Definición de Estrategias de Seguridad de la Información

Wilmar Arturo Castellanos

- Esta presentación se encuentra basada en el material público existente en Internet (SABSA, ISACA, IT Governance Institute, entre otros).
- La propiedad de la información aquí presentada es propiedad de sus respectivos titulares. El autor aporta sus interpretaciones de esta información con base en su experiencia.

Agenda

- Security Governance y Estrategia de Seguridad
- Planeación estratégica de seguridad
- Marcos de referencia para la planeación estratégica de seguridad
- Desarrollo de la estrategia de seguridad

Security Governance y Estrategia de seguridad

Security Governance y Estrategia de seguridad

- "Information Security Governance es responsabilidad del consejo de administración y de la dirección ejecutiva. Debe ser una parte integral y transparente del gobierno corporativo. Consiste en el liderazgo y estructuras de organización y procesos que aseguran que la **seguridad de información sustenta los objetivos y estrategias de la organización**".

IT Governance Institute

Security Governance y Estrategia de seguridad

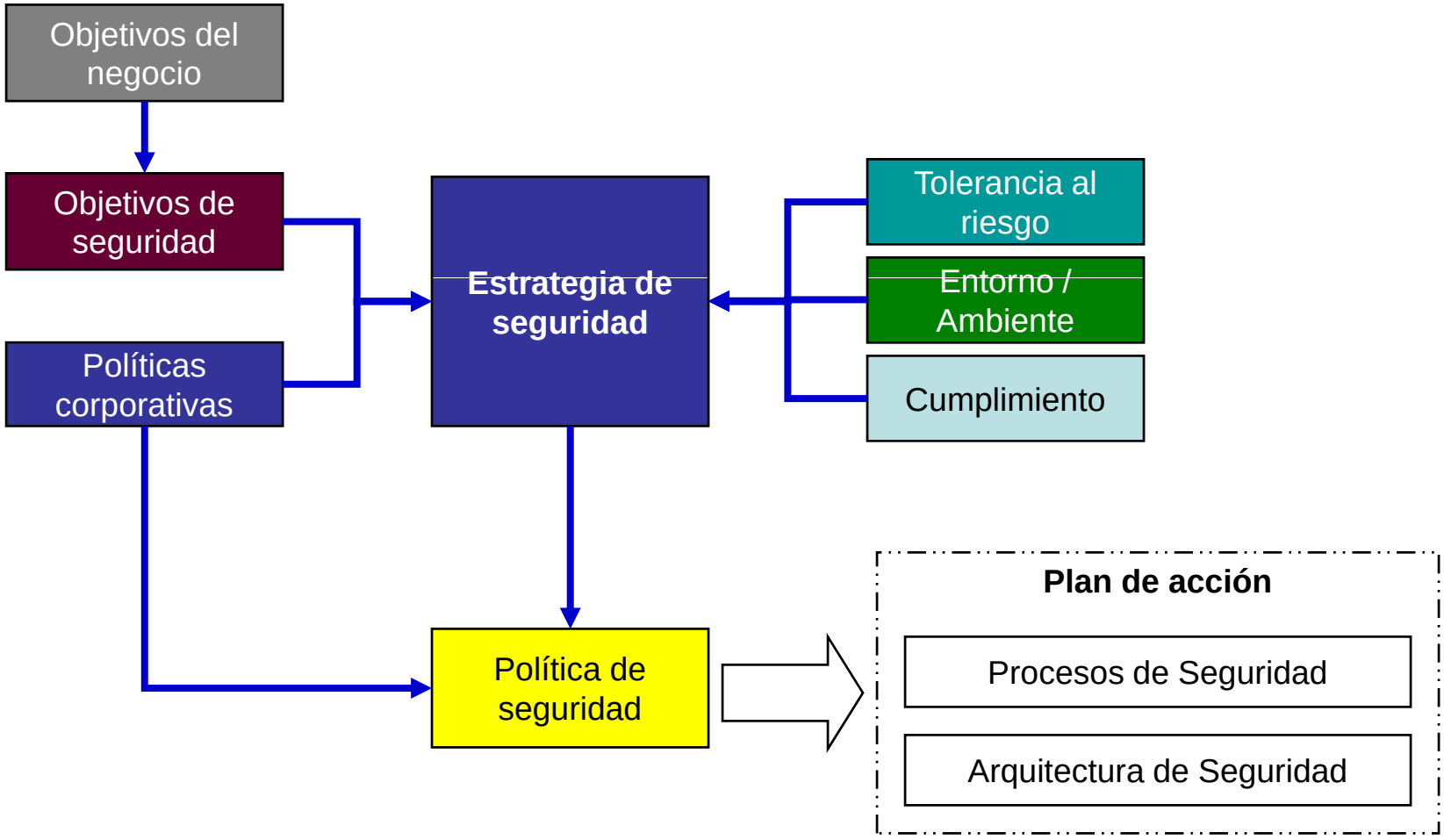
- El objetivo del security governance es garantizar que existe y se mantiene un marco de referencia con el fin de asegurar que las **estrategias de seguridad de la información** están alineadas con los **objetivos del negocio** y que son consistentes con la regulación y leyes aplicables.

