La Optimización de inversiones en TI y en controles de seguridad de información

Carmen Ozores, CISA, CRISC

Consultora en Seguridad de Información

Presidente del ISACA São Paulo Chapter, Brasil

Latin CACS

San Juan, Puerto Rico

Octubre 2011

latin america cacs

ISACA

Trust in, and value from, information systems

Agenda

- Componentes de IT Governance - Value Delivery
- Tomada de decisiones en Inversiones de TI
- Las categorías de inversiones
- ROI – Retorno Esperado de las Inversiones
- ROSI – Retorno de Inversiones en Seguridad de Información
- El modelo BMIS y la dimension de Procesos

Componentes esenciales de IT Governance

Value Delivery

Crear valor, al mismo tiempo en que mantiene y expande el valor existente, y eliminando iniciativas y activos que no tengan valor agregado

Risk management

Manejar los riesgos relacionados a Tecnología de Información y el uso de la TI para auxiliar la gestión de riesgos operacionales y otros riesgos

Resource management

Tener la capacidad adecuada para ejecutar el plan estratégico, proveer recursos suficientes, adecuados y eficientes

Performance measurement

Monitorear el alcance de los objetivos de la organización y conformidad con los requerimientos externos específicos

Componentes esenciales de IT Governance

IT Governance Focus Areas – CobiT 4.1

latin america cacs SM

ISACA®
Trust in, and value from, information systems

Figure 32—COBIT 5 Coverage of Governance Focus Areas	
Focus Area	**Coverage in COBIT 5**
Value Delivery	Covered by the Ensure Value Delivery governance process
Risk Management	Covered by the Ensure Risk Management governance process
Strategic Alignment	Alignment is not a specific (process) activity, but is achieved through successful execution of the processes in the governance and management areas. The combination of the 'evaluate' and 'direct' governance practices in the governance area and the resulting direction given to management constitutes alignment.
Resource Management	Covered by the Ensure Resource Optimisation governance process
Performance Measurement	Covered by: • Monitor governance practices in all governance processes • The Report to Stakeholders governance process • By the output(s) from the management processes in the Monitor, Assess and Inform domain

Figure of CobiT 5 Framework, provides a brief overview on how the governance aspects in each of the focus areas are covered in COBIT 5.

IT Value Delivery

ITGI defines value delivery as follows:

'Value delivery is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT'.

Source: IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, 2003, USA, *www.itgi.org*

IT Value Delivery
Estratégias para extrair valor de TI

- Aquisições e desenvolvimentos em TI bem sucedidos em geral exigem significativa alocação de recursos e portanto devem estar sujeitos ao mesmo tipo de cuidado inicial e monitoramento como qualquer investimento de negócio.

IT Value Delivery
Estratégias para extrair valor de TI

- Los proyectos de TI deben ser seleccionados y gerenciados a través de todo su ciclo de vida y resultar en creación de valor
- Para eso, la capacidad de TI debe ser comprendida, apropiada a demanda del negocio, y alavancada para que se obtenga el valor deseado

latin america cacs

ISACA®
Trust in, and value from, information systems

Categorización de inversiones

- Inversiones en TI están sujetas a las mismas expectativas atribuidas a cualquiera otro tipo de desembolso corporativo:
- la expectativa de que va tener algún retorno
- Gastar los fondos de los accionistas sin mirar con atención los retornos anticipados, puede llevar a gastos impensados y mal direccionados
- El que va a resultar, en lo mejor en una desventaja competitiva y en lo peor caso en una completa falla de la organización

Categorización de inversiones

- Cada organización debe seleccionar y adoptar un esquema de categorización que sea más relevante a su contexto.

- Hay que comprender la finalidad de tener alguna forma de categorización de las inversiones

Por que es importante la categorización de las inversiones en TI ?

- Mejor habilidad de construir y monitorear un portfolio balanceado de inversiones en TI.
  - Una Organización en crecimiento es muy probable que tiene inversiones de todas las categorías.
  - Una combinación adecuada es esencial para garantizar que el riesgo sea entendido y gerenciado, el crecimiento sea encorajado y aun se mantenga el foco sobre las actividades esenciales así como a las inversiones estratégicas de longo plazo.
- Definir de manera más adecuada los riesgos y metas de retorno de las inversiones.
  - Es probable que una inversión estratégica tenga un gran riesgo y una expectativa alta de retorno, así como una inversiones de carácter informacional, tiene menor riesgo y por consecuencia una expectativa más baja de retorno.

latin america cacs℠

ISACA®
Trust in, and value from, information systems

Categorización de inversiones

Un ejemplo de categorización, de Peter Weill de Sloan CISR:

- **Inversiones TRANSACIONALES –** aquellos que proveen la tecnología para procesar transacciones básicas, lo que es repetitivo en el negocio

  Ej.: Procesamiento de prestamos, cobranzas o contabilidad gerencial. El propósito principal de estas inversiones es aumentar la eficiencia y reducir los costos

- **Inversiones INFORMACIONALES –** proveen la información para gerenciar y controlas la organización.

