Mejores Prácticas de Gobierno de TI en las Instituciones Financieras

Administración de Riesgos – Risk IT

Fernando Ferrer Olivares

Banco de la República de Colombia

fferreol@banrep.gov.co

Administración de Riesgos – Conceptos

Herramienta gerencial
(y de gobierno)

que apoya la toma de decisiones organizacionales

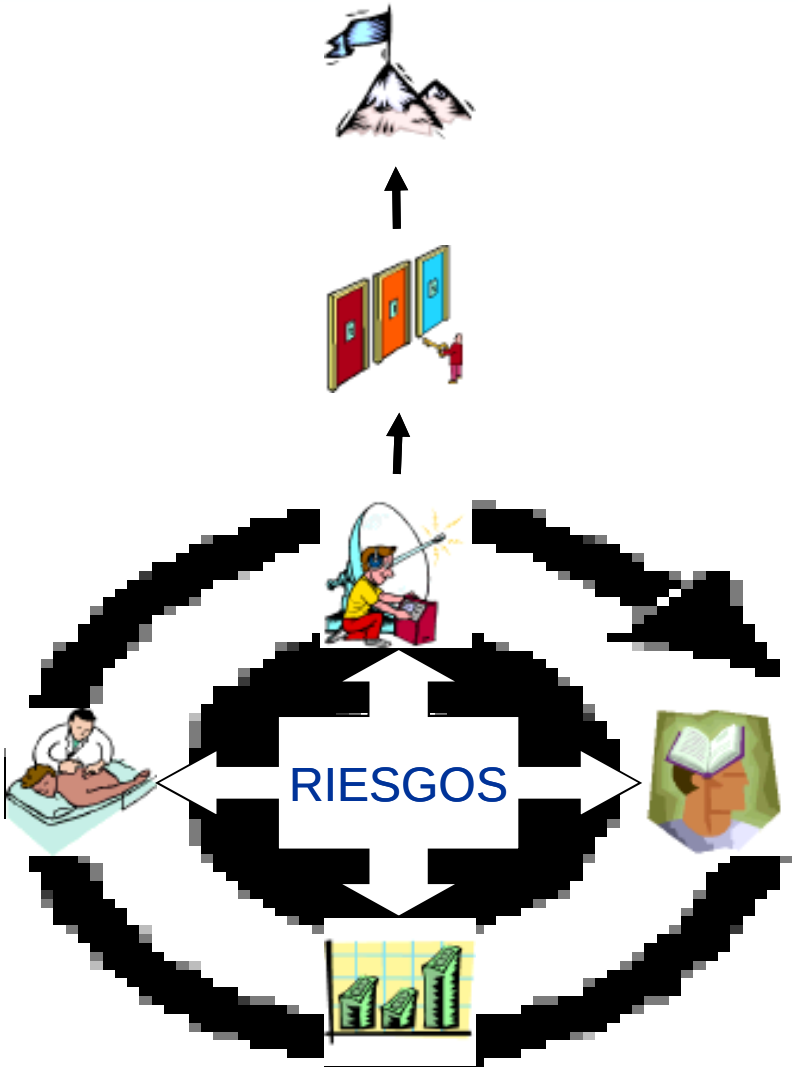
facilitando con ello el cumplimiento de los objetivos del negocio

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

1999

Administración de Riesgos – Conceptos

Proceso iterativo basado en el conocimiento, valoración, tratamiento y monitoreo de los riesgos y sus impactos en el negocio

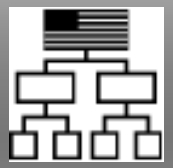


Administración de Riesgos – Conceptos

Aplicable a cualquier situación donde un resultado no deseado o inesperado podría ser significativo en el logro de los objetivos o donde se identifiquen oportunidades de negocio


Proceso


Proyecto


Unidad Organizacional


Sistema de Información

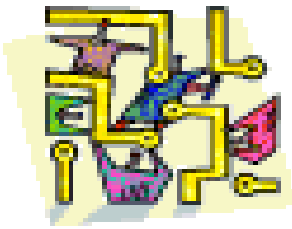

Oportunidad


Ubicación Geográfica

Administración de Riesgos – Cómo implementarla?

Proyecto

Dar la Sostenibilidad



Proceso

Etapas del proyecto

1. Estructuración del Proyecto

- **Investigación**
- **Elaboración Guía Metodológica**
- **Elaboración del Prototipo**
- **Definición de políticas globales**

2. Preser
y aprobación de las políticas globales

3. I

Aprobación de:

- **Alcance**
- **Responsables - Participación**
- **Criterios para priorizar procesos**
- **Mecanismos de Monitoreo y periodicidad**

Etapas del proyecto

4. Divulgación y afinamiento de la Guía Metodológica

5. Implantación de l

- **Sensibilización**
- **Capacitación**
- **Elaboración de talleres**

6. Seguimiento al proyecto

Actualización constante de:

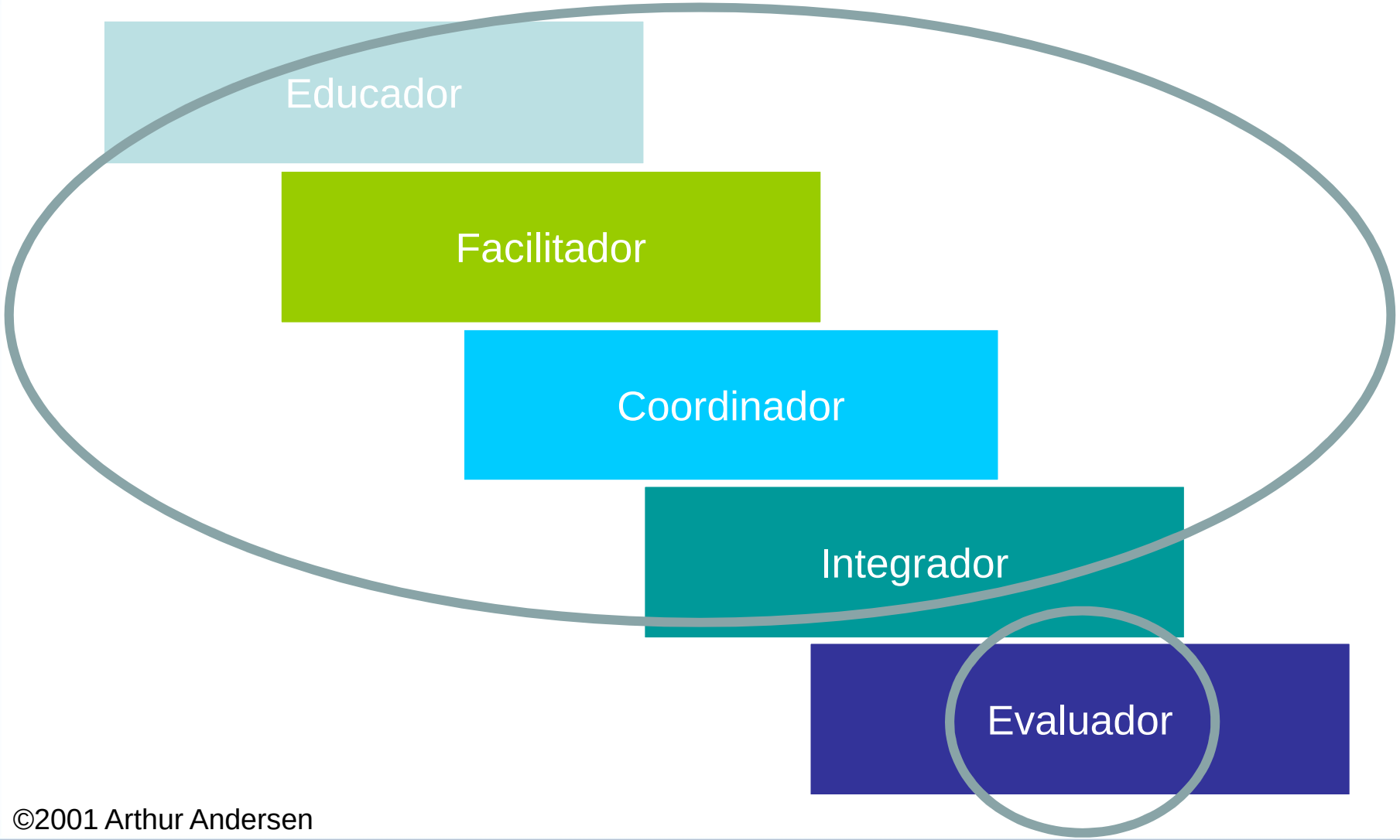
- **Políticas**
- **Guía Metodológica**
- **Software**

Plan de Trabajo - Cronograma

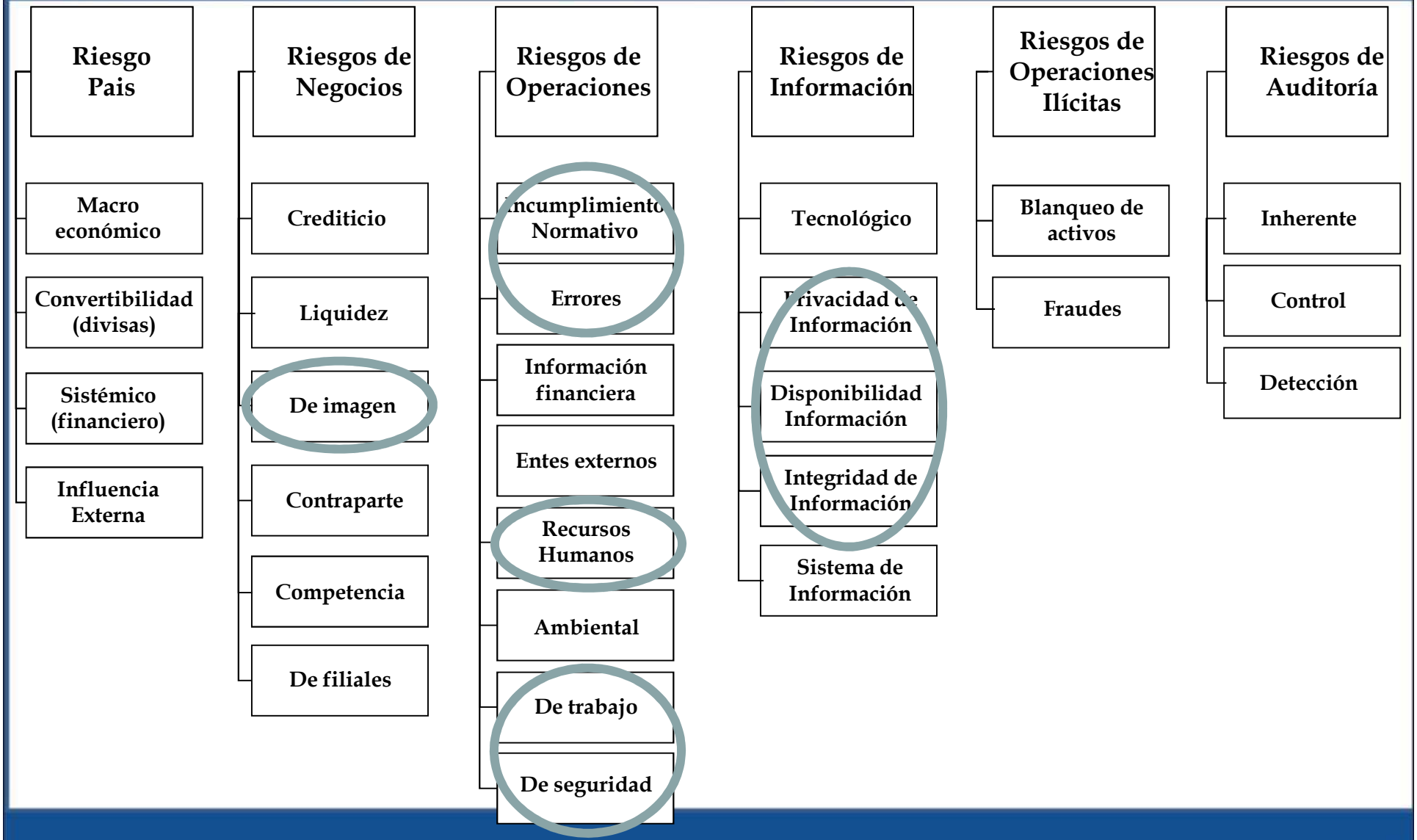
Actividad	T 2 00	T3 00	T4 00	T1 01	T2 01	T3 01	T4 01	T1 02
Estructuración del proyecto								
Presentación al CCSCI y aprobación de políticas globales								
Identificación de procesos u objetos críticos								
Divulgación y afinamiento de la Guía Metodológica								
Implantación de la Guía Metodológica (Bogotá-Sucursales)								
Seguimiento al Proyecto								

