Universidad de Buenos Aires
Facultad de Ciencias Económicas
Biblioteca "Alfredo L. Palacios"

Gestión estratégica de la Seguridad de la información. Análisis del Modelo de Negocios para la Seguridad de la información (BMIS)

Lina, Valeria

2012

Cita APA: Lina, V. (2012). Gestión estratégica de la Seguridad de la información. Análisis del Modelo de Negocios para la Seguridad de la información (BMIS) Buenos Aires : Universidad de Buenos Aires. Facultad de Ciencias Económicas. Escuela de Estudios de Posgrado

Este documento forma parte de la colección de tesis de posgrado de la Biblioteca Central "Alfredo L. Palacios". Su utilización debe ser acompañada por la cita bibliográfica con reconocimiento de la fuente.
Fuente: Biblioteca Digital de la Facultad de Ciencias Económicas - Universidad de Buenos Aires

Tesis Posgrado 001502/0135

cod. 1502/0135

Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Gestión estratégica de la Seguridad de la Información

Análisis del Modelo de Negocios para la Seguridad de la Información (BMIS)

Autor: Lic. Valeria Lina

Tutor del Trabajo Final: Lic. Raúl Saroka

Fecha de presentación: 12 de Agosto de 2012

Cohorte 2011

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Valeria Lina.

DNI 29.317.805

Resumen [1] [2]

La vertiginosa evolución de la tecnología y los sistemas de información ocasiona que sea común observar en una gran cantidad de organizaciones que las estrategias, las políticas, los procesos y los estándares de tecnología y seguridad, son desarrollados sin tener en cuenta como el resto de los factores de la organización pueden impactar en la efectividad del programa que se desea implementar.

ISACA ha desarrollado el modelo BMIS (Business Model for Information Security), basado en la teoría de sistemas, que aborda la interrelación entre las personas, el proceso, la organización y la tecnología. Lo realiza adoptando un enfoque orientado a la organización, centrándose en las personas y los procesos, además de la tecnología.

El BMIS trata de aportar a la estrategia un análisis sistémico del contexto considerando, para el desarrollo de sistema de gestión de seguridad de la información, el impacto del resto de los factores que influyen en el ambiente organizacional.

Para el desarrollo del presente trabajo se ha reunido material bibliográfico que constituye la base teórica del mismo, detallando tanto el modelo como su metodología de implementación práctica. Posteriormente se ha elaborado una conclusión desde la visión del área de Seguridad de la Información sobre el modelo desarrollado y la complejidad de aplicación del mismo.

Palabras clave

Tecnología. Procesos. Cultura. Organización. Estrategia. Seguridad de la información. Análisis de Riesgo. Responsabilidad. Modelo. Ambiente. Teoría de Sistemas. Personas. Enfoque Sistémico.

Tabla de contenido

1. Introducción [1] [2]

La tecnología ha avanzado, y continúa avanzando a un ritmo vertiginoso. Las compañías adoptan nuevas soluciones para resolver necesidades que surgen de los nuevos desafíos a los que se enfrentan, incorporan recursos humanos y procesos que satisfacen necesidades del negocio. Sin embargo, en este contexto, no podemos afirmar que la seguridad de la información esté avanzando de la mano de dichos cambios, acompañando la estrategia de la organización.

La Seguridad de la Información aún es vista como responsabilidad de la Gerencia de Sistemas, y se la relaciona directamente con la implementación de nuevas tecnologías (software o hardware) de seguridad, y no como un proceso transversal a la compañía que relaciona personas, procesos, la organización y tecnología, y que debe alinearse con los objetivos organizacionales.

El presente trabajo se centra en el modelo BMIS (Modelo de Negocios para la Seguridad de la Información) desarrollado por ISACA analizando los cuatro elementos que presenta (personas, proceso, organización y tecnología) y las interrelaciones existentes entre los mismos, evaluando el impacto de cada uno de ellos en la estrategia de seguridad de la información. El modelo busca ofrecer una herramienta que relacione, a través del análisis sistémico, los proyectos de seguridad con la estrategia del negocio.

Se pretende demostrar, mediante la explicación del modelo, que una efectiva estrategia de seguridad de la información, no es sólo una cuestión técnica, sino que se basa también en comprender, las relaciones propias entre la organización, los procesos, los individuos y la tecnología.

2. Objetivos

El objetivo de este trabajo es analizar el modelo presentado por ISACA desarrollando los cuatro factores que presenta y la interrelación entre los mismos, evaluando el impacto de cada uno de ellos en la estrategia de seguridad de la información. Asimismo, explicar la metodología para llevar el modelo teórico a la práctica de seguridad de una organización.

3. El Modelo de Negocios para la Seguridad de la Información (BMIS) [1]

El objetivo principal de la publicación del BMIS es otorgar a los especialistas en seguridad de la información, un enfoque práctico que los acerque al negocio; aportar una visión sobre los procesos dentro de la organización que impactan o son impactados por la seguridad de la información.

La visión del modelo se separa del tradicional pensamiento lineal para abordar un enfoque sistémico de la administración de la seguridad.

El concepto de enfoque sistémico aplicado a la seguridad de la información, dio lugar al desarrollo de un Marco de Trabajo para la Gestión de la Seguridad, también llamado SSM[1], esta visión analiza la seguridad de la información desde la perspectiva organizacional, incluye las personas, procesos, tecnología y organización, así como también los socios, proveedores, clientes, es decir, el entorno. De esta forma se pretende involucrar a la alta dirección de la organización para lograr el compromiso de la misma con la seguridad de la información y no solo buscar una inversión en tecnología. [3]

Sobre este enfoque sistémico del "SSM" es sobre el cual se ha construido el BMIS para brindar un modelo bien definido y estructurado para su uso práctico.

3.1. El Modelo [1]

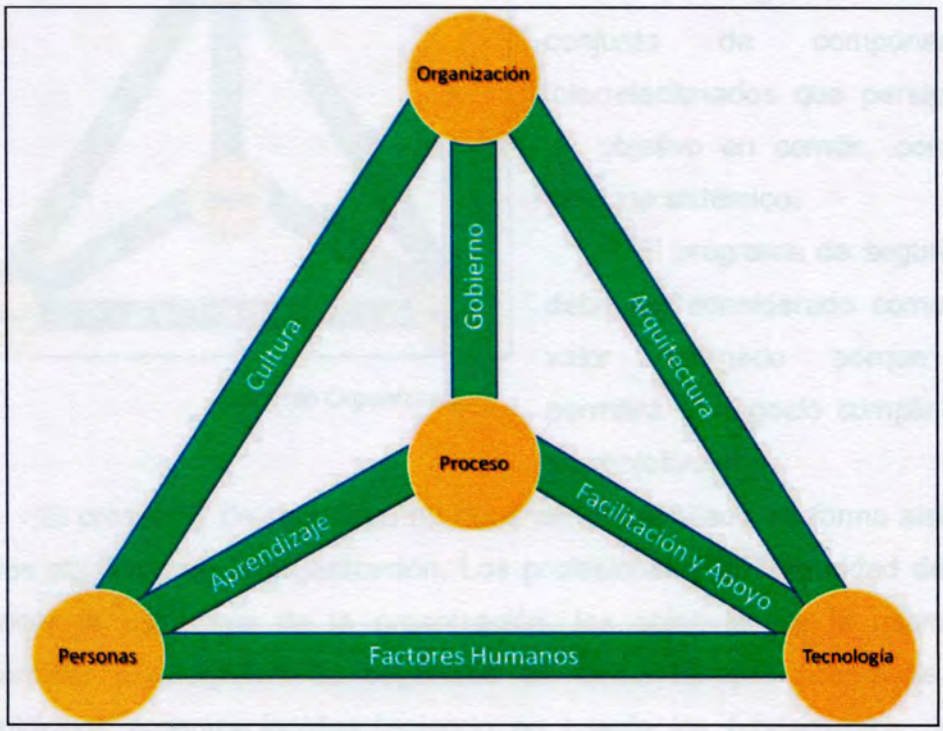
El BMIS es un modelo tridimensional compuesto por cuatro elementos:

- Organización *(Organisation)*
- Proceso *(Process)*
- Personas *(People)*
- Tecnología *(Technology)*

y seis relaciones dinámicas (RDs) que unen dichos elementos:

[1] System Security Management.

- Cultura *(Culture)*
- Aprendizaje *(Emergence)*
- Gobierno *(Governing)*
- Facilitación y apoyo *(Enabling & Support)*
- Arquitectura *(Architecture)*
- Factores Humanos *(Human Factors)*



Visión general del Modelo de Negocios para la Seguridad de la Información [2]

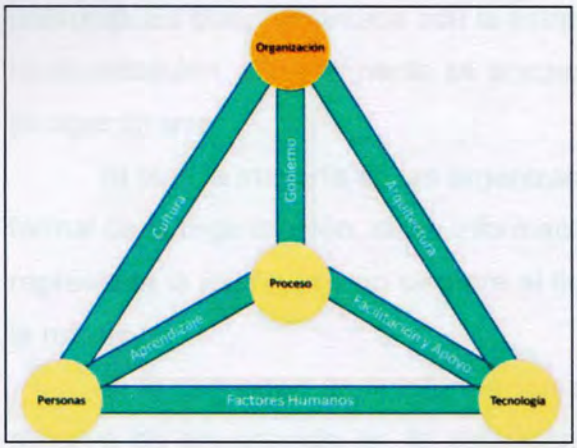
Es importante comprender que las RDs representan la relación entre elementos, si uno de ellos cambia, el resto también sufrirá cambios. Asimismo cabe destacar que no solo afectará a los dos extremos de la interconexión, sino también puede tener efectos sobre el resto de los elementos existentes en el modelo.