Security Governance y Estrategia de seguridad

El **alineamiento estratégico** de los objetivos de la seguridad de la información con los objetivos del negocio es un elemento crítico para un gobierno efectivo de seguridad.

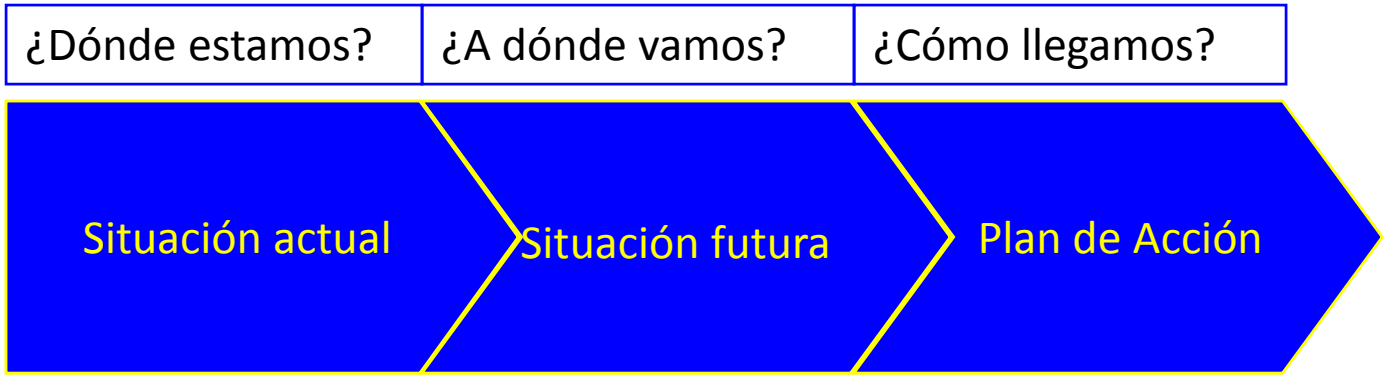
Security Governance y Estrategia de seguridad

La **estrategia de seguridad de la información** es un patrón frente al cual una compañía toma sus decisiones de protección de la información con base en sus objetivos y propósito. El proceso de toma de decisiones requiere de la definición de una **política** y de un **plan de acción** para alcanzar los objetivos de seguridad de la información. La estrategia permite definir los **procesos y estructuras** requeridos para satisfacer las necesidades de seguridad de la información de los accionistas, empleados, clientes y comunidad.


Objetivos del negocio
Objetivos de seguridad
Políticas corporativas
Estrategia de seguridad
Tolerancia al riesgo
Entorno / Ambiente
Cumplimiento
Política de seguridad
Plan de acción
Procesos de Seguridad
Arquitectura de Seguridad

Planeación estratégica de seguridad

Proceso estándar de una planeación estratégica



Alineamiento estratégico, análisis de la situación actual y definición de la futura

COBIT	SABSA *	ISO27002
CMM	GAISP	Otros

* Sherwood Applied Business Security Architecture

Objetivo de la estrategia de seguridad

Proteger los recursos de información de la organización.