Planeado En ejecución Permanente

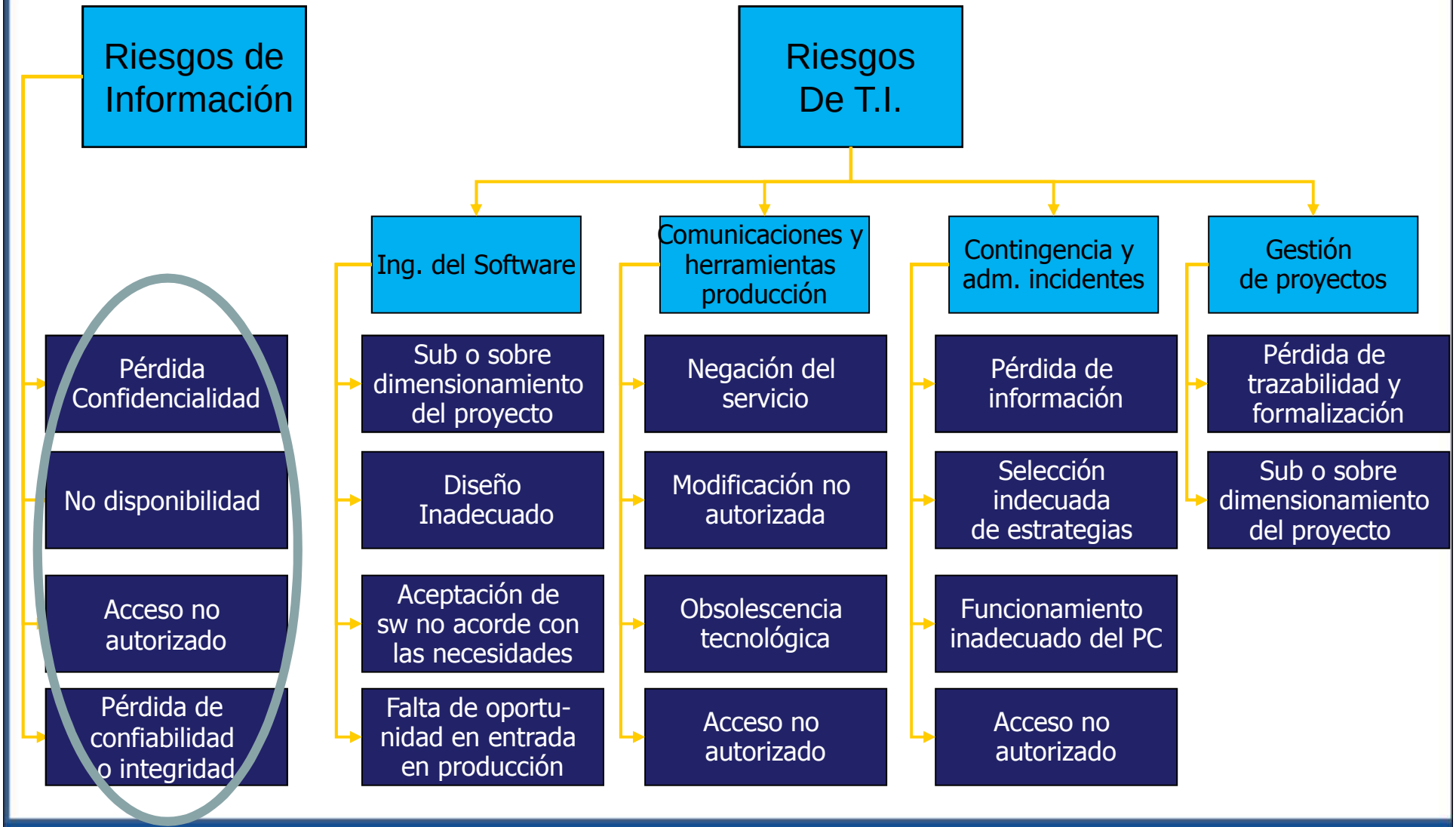
5 roles claves para un auditor interno de clase mundial



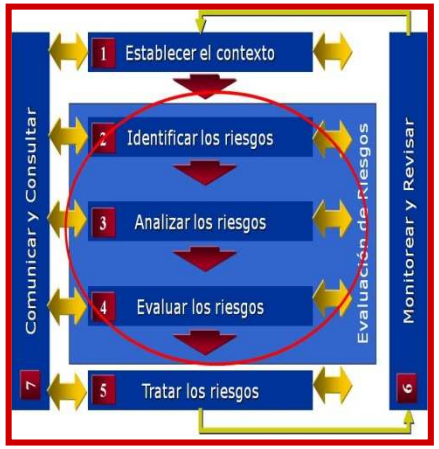
Administración de Riesgos – Tipificación

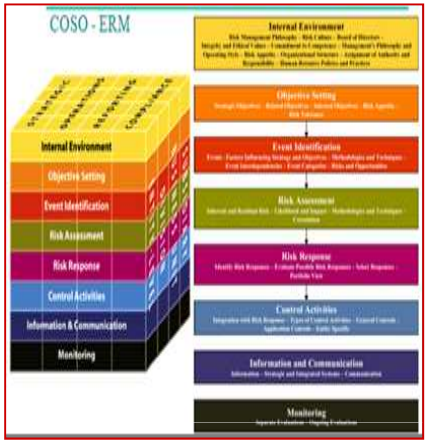


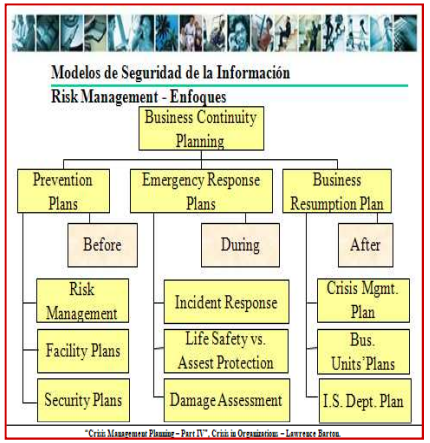
Administración de Riesgos – Tipificación

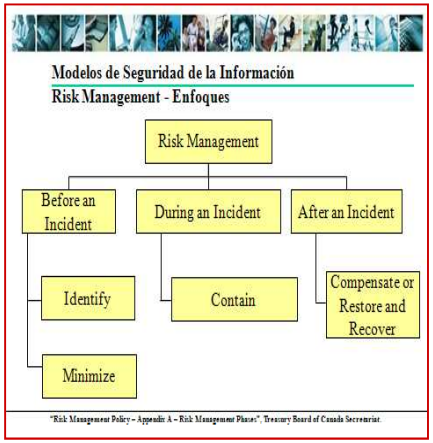


Metodología - Algunos documentos analizados

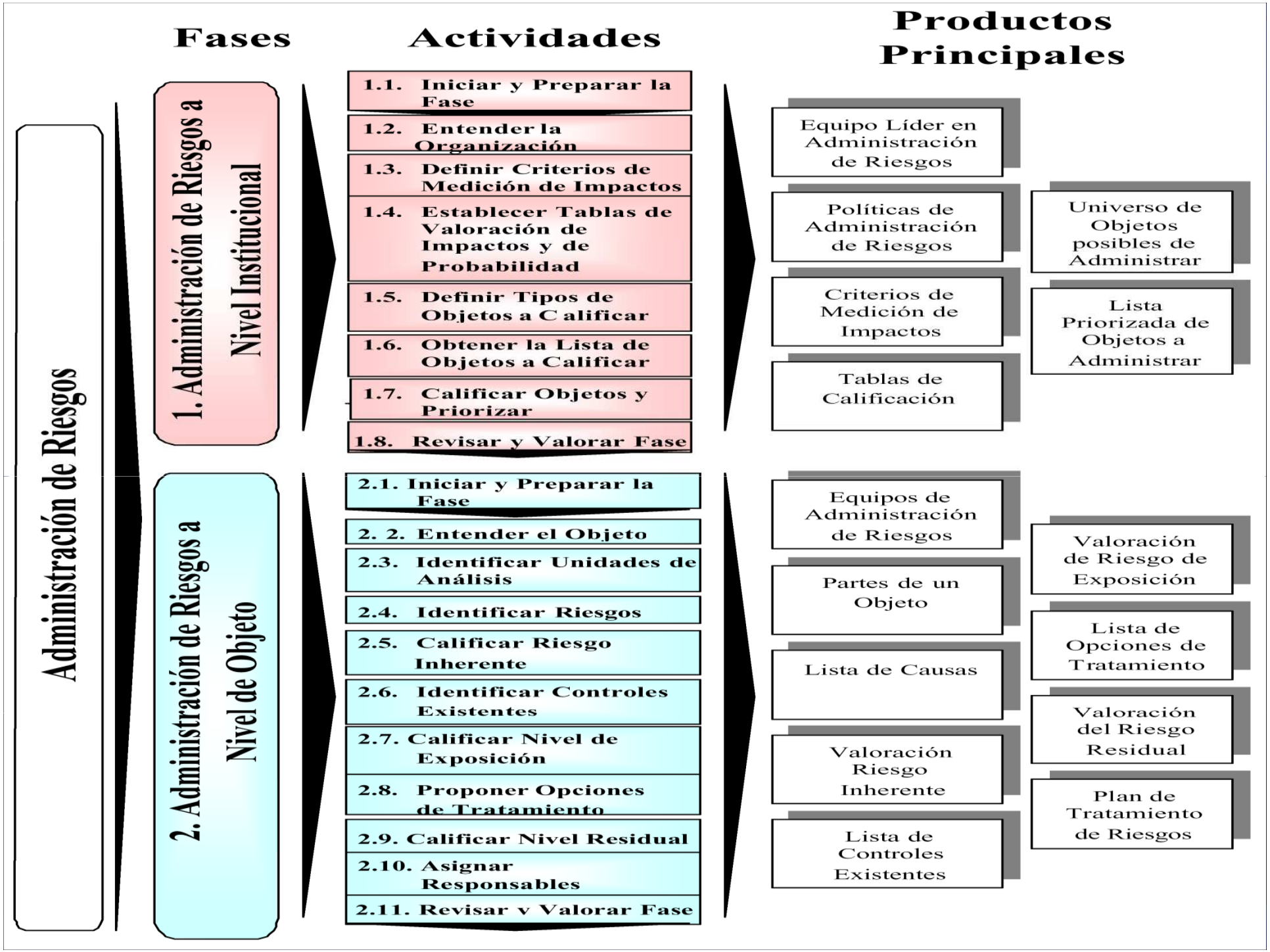








- **COCO - Instituto Canadiense de Contadores Certificados (CICA)**
- **IFAC - Financial & Management Accounting Commitee**
- **A Guide to Security Risk Management for Information Technology Systems - Goverment of Canada, Communications Security**
- **Mc2 Management Control Concepts - David Mcnamee**
- **Risk Management - Chester Simmons**
- **MAGERIT - Metodología de Análisis y Sesión de Riesgos de los Sistemas de Información - Versión 1.0**
- **ISO31000**
- **ISO 27002 Y 5**
- **OCTAVE**
- **ISF**
- **CRAMM**
- **Westerman book**
- **Muchos más ….**


Fases
Actividades
Productos Principales
Administración de Riesgos
1. Administración de Riesgos a Nivel Institucional
1.1. Iniciar y Preparar la Fase
1.2. Entender la Organización
1.3. Definir Criterios de Medición de Impactos
1.4. Establecer Tablas de Valoración de Impactos y de Probabilidad
1.5. Definir Tipos de Objetos a C alificar
1.6. Obtener la Lista de Objetos a Calificar
1.7. Calificar Objetos y Priorizar
1.8. Revisar y Valorar Fase
Equipo Líder en Administración de Riesgos
Políticas de Administración de Riesgos
Criterios de Medición de Impactos
Tablas de Calificación
Universo de Objetos posibles de Administrar
Lista Priorizada de Objetos a Administrar
2. Administración de Riesgos a Nivel de Objeto
2.1. Iniciar y Preparar la Fase
2. 2. Entender el Objeto
2.3. Identificar Unidades de Análisis
2.4. Identificar Riesgos
2.5. Calificar Riesgo Inherente
2.6. Identificar Controles Existentes
2.7. Calificar Nivel de Exposición
2.8. Proponer Opciones de Tratamiento
2.9. Calificar Nivel Residual
2.10. Asignar Responsables
2.11. Revisar v Valorar Fase
Equipos de Administración de Riesgos
Partes de un Objeto
Lista de Causas
Valoración Riesgo Inherente
Lista de Controles Existentes
Valoración de Riesgo de Exposición
Lista de Opciones de Tratamiento
Valoración del Riesgo Residual
Plan de Tratamiento de Riesgos

FELABAN
FEDERACIÓN LATINOAMERICANA DE BANCOS

2009

Administración de Riesgos (relacionados a) de TI

- **Abarca todos los riesgos relacionados con TI: No está limitado a Seguridad de la Información**
  - **Entrega de proyectos tarde, problemas de cumplimiento, inadecuado alineamiento entre TI y el negocio, problemas en la entrega de los servicios de TI, arquitectura de TI inflexible, arquitectura de TI obsoleta**
- **Cubre todas las actividades de Administración de Riesgos**
  - **Incluyendo Gobierno del Riesgo, Cultura del Riesgo, etc...**
- **Cubre los riesgos de negocio debidos a las actividades relacionadas con TI**

Riesgos relacionados con TI = impactos al negocio materializados debido a eventos relacionados con TI

Características o cualidades de un buen Marco de Trabajo para la Administración de Riesgos (relacionados a TI)

	Característica
1	Visión comprehensiva de la administración de riesgos, no solo técnica/mecánica
2	Específico a la materia sujeto, ej. TI
3	Visión de inicio a fin de la materia sujeto, ej. visión amplia de los riesgos relacionados a TI
4	Orientado al negocio
5	Suministra un proceso continuo, desde la identificación de riego hasta el monitoreo y la retroalimentación continua
6	Cubre todas las opciones de tratamiento
7	Disponibilidad/Accesibilidad

Características o cualidades de un buen Marco de Trabajo para la Administración de Riesgos (relacionados a TI)