[2] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. *The Business Model for Information Security.* USA : ISACA, 2010, pp 13

3.2. Los elementos [1]

3.2.1. Organización [1]

"Red de personas interactuando, utilizando procesos para canalizar dicha interacción" [3]



Elemento Organización [4]

La Organización es vista desde el "management" como un conjunto de componentes interrelacionados que persiguen un objetivo en común, con un enfoque sistémico.

El programa de seguridad debe ser considerado como un valor agregado porque le permitirá al negocio cumplir con sus objetivos.

El programa de seguridad no debe ser desarrollado en forma aislada de los objetivos de la organización. Los profesionales de seguridad deben conocer la estrategia de la organización, los objetivos de la misma y desarrollar el programa de seguridad de forma tal que acompañe las definiciones organizacionales teniendo en cuenta los fundamentos de la seguridad: confidencialidad, disponibilidad e integridad.

---

[3] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. *The Business Model for Information Security.* USA : ISACA, 2010, pp 14

[4] Ídem

La organización formal [1] [3]

Se denomina organización formal a la estructura definida por lo niveles más altos de la institución; incluye organigramas, políticas documentadas y directivas que serán los lineamientos que deberá seguir el personal. Es complementada con la estrategia definida por sus directivos de la organización. Generalmente se encuentra representada gráficamente por el organigrama.

Si bien la mayoría de las organizaciones cuenta con la representación formal de la organización, dicha información es limitada en cuanto a que solo representa la jerarquía y no siempre el flujo de información con el que opera la misma.

Si la seguridad de la información se encuentra considerada como un objetivo de importancia en la definición de la estrategia, la estructura lo debería reflejar en términos de diseño y gente. Asimismo, los niveles que continúan en la jerarquía (gerencias, departamentos, unidades, etc.) serán más eficientes en trabajar para cumplir esa meta.

La meta principal del programa de seguridad es acompañar al negocio en alcanzar sus objetivos. Conocer dichos objetivos, permitirá que el programa se enfoque en los activos de información críticos en lugar de medidas generales de protección.

La organización informal [3]

Paralelamente a la organización "oficial", existe una organización informal donde se opera sin políticas escritas. Si bien los organigramas definen las relaciones jerárquicas y responsabilidades, no siempre es la forma real en la que la información recorre la organización.

El impacto de la organización en la seguridad [1]

Si la seguridad de la información es considerada en el diseño de la estrategia como una meta importante, se logrará instalar la problemática de seguridad en toda la organización.

Reconocer a la seguridad como parte de la estrategia organizacional permitirá lograr la aceptación a través de toda la organización (formal e informal), permitiendo a la "gerencia" de seguridad mayor espacio para el desarrollo del programa de seguridad.

El elemento "organización" se conecta al elemento "personas" a través de la "cultura", al elemento "procesos" a través del "gobierno" y al elemento "tecnología" a través de la "arquitectura".

Los cambios que se realicen en cualquiera de los elementos mencionados o en sus conexiones, impactarán en el resto. Es fundamental entender que cuando se realicen cambios, se reflejará el impacto en todo el sistema.

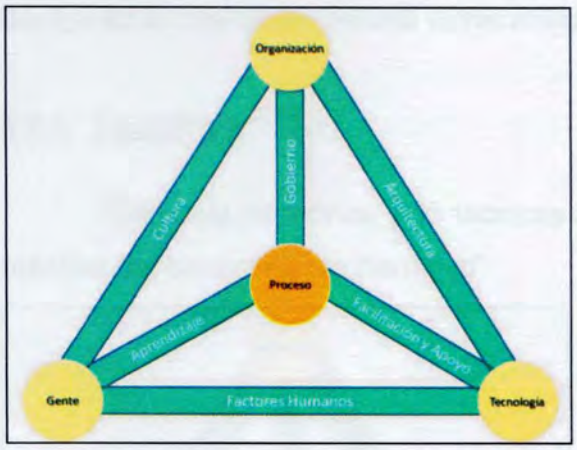
El elemento "Organización" es el que mostrará al negocio el valor del programa de seguridad y tendrá una gran influencia en el éxito del mismo.

3.2.2. Procesos [1] [3] [4]

"Conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes (incluyendo otros procesos) manipula las entradas, y genera salidas. Los procesos tienen razones claras de negocio para existir, propietarios responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño"[5]

[5] Institute, IT Governance. Control Objectives for Information and related Technology. Illinois : s.n., 2007, pp 192

Se considera que un proceso se encuentra maduro cuando está bien definido, administrado y medible, y optimizado.



Elemento Proceso [6]

El elemento proceso se conecta al resto de los elementos a través de tres interconexiones dinámicas: Gobierno, Aprendizaje, Facilitación y Apoyo.

Enfoque sistémico

Trabajar con un enfoque sistémico permite identificar todas las debilidades y luego poder buscar los puntos comunes que los atraviesan; de esa forma obtendremos la causa raíz de las fallas en el proceso que estamos analizando y no solo solucionaremos los síntomas que hemos identificado individualmente.

Dentro del modelo BMIS, el elemento Proceso consiste de diversos procesos individuales que dan soporte a distintos aspectos de la seguridad, esto permite a los ejecutivos de seguridad manejar entornos complejos y dinámicos.

Los procesos deben contar con una componente de retroalimentación, que le permitirá al proceso "aprender", es decir, que colaborará con la mejora y el ajuste del proceso en función a los cambios en el negocio.

Se considera demora[7] el período de tiempo en el que proceso se encuentra operando, recibimos la retroalimentación y la misma es integrada al proceso.

---

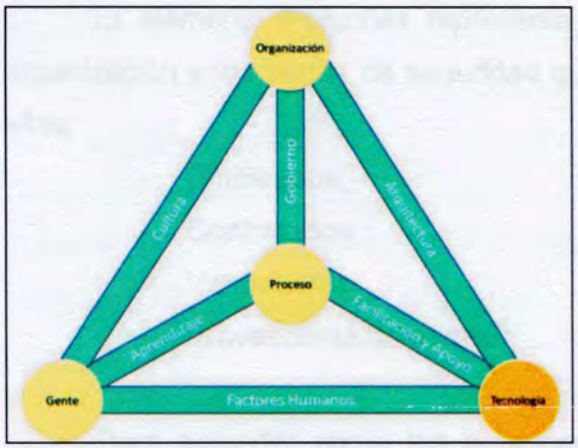
[6] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 18

[7] *Delay*

Esta demora en ajustar el proceso, desde el punto de vista de seguridad, implica un aumento del riesgo porque represente una ventana de tiempo en la cual tenemos una vulnerabilidad que no estamos considerando.

3.2.3. Tecnología [1] [3]

"Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico"



Elemento Tecnología [9]

La tecnología incluye toda aplicación técnica o conocimiento utilizado en la organización y abarca mucha más que solo IT[8].

Dentro del modelo BMIS, el elemento Tecnología, se refiere a toda implementación técnica o conocimiento utilizado que pueda tener un impacto en la seguridad de la información.

El elemento Tecnología, posee la capacidad de identificar y mitigar vulnerabilidades de seguridad a través de la implementación de controles basados en tecnología.

La selección de la tecnología a implementar debe ser realizada en base a la utilidad, eficiencia y productividad de toda la organización. Luego se debe entrenar al personal que la utilizará y programar monitoreos para validar que se encuentre funcionando debidamente.

Si la tecnología es implementada e ignorada, puede dar una falsa sensación de seguridad a la organización. Existen muchos casos de

---

[8] *Information Technology = Tecnología de la Información*

[9] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 20

organizaciones que han implementado una gran cantidad de tecnología y han sido vulneradas.

Algunos ejemplos:

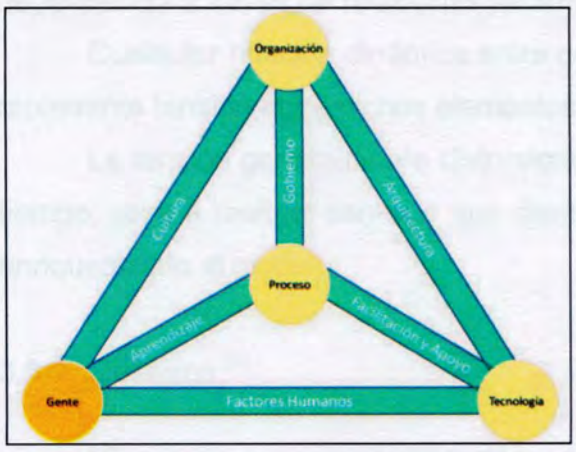
- Intrusión en la compañía RSA y robo de información [6]
- Nuevo ataque a Sony con 93.000 cuentas comprometidas [7]

3.2.4. Personas [1]

El elemento Personas representa a los recursos humanos en una organización y los temas de seguridad que se encuentran relacionados con ellos:

- Empleados
- Contratados
- Vendedores
- Proveedores de servicio

Para entender como las personas afectan y son afectadas por la seguridad de la información, es necesario estudiar la interacción de las personas con el resto de los elementos del modelo a través de las relaciones dinámicas (enfoque sistémico).