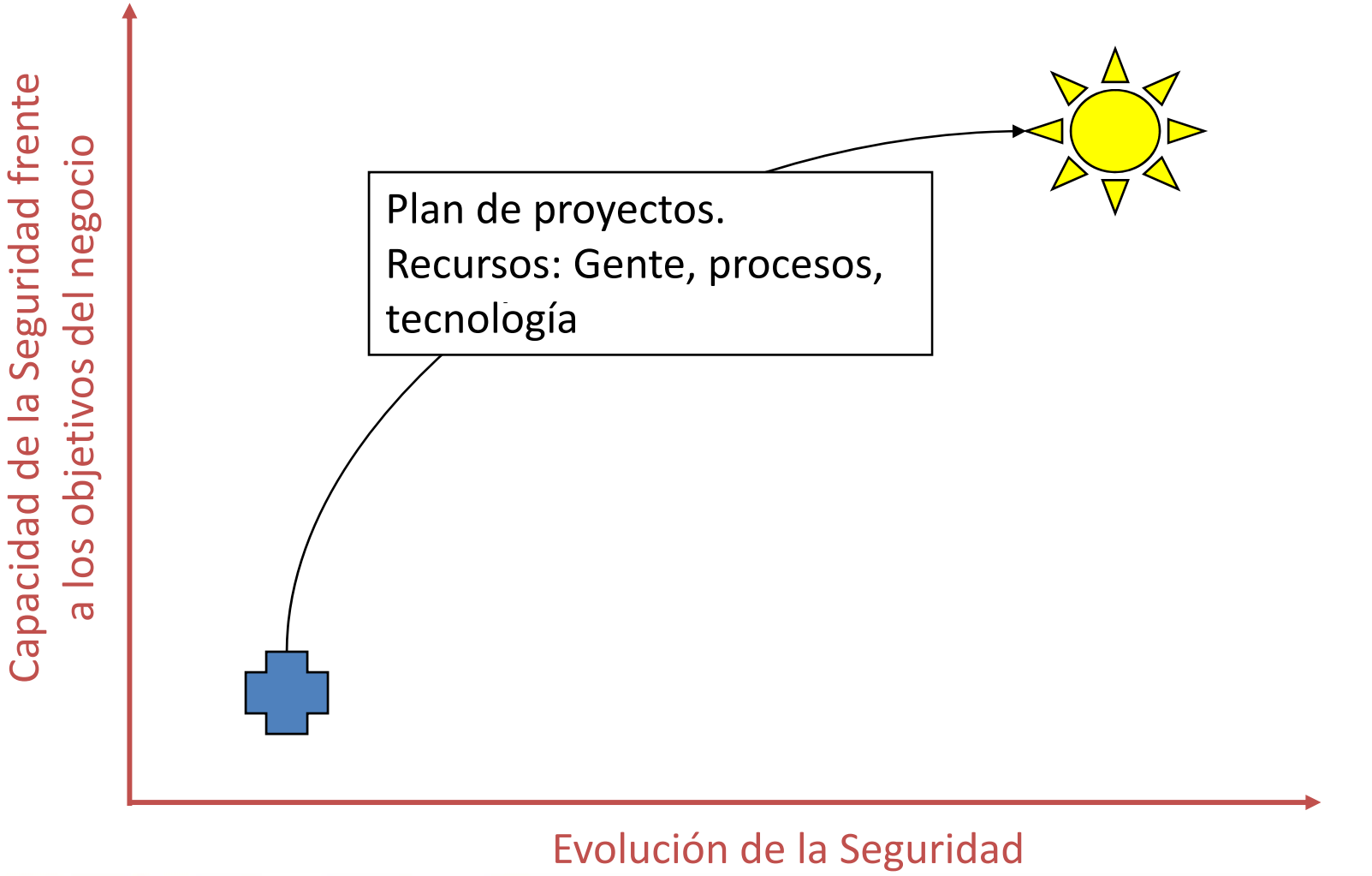
¿Qué es Proteger?

- COBIT: Criterios de información, objetivos de control
- ISO27002: Objetivos de control y controles
- SABSA (porqué, cómo, quién, dónde), otros

¿Cuáles Recursos de Información?

- ISO27002 – 7.1 y 7.2 – Responsabilidad y Clasificación
- COBIT: Aplicaciones, Información, Infraestructura, Gente
- SABSA (qué, cuándo), otros

Alineamiento estratégico


Capacidad de la Seguridad frente a los objetivos del negocio
Plan de proyectos.
Recursos: Gente, procesos, tecnología
Evolución de la Seguridad

Proceso estándar de una planeación estratégica

¿Dónde estamos?

Situación actual

- Entender los objetivos y estrategia del negocio.
- Identificar, analizar y evaluar la situación actual de la seguridad de la información.
- Definir los requerimientos de seguridad para el negocio.

Proceso estándar de una planeación estratégica

¿A dónde vamos?

- Definir la situación deseada de la seguridad – objetivos estratégicos.
- Establecer la brecha frente a la situación actual.

Proceso estándar de una planeación estratégica

¿Cómo llegamos?

Plan de Acción

- Definir el plan de acción para cerrar la brecha:
  - Acciones rápidas
  - Proyectos
    - Objetivos, recursos, beneficios
  - Programas
    - Programa de seguridad
    - Programa de conciencia, educación y entrenamiento

Marcos de referencia para la planeación estratégica de seguridad

SABSA

Punto de vista del negocio	Arquitectura contextual
Punto de vista de los arquitectos	Arquitectura conceptual
Punto de vista de los diseñadores	Arquitectura lógica
Punto de vista de los implementadores	Arquitectura física
Punto de vista del comerciante	Arquitectura de componente
Punto de vista del Gerente de infraestructura	Arquitectura operacional