		COBIT 4.1 Suite	Comentario
1	Visión comprehensiva de la administración de riesgos, no solo técnica/mecánica		La dimensión del riesgo es mencionada en COBIT
2	Específico a la materia sujeto, ej. TI		COBIT es todo sobre controles de TI
3	Visión de inicio a fin de la materia sujeto, ej. visión amplia de los riesgos relacionados a TI		COBIT no describe los riesgos relacionados con TI en forma explícita, aún cuando la dimensión de la administración del riesgo es presente. COBIT va más allá de los riesgos de seguridad
4	Orientado al negocio		COBIT provee un enlace entre Objetivos de negocio y de TI, suministrando así una orientación al negocio
5	Suministra un proceso continuo, desde la identificación del riesgo hasta el monitoreo y la retroalimentación continua		COBIT es un modelo de procesos, pero no es específicos al riesgo, la administración de riesgos no es explicita, no es un modelo de inicio a fin de administración del riesgo
6	Cubre todas las opciones de tratamiento		COBIT especifica controles de TI, pero sin relacionarlos a riesgos específicos; no describe otras opciones de tratamiento al riesgo en detalle
7	Disponibilidad/Accesibilidad		COBIT es público y disponible gratuitamente

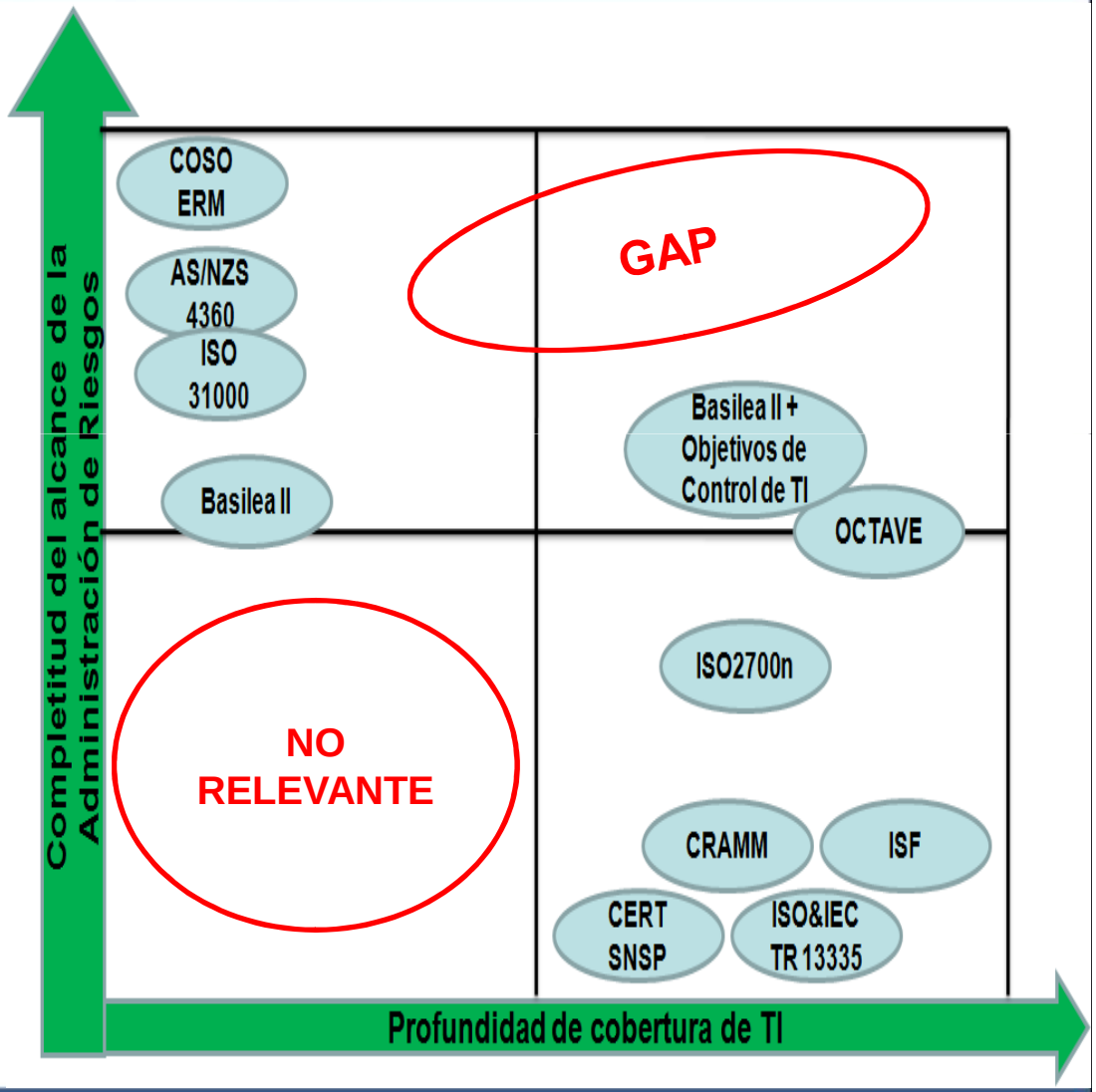
Características o cualidades de un buen Marco de Trabajo para la Administración de Riesgos (relacionados a TI)

		COBIT 4.1 Suite	COSO ERM	ISF	AS/NZS 4360 – ISO 31000	ISO 27005
1	Visión comprehensiva de la administración de riesgos, no solo técnica/mecánica					
2	Específico a la materia sujeto, ej. TI					
3	Visión de inicio a fin de la materia sujeto, ej. visión amplia de los riesgos relacionados a TI					
4	Orientado al negocio					
5	Suministra un proceso continuo, desde la identificación del riesgo hasta el monitoreo y la retroalimentación continua					
6	Cubre todas las opciones de tratamiento					
7	Disponibilidad/Accesibilidad					

Administración de riesgos relacionados con TI - Frameworks

- Varios estándares & marcos de trabajo disponibles
  - Orientados a la administración de riesgos empresariales genéricos
  - Orientados a la seguridad de TI

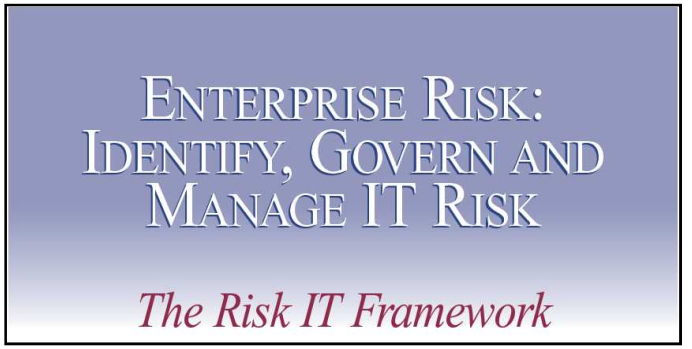
- No existe disponible (aún) un marco de trabajo comprehensivo de riesgos relacionados a TI



The Risk IT Framework

- Borrador liberado en 2009
- 94 páginas
- Pdf descargable gratuitamente

  http://www.isaca.org/Template.cfm?Section=Risk_IT&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=79&ContentID=48749



- Trabajo "colaborativo" de practicantes y expertos
  - Autores y Equipo de Desarrollo (5-0)
  - IT Risk Task Force (7-0)
  - Revisores expertos (61-2)

- Consulta de prácticas y metodologías existentes y emergentes para una administración efectiva de riesgos de TI
- Parte de la Iniciativa de Risk IT

La Iniciativa Risk IT

- **Esfuerzo dirigido a ayudar a las empresas a administrar los riesgos relacionados con TI**

The Risk IT Framework

ITGI ha desarrollado un marco de trabajo, buscando llenar el vacío en el espacio comprehensivo/ cobertura:

- ✓ **Comprehensivo en términos de abarcar todos los dominios y actividades de administración de riesgos, NO limitado a implementar controles exclusivamente**
- ✓ **Cobertura, en términos de cubrir todos los potenciales riesgos relacionados a TI que pueden afectar la realización de los objetivos de negocio**

		RISK IT
1	Visión comprehensiva de la administración de riesgos, no solo técnica/mecánica	
2	Específico a la materia sujeto, ej. TI	
3	Visión de inicio a fin de la materia sujeto, ej. visión amplia de los riesgos relacionados a TI	
4	Orientado al negocio	
5	Suministra un proceso continuo, desde la identificación del riesgo hasta el monitoreo y la retroalimentación continua	
6	Cubre todas las opciones de tratamiento	
7	Disponibilidad/Accesibilidad	

Conceptos

Riesgo de TI

- riesgo de negocio asociado con el uso, la propiedad, operación, participación, influencia y adopción de TI dentro de una empresa
- consiste de eventos relacionados con TI que pueden potencialmente impactar el negocio
- incluye tanto frecuencia y magnitud incierta
- crea retos en alcanzar los objetivos y metas estratégicas y en el aprovechamiento de las oportunidades

Audiencia del IT Risk Framework

- **Gerentes y practicantes encargados de satisfacer este requerimiento general y estratégico**

 **Altos ejecutivos y Juntas Directivas** o **Establecen la dirección y monitorean el riesgo a nivel empresarial**	 **Profesionales de administración de riesgos** o **Requieren de asesoría específica en riesgos de TI**
 **Gerentes de TI y de departamentos** o **Definen los procesos de administración de riesgos**	 **Interesados externos**

Principios y Bloques de construcción

Gobierno Empresarial

Conexión a objetivos del negocio
Alineación de administración de riegos de negocio y de TI
Balancear los costos y beneficios de administrar riesgos

Administración Efectiva

Promover comunicación sobre riesgos de TI
Establecer el tono correcto – Accountability apropiada y niveles de riesgo tolerables bien definidos
Proceso continuo – del día a día

Establecer responsabilidad

Establecer objetivos y definir el apetito y la tolerancia

Identificar, analizar y describir riesgos

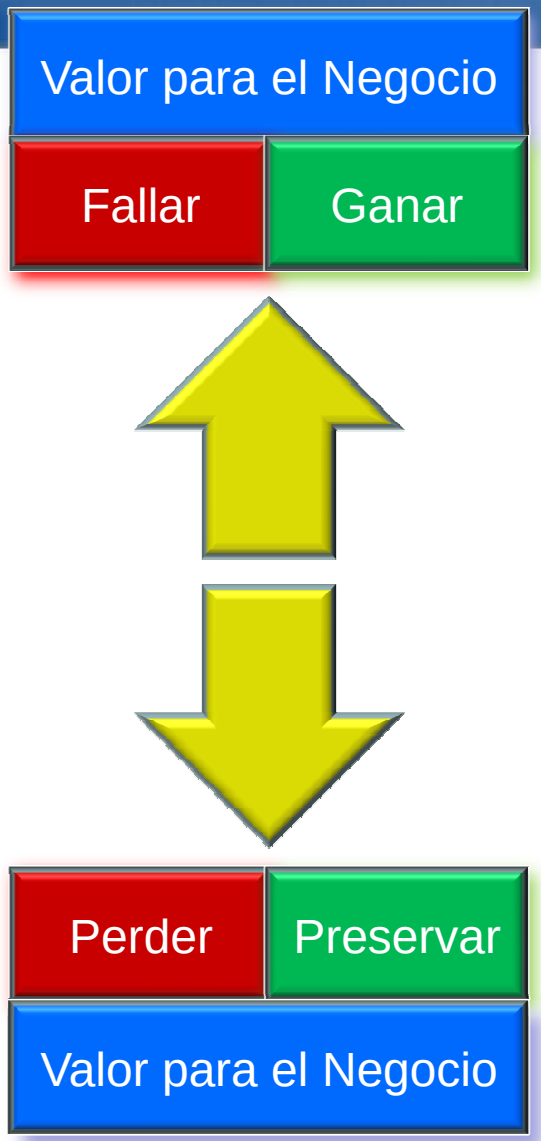
Monitorear la exposición al riesgo

Tratar los riesgos de TI

Encadenar con guías existentes

Riesgos de TI - Categorías

Logro de los beneficios (valor) de TI	**Habilitar tecnología para nuevas iniciativas de negocio, habilitar tecnología para operaciones efcicientes**
Entrega de Soluciones (Proyectos) de TI	**Calidad, relevancia y cobertura de los proyectos**
Entrega de Servicios de TI	**Interrupciones en los servicios de TI, problemas de seguridad, problemas de cumplimiento**



La comunicación

Communication From Others to Stakeholder →	Stakeholders	→ Communication From Stakeholder to Others
• Executive summary risk reports • Current risk exposure/profile • KRIs	**Executive management and board**	• Enterprise appetite for risk • Key performance objectives • IT risk RACI charts • Risk policies, expressing management's risk tolerance • Risk awareness expectations • Risk culture
• IT risk management scope and plan • IT risk register • Risk analysis results • Executive summary risk reports • Integrated/aggregated risk report • KRIs	**CRO and enterprise risk committee**	• Enterprise appetite for risk • Residual risk exposures • Operational risk information: residual exposures
• Enterprise appetite for risk • IT risk management scope and plan • Key performance objectives • IT risk RACI charts • Enterprise IT risk assessment request • IT risk framework and scoring methodology • IT risk register	**CIO**	• Residual risk exposures • Operational risk information • Business impact of the IT risk and impacted business units • Ongoing changes to risk factors (threats)
• Key performance objectives	**CFO**	
• IT risk management program charter • IT risk management scope • Plans for ongoing business and IT risk communication • Risk culture • Business impact of the IT risk and impacted business units • Ongoing changes to risk factors	**Business management and business process owners**	• Control and compliance monitoring
• Key performance objectives • IT risk management plan • Enterprise-wide IT risk assessment request • IT risk framework and scoring methodology • IT risk register • Risk culture	**IT management (including security, service management)**	• Residual risk exposures
• Key performance objectives • IT risk RACI charts • IT risk management plan • Control and compliance monitoring	**Compliance and audit**	• Audit findings
• Risk awareness expectations • Risk culture	**HR**	• Potential IT risk • Support on risk awareness initiatives
• Control and compliance monitoring	**External auditors**	• Audit findings
• Public opinion, legislation • Risk executive summary report • In general, all communications intended for the board and executive management	**Regulators**	• Requirements for controls and reporting
• Executive summary risk reports	**Investors**	• Risk tolerance levels for their portfolio of investments
• Summary risk reports, including residual risk, risk to key assets, controls maturity levels, audit findings	**Insurers**	• Insurance coverage (property, business interruption, D & O)
• Risk awareness expectations • Risk culture	**Staff**	• Potential IT risk issues