Elemento Personas [10]

Las Personas dentro de una organización tienen sus propias creencias, valores y conductas que son resultado de sus personalidades y experiencias. El marco corporativo afecta y es afectado por estos atributos dado que define sus propias creencias, valores y comportamientos y el estándar

[10] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 23

que se espera que cumplan (cultura organizacional).

Es crítico para los profesionales de seguridad trabajar en forma conjunta con las áreas de Recursos Humanos y Legales para tratar temas relacionados con las estrategias de reclutamiento, puesto de trabajo y finalización de la relación laboral, dado que esto influirá en la seguridad de la información desde su relación con las personas.

Las Personas tienen influencia en la seguridad de la información a través de su interacción con el ambiente organizacional. Son ellos, a través de su comportamiento, quienes determinan la aceptación de un control. Un control implementado pero no aceptado por la gente puede llevar a que la organización se encuentre ante un mayor nivel de riesgo porque la implementación causó una falsa sensación de seguridad debido a que el control se encuentra implementado pero no es cumplido.

3.3. Las Relaciones Dinámicas (RDs) [1] [3]

Los elementos que compone el BMIS no existen en forma individual, es decir, en la práctica podemos ver que un cambio en alguno de los elementos tiene influencia en el resto. El modelo BMIS expresa esta dependencia a través de relaciones dinámicas (RDs) entre los elementos.

Cualquier relación dinámica entre dos elementos es flexible y también representa tensión entre dichos elementos.

La tensión generalmente distorsiona el modelo, y en el transcurso del tiempo, lleva a realizar cambios que disminuyen la tensión entre elementos enriqueciendo el modelo.

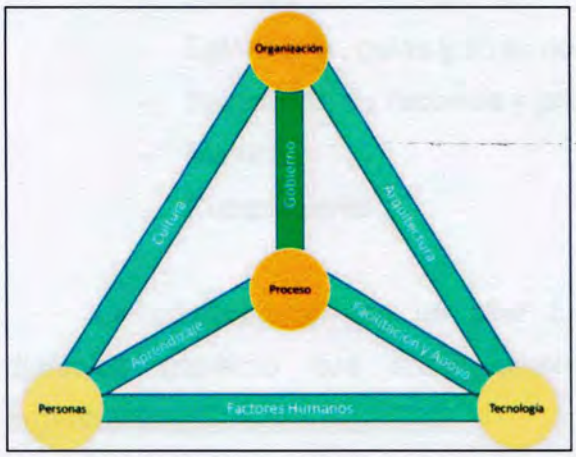
3.3.1. Gobierno [1]

"Conjunto de responsabilidades y prácticas ejercidas por la Dirección y los ejecutivos con el objetivo de proveer la dirección estratégica, asegurar que los objetivos sean alcanzados, determinar que los riesgos son

gestionados apropiadamente y verificar que los recursos de la organización son utilizados responsablemente"[11]

Dentro del modelo BMIS, la relación dinámica Gobierno, traduce lo enunciado al nivel del elemento Organización, fomentando el cumplimiento de metas, estableciendo límites y controles.

Siendo la conexión entre los elementos Organización y Proceso, representa la acción de poner lo definido en el gobierno en práctica dentro del BMIS.



Relación Dinámica Gobierno[12]

La retroalimentación que recibe la relación dinámica Gobierno, proviene de las relaciones dinámicas Cultura y Arquitectura, las cuales actúan en el diseño y la estrategia. Por ejemplo, si el elemento Tecnología no es adecuado para las necesidades de seguridad de la organización, la relación dinámica Arquitectura, generará una tensión que distorsionará el modelo provocando cambio en el diseño que a su vez modificará la estrategia que afectará a la relación dinámica Gobierno. Cambios en dicha relación dinámica modificará los procedimientos y prácticas en el elemento Proceso.

Los procesos deben encontrarse alineados con los objetivos de la organización. Gobernar implica establecer el enfoque en que debe ser alcanzado en los distintos procesos organizacionales (elemento Proceso).

[11] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 25

[12] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 26

Enfoque [1] [3]

Gobernar implica todas las actividades tácticas necesarias para cumplir con la estrategia de la organización.

Toda acción que sea tomada debe tener una justificación clara y racional y deben ser relacionado con la estrategia y los objetivos organizacionales.

La relación dinámica Gobierno, incluye:

- Políticas
- Estándares, guías y otras normas
- Asignación de recursos y prioridades
- Métricas
- Cumplimiento[13]

La comunicación es un pilar fundamental dentro de la relación dinámica gobierno que debe encontrarse intrínseca en la cultura organizacional.

La gestión de riesgos requiere que la estrategia y responsabilidad por la seguridad se encuentre en manos de los directivos y altos ejecutivos de la organización. En muchas organizaciones la seguridad es relacionada como un tema de TI y no como un requerimiento estratégico.

3.3.2. Cultura [1] [3] [8]

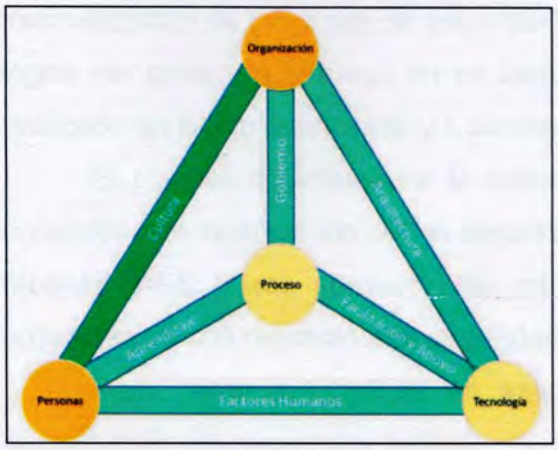
"Patrón de conductas, creencias, suposiciones, actitudes y maneras de hacer las cosas"[14]

El modelo BMIS considera dos clases de cultura, la organizacional y la individual.

[13] *Compliance*

[14] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 27

La cultura organizacional es formada por la estrategia, el diseño de la organización y el comportamiento de las personas en el trabajo. La cultura individual, puede ser diversa y heterogénea. Ambas son tomadas en cuenta cuando dentro del modelo se analiza la relación dinámica Cultura y su influencia en la seguridad.



Relación Dinámica Cultura [15]

Para poder mejorar el programa de seguridad, es necesario entender y examinar la cultura existente dentro de la organización. Incorporar la seguridad a la cultura es un trabajo arduo, la cultura individual es compleja de ser modificada, sin embargo es posible enfocarnos en cambiar la cultura organizacional y este debe ser el inicio de formar la cultura en seguridad.

Incorporar la seguridad de la información a la cultura

Los directivos de seguridad deben comprender que lo que es mejor para la organización es importante para la "cultura de seguridad", por ejemplo, si el personal es leal a la organización, probablemente gestionen la información de forma más segura.

La cultura es uno de los factores más importantes en el éxito o fracaso de una organización, es por ello que los profesionales de seguridad deben esforzarse en crear una "cultura de seguridad" que no solo se enfoque en la importancia de la seguridad de la información, sino que incluya las prácticas de seguridad de la información en las actividades diarias de la organización. Logrando esto aumentamos la posibilidad de mantener los activos de información protegidos.

[15] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 28

Una de los objetivos principales del programa de seguridad debe ser modificar la cultura organizacional de forma tal que, mediante la internalización de prácticas de seguridad, la misma deje de ser reactiva para lograr ser proactiva, y luego en un segundo estadío de madurez, logre ser realizada en forma intencional y a conciencia.

El objetivo de influenciar la cultura es que la organización tome una conducta más relacionada con la seguridad de la información, lo fortaleza del modelo BMIS puede aprovecharse para mejorar la actitud general de la organización con respecto a la seguridad.

Para crear una cultura de seguridad se deben internalizar en la organización los siguientes puntos:

- Campañas de concientización: Pueden consistir en actividades generales de concientización sobre la seguridad de la información y sesiones de capacitación continua sobre temáticas de seguridad.
- Grupos multifuncionales: Comités compuestos por integrantes de diversas áreas que trabajen en conjunto para mejorar la actitud frente a la seguridad de la organización.
- Compromiso de la alta gerencia: Es fundamental el soporte de la alta gerencia para que puedan transmitir el apoyo en los temas de seguridad a través de toda la organización.

El cambio cultural no es algo que se logre de inmediato solo con un programa de concientización y capacitación, mediante al apoyo de los ejecutivos o modificando los procedimientos para incorporar prácticas seguras pero son estas medidas las que colaborarán al cambio organizacional a través del tiempo.