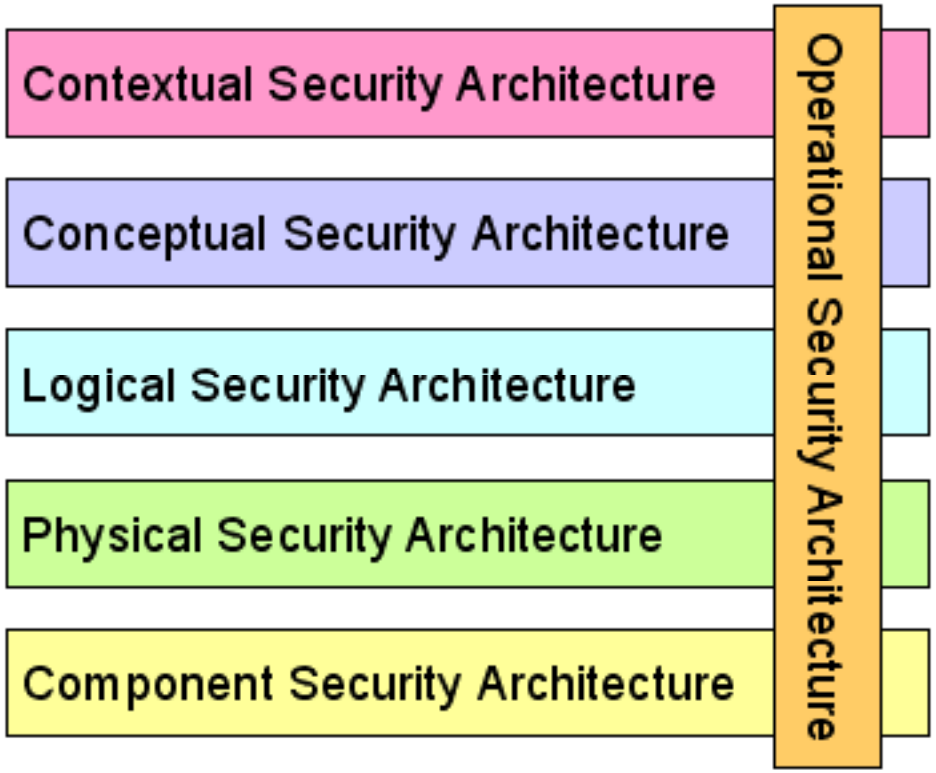
SABSA

Arquitectura contextual	Describe los requerimientos de negocio
Arquitectura conceptual	La visión estratégica a alto nivel
Arquitectura lógica	Servicios de seguridad
Arquitectura física	Mecanismos de seguridad
Arquitectura de componente	Productos de seguridad y herramientas
Arquitectura operacional	Administración y operación de la seguridad

SABSA

Qué estoy tratando de asegurar	Los ACTIVOS a proteger
Cómo estamos tratando de hacerlo?	Las FUNCIONES asociadas con los activos
Donde se intentará asegurar?	La UBICACIÓN que se asegurará
Quién está involucrado?	GENTE y aspectos de la organización
Cuándo se debe aplicar seguridad	El TIEMPO preciso
Porqué tenemos que hacerlo?	La MOTIVACIÓN

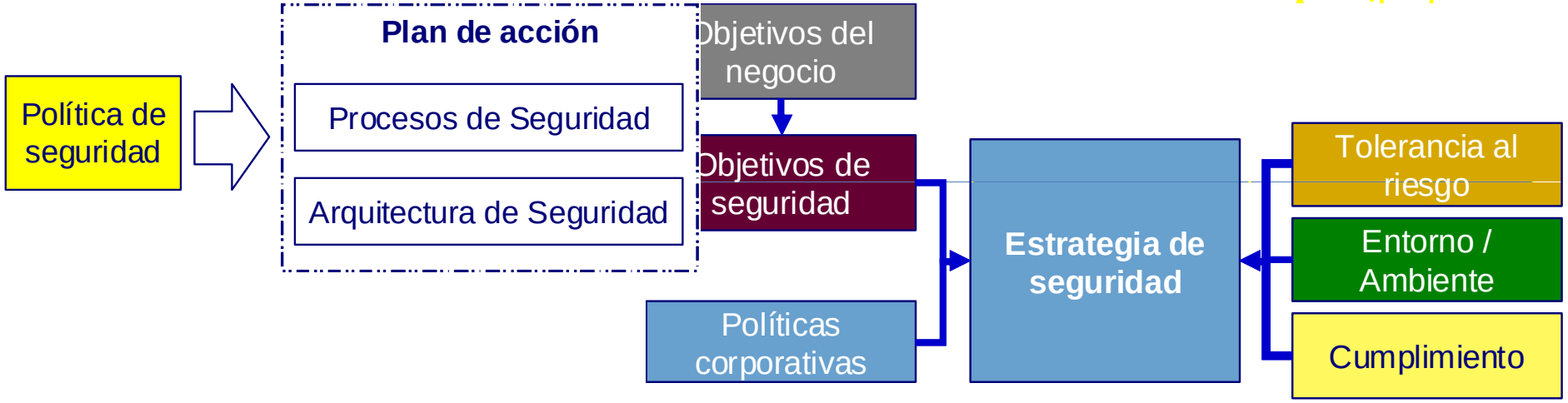
SABSA


Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Operational Security Architecture