  Ej.: Los sistemas en esta categoría incluyen en general sistemas gerenciales, de control financiero, sistemas de apoyo a tomo de decisiones, planeamiento, comunicación y contabilidad.

- **Inversiones ESTRATÉGICAS –** en general son designados a agregar el real valor al negocio, por el aumento de ventaja competitiva, posibilitando la entrada en nuevos mercados, o por otro lado aumentando la capacidad de rendimiento.

  Ej.: un nuevo sistema para transacciones vía Internet, un canal de marketing por TV a cabo. Cambios a un modelo de computación en nube, es también un ejemplo.

Categorización de inversiones

- Es importante considerar una categoría de proyectos mandatorios, debido a requisitos legales, como normas especificas de un sector de la industria, regulaciones ambientales, aspectos de responsabilidad social, o normas de supervisión bancaria, del sector publico, etc.

- *El desafío de la gerencia esta en promover procesos de negocios solidos, no solo para atender a las reglamentaciones, como también para aumentar la eficiencia del negocio, o reducir la ocurrencia de fallas o indisponibilidad de los sistemas.*

Principales componentes do proceso de aprobación de investimentos de TI

- Elaborar un **business case** completo y basado en estándares corporativos consistentes con definiciones acordadas (ejemplo, tasas, impuestos, tasas de inflación, etc.)
- Un **comité de aprobación** representado de manera adecuada tanto por la área de negocios cuanto de TI, para garantizar que las decisiones sean tomadas de manera independiente, con adecuada transparencia de todos los componentes del business case, y incluyendo el alineamiento estratégico y los retornos financieros
- **Consideración adecuada de métricas** financieras relevantes sobre el retorno esperado de los proyectos candidatos, incluyendo los indicadores clave tales como valor presente neto (NPV), tasa interna de retorno y periodo de *payback*
- **Provisiones para una buena ´accountability´** de los resultados obtenidos
- **Definición de tasas de retorno** de las inversiones más apropiadas.

latin america cacs℠

ISACA®
Trust in, and value from, information systems

Definir e Cuantificar os Beneficios Esperados

- Un Business Case completo para las inversiones relacionadas a TI deben tener claro la definición de los beneficios de negocio para posibilitar que se calcule el retorno esperado
- Estos beneficios en general recaen en dos principales categorías: directos o indirectos (*soft).* Los beneficios directos en general se constituyen de beneficios financieros cuantificables a que el nuevo sistema tiene la expectativa de crear
- En general hay una combinación de:

  • Economía de costos por medio de, por ej., reducciones en cantidad de personal, reducción de costos de manutención de estuques, más bajo costo de producción, o un *cash flow* mejorado por un proceso de cobros más ágil

  • Aumento de la receta por medio de la habilidad de adentrar en nuevos mercados, diferentes o más grandes, o por ej. El lanzamiento de un nuevo producto o servicio

Monitoreo de los beneficios

- Es esencial mantener una practica de monitoreo de los beneficios reales atingidos por lo desarrollo y implementación de soluciones de negocios relacionadas a TI

- El monitoreo de los beneficios debe ocurrir a partir de la implementación del proyecto. En caso de proyectos más grandes, un cuadro confiable de los beneficios alcanzados puede ser posible solo muchos meses o algunos años, después de la implementación, así mismo es importante que se establezca un monitoreo en todas las fases del proyecto

Estimativa de retorno ajustada al riesgo

- Aspectos importantes en análisis del proyecto de TI
  - Foco en retorno ajustado al riesgo
  - Utilizar metodologías de cálculo de risco e retorno esperado
  - Definir y cuantificar los beneficios esperados
  - Evaluar los beneficios realizados de los investimentos