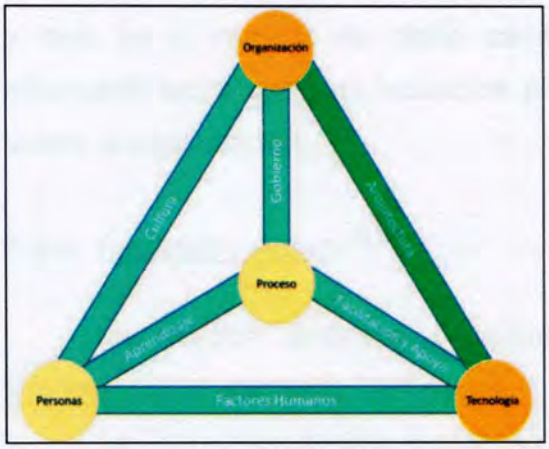
La "cultura de seguridad" madura a medida que las prácticas de seguridad se ven embebidas en las actividades diarias, de esta forma, las conductas, valores y actitudes se van realmente modificando y las mismas pasarán a una nueva generación como normas y reglas ya establecidas. Es en ese momento cuando podemos realmente percibir que los cambios han efectivamente impactado en la cultura organizacional.

3.3.3. Arquitectura [1] [3]

"Descripción del diseño de los componentes de un sistema, o de un elemento del sistema (por ejemplo tecnología), las relaciones entre ellos, y la manera en la cual apoyan a los objetivos del negocio"[16]

Dentro del modelo BMIS la Arquitectura conecta los elementos Organización y Tecnología.

Cuando hablamos de seguridad o TI, es usual utilizar el término arquitectura cuando nos referimos a infraestructura (hardware, software, etc.). Luego esta infraestructura es complementada con los procesos, las políticas y procedimientos definidos en la organización. Es importante tener en cuenta que el término arquitectura abarca mucho más que solo la infraestructura.



Relación Dinámica Arquitectura [17]

La arquitectura comienza como un concepto, un conjunto de objetivos que deben ser cumplidos, luego evoluciona hacia un modelo y posteriormente a la preparación de proyectos y herramientas que se utilizarán para transformar ese modelo en un producto terminado. Finalmente, se obtiene la construcción en sí misma, la salida de todas las fases atravesadas anteriormente.

La interacción entre los elementos Organización y Tecnología, relacionados a través de la Arquitectura, es bidireccional, es decir que cada uno puede y será influenciado por el otro. Por ejemplo, la tecnología aplicada en la organización, no es una elección aislada llevada a cabo por la

[16] Laree Kiely, Ph.D. and Terry Benzel. Systemic Security Management. s.l. : Institute for Critical Information Infrastructure, 2003, pp 43

[17] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 32

Gerencia de TI, debe tener si razón de ser en los requerimientos del negocio y los objetivos organizacionales que acompañan la estrategia.

El elemento Tecnología debe retroalimentar e influir a la Organización en forma de mediciones y métricas (costos, capacidad, disponibilidad, complejidad, requerimientos de espacio y energía, consideraciones en la arquitectura, etc.).

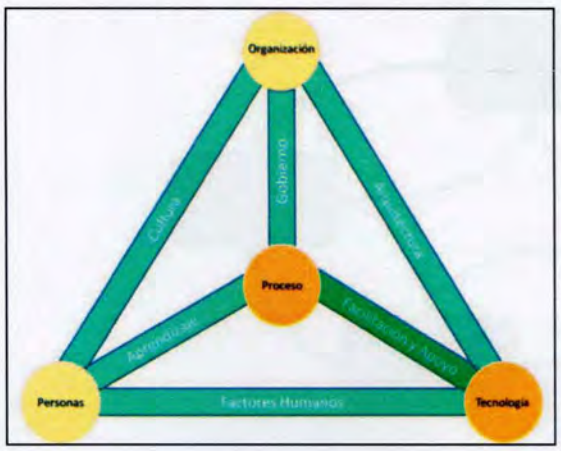
La Arquitectura debe trasmitir cualquier información relacionada con cambios tecnológicos al elemento Organización, en términos de qué cambio y cuál es el impacto de dicho cambio en el negocio. Asimismo debe informarle sobre cambios indirectos producidos por el contexto en el que existe la organización.

3.3.4. Facilidad y Apoyo [1] [3]

La relación dinámica Facilidad y Apoyo, relaciona el elemento Proceso con el elemento Tecnología.

La Tecnología facilita el proceso, y el proceso acompaña o "ayuda" el desarrollo y la operación e tecnología.

Esta relación dinámica muestra por un lado un proceso equilibrado para apoyar a la tecnología en la organización, y por el otro muestra el efecto de la tecnología en los procesos de negocio.



Relación Dinámica Facilidad y Apoyo[18]

La Tecnología debe ser seleccionada, evaluada, implementada y controlada. Los Procesos deben ser diseñados, desarrollados, implementados y utilizados. El problema con el que suelen encontrarse las organizaciones no es la falta de

[18] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 36

tecnología ni de procesos, el problema reside en la sinergia entre ambos. Las organizaciones deben trabajar para que los procesos sean acompañados por tecnología, y el uso de la tecnología apoyada por los procesos.

La relación Proceso – Tecnología, suele presentar tensión debido a la diferencia en cómo se deben llevar los procesos a cabo, suelen encontrarse opuestos en vez de trabajando en forma sinérgica.

La pregunta que surge de esta relación es si el proceso está dando lugar o facilitando la tecnología, o si la tecnología está dando soporte al proceso.

La mayoría de las organizaciones falla en enfocarse más en la tecnología en si misma, que en entender que proceso de negocio la tecnología acompañará. Enfocarse solo en la tecnología sin considerar los procesos que deben soportarla es un riesgo debido a que no es sostenible en el tiempo y no se encuentra conectada con las personas, la cultura y el resto de los procesos organizacionales.

En función a esto, el BMIS propone un proceso cíclico de selección de tecnología que permite, a diferencia de un enfoque lineal, volver hacia los pasos anteriores para realizar ajustes en caso de ser necesario.

Ciclo de selección de tecnología [19]

[19] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 37

Ningún paso se encuentra totalmente completo, dado que todos interactúan y pueden ser modificados a los largo del ciclo.

Los procesos son formas de alcanzar objetivos, sin los objetivos los procesos no son medibles y no serían utilizados. La Tecnología no tiene razón de ser si no le permite a la organización alcanzar sus objetivos en implementar su estrategia. Por lo tanto, se puede observar una dependencia entre los elementos Proceso y Tecnología que dificulta tratarlos en forma separada.

Los componentes clave de la relación dinámica Facilidad y Apoyo son:

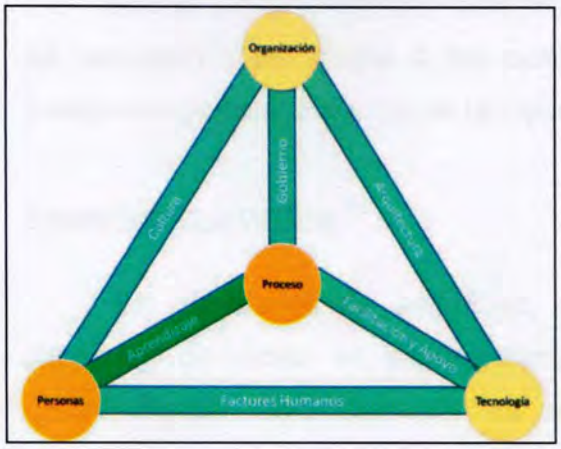
- Objetivos de Negocio: IT es un facilitador del negocio que colabora con la reducción de costos y mejoras en la productividad.
- Requerimientos del Negocio: Los requerimientos del negocio son el conjunto de requerimientos que el sistema debe cumplir satisfactoriamente.
- Arquitectura de la organización y marco de trabajo de los procesos: Los planes y metas de tecnología deben encontrarse alineados con los planes y metas del a organización.
- Grupos de trabajo multifuncionales: Contar con grupos de trabajo multifuncionales que colaboren con el entendimiento del negocio y desarrollando la arquitectura empresarial.

3.3.5. Aprendizaje, Mejora Continua, Evolución[20] [1] [3]

Dentro del BMIS, la traducción de "Emergence", puede ser asemejado a los conceptos de emergente, aprendizaje, mejora continua, evolución. Significa nuevas oportunidades para el negocio, nuevos comportamientos, nuevos procesos y otros elementos de seguridad; como los subsistemas entre las personas y los procesos evolucionan. Dentro del trabajo lo

[20] Emergence

denominaremos Aprendizaje abarcando los tres conceptos antes mencionados.



Relación Dinámica Aprendizaje [21]

La forma en la que el elemento Personas interactúa con los procesos se encuentra siempre caracterizado por la relación Aprendizaje, lo cual la transforma en una conexión clave en el modelo. Es un área de ambigüedad y evolución, que si se gestiona en forma correcta, puede mejorar la habilidad con la que cuente la organización para ajustarse a los cambios, sobrevivir un evento imprevisto e innovar.