SABSA – Matriz de desarrollo

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

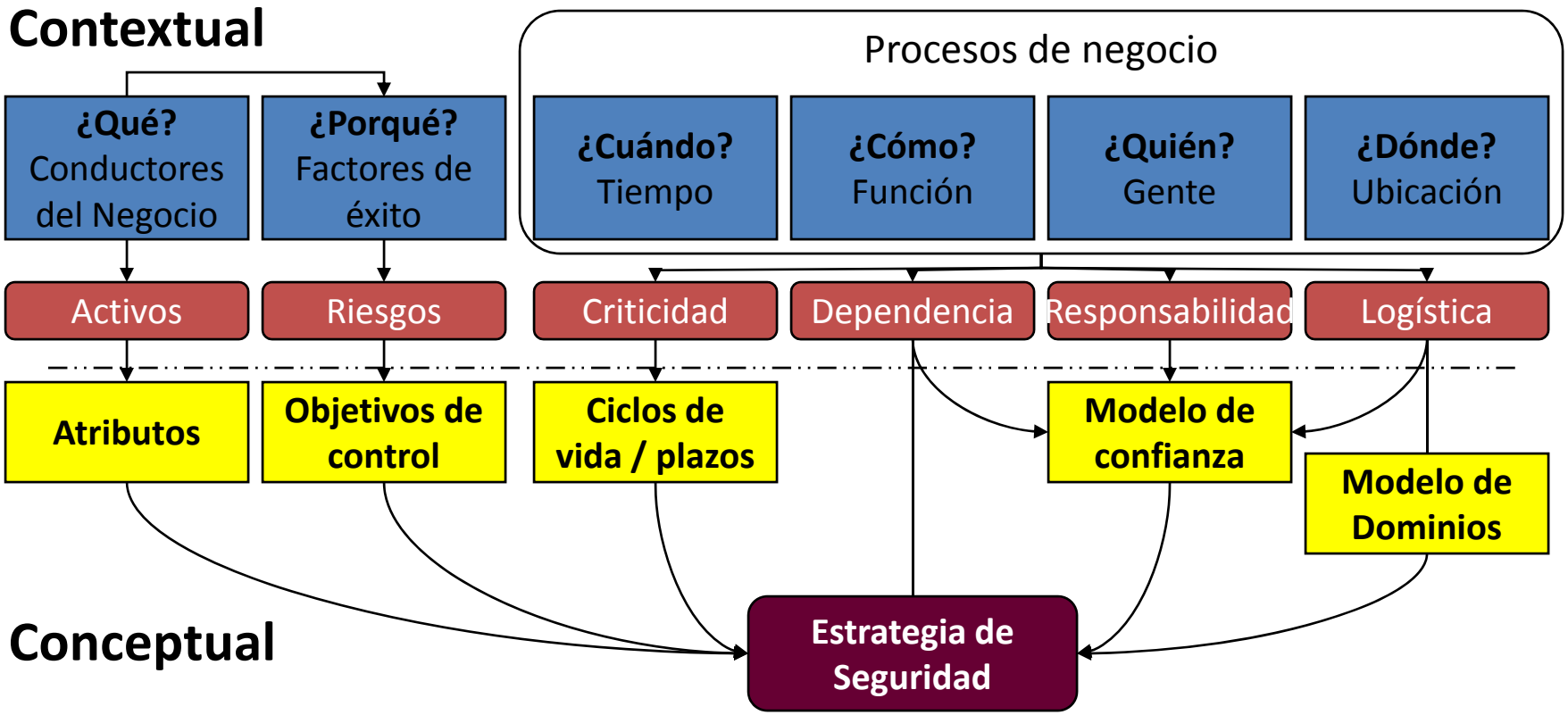
SABSA Proceso de desarrollo



SABSA

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines

SABSA

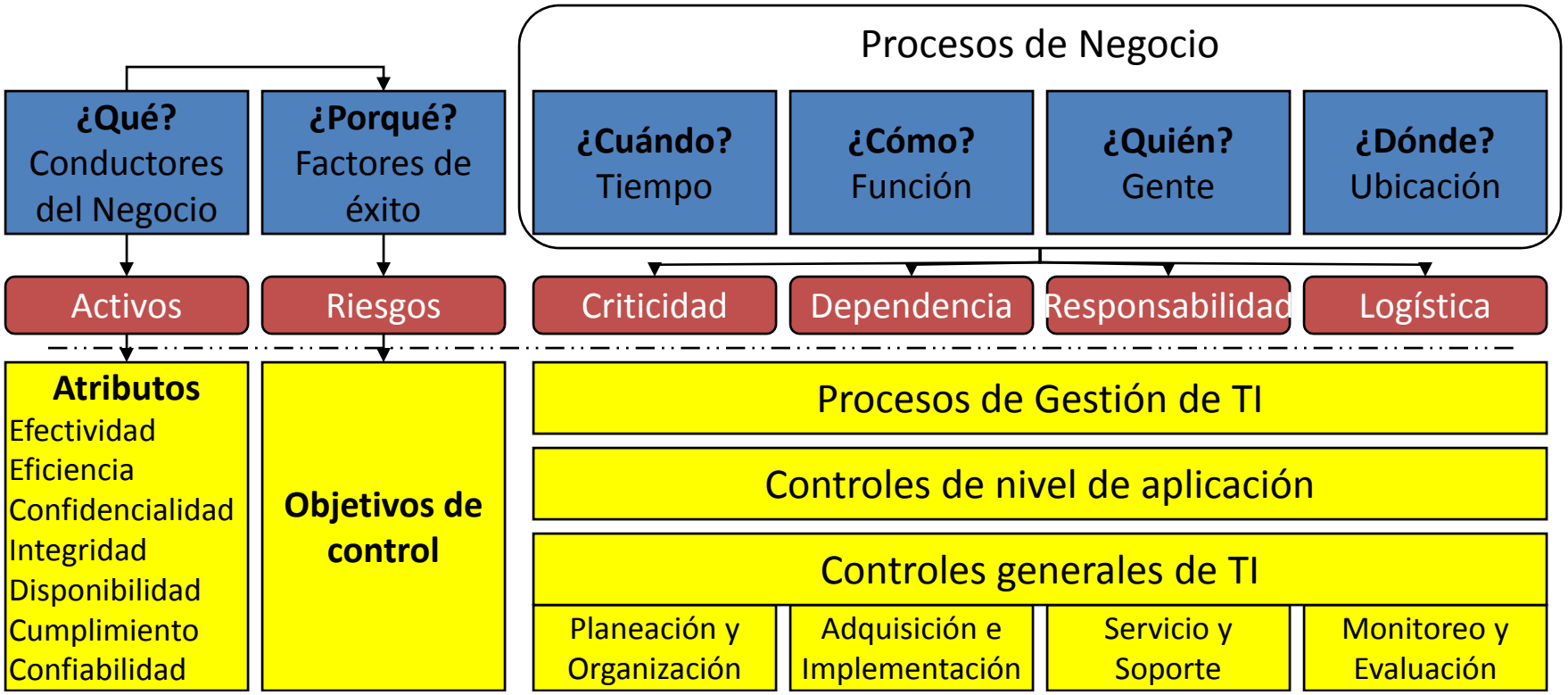

Contextual
Procesos de negocio
¿Qué? Conductores del Negocio
¿Porqué? Factores de éxito
¿Cuándo? Tiempo
¿Cómo? Función
¿Quién? Gente
¿Dónde? Ubicación
Activos
Riesgos
Criticidad
Dependencia
Responsabilidad
Logística
Atributos
Objetivos de control
Ciclos de vida / plazos
Modelo de confianza
Modelo de Dominios
Conceptual
Estrategia de Seguridad

SABSA– Atributos del Negocio

Atributos de usuario	Accesible, exacto, consistente, segregado, educado, conciente, motivado, informado, protegido, confiable, soportado
Atributos de gestión	Automatizado, cambios controlados, costo-efectivo, eficiente, mantenible, medido, soportable
Atributos operacionales	Disponible, libre de error, interoperable, productivo, recuperable
Atributos de gestión del riesgo	Controlado en acceso, integridad, autenticado, autorizado, flexible, privado, confidencial, no repudiable