Análisis de estimativas de riesgos y retornos en inversiones

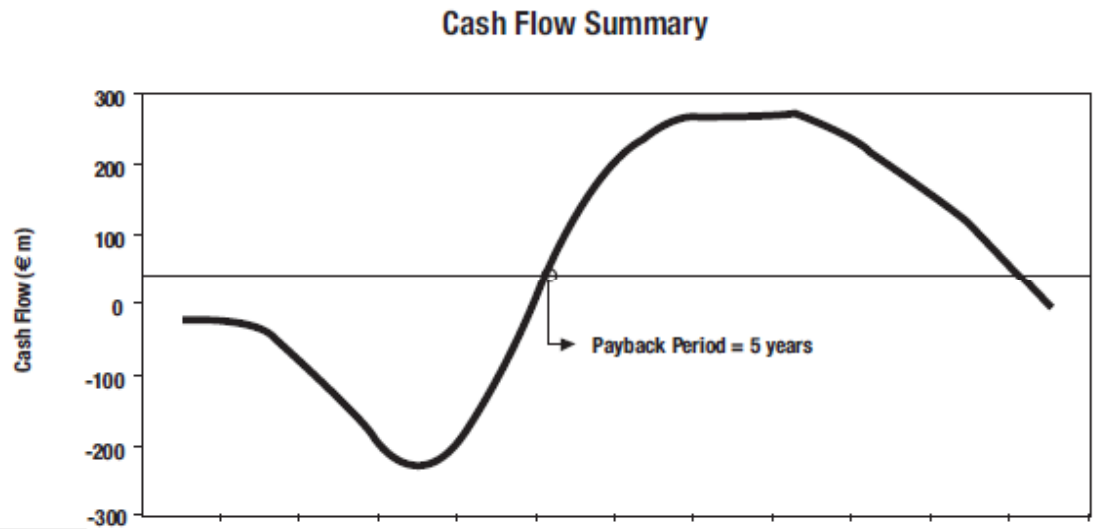
- Las figuras a seguir muestran algunos ejemplos de técnicas utilizadas para el análisis de estimativas de riesgos y retornos esperados en inversiones

- Son técnicas que se aplican igualmente a inversiones de TI, de manera similar a otras inversiones de la organización

Source: ISACA White Paper ´Optimizing Value Creation from IT Investiments

Análisis de retorno de inversiones

Figure 4—Payback Period Example



Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
# of projects running	1	8	16	25	19	12	9	3	2	2	1	1
# of projects generating benefits (investment horizon max 8 years)	0	1	5	12	21	23	24	21	14	6	3	0

SeaQuation
Enterprise Portfolio Intelligence

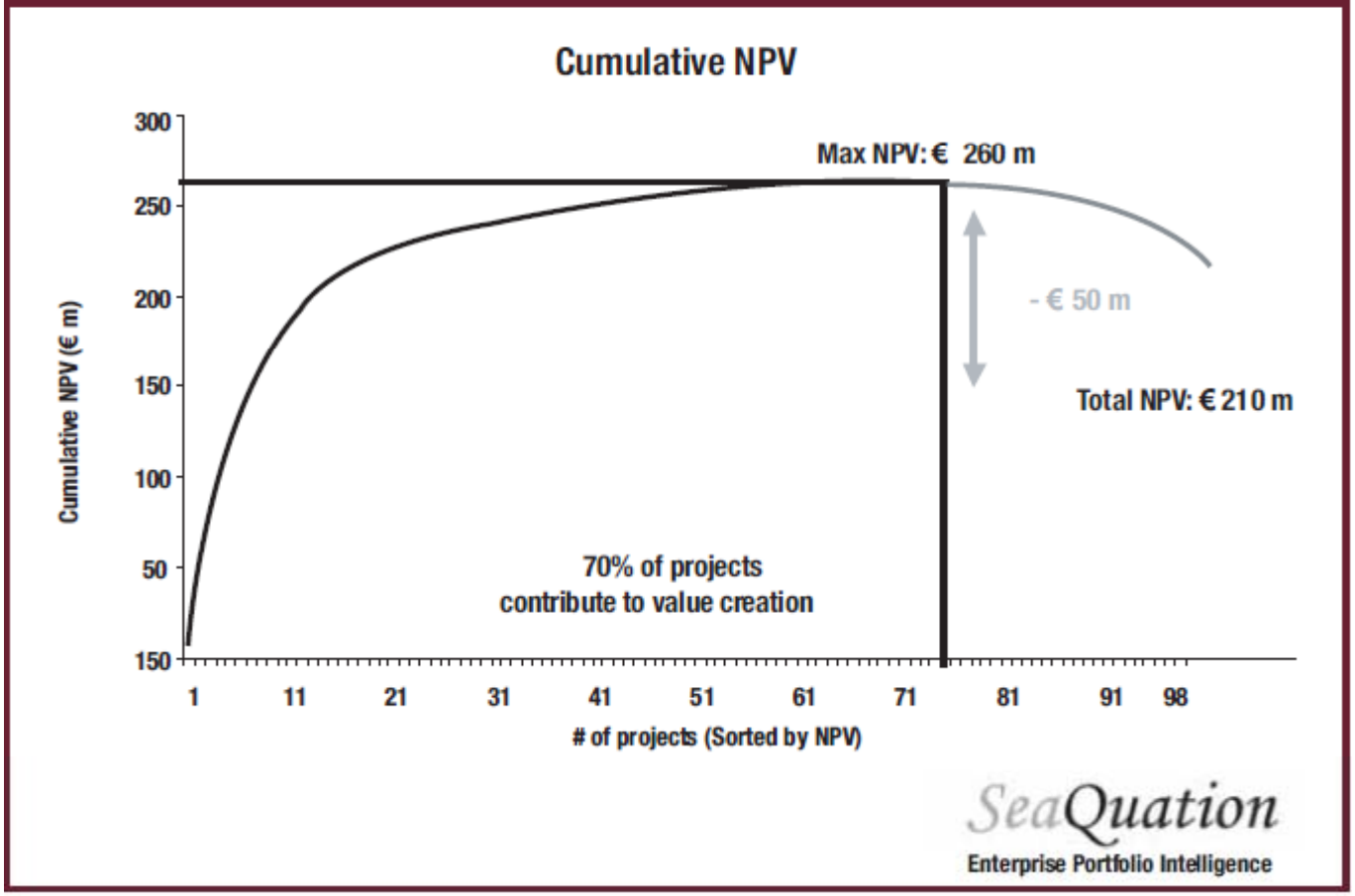
Source: ISACA White Paper ´Optimizing Value Creation from IT Investiments