Dado que los procesos los ejecutan seres humanos, podemos observar que la ejecución de un procesos dentro de una organización varía a través del tiempo y cada vez que es ejecutado. Por lo tanto para poder entender el impacto de esto en la seguridad de la información debemos dividirlo en lo que indica el procedimiento escrito, la ejecución de las tareas basados en la reglas establecidas por la política de seguridad y la ejecución que realiza la persona que lleva a cabo el proceso, que no se encuentra definido ni en el procedimiento ni en la política.

Debido al factor azaroso que se encuentra intrínseco debido a que el proceso es llevado a cabo por un ser humano, y no podemos predecir que piensa o como actuará, es que cobran mayor importancia las relaciones dinámicas Factores Humanos y Cultura.

El concepto de "emergence" puede ser positivo o negativo. Puede ser tomado como un proceso de aprendizaje para entender y mejorar la seguridad de la información, o puede referirse al aumento de incidentes de

[21] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 42

seguridad y la falta de alineación entre la seguridad de la información y los objetivos del negocio.

Por lo tanto, la relación dinámica Aprendizaje introduce un elemento de evolución y se adapta a los cambios inesperados o imprevistos que pueden surgir en el día a día de la organización.

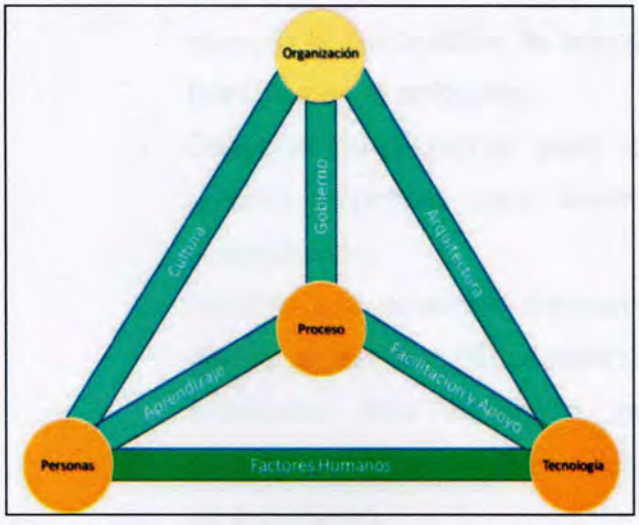
Pensamiento proactivo [3]

En cuestiones de seguridad, hoy es un requisito contar con la capacidad de pensar en forma proactiva, adelantándonos a lo que puede pasar. Pensar continuamente de qué forma pueden atacar nuestra organización y estar preparados para las distintas situaciones.

Teniendo como objetivo la seguridad de la organización, debemos analizar y conocer todos los elementos y relaciones dinámicas para poder estar preparados y desarrollar medidas proactivas en vez de reaccionar ante un incidente.

3.3.6. Factores Humanos [1] [3]

La relación dinámica Factores Humanos conecta los elementos Personas y Tecnología. Principalmente estudia como los humanos interactúan con la tecnología y el desarrollo de herramientas que facilitan cumplir con determinados objetivos.



Relación Dinámica Factores Humanos [22]

Esta relación "Personas – Tecnología" es necesaria debido a que

[22] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 43

muchas de las debilidades de seguridad que se detectan se deben a la forma en que las personas hacen uso de la tecnología, y al nivel de concientización, entendimiento y adherencia a las buenas prácticas recomendadas de seguridad que se haya logrado en la organización.

La Tecnología como elemento, tiene la capacidad para mejorar la calidad de trabajo y la forma en la cual los empleados realizan día a día sus tareas.

La tensión en la relación dinámica se percibe cuando existen problemas o deficiencias en la interacción "humano - sistema" de un sistema de seguridad existente. Para diagnosticar e identificar el problema y poder distender la tensión que se produce entre los elementos, se pueden evaluar los siguientes aspectos de mejora en la organización:

- Cambiar el diseño del equipamiento físico con el cual los recursos humanos se encuentran trabajando (cambios en el equipo).
- Enfocarse mas en modificar (automatizar o reasignar) lo que el operador realiza más que cambiar el dispositivo que utiliza (cambios en la tarea).
- Implementar mejoras en factores que influyen en el ambiente donde el operador está desarrollando la tarea, como por ejemplo la iluminación, la temperatura, el nivel de ruido, etc. (cambios en el ambiente).
- Capacitar al personal para que se encuentre lo mejor preparado posible para llevar a cabo la tarea asignada (capacitación).
- Realizar una selección exhaustiva del personal que cumplirá con la tarea. Se debe seleccionar aquel individuo que se encuentre mas calificado para el trabajo y reforzar determinadas habilidades en los equipos de trabajo (selección de individuos).

Es fundamental que la tecnología implementada por el área de seguridad considere la aceptación del usuario en su análisis. Si se detecta que la tecnología a implementada para proteger los activos de información

de la organización comienza a entorpecer la productividad o interrumpir la operatoria diaria, no se puede considerar ni eficiente ni efectiva. Por lo tanto es clave considerar la aceptación del usuario cuando se implementan controles.

Tanto la relación dinámica factores humanos como la cultura son las conexiones que dan forma al comportamiento del usuario, por lo tanto ambos aspectos deben ser tenidos en cuenta.

El gran riesgo de la implementación de tecnología con fines de seguridad en una implementación es la generación de una falsa sensación de seguridad en la organización, es decir, que si bien la tecnología se puede encontrar adecuadamente implementada (desde el punto de vista técnico), el personal siempre puede de alguna forma esquivar los controles de seguridad y esto pone en riesgo a la organización que simplemente descansa en la tecnología implementada olvidando que debe considerar la interrelación de todos los factores para que la implementación sea exitosa y cumpla su objetivo.

Cuando se confía ciegamente en la tecnología sin entenderla, hasta las debilidades más obvias pueden ser pasados por alto. Esto puede ocurrir en todos los niveles de la organización:

- Los directivos depositan su confianza en la tecnología y las soluciones técnicas para proveer seguridad en la infraestructura.
- Los gerentes confían en la existencia de controles basados en las políticas de seguridad para asegurarse que no existen debilidades.
- El resto del personal considera que no representa una debilidad de seguridad porque de eso se encarga otra persona y mientras sigan los procedimientos tal cual se encuentran escritos no existe riesgo.

Los puntos a tener en cuenta por esta relación dinámica Factores Humanos son:

- Que no se comprendan los requerimientos de seguridad, o peor aún, que se falle en entender la razón de la existencia los mismos.
- Que los conceptos de riesgo de negocio y el posible impacto en la seguridad no sean considerados dentro de los análisis.
- Qué se falle en conocer e implementar los controles disponibles en el sistema que apoyan la seguridad de la información.
- Que se cometan errores humanos debidos a poca memoria o falta de atención en los detalles
- La existencia de factores externos que influyen a los recursos humanos tales como soborno, corrupción y problemas sociales.
- La tendencia natural de la gente a utilizar los recursos tecnológicos que le provee la organización para objetivos personales.

Es importante comprender que esta relación es la más crítica en la gestión de la seguridad y es siempre la parte más débil.

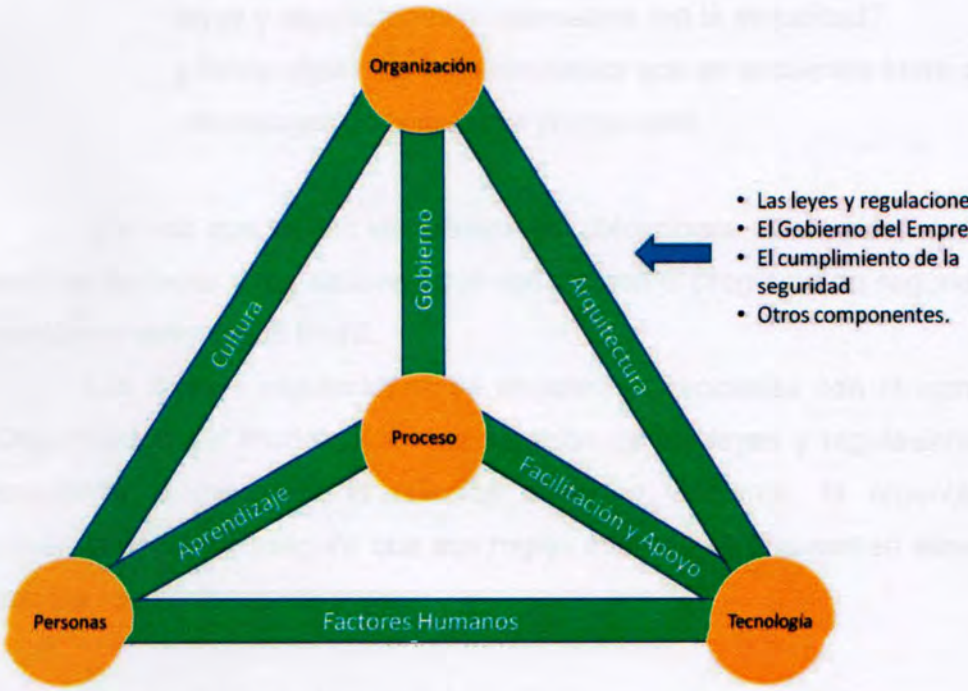
Lograr entender los factores humanos y a relación con los elementos personas y tecnología requieren lograr analizar los detalles, implementar todos los controles y restricciones que tengamos disponibles a través de los sistemas y sobre todo establecer un proceso continuo de capacitación y concientización en toda la organización.