Responsabilidades y Accountability

Role Definitions		Risk Governance			Risk Evaluation			Risk Response		
Role	Definition of the Role	Common Risk View	Integrate with ERM	Risk-aware Decisions	Collect Data	Analyse Risk	Maintain Risk Profile	Articulate Risk	Manage Risk	React to Events
Board	The group of the most senior executives and/or non-executives of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources	A	A							
Chief executive officer (CEO)	The highest-ranking officer who is in charge of the total management of the enterprise	A/R	A/R						A	
Chief risk officer (CRO)	The individuals who oversees all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.	A/R	R	A/R	A/R	A/R	A	A/R	A/R	A/R
Chief information officer (CIO)	The most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. The CIO typically chairs the governance council that manages the portfolio.	R	A/R	A/R	R	A/R	A/R	R	R	R
Chief financial officer (CFO)	The most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks	R								
Enterprise risk committee	The group of executives of the enterprise who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee.	R		A/R		R		A		
Business management	Business individuals with roles relating to managing (a) programme(s)	A/R	R	A		A/R	A/R	A	R	R
Business process owner	The individual responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities.	R	R	R	R	R	A/R	R	R	A
Risk control functions	The functions in the enterprise responsible for managing specific risk domains (e.g., chief information security officer, business continuity plan—disaster recovery, supply chain, project management office)	R	R	R	R	R	R	R	R	R
Human resources (HR)	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise	R								
Compliance and audit	The function(s) in the enterprise responsible for compliance and audit	R								R

RISK IT - Estructura

❑Interfaz COBIT-VAL IT

❑Modelo de procesos

Dominios

- Objetivos y Métricas x Dominio
- Modelo de Madurez de Alto Nivel
- Modelo de Madurez Detallado o por Atributos

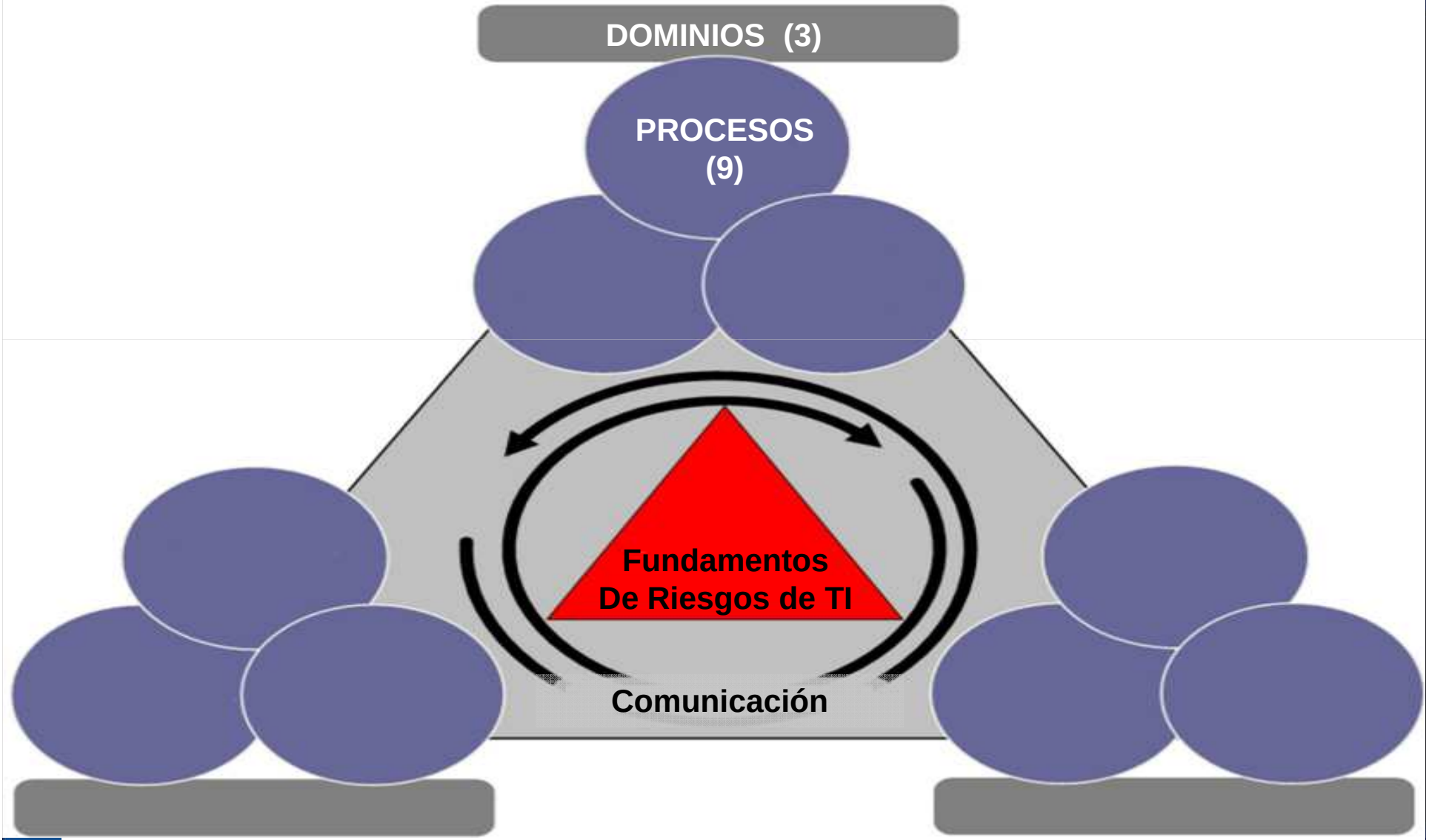
Procesos

- Objetivos y Métricas x Proceso
- Matriz RACI

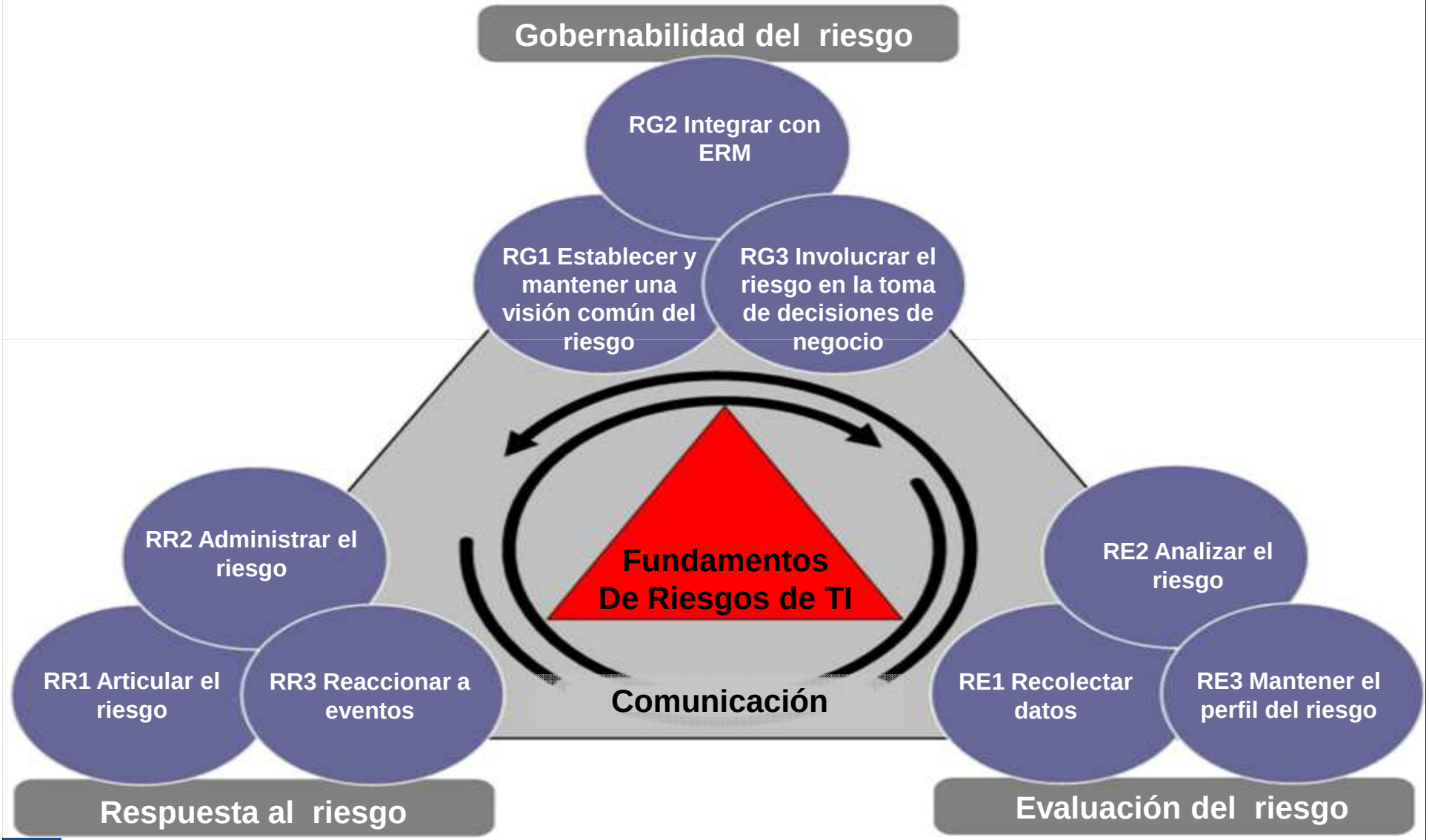
Actividades Claves

- Descripción (Objetivo de Control)
- Entradas/Salidas (Risk IT, COBIT & VAL IT)
- Objetivos y Métricas para Actividades Claves