latin america cacs SM

ISACA®
Trust in, and value from, information systems

Análisis de retorno de inversiones

Figure 6—Cumulative NPV Example



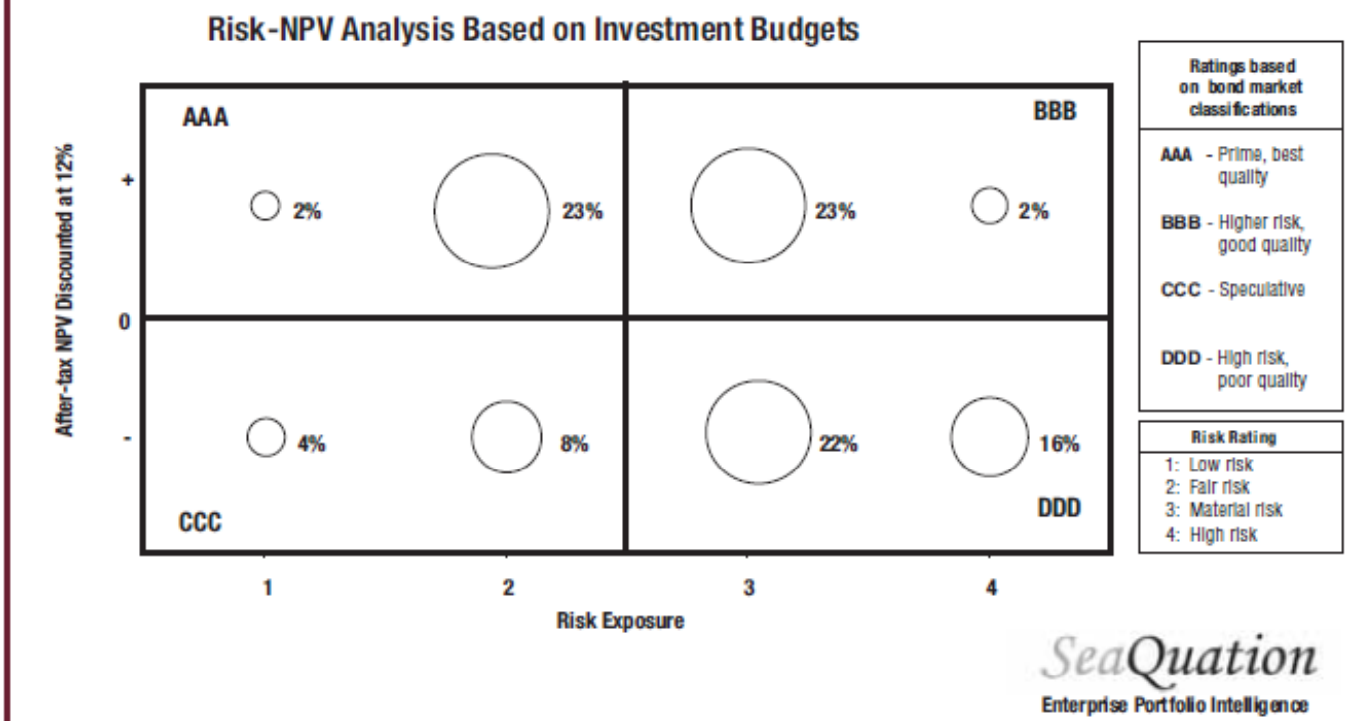
Source: ISACA White Paper ´Optimizing Value Creation from IT Investiments