Atributos legales y regulatorios	Admisible, cumple, se puede hacer cumplir, asegurable, resoluble
Atributos de estrategia técnica	Flexible, extendible, integrable, migrable, escalable, simple, trazable
Atributos de estrategia del negocio	Mejora imagen, habilita al negocio, competente, confiable, creíble, gobernable.

COBIT


Procesos de Negocio
¿Qué? Conductores del Negocio
¿Porqué? Factores de éxito
¿Cuándo? Tiempo
¿Cómo? Función
¿Quién? Gente
¿Dónde? Ubicación
Activos
Riesgos
Criticidad
Dependencia
Responsabilidad
Logística
Atributos
Efectividad
Eficiencia
Confidencialidad
Integridad
Disponibilidad
Cumplimiento
Confiabilidad
Objetivos de control
Procesos de Gestión de TI
Controles de nivel de aplicación
Controles generales de TI
Planeación y Organización
Adquisición e Implementación
Servicio y Soporte
Monitoreo y Evaluación

Otras fuentes de atributos o principios

GAISP
Generally Accepted Information Security Principles

- Asignación de responsabilidad (accountability)
- Conciencia
- Ética
- Multidisciplinariedad
- Proporcionalidad
- Integración
- Oportunidad
- Evaluación de riesgos
- Equidad