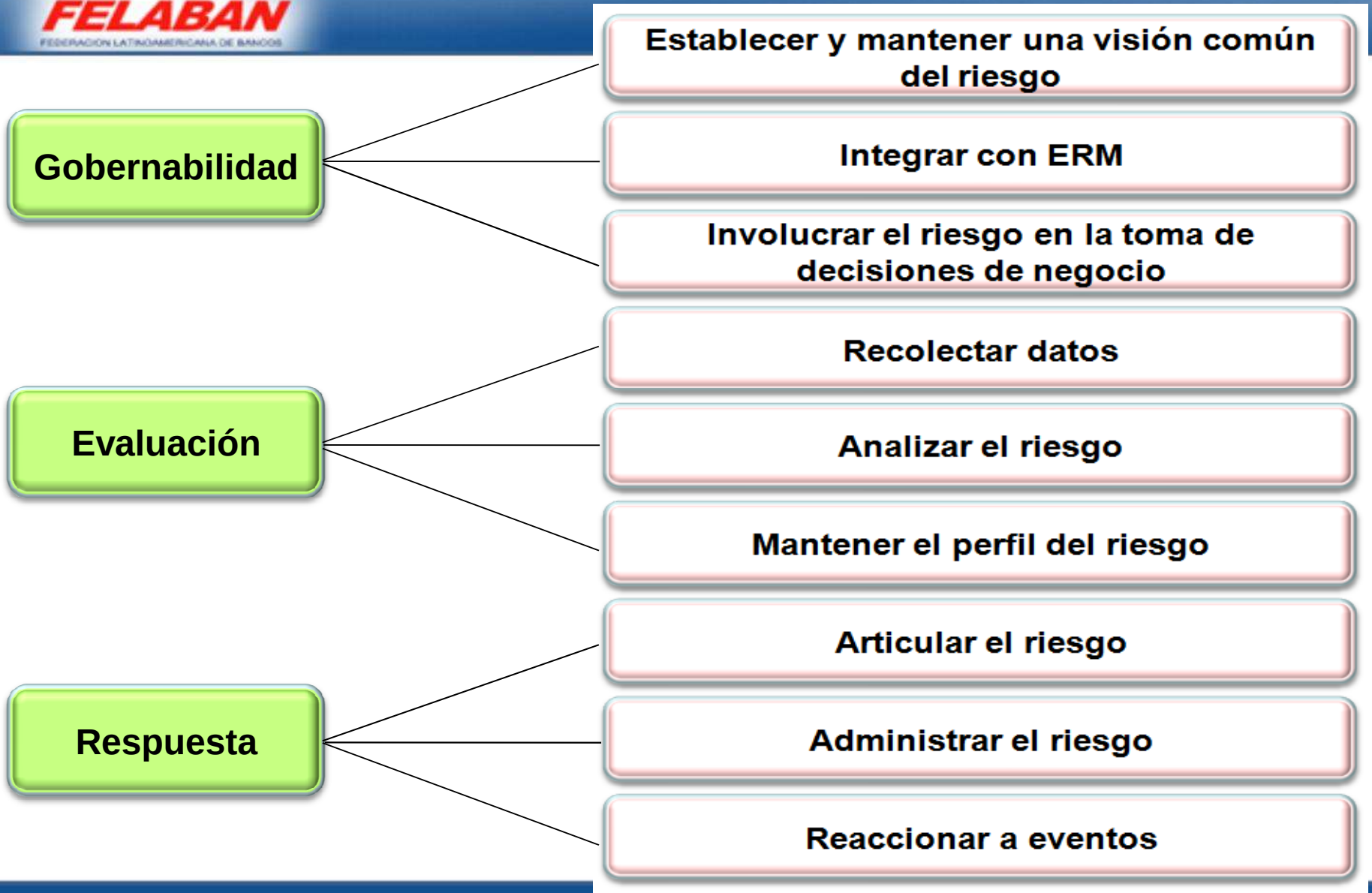
Componentes de Risk IT



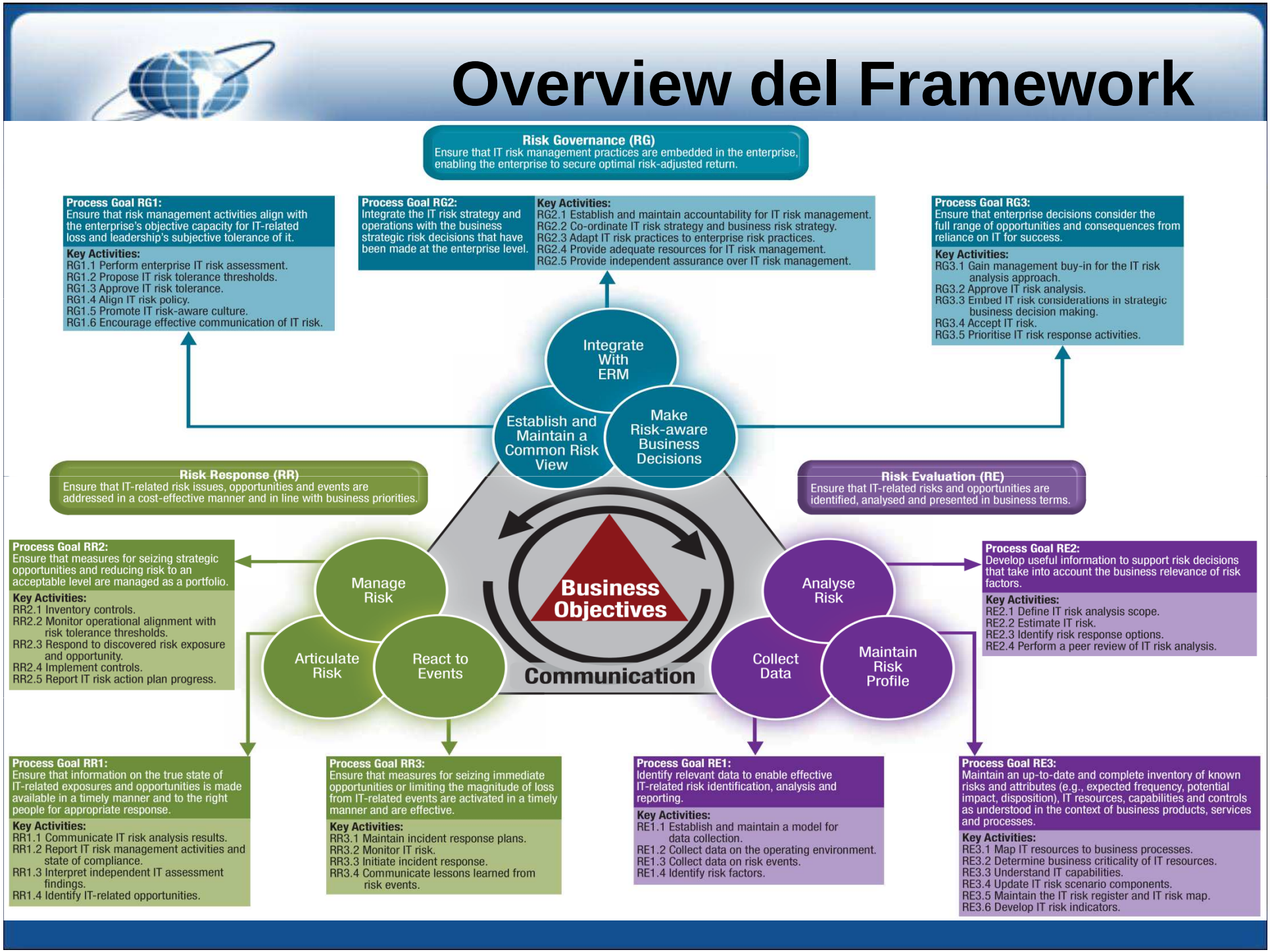
Componentes de Risk IT



Dominios y Procesos



Overview del Framework



RG Gobernabilidad del Riesgo

Risk Governance (RG)
Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.

Process Goal RG1:
Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.

Key Activities:
RG1.1 Perform enterprise IT risk assessment.
RG1.2 Propose IT risk tolerance thresholds.
RG1.3 Approve IT risk tolerance.
RG1.4 Align IT risk policy.
RG1.5 Promote IT risk-aware culture.
RG1.6 Encourage effective communication of IT risk.

Process Goal RG2:
Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.

Key Activities:
RG2.1 Establish and maintain accountability for IT risk management.
RG2.2 Co-ordinate IT risk strategy and business risk strategy.
RG2.3 Adapt IT risk practices to enterprise risk practices.
RG2.4 Provide adequate resources for IT risk management.
RG2.5 Provide independent assurance over IT risk management.

Process Goal RG3:
Ensure that enterprise decisions consider the full range of opportunities and consequences from reliance on IT for success.

Key Activities:
RG3.1 Gain management buy-in for the IT risk analysis approach.
RG3.2 Approve IT risk analysis.
RG3.3 Embed IT risk considerations in strategic business decision making.
RG3.4 Accept IT risk.
RG3.5 Prioritise IT risk response activities.

Risk Response (RR)
Ensure that IT-related risk issues, opportunities and events are

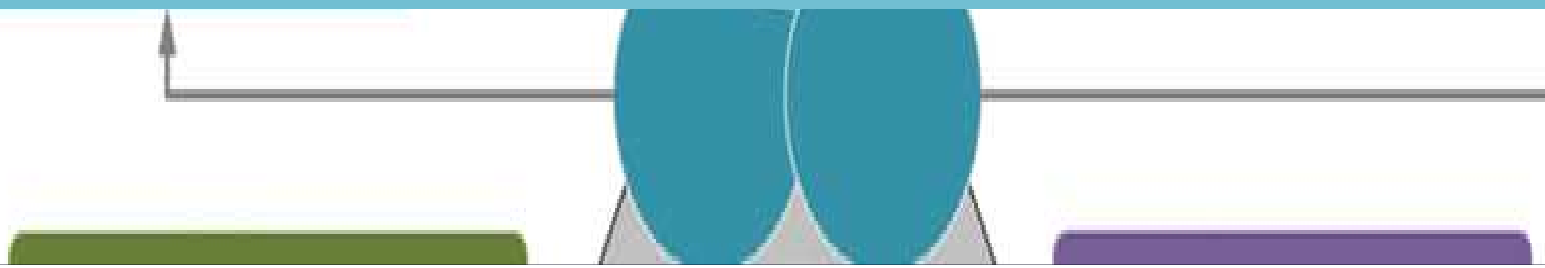
Risk Evaluation (RE)
Ensure that IT-related risks and opportunities are

RG Gobernabilidad del Riesgo
RG1 Establecer y mantener una visión común del riesgo

RG Asegurar que las prácticas de administración de riesgos de TI estén embebidas en la empresa, permitiéndole asegurar un óptimo retorno ajustado al riesgo

Asegurar que las actividades de administración de riesgos de TI estén alineados con la capacidad objetivo de la organización para pérdidas relacionadas con TI y la tolerancia subjetiva del liderazgo

RG1.1 Desarrollar un marco de trabajo de administración de riesgos de TI específico a la empresa
RG1.2 Desarrollar métodos de administración de riesgos de TI
RG1.3 Realizar una valoración de riesgos de TI a nivel empresarial
RG1.4 Proponer umbrales para la tolerancia al riesgo de TI
RG1.5 Aprobar la tolerancia al riesgo de TU
RG1.6 Alinear las declaraciones de políticas y estándares con la tolerancia al riesgo de TI
RG1.7 Promover una cultura de concientización de riesgos de TI
RG1.8 Promover una comunicación efectiva de riesgos de TI



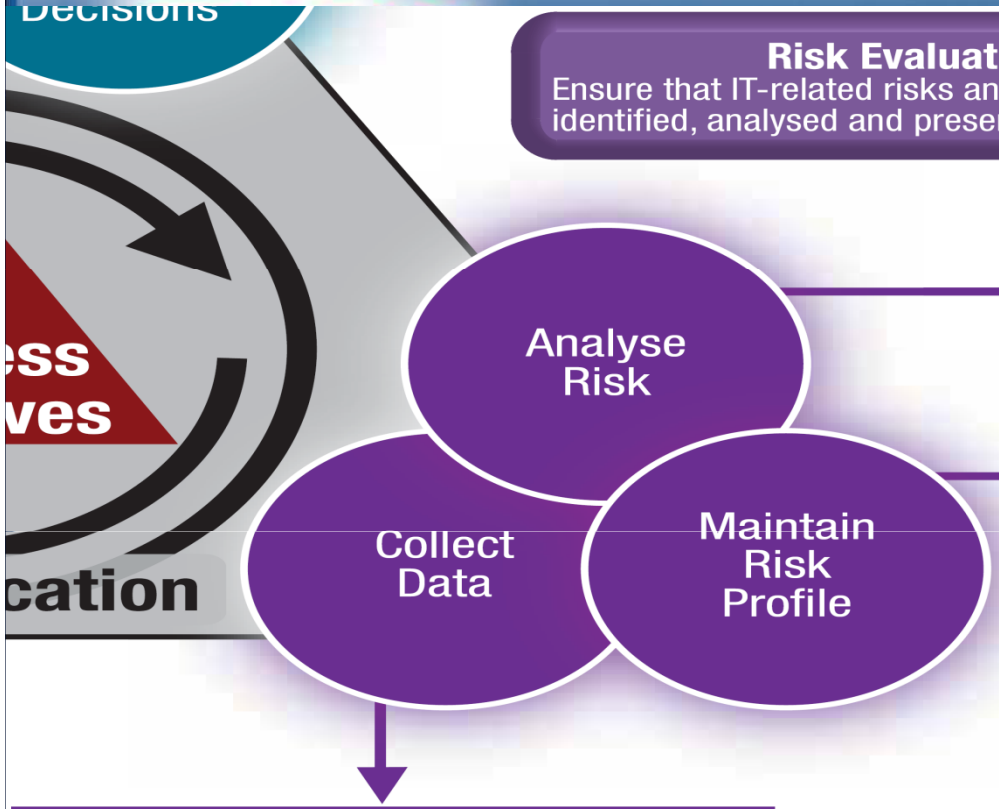
Gobernabilidad del Riesgo
Otras actividades claves de mi gusto

RG2.1 Establecer accountability a nivel empresarial para la administración del riesgo de TI (& responsabilidad)
Reconocimiento, aprobación, incentivos y sanciones
Estructuras, unidades de negocio, control del riesgo & auditoría
RG2.2 Establecer accountability para temas claves de riesgos de TI
Establecimiento & monitoreo de KRIs
Relacionar desempeño & riesgo
Roles con dominios específicos
Establecer roles en niveles más bajos
RG2.3 y RG2.4 Convergencia de prácticas
RG2.5 Suministrar adecuados recursos
Personas, procesos, sistemas de información, presupuestos
Expectativas de reguladores & auditores externos

RG3.3 Incluir los riesgos de TI en la toma de decisiones estratégicas
RG3.4 Aceptar el riesgo de TI
RG3.5 Priorizar las actividades de respuesta a los riesgos de TI

RE Evaluación del Riesgo

Risk Evaluation (RE)
Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.



Process Goal RE2:
Develop useful information to support risk decisions that take into account the business relevance of risk factors.

Key Activities:
RE2.1 Define IT risk analysis scope.
RE2.2 Estimate IT risk.
RE2.3 Identify risk response options.
RE2.4 Perform a peer review of IT risk analysis.

Process Goal RE1:
Identify relevant data to enable effective IT-related risk identification, analysis and reporting.

Key Activities:
RE1.1 Establish and maintain a model for data collection.
RE1.2 Collect data on the operating environment.
RE1.3 Collect data on risk events.
RE1.4 Identify risk factors.

Process Goal RE3:
Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services and processes.

Key Activities:
RE3.1 Map IT resources to business processes.
RE3.2 Determine business criticality of IT resources.
RE3.3 Understand IT capabilities.
RE3.4 Update IT risk scenario components.
RE3.5 Maintain the IT risk register and IT risk map.
RE3.6 Develop IT risk indicators.

RE Evaluación del Riesgo
Otras actividades claves de mi gusto

RE1.1 Establecer & mantener un modelo para la recolección de datos Internos & Externos
Factores de riesgo, eventos, problemas, amenazas, vulnerabilidades, pérdidas

RE2.1 Determinar el análisis de riesgos
RE2.2 Estimar riesgos
Frecuencia & magnitud
RE2.3 Identificar opciones de respuesta al riesgo
Aceptar, explotar, mitigar, transferir & evitar
RE2.4 Realizar una revisión de colegas de los resultados del análisis

RE3.4 Conectar los tipos de amenazas & las categorías de impacto para el negocio
RE3.5 Mantener el registro de riesgos de TI & el mapa de riesgos de TI
RE3.6 Diseñar & comunicar los indicadores de riesgo de TI

RR Respuesta al Riesgo

Risk Response (RR)
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

Process Goal RR2:
Ensure that measures for seizing strategic opportunities and reducing risk to an acceptable level are managed as a portfolio.