latin america cacs SM

ISACA®
Trust in, and value from, information systems

Análisis de retorno de inversiones

Figure 7—Balance Between Risk and NPV Example



Source: ISACA White Paper ´Optimizing Value Creation from IT Investiments

latin america cacs SM

ISACA®
Trust in, and value from, information systems

El Modelo Gordon-Loebl
Discusión acerca del ROSI

- Según el modelo Gordon-Loeb, en general no es económico investir en actividades de seguridad en más de 37% de las pierdas esperadas que pueden ocurrir de una falla de seguridad !
- La discusión que esta teoría propone es como estimar as pierdas esperadas y no solo se basar en las vulnerabilidades de riesgo más alto
  - Una modelaje financiera de la estimativa del valor optimo de inversiones en proyectos de seguridad de la información

R.O.S.I., Retorno de Inversiones en Seguridade de la Información)

latin america cacs

ISACA®
Trust in, and value from, information systems

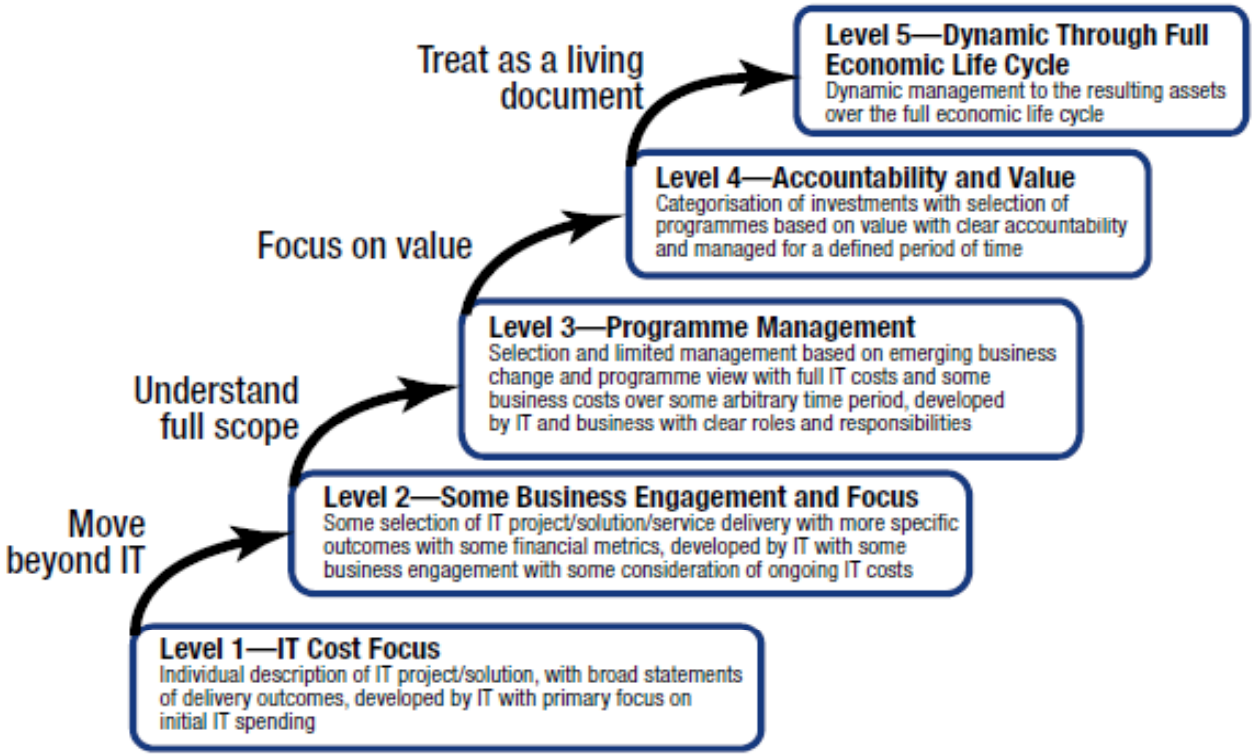
Componentes del Business Case

En lo mínimo, un business case debe incluir:

- **Los motivos para la inversión –** La oportunidad o problema que esta inversiones tiene la intención de atender
- **La solución y la abordaje recomendados –** Incluye alternativas consideradas y un cronograma propuesto
- **Los beneficios que se tiene como objetivos –** Un alineamiento con la estrategia de negocios, como van a ser medidos los beneficios y **quien** en las funciones de negocios va a ser el responsable por garantízalos

4. Getting Started—How to Use This Guide to Improve a Business Case Process

Figure 8—Business Case Maturity Levels 1 to 5



Level 1	Level 2	Level 3	Level 4	Level 5
IM1.1	IM1.2, IM2.1	IM3.1	IM4.1, IM4.2, IM4.3, IM5.1, IM5.2, IM5.3	IM8.1

Applicability of Val IT Framework 2.0 Key Management Practices

Integrar los esfuerzos de governança de TI y las implementaciones visando compliance

Process Improvements

- Implementation Philosophies[1]
  - Unnecessary burden Approach
  - Necessary cost of doing business approach
  - Internal control culture approach
  - Cultural change and process approach

La manera como las organizaciones entienden la necesidad de controles internos, como exigido por las reglamentaciones va a guiar la calidad de la efectividad de sus controles.

[1] *Source: Marchetti, Anne, 'Beyond Sarbanes-Oxley Compliance'*

Unnecessary burden Approach

- La gerencia executiva adopta una abordaje de ´el compliance es un mal necesario´
- Estas organizaciones en general tiene una estructura de controles ineficaces
- La postura de la alta gerencia tiene influenza negativa en la postura general de la organización

Governance y Compliance de manera integrada

- *'Mapping the organization's processes may reveal hidden opportunities for shared services, occasions to streamline processes and reduce costs.'* [1]

En este libro la autora propone un modelo de compliance en que la organización puede integrar sus esfuerzos de *governance* y de *compliance*