OECD
Organisation for Economic Co-operation and Development

- Concientización
- Responsabilidad
- Respuesta (incidentes)
- Ética
- Democracia
- Evaluación del riesgo
- Diseño y realización de la seguridad
- Gestión de la seguridad
- Re-evaluación

Desarrollo de la estrategia de seguridad

Situación actual

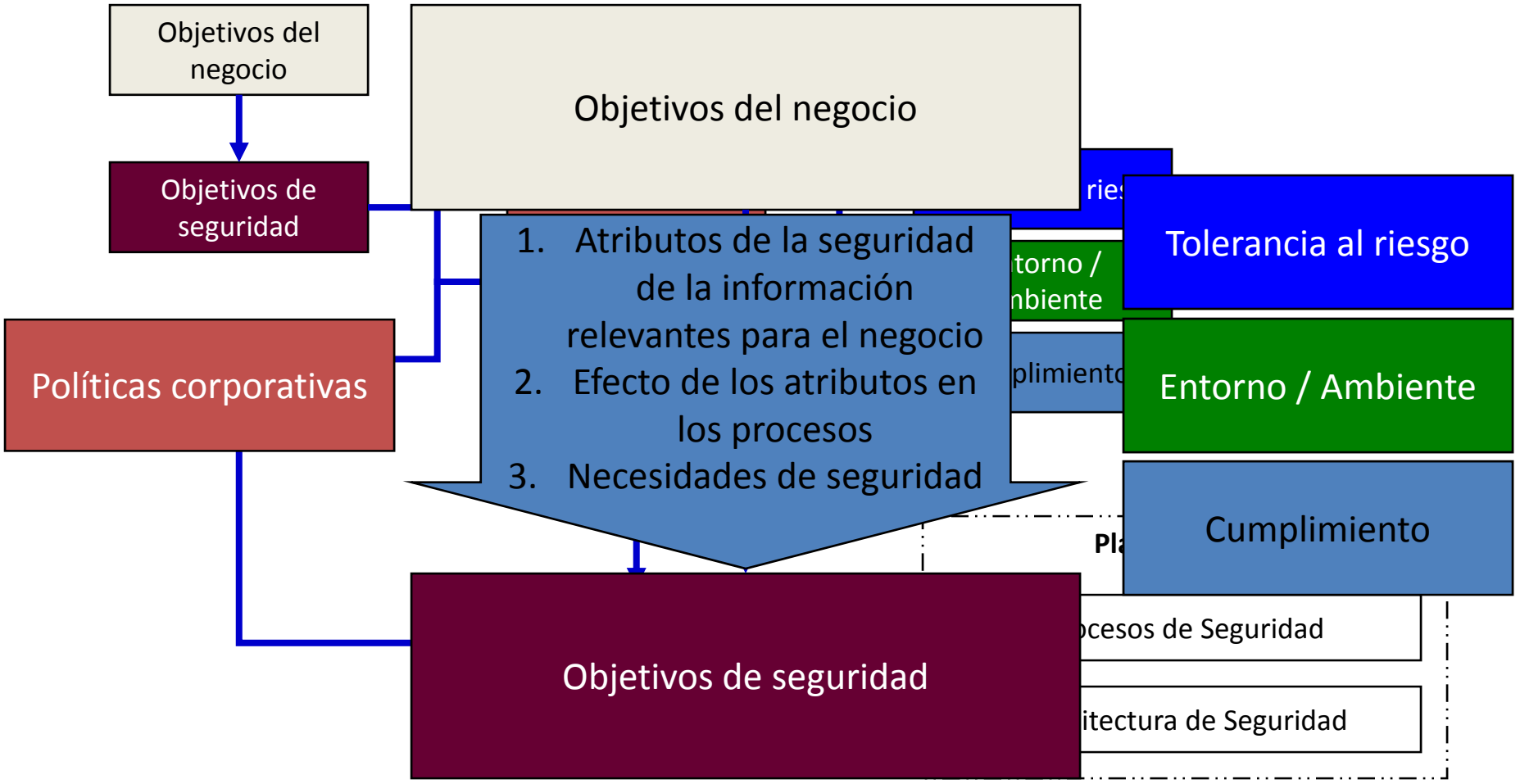
- **Objetivos estratégicos del negocio**
  - Basados en la Misión - Visión o MEGA del negocio
  - Requieren conservar principalmente ciertos **atributos de seguridad** para contribuir al negocio
  - Generan **necesidades de seguridad** que deben ser cubiertas (situación futura)

Situación actual

- **Atributos y Procesos del negocio**
  - El cumplimiento de la Misión-Visión o MEGA del negocio depende de que se garanticen unos atributos.
  - Cada atributo tiene una relevancia específica para el logro de los objetivos de negocio, dentro de cada proceso de la organización.