4. Uso práctico del BMIS [1]

4.1. Analizar el programa de seguridad existente

Como un primer paso para comenzar a implementar el modelo BMIS dentro de la organización es analizar el programa de seguridad existente y las soluciones que ya se encuentran implementadas. En la mayoría de las organizaciones, cualquiera sea su estadío de madurez con respecto a seguridad, existe algún tipo de programa de seguridad, tal vez en forma de políticas y reglas, o de soluciones técnicas que se encuentran implementadas.

Existen diversas formar de realizar el análisis del programa de seguridad y cualquiera de ellas puede ser utilizado, el BMIS propone evaluar en esta fase[23]:



- Las leyes y regulaciones
- El Gobierno de la organización

[23] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 48

- El cumplimiento de la seguridad
- Otros componentes.

Para lograr un modelo óptimo de seguridad de la información para la organización, es necesario tener en cuenta los factores tanto positivos como negativos sobre el sistema de seguridad de la información.

Leyes y Regulaciones

El negocio debe ser analizado en función a su ubicación, la relación con sus clientes y proveedores, y la cadena de abastecimiento en general. Las preguntas a realizarse en este punto son:

- ¿Desde donde se administra la organización? ¿Cuáles son las ubicaciones de mayor relevancia?
- ¿Existen ubicaciones de alto riesgo, medido en términos de leyes y regulaciones relacionadas con la seguridad?
- ¿Existe algún cliente o proveedor que se encuentra fuera de las ubicaciones consideradas principales?

Una vez que se han identificado las ubicaciones principales, se puede asociar las leyes y regulaciones que aplican con el programa de seguridad, y posteriormente con el BMIS.

Las leyes y regulaciones se encuentran asociadas con el elemento Organización del modelo. La interpretación de las leyes y regulaciones se encuentra a cargo de la relación dinámica Gobierno, la organización continuamente se asegura que sus reglas internas se encuentren alineadas con las regulaciones externas.

El Gobierno de la Organización

La organización adopta reglas externas y las incluye dentro de la estrategia organizacional. El programa de seguridad, como parte de la organización, debe adoptar esas regulaciones dado que fue definido dentro de la estrategia de la organización.

El gobierno de la institución se encuentra asociado con el elemento Organización del modelo y es implementado a través de la relación dinámica Gobierno.

Cumplimiento de la Seguridad

Adicionalmente a los requerimientos de seguridad impuestos por leyes y regulaciones del país o ubicación donde se encuentra la organización, ésta debe asegurar un nivel general de cumplimiento con la seguridad. Esto se refiere a aquellos requerimientos relacionados con seguridad que surgen del negocio, por ejemplo requerimientos de auditorías contables externas, la mayoría de las organizaciones descansan en los controles de TI para procesos relativos a las finanzas.

Los requerimientos de cumplimiento se encuentran relacionados a los elementos de Tecnología y Organización dentro del modelo BMIS. En algunos casos también puede ser necesario asociarlo al elemento Personas cuando la conducta de los recursos humanos también se encuentra dentro de los puntos de cumplimiento.

La internalización y reconocimiento de los requerimientos de cumplimiento en el alto nivel de la organización, es una parte de la relación dinámica gobierno, alineado con las leyes, regulaciones y gobierno de le organización. Los requerimientos que se cumplimentan en niveles más bajos tales como gestión de datos, son parte de la relación dinámica Arquitectura. Los requerimientos que se encuentren asociados con el personal de la organización deben ser reflejados en la relación dinámica Cultura, por ejemplo cuando se pretende que presten conformidad con el código de ética de la organización y adhieran a lo normado en el documento.

Otros componentes del programa de seguridad

Luego de analizar los componentes explicados anteriormente, es necesario evaluar la existencia de otros temas a incluir en el programa de seguridad que no se hayan incluido hasta el momento. Por ejemplo:

- Políticas de seguridad y estándares corporativos
- Programas de continuidad del negocio

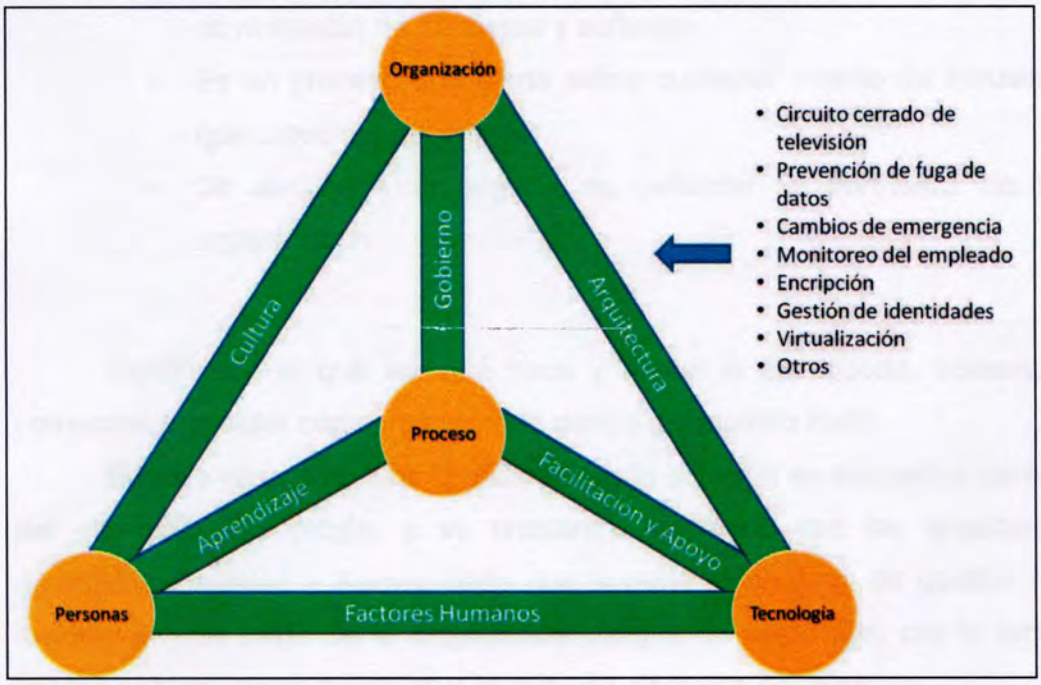
- Requerimientos de certificación (por ejemplo, ISO 27000)

Dependiendo del componente de seguridad que será integrado, la asociación puede llegar a ser con todos los elementos y relaciones dinámicas del modelo BMIS. Cada componente y/o servicios debería ser analizado en detalle y luego asociarlo a un elemento o relación dinámica dentro del BMIS.

4.2. Poblando el BMIS con las medidas y soluciones de seguridad existentes [1]

Obteniendo Información

Para que el BMIS sea efectivo, es necesario analizar todas las medidas y soluciones de seguridad existentes en la organización para tomar conocimiento de las mismas e integrarlas adecuadamente[24].



[24] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 50

Integrando soluciones individuales

Luego de haber identificado la mayoría de las medidas y soluciones de seguridad existentes en la organización, integrarlas en el modelo BMIS requiere simplemente compararlas con todos los elementos y relaciones dinámicas para lograr identificar las asociaciones más relevantes. Los puntos a analizar para determinar dicha asociación son:

- ¿Qué es la solución? (tecnología, organizacional, procesos, basada en gente)
- ¿Qué hace la solución y que riesgo de seguridad mitiga?
- ¿A qué le da soporte la solución?

Como ejemplo, se puede analizar un sistema de detección de intrusos, respondiendo las preguntas listadas anteriormente podemos decir que:

- La solución es tecnología, en este caso puede ser una combinación de hardware y software.
- Es un proceso que alerta sobre cualquier intento de intrusión que provenga del exterior.
- Se encuentra encargado de defender el perímetro de la organización.

Identificado el qué es, qué hace y a qué le da soporte, podemos comenzar a analizar cómo incorporarlo dentro del modelo BMIS.

En este caso podemos identificar que la solución se encuentra dentro del elemento Tecnología, y se encuentra vinculado con las relaciones dinámicas Facilidad y Apoyo, dado que soporta el proceso de gestión de incidentes y es parte de la arquitectura integral de seguridad, por lo tanto también se encuentra asociado a la relación dinámica Arquitectura.

Luego de identificar las medidas y soluciones, y lograr incorporarlas al modelo BMIS, es útil construir una tabla que asocie cada elemento con la solución de seguridad asociada para luego asignar responsabilidades a las tareas.