[1] *Source: Marchetti, Anne, 'Beyond Sarbanes-Oxley Compliance'*

latin america cacs℠

ISACA®
Trust in, and value from, information systems

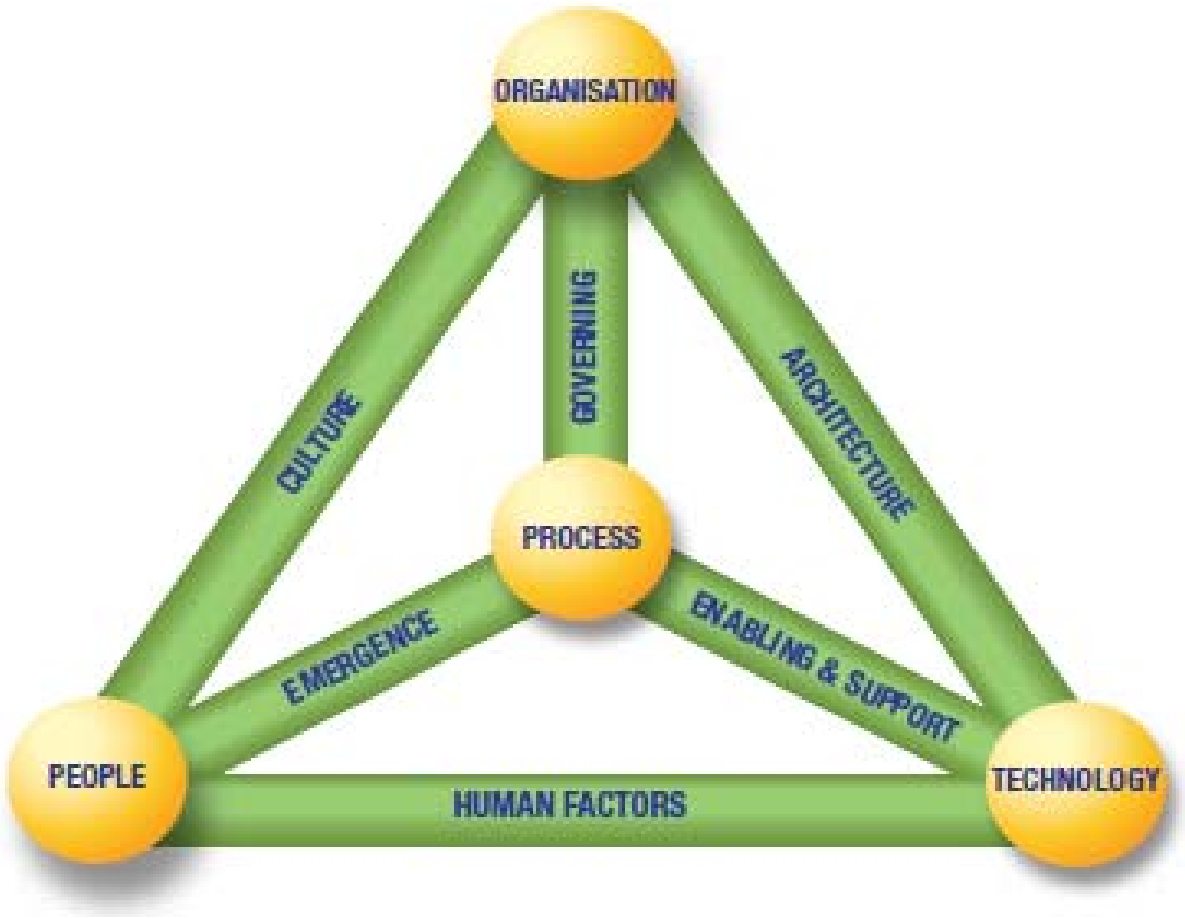
Dimensões do Modelo BMIS

- BMIS es un modelo tridimensional, que consiste en cuatro elementos y seis interconexiones dinámicas (DI, dynamic interconnections)
- El modelo es dinámico, o sea, y se puede cambiar desde el punto de vista de lo observador, si tiene como foco una de las dimensiones (figura a seguir)

- Todas las partes de BMIS interactúan y los elementos se interconectan por las Dis, donde las interdependencias son resultado de una abordaje sistémica.

Source: BMIS, The Business Modelfor Information Security

Dimensiones del Modelo BMIS

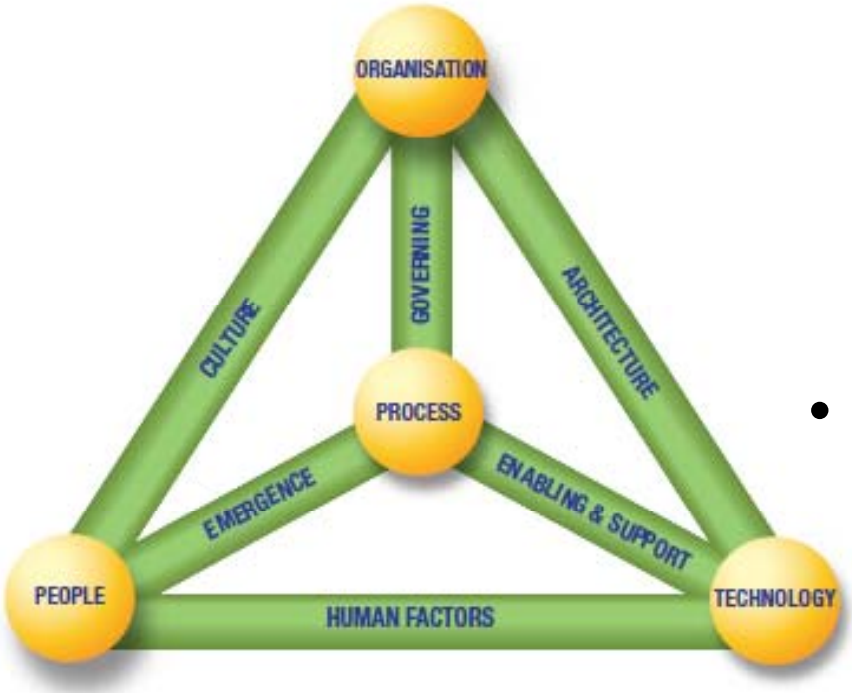


latin america cacs SM

ISACA®
Trust in, and value from, information systems

Dimensiones del Modelo BMIS

Todas las partes de BMIS interactúan y los elementos se interconectan por las Dis, donde las interdependencias son resultado de una abordaje sistémica.