Key Activities:
RR2.1 Inventory controls.
RR2.2 Monitor operational alignment with risk tolerance thresholds.
RR2.3 Respond to discovered risk exposure and opportunity.
RR2.4 Implement controls.
RR2.5 Report IT risk action plan progress.

Process Goal RR1:
Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.

Key Activities:
RR1.1 Communicate IT risk analysis results.
RR1.2 Report IT risk management activities and state of compliance.
RR1.3 Interpret independent IT assessment findings.
RR1.4 Identify IT-related opportunities.

Process Goal RR3:
Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT-related events are activated in a timely manner and are effective.

Key Activities:
RR3.1 Maintain incident response plans.
RR3.2 Monitor IT risk.
RR3.3 Initiate incident response.
RR3.4 Communicate lessons learned from risk events.

RR Respuesta al Riesgo
Otras actividades claves de mi gusto

RR1.1 Reportar los resultados del análisis de riesgos de TI
Riesgos & oportunidades
RR1.2 Reportar las actividades de administración de riesgos & el estado de cumplimiento

RR2.2 Monitorear el alineamiento operacional con la tolerancia
RR2.4 Implementar controles
RR2.5 Reportar el progreso del plan de acción

RR3.1 Mantener los planes de respuesta a incidentes
Contabilizar?
RR3.4 Conducir revisiones post-mortem de los incidentes relacionaos con TI

Guía de Técnicas

Figure 14—Techniques Guide Overview

Domain/Process	Risk Governance			Risk Evaluation			Risk Response		
Technique/Guidance	RG1 Establish and Maintain a Common Risk View	RG2 Integrate with Enterprise Risk Management	RG3 Make Risk-aware Business Decisions	RE1 Collect Data	RE2 Analyse Risk	RE3 Maintain Risk Profile	RR1 Articulate Risk	RR2 Manage Risk	RR3 React to Events
1 Defining a risk universe and scoping	■	■	■						
2 Constructing risk scenarios				■	■	■	■		
3 Sample generic IT risk scenarios				■	■	■	■		
4 Describing risk—expressing impact in business terms	■	■			■		■		
5 Describing risk—COBIT business goals mapping with other impact criteria	■	■			■		■		
6 Describing risk—qualitative and quantitative methods	■	■			■		■	■	
7 Describing risk—expressing impact	■	■			■		■	■	
8 Describing risk—expressing frequency	■	■			■		■	■	
9 Risk factors in the risk assessment process	■	■	■		■		■	■	
10 Describing risk—risk maps, risk register?	■	■	■		■	■	■		
11 Defining risk appetite and risk tolerance	■	■	■		■	■	■		
12 A risk analysis workflow					■				
13 Risk aggregation					■	■	■	■	
14 Key risk indicators and risk reporting	■	■	■	■			■	■	
15 Risk response and prioritisation				■				■	■
16 Using COBIT and Val IT to map controls to risk scenarios				■				■	■
17 Risk profiles	■	■				■	■		
18 Risk communication flows	■	■	■	■	■	■	■	■	■
Appendix I—How COBIT and Val IT practices can help manage risk								■	■
Appendix II—Risk management principles and practices in Risk IT vs. other frameworks	■	■	■	■	■	■	■	■	■

Técnicas/Guías vs. Dominios/Procesos

	Gobierno del Riesgo			Evaluación del Riesgo			Respuesta al Riesgo		
	RG1 Establecer y mantener una visión común del riesgo	RG2 Integrar con la Administración de Riesgos empresarial	RG3 Tomar decisiones de negocio con conciencia del riesgo	RE1 Recolectar datos	RE2 Analizar riesgos	RE3 Mantener el perfil del riesgo	RR1 Articular el riesgo	RR2 Administrar el riesgo	RR3 Reaccionar a eventos
1	Definición del universo de riesgos y del alcance de la administración de riesgos								
2	Construcción de escenarios de riesgo								
3	Descripción del riesgo – expresando el impacto en términos de negocio								
4	Muestra genérica de escenarios de riesgo de TI								
5	Descripción del riesgo – mapeando objetivos de negocio de COBIT con otros criterios								
6	Descripción del riesgo – métodos cualitativos y cuantitativos								
7	Descripción del riesgo – expresión de impactos								
8	Descripción del riesgo – expresión de la frecuencia								
9	Factores de riesgo en el proceso de valoración del riesgo								
10	Descripción del riesgo – mapas de riesgo, registro del riesgo?								

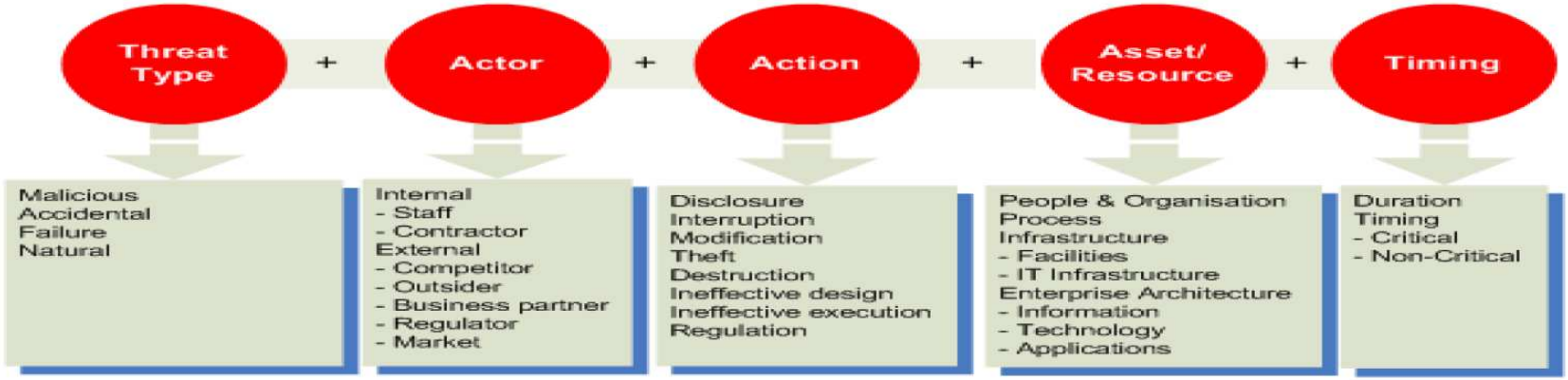
Técnicas/Guías vs. Dominios/Procesos

	Gobierno de riesgo			Evaluación del riesgo			Respuesta al Riego		
	RG1 Establecer y mantener una visión común del riesgo	RG2 Integrar con la Administración de Riesgos empresarial	RG3 Tomar decisiones de negocio con conciencia del riesgo	RE1 Recolectar datos	RE2 Analizar riesgos	RE3 Mantener el perfil del riesgo	RR1 Articular el riesgo	RR2 Administrar el riesgo	RR3 Reaccionar a eventos
1 1	Definición del apetito y la tolerancia al riesgo								
12	Un flujo de trabajo del análisis del riesgo								
13	Agrupamiento de riesgos								
14	Indicadores claves de riesgo y reporte de riesgos								
15	Respuesta al riesgo y priorización								
16	Uso de COBIT y VAL IT para mapear controles en escenarios de riesgo								
17	Perfiles de riesgo								
18	Flujos de comunicación de riesgos								
Ap I	Cómo las prácticas de COBIT y VAL IT pueden ayudar a administrar riesgos								
Ap II	Los principios y prácticas de administración de riesgos en RISK IT vs. Otros frameworks								

1 Definición del universo de riesgos y del alcance de la administración de riesgos

- Análisis de la cadena de valor empresarial
- Análisis de procesos y procedimientos de negocio
- Mapeo de recursos de TI & procesos de negocio

2 Escenarios de Riesgo



3 y 5. Descripción del riesgo – expresando el impacto en términos de negocio

Pérdida financiera

Pérdida de clientes

Pérdida de continuidad

Económicas
Imagen
Servicio a clientes
Cumplimiento

OBJETIVOS DE NEGOCIO

4A (Westerman/Hunter)
- Agilidad
- Exactitud
- Acceso
- Disponibilidad

BSC (Objetivos de negocio de COBIT)
- Financiero
- Cliente
- Interno
- Crecimiento

O

Criterios de Información COBIT
- Efectividad
- Eficiencia
- Confiabilidad
- Integridad
- Confidencialidad
- Cumplimiento
- Disponibilidad

Criterios de Impacto BSC Extendido
- Valor de las acciones
- Participación en el mercado
- Ingresos/Rentabilidad
- Costo de capital
- Satisfacciòn del cliente
- Impacto regulatorio
- Recursos
- Ventaja competitiva
- Reputaciòn

Destrucción del centro de cómputo → Incendio → Tormentas eléctricas

6. Descripción del riesgo - Métodos cualitativos y cuantitativos

- Impacto
  - Alto, Medio, Bajo
  - 1 .. X
  - $
  - Variables

- Probabilidad
  - Alto, Medio, Bajo
  - 1 .. X
  - Frecuencia, Probabilidad
  - Variables

- Delphi
- ALE (Pérdida anual esperada)
- Montecarlo

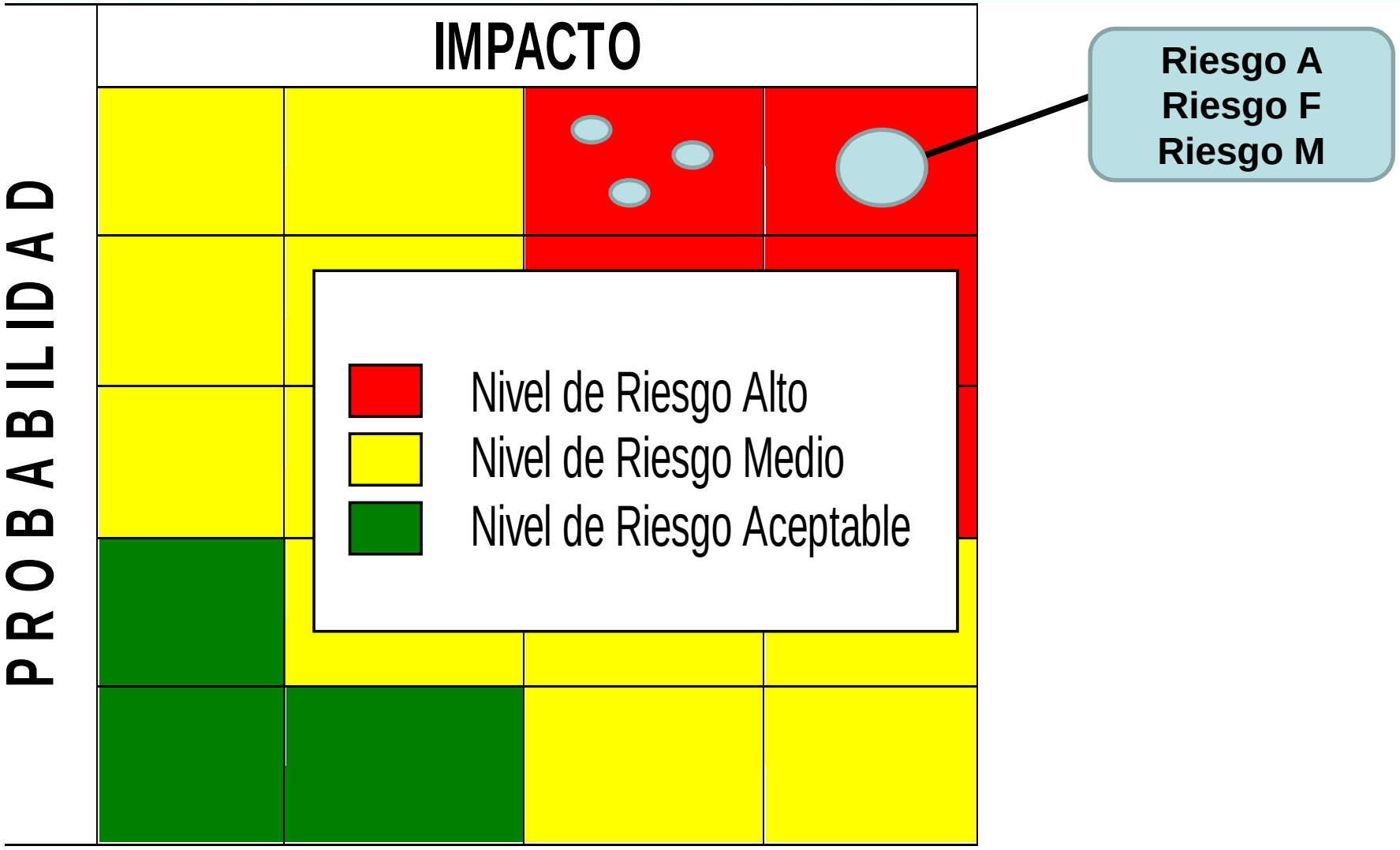
7 y 8. Descripción del riesgo - expresión de Impactos y Frecuencias

- $
- Interpretación
  - 1 escala
  - Varias escalas
  - Método de scoring sencillo
  - Método de scoring con puntajes