Elementos y Soluciones de seguridad	
Elemento	**Solución de seguridad asociada**
Organización	- Política de seguridad de la información - Estándares y guías de seguridad de la información
Tecnología	- Herramientas de gestión de identidades - Seguridad del perímetro
Procesos	- Proceso de planeamiento de la seguridad - Proceso de monitoreo de seguridad de la información
Personas	- Capacitación y concientización - Investigaciones

Las soluciones identificadas, a medida que vamos utilizando el modelo BMIS no son estáticas, el enfoque sistémico del modelo requiere que ser revise continuamente y se actualicen las soluciones, y como ellas interactúan con los elementos y las relaciones dinámicas.

Integrando soluciones gestionadas por terceras partes

Los productos o servicios no suelen cambiar demasiado solo por ser gestionados por terceras partes, la diferencia generalmente radica en la relación contractual y la responsabilidad de las soluciones de seguridad críticas.

Las soluciones de seguridad gestionadas por terceras partes se pueden dividir en:

- Procesos
- Tecnología
- Recursos Humanos

Desde el punto de vista del modelo BMIS, los resultados de una solución gestionada deberían ser los mismos que obtendríamos si el servicio fuera gestionado internamente. Por lo tanto, puede ser integrado al modelo como cualquier otro producto o servicio interno.

La diferencia principal es que la entrega y la calidad de los resultados se encuentran regulados por un contrato que establece como será la relación entre las partes. Asimismo dicho contrato establecerá las métricas que se aplicarán para validar que el contrato esté siendo cumplido.

Dentro del modelo BMIS, el contrato y su medición se encuentra en la relación dinámica Gobierno, muestra como el elemento Organización controla el elemento Proceso, aún cuando nos refiramos a terceras partes.

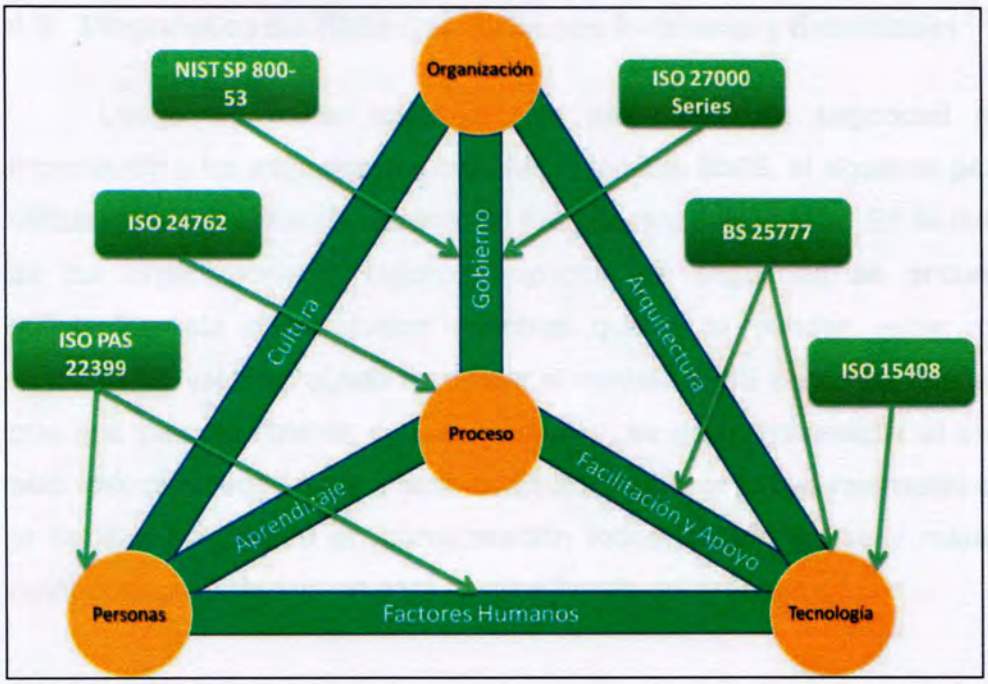
4.3. Alineando los estándares y marcos de trabajo al modelo BMIS [1]

Actualmente una gran cantidad de organizaciones se encuentran alineándose con las mejores prácticas del mercado, adoptando estándares de clase mundial para su funcionamiento. El modelo BMIS fue diseñado para poder adaptarse a los estándares y mejores prácticas que hoy se utilizan en la seguridad de la información.

Gestión de la Seguridad de la Información

Los estándares de seguridad de la información que utiliza la organización, deben ser alineados con el modelo BMIS. Las políticas y estándares se encuentran posicionadas en la relación dinámica Gobierno, dado que tienen influencia en los elementos Organización y Proceso. El modelo es alineado en función a la temática del estándar y luego cada capítulo o contenido es también alineado para ser relacionado con el elemento o relación dinámica que corresponda.

Realizar este análisis llevará a los Gerentes de Seguridad a una serie de relaciones entre el modelo y el contenido del estándar de seguridad, que luego le permitirá identifica los roles y responsabilidades dentro de la organización de seguridad de la información.



Relación entre los estándares de seguridad más reconocidos y el BMIS[25]

4.4. Gestión general de TI

Adicionalmente a los estándares de seguridad de la información, una gran cantidad de organizaciones han adoptado e implementado guías genéricas de TI (por ejemplo ITIL) que son mas abarcativos que la seguridad solamente, sin embargo contienen componentes que deben ser considerados cuando trabajamos con seguridad de la información. El modelo BMIS debe alinearse con estos estándares y marcos de trabajo en forma similar que lo realiza con los específicos de seguridad de la información.

Una de las formas que los Gerentes de Seguridad pueden lograr alienar los estándares generales de tecnología con el BMIS es mediante la utilización de COBIT.[26]

[25] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010, pp 56

[26] Control OBjectives for Information and related Technology

4.5. Diagnóstico del BMIS: identificando fortalezas y debilidades [1]

Luego de haber integrado las soluciones de seguridad de la información y los estándares existentes al modelo BMIS, el siguiente paso es utilizarlo para realizar un análisis de fortalezas y debilidades. En la mayoría de las organizaciones, algunos aspectos de seguridad se encuentran suficientemente desarrollados mientras que otros pueden estar menos maduros. El valor agregado de utilizar el modelo BMIS para este análisis, es que nos permite obtener causas y efectos, es decir, no realizar el análisis solo enfocándonos en los síntomas aislados sino en lo que realmente causa la debilidad, teniendo en consideración todos los elementos y relaciones dinámicas que intervienen para llegar a la raíz del problema.

Análisis situacional

El primer paso para identificar fortalezas y debilidades, es a través de la realización de un análisis situacional.

Dado que el modelo BMIS se basa en un enfoque sistémico, cualquier elemento o relación dinámica del modelo puedo tomarse como punto inicial de partida.

Para cada elemento del modelo, debe contener como mínimo la siguiente información que fue relevada en las fases anteriores:

- Políticas, métodos y controles existentes
- Procedimientos, herramientas y soluciones existentes
- Partes relevantes de los estándares de seguridad de la información
- Partes relevantes de estándares generales de tecnología informática

La forma más práctica de representar esta información es a través de una tabla:

Fortalezas y debilidades del elemento "Personas" [1]		
Ítem	*Tipo*	*Fortaleza / Debilidad*
Política de Seguridad de la Información	Política	Debilidad: existe pero no se encuentra actualizada
Capacitación en materia de seguridad	Procedural	Fortaleza: tiene los contenidos apropiados y es llevada a cabo periódicamente

Para cada elemento y relación dinámica, este ejercicio nos dará una noción de lo que se realizó con respecto a la seguridad de la información, y el nivel de madurez en el que se encuentra.

El segundo paso en el análisis situacional, es rearmar las tablas en términos de cada ítem. Por ejemplo, para evaluar el ítem sistema de detección de intrusos:

Análisis individual			
Sistema de detección de intrusos			
Elemento Tecnología	*Relación dinámica Arquitectura*	*Relación dinámica Facilidad y Apoyo*	*Relación dinámica Factores Humanos*
Fortaleza: Es una solución técnica exhaustiva	**Neutral:** Es apoyada por la infraestructura	**Debilidad:** Existe una gran cantidad de falsos positivos, es lento, algunas intrusiones reales podrían filtrarse	**Neutral:** Los empleados no tienen acceso directo a la herramienta.

Analizar los ítems desde este punto de vista, permite identificar debilidades aunque desde el punto de vista tecnológico la solución sea robusta.

Luego de completar el análisis situacional, el modelo BMIS resaltará los síntomas de las debilidades o fortalezas y las diferencias debidas a la percepción en la evaluación. Esta visión sistémica asegura que cada solución de seguridad o procedimiento sea analizado desde todas las perspectivas.

Análisis de causa – raíz

Luego de finalizado el análisis situacional, se conocen todas las fortalezas y debilidades de cada elemento y relación dinámica dentro del modelo. En la práctica, la causa real de una debilidad de seguridad no es la que parece ser en un análisis superficial, sino que su raíz se encuentra en otra parte de la organización. Para llegar a la causa raíz, el modelo BMIS, provee una guía que permitirá ubicarla dentro de la organización:

- ¿Es una debilidad trivial?
- ¿Es la causa raíz dentro de los elementos donde la debilidad fue identificada?
- ¿Es la causa raíz dentro de las relaciones dinámicas que asocian otros elementos?
- ¿Es la causa raíz en otro elemento e indirectamente conectado a la debilidad bajo análisis?