- Si se cambia una parte del modelo, otras partes también van a cambiar. En un universo de seguridad de la información bien gobernado, el modelo es visto siempre en equilibrio.

- Si las partes del modelo se modifican, o se la deficiencia en la seguridad no es tratada, el equilibrio del modelo va a se presentar destorcido.

latin america cacs℠

ISACA®
Trust in, and value from, information systems

Modelo BMIS
La dimensión Proceso

- El elemento proceso es único y provee un *link* vital a todos los DIs del modelo

  Los Procesos son actividades estructuradas que fueran creadas para alcanzar un resultado particular a través de aplicación consistente de tareas individuales o en conjunto

  - El elemento proceso explica las practicas y procedimientos en la manera como las personas y organizaciones quieren tener realizadas
  - El proceso es un elemento fundamental que simboliza los requerimientos para una organización desarrollar, formalizar, educar y reforzar las practicas y procedimientos de seguridad de una manera continua

Source: BMIS, The Business Modelfor Information Security

Modelo BMIS
La dimensión Proceso

Abordaje Sistémica de los Procesos

- Una abordaje ´holística´ define el proceso como una unidad completa en que una parte del proceso posibilita el entendimiento y funcionamiento de otras partes del proceso.
- No hay así, un único proceso de seguridad de información, y el elemento proceso de BMIS comúnmente va a se formar por un numero grande de procesos individuales que suportan los varios aspectos de la seguridad

Source: BMIS, The Business Modelfor Information Security

Modelo BMIS
La dimensión Proceso

Para mejorar el programa de seguridad de información, los gestores necesitan examinar y entender la cultura que existe en la organización, y por tanto extender los puntos fuertes de la cultura asi como reconoces y mejorar las fragilidades para crear una cultura que tenga en su abordaje de seguridad una real intencion presente en todos los participantes del proceso.

Source: BMIS, The Business Modelfor Information Security

Modelo BMIS
La dimensión Proceso

- Las fases de implementación de BMIS
  - Integrar totalmente el programa de seguridad existente
  - Analizar y internalizar las medidas de seguridad y soluciones adoptadas
  - Alinear los estándares y regulaciones vigentes y los modelos utilizados (frameworks) al BMIS
  - Identificar de manera clara las fortalezas y las debilidades en la seguridad existente
  - Utilizar el sistema de seguridad dinámica introducido por BMIS
  - Gestionar las emergencias en la organización para maximizar las mejorías en seguridad

Consideraciones Finales

- Las expectativas de retorno deben estar relacionadas al riesgo, así una alta probabilidad de fallas, los proyectos de más alto riesgo deben tener una alta tasa anticipada de retorno

  Todas las inversiones, sean relacionadas a TI o no, deben ser aprobadas a partir de un entendimiento completo de los costos estimados y el calculo del retorno anticipado

- Garantizar que los proyectos ciertos sean aprobados en primer plan, implica en una correcta previsión de los costos totales de proyecto al largo de su tiempo de vida, considerando la cuantificación de los beneficios

  Establecer mecanismos de monitoreo va a ser vital para garantizar que el proceso sea eficiente y sea parte de la cultura de la organización

Preguntas ?

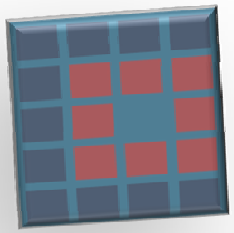
Questions ?

Comentarios !

Muchas Gracías !

Thank you

Obrigada



Ozores Consultoria

Carmen Ozores, CISA, CRISC

Presidente

ISACA São Paulo Chapter, Brasil

carmen.ozores@isaca.org.br

+55 11 9687 7081

latin america cacs SM

ISACA®

Trust in, and value from, information systems

Referencias

- ISACA and ITGI Publications:

  The Business Case Guide: Using Val IT 2.0, an ISACA Professional Guide

  Optimising Value Creation From IT Investments´, ITGI

  G41 Return on Security Investment (ROSI)´, IT Audit and Assurance Guideline

  BMIS, The Business Modelfor Information Security

- CobiT 5 Framework, Exposure Draft, June 2011, download at: *www.isaca.org*
- MARCHETTI, Anne M., ´Beyond Sarbanes-Oxley Compliance: Effective Enterprise Risk Management´, Ed. Wiley, USA, 2005
- ´The Economics of Information Security Investment´, LAWRENCE A. GORDON and MARTIN P. LOEB, University of Maryland

latin america cacs

ISACA®

Trust in, and value from, information systems