PERDIDA DE IMAGEN		
Descripción	Cuantificación	Impacto
Se entiende como la posibilidad de que se vea perjudicada la imagen organizacional	1	A nivel Departamental
	2	A nivel Organizacional
	3	A nivel País
	4	A nivel Latinoamérica
	5	A nivel Mundial

Cuantificación	Probabilidad
1	Rara Vez
2	Poco Probable
3	Posible
4	Probable
5	Siempre

10. Descripción del riesgo - Mapas de riesgo



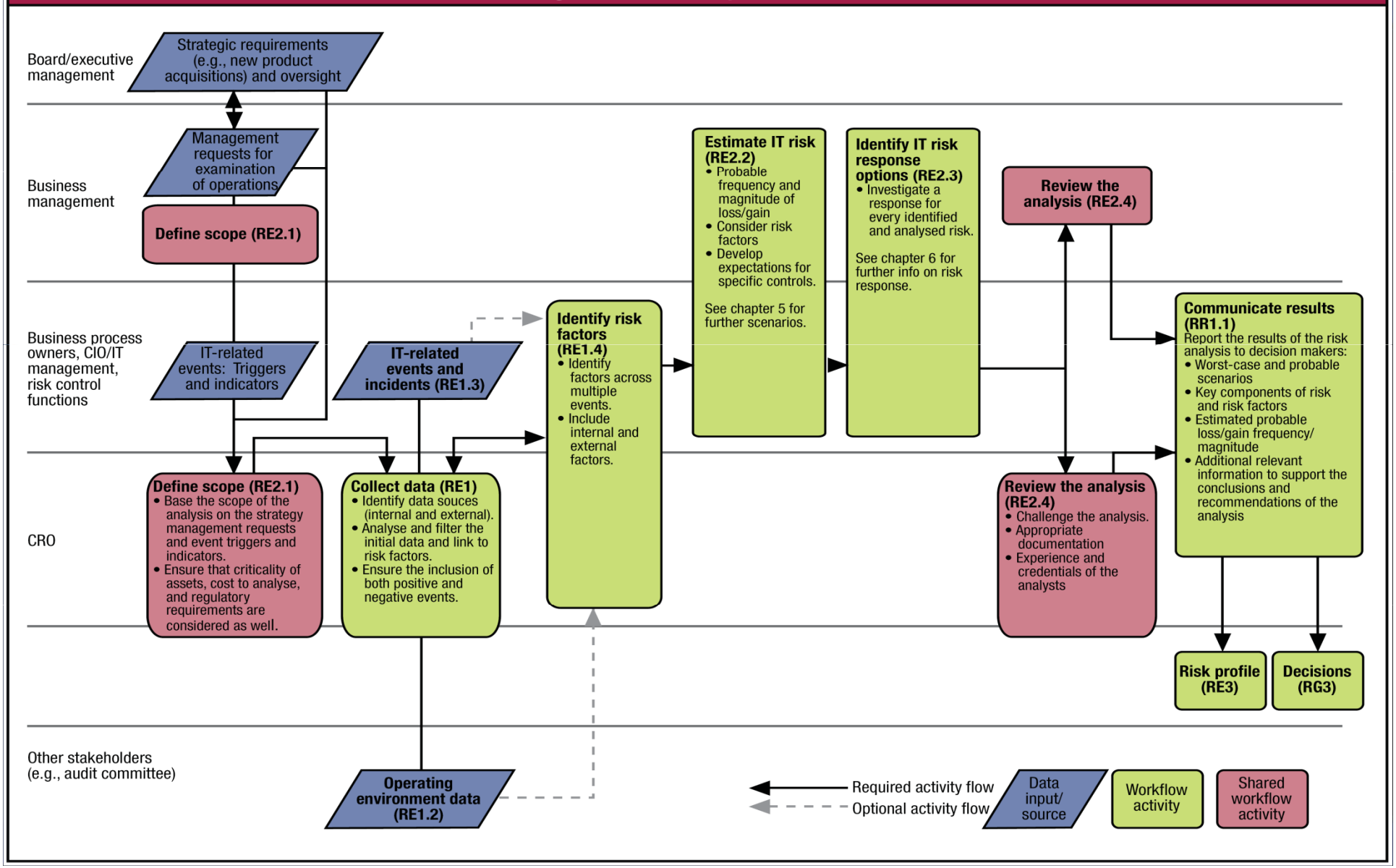
11. Definiendo el apetito y la tolerancia al riesgo

- **Apetito = Monto general de riesgo que una empresa u otra entidad está dispuesta a aceptar en la búsqueda de su misión (o visión)**

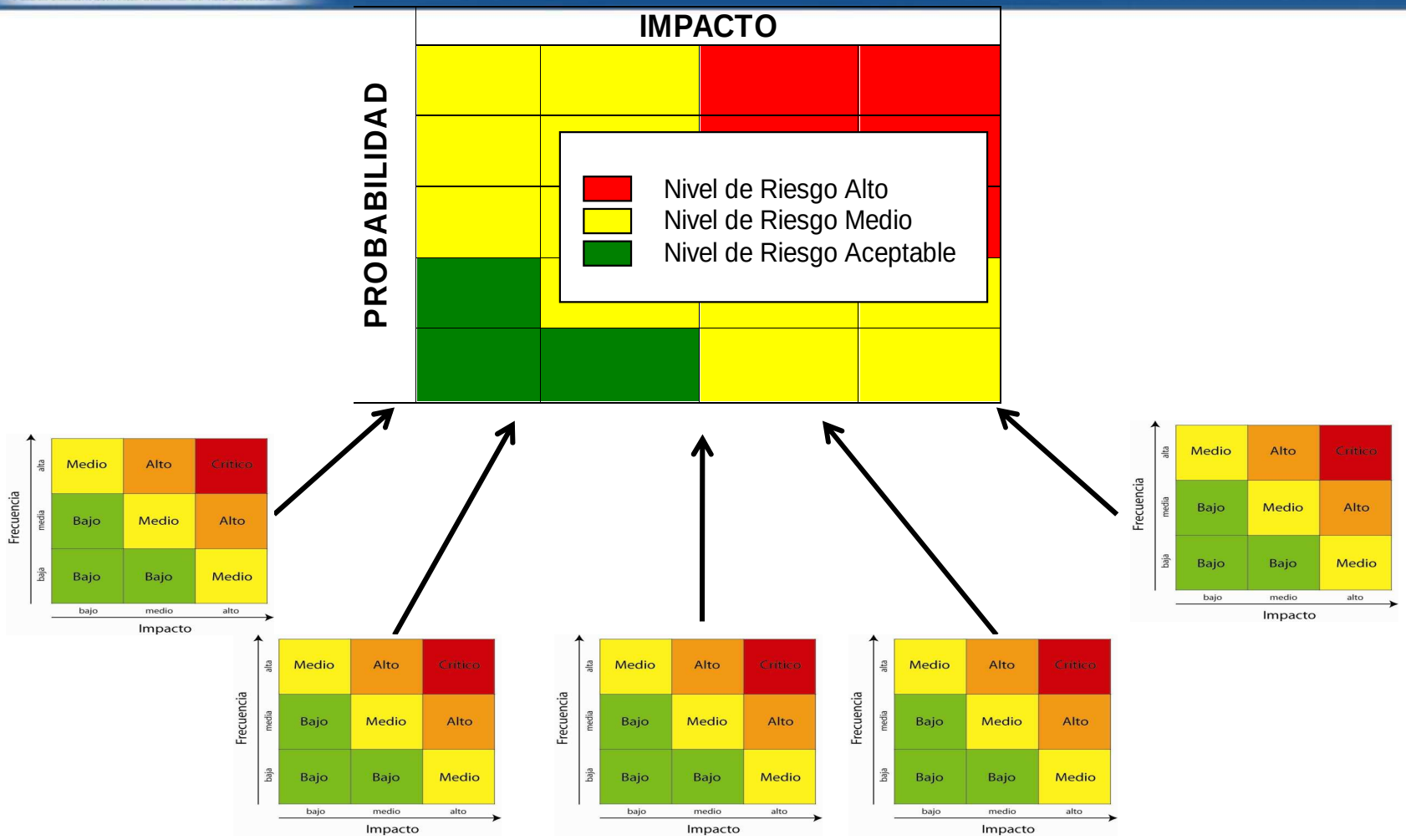
- **Tolerancia = Variación relativa al logro de un objetivo (normalmente es medida de mejor forma utilizando las mismas unidades que se utilizan para medir el objetivo relacionado)**
  - **Región intolerable**
  - **Región tolerable o ALARP (as low as reasonably practicable)**
  - **Región aceptable**

COSO ERM

12. El flujo de trabajo del análisis de riesgo



13. Agrupamiento de riesgos



14. Indicadores clave de riesgos y reporte de riesgos

- **KRI – Key Risk Indicator**
  - **Son indicadores que proporcionan una alerta temprana**
  - **Reportan información observable, no realizan estimaciones futuras**

15. Opciones y Priorización de las Respuestas al Riesgo

Factores influyentes en la selección y priorización de la Respuesta al riesgo

- Costo de respuesta para reducir el riesgo dentro de niveles tolerables
- Importancia del riesgo
- Capacidad para implementar la respuesta
- Efectividad de la respuesta
- Eficiencia de la respuesta

Riesgos excediendo el nivel de tolerancia

→ Seleccionar opciones de respuesta al riesgo ←

Respuestas al Riesgo

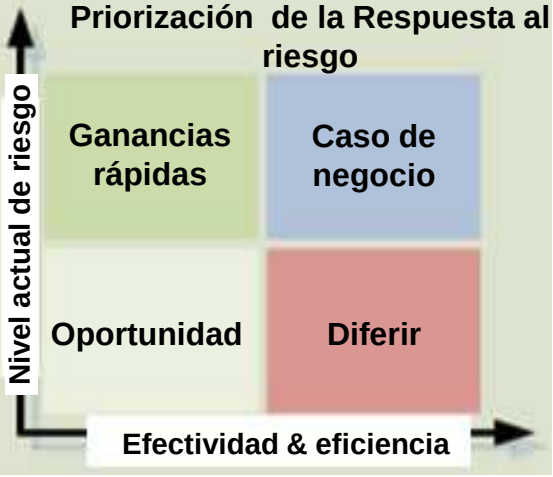
→ Priorizar opciones de respuesta al riesgo ←

Respuestas al Riesgo Priorizadas

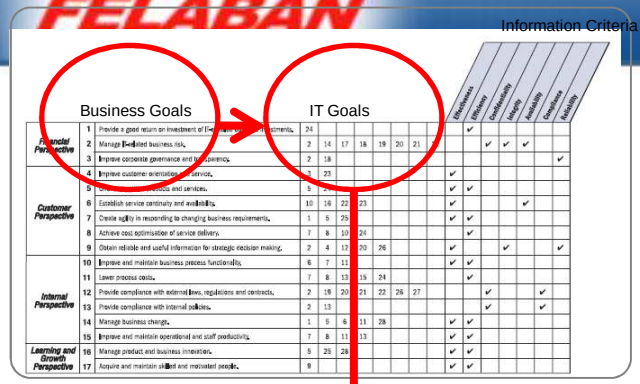
Opciones de Respuesta al riesgo

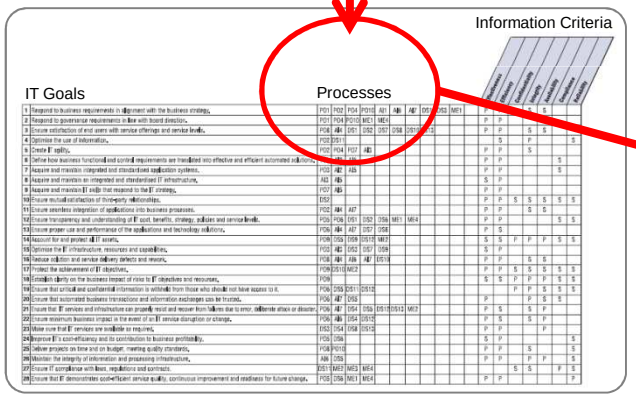
Mitigar	Evitar
Transferir / Compartir	Aceptar