4.6. Poniendo en marcha el modelo BMIS: mejora continua [1]

En función a lo desarrollado anteriormente, y la base del modelo BMIS, cualquier cambio que llevemos a cabo para reforzar una fortaleza o mitigar una debilidad afectará no solo el elemento o relación dinámica con la que estemos trabajando, sino que inevitablemente llevará a el cambio en otra parte del sistema.

El BMIS propone separar el sistema en componentes que podemos manejar, pequeños subsistemas.

Los subsistemas muestran fácilmente como pueden verse influenciados por actividades internas y/o externas, y qué consecuencias habrá si la influencia es ejercida para un lado u otro. Para los responsables de seguridad, el BMIS resalta los resultados que una inversión en seguridad puede lograr, y cuál es el resultado esperado.

El modelo utiliza un enfoque circular en vez de un enfoque lineal.

Basados en un subsistema circular, las mejoras y las acciones pueden ser realizadas donde serán más efectivas. Con el fin de poder explicar no solo lo que está fallando en un proceso de seguridad, sino también el motivo por el cual falla, el BMIS recomienda que cada proceso de seguridad sea llevado a un subsistema circular, con un enfoque sistémico.

Pasos de mejora y acciones

En cualquiera de los subsistemas de seguridad, existen algunos puntos en los cuales los Gerentes de Seguridad pueden influir. Por ejemplo a través de una inversión o reforzando algunos puntos de seguridad. El punto de vista sistémico del BMIS resalta las opciones de inversión o mejora técnica en cada subsistema.

Aprovechando la dinámica del sistema

Cualquier sistema, reacciona a los cambios desde adentro hacia fuera. El sistema avanzará o retrocederá dependiendo de sus dependencias circulares.

5. Conclusiones

Como profesional de la seguridad, uno de los mayores desafíos es lograr posicionar a la seguridad de la información como un proceso de negocio, es lograr que dentro de los objetivos organizacionales y la estrategia que define el camino de la organización se encuentren los aspectos de seguridad que apoyaran a los procesos de negocio para que la organización alcance sus objetivos.

Años atrás la seguridad era solo informática, y no se evaluaba la posibilidad de que fuera un factor clave para los procesos de negocios. Hoy esa visión fue mutando y nos encontramos con la idea de seguridad de la información como proceso crítico dentro de la organización.

En la actualidad existen requerimientos legales que cumplimentar, procesos de negocio que son soportados enteramente por tecnología, optimizaciones que son llevadas a cabo a través de la implementación de nuevas tecnologías. Una adecuada gestión de la seguridad de la información colaborará sin duda con los objetivos organizacionales, y será un factor fundamental del éxito de la organización.

Es por eso, que los profesionales de seguridad necesitamos un modelo que nos permita despegar a la seguridad de esa visión técnica y lograr ser un componente más de la organización, poder explicarnos en términos de negocio y poder conocer en profundidad como nuestras decisiones influenciarán y serán influenciadas por otros elementos. Asimismo mediante este entendimiento lograremos que otros profesionales comprendan la importancia de la seguridad de la información y su misión dentro de la organización.

La puesta en marcha del presente modelo no es un camino fácil en organizaciones ya establecidas, dado que requiere en el transcurso de su implementación un cambio de mentalidad no solo en la organización, sino en quienes llevamos adelante la tarea de implementar los procesos de seguridad en la misma. Si bien las nuevas generaciones provienen de carreras donde cada vez más la gestión y la relación con el negocio se encuentran dentro de la currícula, aún nos encontramos en un período de transición cultural en donde ver la seguridad de la información como una

pieza más de la cadena de valor, que influenciará y será influenciado por la organización no se encuentra en la mirada de los niveles gerenciales que en muchos casos recién comienzan a entender el tema.

La interrelación entre el área de seguridad y el resto de las áreas muchas veces es compleja porque no comprenden la utilidad de las medidas de seguridad, no siempre se obtiene la colaboración necesaria, lo cual dificulta contar con la participación activa de usuarios claves para impulsar o institucionalizar la seguridad de la información.

Asimismo el modelo BMIS no se encuentra dentro de los modelos o metodologías conocidas que quienes comienzan a transitar o están transitando el camino de la seguridad suelen incorporar como guías en la forma de desempeñar sus tareas, es decir, en las formaciones en materia de seguridad escuchamos hablar infinidad de veces de las normas ISO, COBIT, la relación con ITIL y otras prácticas, pero no del modelo que hemos presentado en este trabajo. Considero que esto perjudica su implementación porque tratar de incluirlo en una etapa tardía del desarrollo del área aumenta significativamente la resistencia al cambio y el esfuerzo de institucionalizarlo cuando ya existe una forma de trabajo arraigada. No es imposible implementarlo, pero si difícil adaptarse a esta nueva visión de la seguridad.

El modelo BMIS explicado en el presente trabajo, nos ayuda a alinearnos con el negocio, y poder vincularnos con los elementos que van más allá de los tecnológicos. Luego de analizar el modelo, considero que la aplicación del mismo no es compleja, es decir, no implica una serie de fases que solo un grupo de consultores especialistas en el modelo pueda seguir. El mismo se encuentra claramente explicado a lo largo del documento principal, y creo que con un equipo de trabajo multidisciplinario (técnico – funcional) dentro de una organización puede ser llevado a cabo.

Intuitivamente muchos profesionales de seguridad ya nos encontramos utilizando el enfoque sistémico propuesto, tal vez informalmente, pero implementar el modelo a conciencia nos permite asegurarnos que hemos cubierto todas los puntos de vista posibles, y que no hemos pasado por alto aquellos factores que afectan a la seguridad ni como la seguridad los afecta.

El BMIS incorpora todos los elementos que componen una organización y sus relaciones principales, logra integrar todas las soluciones, estándares y marco normativo ya existentes, centralizando en un solo modelo toda la gestión de la seguridad. No inventa nuevamente lo que ya está inventado, es decir, no trata de cambiar todo lo que se encuentra establecido en la organización como si nunca hubiera existido, sino que incorpora el análisis de las soluciones y procesos existentes para poder mejorarlos y adaptarlos al modelo.

Comenzar a utilizarlo es también una estrategia efectiva para mostrar los resultados de la gestión de seguridad explicados en términos de impacto en el resto de los factores organizacionales. Nos posiciona como pares con otros procesos de negocio y nos permite demostrar que ya no cumplimos un rol estrictamente técnico y complejo de transmitir en una presentación gerencial.

Como mencioné al comienzo del trabajo una efectiva estrategia de seguridad de la información, no es sólo una cuestión técnica, sino que se basa también en comprender, las relaciones propias entre la organización, los procesos, los individuos y la tecnología, y el modelo BMIS nos permite poner en práctica esta necesidad de comprender.

6. Glosario

- **Modelo** (model): Representación simplificada de un sistema o fenómeno. [9]
- **Marco de trabajo** (framework): Provee información detallada sobre cómo llevar a cabo una tarea. [1]
- **Estándar** (stardard): Que sirve como tipo, modelo, norma, patrón o referencia [5]. Práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la organización o por el equipo gerencial de TI. Los estándares se pueden implantar para dar soporte a una política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento. [4]
- **Retroalimentación** (feedback): Función de compartir observaciones, dudas y sugerencias entre personas o divisiones de la organización con el fin de mejorar la performance organizacional y personal. [9]
- **Tecnología de la Información** (Information Technology): El hardware, software, comunicaciones y otras facilidades utilizadas para ingresar, almacenar, procesar, transmitir y producir una salida de información en cualquier formato. [9]
- **COBIT:** Es un conjunto de mejores prácticas para el manejo de información. es un marco de referencia para la dirección de IT, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio [4]
- **Teoría de Sistemas:** Un sistema debe ser visto en forma holística, no como la mera suma de sus partes para ser apropiadamente comprendido. El enfoque holístico examina el sistema como una unidad completa. [2]

7. Bibliografía

[1] ISACA - Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany. The Business Model for Information Security. USA : ISACA, 2010.

[2] Hamidovic, Haris. BMIS - An Introduction to the System Environment. ISACA Journal, Vol. 4. (2011)

[3] Laree Kiely, Ph.D. and Terry Benzel. Systemic Security Management. s.l. : Institute for Critical Information Infrastructure, 2003.

[4] Institute, IT Governance. Control Objectives for Information and related Technology. Ilinois : s.n., 2007.

[5] Real Academia Española, Diccionario de la Lengua Española. www.rae.es. (consultada el 20/11/2011).

[6] Security by Default, Blog. http://www.securitybydefault.com/2011/03/intrusion-en-la-compania-rsa-y-robo-de.html (consultada el 19/12/2011).

[7] Open Security, Blog. http://www.opensecurity.es/93000-cuentas-comprometidas-en-un-nuevo-ataque-a-sony/ (consultada el 15/01/2012).

[8] ISACA. An Introduction to the Business Model for Information Security. Ilinois : s.n., 2009.

[9] ISACA, Glossary. http://www.isaca.org/Pages/Glossary.aspx?tid=585&char=M. (consultada el 24/03/2012).