role Relationship Diagram	Locations Diagram	Event Diagram
Physical	Rules Specification	Process Function Specification	Data Entity Specification	Role Specification	Location Specification	Event Specification
Detailed	Rules Details	Process Details	Data Details	Role Details	Location Details	Event Details

Fig 2. Modelo de Arquitectura de Zachman [6]

4) Habilitación y Soporte: Esta es la conexión entre tecnología y procesos de tal forma que la tecnología habilita el proceso de la organización y los procesos soportan el uso de la tecnología. Elementos como: procesos balanceados, rápida adaptación a cambios, uso de controles apropiados y un enfoque fuerte en la seguridad, permiten un funcionamiento correcto en la habilitación y el soporte. La habilitación y el soporte permiten seleccionar, evaluar, implementar y controlar en cuanto a tecnología y para los procesos permite diseñar, desarrollar, implementar y ser utilizados.

5) Mejoramiento Continuo: La seguridad de la información implica un aprendizaje continuo de las personas y de los procesos, esto indica que los elementos que tienen importancia en esta conexión son los procesos y las personas. Esta conexión también puede implicar nuevas oportunidades de negocio, nuevo procesos y procedimientos que impliquen seguridad de la información o a ayudan personalizar, ampliar y mejorar las normas que ya existen, esto puede darse de forma negativa o positiva, el primero debido a problemas encontrados para los cuales no hay explicación alguna y el segundo para el continuo aprendizaje.

6) Factores Humanos: Esta es la relación entre las personas y la tecnología, esta relación se da debido a que los mayores ataques a la tecnología se dan por las personas, debido a la forma como la utilizan, pero a su vez la tecnología apoya de la mejor forma el trabajo de las personas. El enfoque que propone el modelo BMIS para esta relación son: Diseño de equipos, diseño de tareas, diseño del medio ambiente, entrenamiento de las personas y selección del personal.

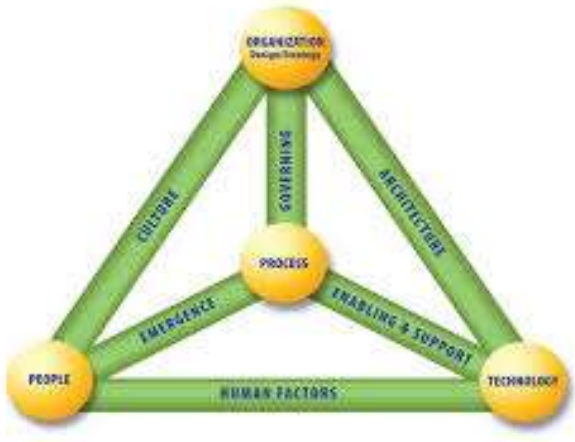

Fig 3. Modelo BMIS de ISACA. [7]

Este modelo es la presentación formal de una política de seguridad que debe identificar reglas y prácticas que regulan como un sistema maneja, protege y se distribuye la información. Además este modelo sirve para proveer un sistema que ayude a comprender diferentes conceptos como proveer una representación de seguridad clara.

Es importante que al momento de formular las políticas de seguridad de la información se efectué un análisis de riesgos informáticos, reunirse con los departamentos comunicar a todo los elementos involucrados sobre el desarrollo de las política incluyendo los beneficios y riesgos relacionados con sus elementos de seguridad.

Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en proteger la información o monitorear periódicamente los procedimientos y operaciones de de forma tal que ante cambios puedan actualizarse oportunamente, detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Este modelo de seguridad protege, administra de modo que los elementos relacionados puedan tener un acceso seguro a los servicios y los datos que dispongan. Pero hay razones que impiden la aplicación de las políticas de seguridad informática se debe ser capaz de convencer de la necesidad y beneficios de buenas políticas de seguridad informáticas, otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los especialistas en seguridad que llevan a no comprender exactamente los motivos de las inversiones.

Esta situación ha llevado a exponerse a graves problemas de seguridad y riesgos innecesarios que en muchos casos comprometen información sensible y por ende su imagen ante esta situación los encargados de la seguridad deben confirmar que los elementos entiendan los asuntos importantes de la seguridad y sus alcances.

Si se quiere que las políticas de seguridad sean aceptadas deben integrarse a las estrategias de su misión y visión con el propósito de que los que toman las decisiones reconozcan su importancia e incidencia en las proyecciones y utilidades.

Es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad ellas deben responder a intereses y necesidades organizacionales basadas en la visión que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos.

III. Posibles pasos para trabajar en BMIS

El negocio se debe analizar en términos de ubicación geográfica, una vez se hayan identificado factores del negocio como: países y regiones, se pueden asignar a los programas de seguridad las leyes y reglamentos y luego aplicarlas al BMIS.

En el modelo BMIS los gerentes de seguridad deben recopilar poco a poco toda la información existente de las soluciones de herramientas y procesos, debido a la naturaleza del modelo se permiten adiciones y cambios posteriores en las listas, luego no tienen que ser tan exhaustivas.

Una vez que se integren las soluciones existentes, formaran un patrón que verá reflejado en cada uno de los elementos del BMIS.

El BMIS está diseñado de tal forma que posee una flexibilidad propia para adaptarse a las normas que se estén usando en la seguridad de la información. Se debe hace una análisis en profundidad de las fortalezas, debilidades, las causas y el efecto

IV. Conclusiones

Como se ve en la figura el modelo es un sistema que se relaciona entre sí, si alguno de los elementos falta podría haber un desequilibrio que puede permitir huecos sensibles a ataques.

Este modelo es una buena guía para implementar seguridad de la información, ya que permite observar de forma muy completa el negocio y así poder determinar cuál es el mejor sistema de seguridad de la información. Impleméntelo de la mano de cada una de las partes del negocio, ubíquelas en cada uno de los elementos y

demuéstreles como es pieza fundamental en el desarrollo del objetivo y como con la ayuda de la seguridad de la información pueden conseguirla de la mejor forma.

El modelo BMIS es una buena herramienta para integrar a los ejecutivos y alta gerencia del negocio en la implementación del sistema de gestión de la seguridad, confirmándoles como cada uno de los elementos es fundamental en el negocio y como la seguridad le ayuda en su objetivo estratégico, en la misión o en la visión que tenga del negocio, brindándole herramientas para proteger sus activos físico, humanos, tecnológicos, etc.

REFERENCIAS

[1] Introducción al Modelo BMIS, Resumen elaborado por Ing Juan Carlos Alarcon S. PMP, CISM, 2010

[2] http://www.slideshare.net/RodolfoCarrion/el-modelo-de-negocios-para-la-seguridad-de-la-informacin

[3] Modelo de Negocios para la Seguridad de la Informacion. http://www.bscconsultores.cl/descargas/D.3%20Modelo%20de%20Negocios%20para%20la%20Seguridad%20de%20la%20Informacin.pdf

[4] Propio del Autor

[5] Isaca, *Manual de Preparación al Examen CISM 2012*, Certifiec Information Security Manager.

[5] http://es.wikipedia.org/wiki/Marco_de_Trabajo_Zachman

[6] Modelo BMIS de ISACA, http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

[7] ISO/IEC 42010, http://es.wikipedia.org/wiki/ISO/IEC/IEEE_42010

[8] Fondo de Tecnologías de la Información y las Comunicaciones, *Modelo de Seguridad de la Información para la estrategia de Gobierno en Línea 2.0*, Diciembre de 2011