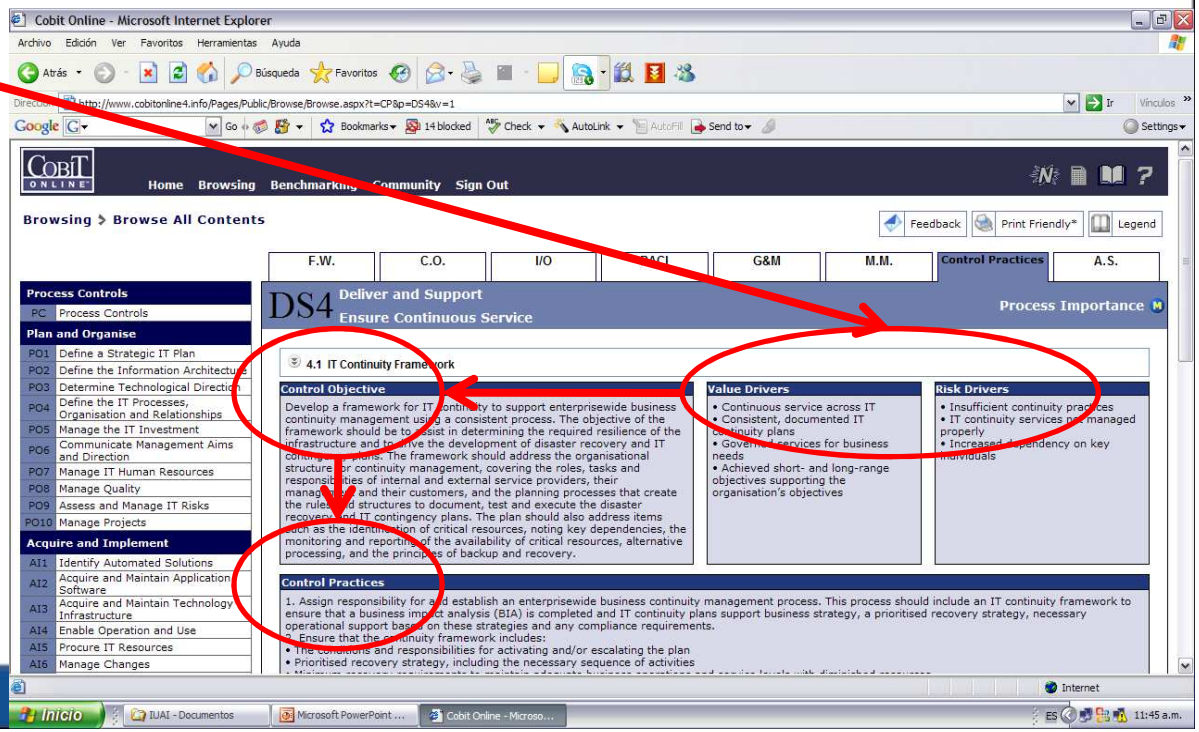
Priorización de la Respuesta al riesgo



16. Uso de COBIT & VAL IT

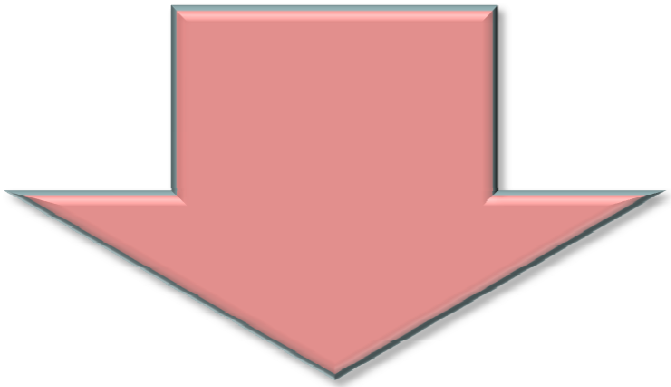






Riesgo y Oportunidad

TI como Inhibidor o Destructor de Valor

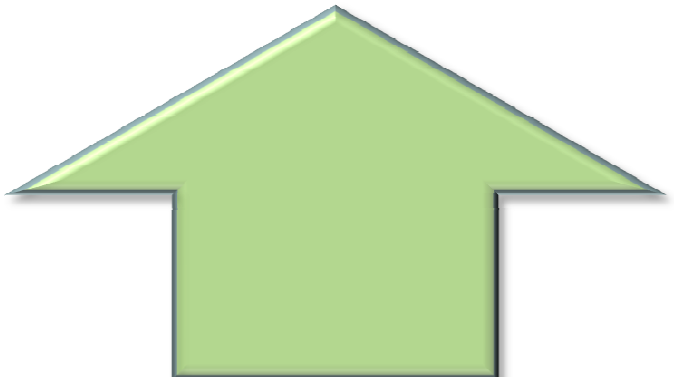


Riesgo de TI

- **Eventos relacionados con TI adversos que destruyen el valor**
- **Valor de negocio reducido o no alcanzado mediante TI**
- **Oportunidades de negocio asistidas por TI omitidas**

Oportunidad de TI

- **Identificar nuevas oportunidades de negocio mediante el empleo de TI**
- **Mayor valor de negocio a través del uso óptimo de las capacidades de TI**



TI como Habilitador de Valor

16. Uso de COBIT & VAL IT

Description

An explanation of the initiative's sponsors, the purpose and scope of the initiative, and the timeframe for implementation

Business Impact

Revenue Generation

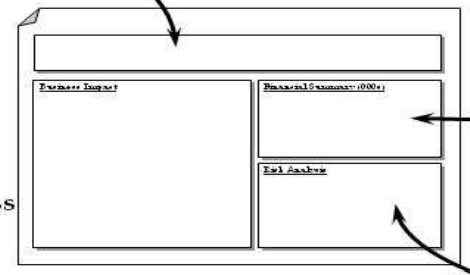
Reflects the expected impact of the program on increasing the volume and quality of new business

Product/Service Quality

Reflects the expected impact of the program on the speed and overall quality of service delivered to customers

Operating Efficiency

Reflects the expected impact of the program on the ability to contain and reduce costs



Financial Summary

A breakdown of the initiative's financial components, such as NPV, payback, and expected benefits and costs. All figures are very preliminary and are intended only for prioritization of initiatives. For comparative purposes, all initiatives are assumed to launch in 1998

Risk Analysis

Risk of Doing, Risk of Not Doing

Reflects the overall risk involved in choosing to implement or not implement the initiative

Figure 7—Balance Between Risk and NPV Example

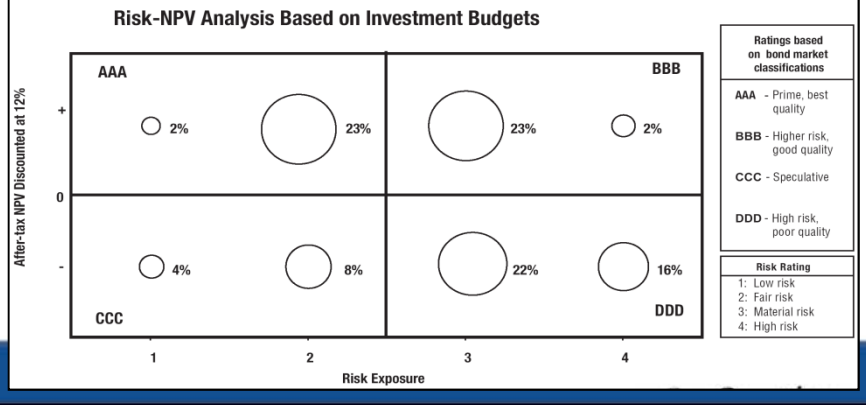
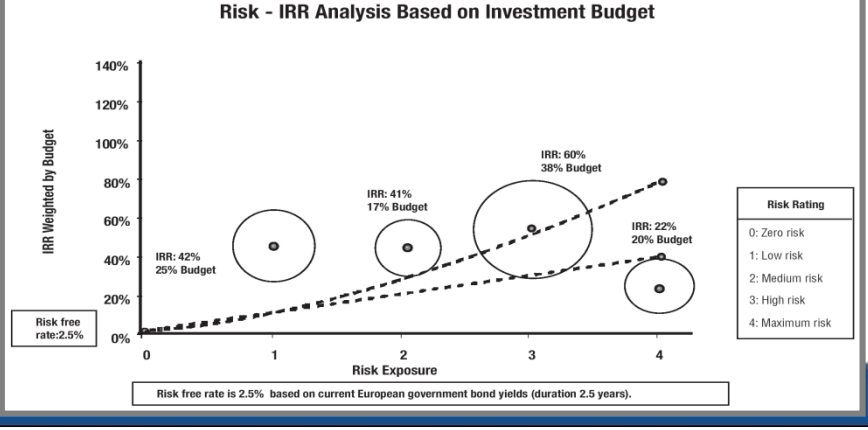
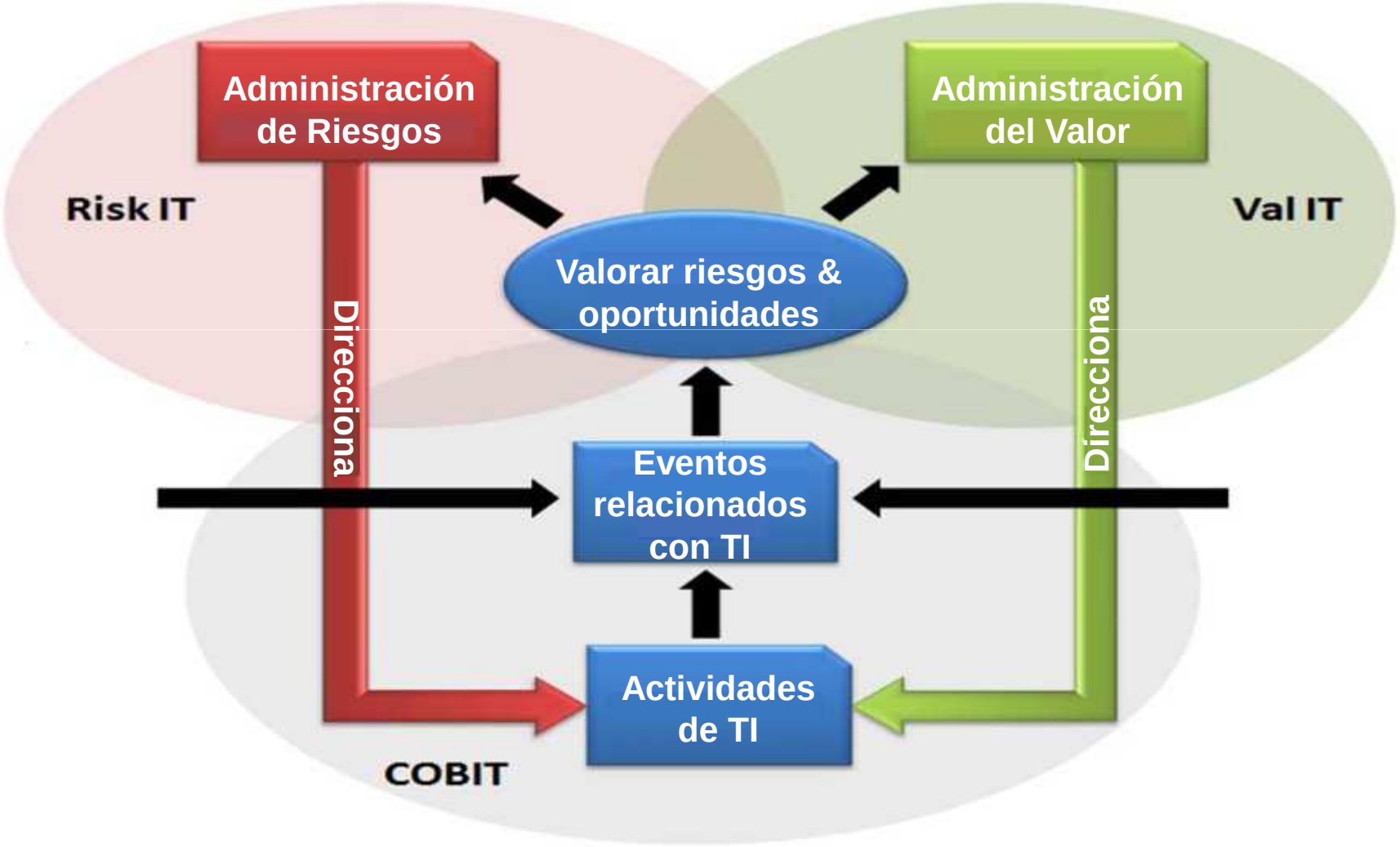


Figure 8—Efficient Frontier Risk-adjusted Returns Example



Riesgo y Oportunidad y los 3 Frameworks del ITGI



Apoyo adicional de ISACA

- **ISACA apoya la administración de riesgos relacionados con TI, en los siguientes documentos:**
  - **COBIT 4.1 – Proceso PO9**
  - **IT Governance Domains and Practices – IT Risk Management**
  - **Prácticas de Control**
  - **Guía de Aseguramiento**
  - **Controles de Aplicación**
  - **Objetivos de control para SOX**
  - **Objetivos de Control para Basilea II**
  - **COBIT Security Baseline**

The Risk IT Framework

- **RISK IT complementa a COBIT, el cual:**
  - ✓ **proporciona un marco global para la entrega de servicios de información de alta calidad**
  - ✓ **establece buenas prácticas genéricas para la administración del riesgo**

- **RISK IT establece buenas prácticas específicas para gobernar, identificar y administrar los riesgos de TI**

The Risk IT Framework

- **RISK IT:**
  - ✓ **Facilita obtener una visión exacta de los riesgos relacionados a TI**
  - ✓ **Ofrece guías sobre como administrar los riesgos de TI desde el principio hasta el fin**
  - ✓ **Se integra con las estructuras de riesgo y de cumplimiento dentro de la empresa**
  - ✓ **Promueve la propiedad de los riesgos en la organización**
  - ✓ **Facilita obtener el perfil de riesgo para entenderlo mejor**
  - ✓ **Permite tomar decisiones bien informadas sobre la extensión, el apetito y la tolerancia al riesgo**
  - ✓ **Permite entender como responder al riesgo**

Conclusiones
Factores Críticos de Éxito

- Compromiso de las directivas de la Organización
- Guía Metodológica – Risk IT
- Facilitadores expertos en Administración de Riesgos
- SW de apoyo a la implantación de la Guía Metodológica

Conclusiones
Beneficios para la Organización

Conclusiones
Beneficios para el Departamento de Auditoría

Estandarización y formalización del método de trabajo

Alimentación del plan anual de actividades

Apoyo al cumplimiento de los objetivos del Departamento

BENEFICIOS

Integración del control con las políticas directivas

Mayor efectividad de nuestras asesorías

Mayor cobertura de la administración de Riesgos

Enfoque hacia los riesgos del Negocio

FELABAN
FEDERACIÓN LATINOAMERICANA DE BANCOS

Preguntas ?