Situación actual – Alineamiento estratégico

- El negocio tiene sus objetivos estratégicos.
- Igualmente permite obtener atributos clave del negocio que deben ser satisfechos por la seguridad de la información.
- A partir de estos atributos se pueden derivar los objetivos estratégicos de seguridad de la información que permitirán garantizar dichos atributos.


Objetivos del negocio
Objetivos de seguridad
Políticas corporativas
Objetivos del negocio
1. Atributos de la seguridad de la información relevantes para el negocio
2. Efecto de los atributos en los procesos
3. Necesidades de seguridad
Objetivos de seguridad
Tolerancia al riesgo
Entorno / Ambiente
Cumplimiento
cesos de Seguridad
itectura de Seguridad

Situación actual – Identificación de atributos

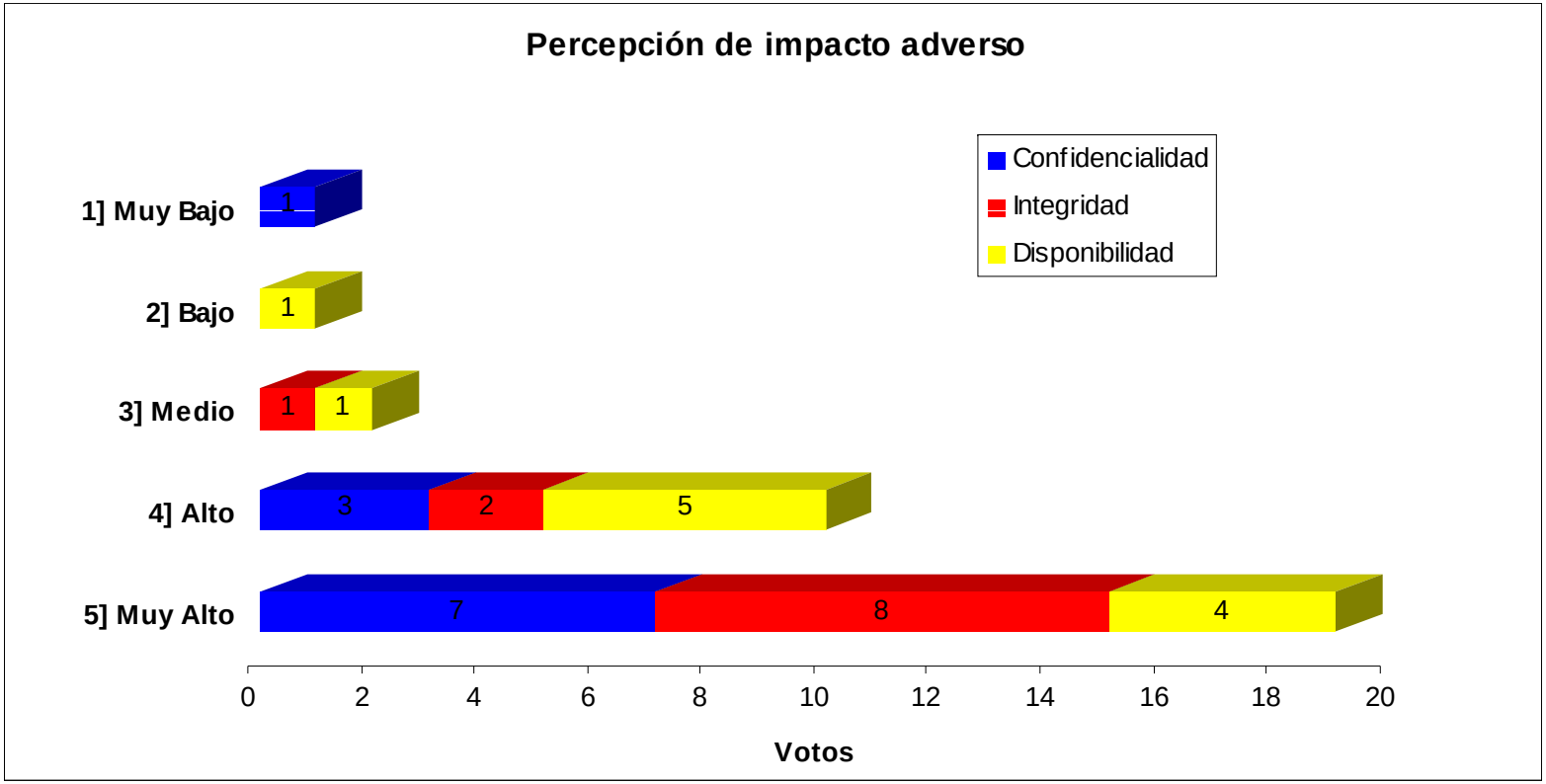
- Entendimiento de objetivos estratégicos del negocio
- Identificación de los atributos del negocio
- Identificación de los atributos de negocio más relevantes en su conjunto para el cumplimiento de la estrategia
- Los atributos clave identificados son base para la clasificación de información y para definir la MEGA de seguridad de información

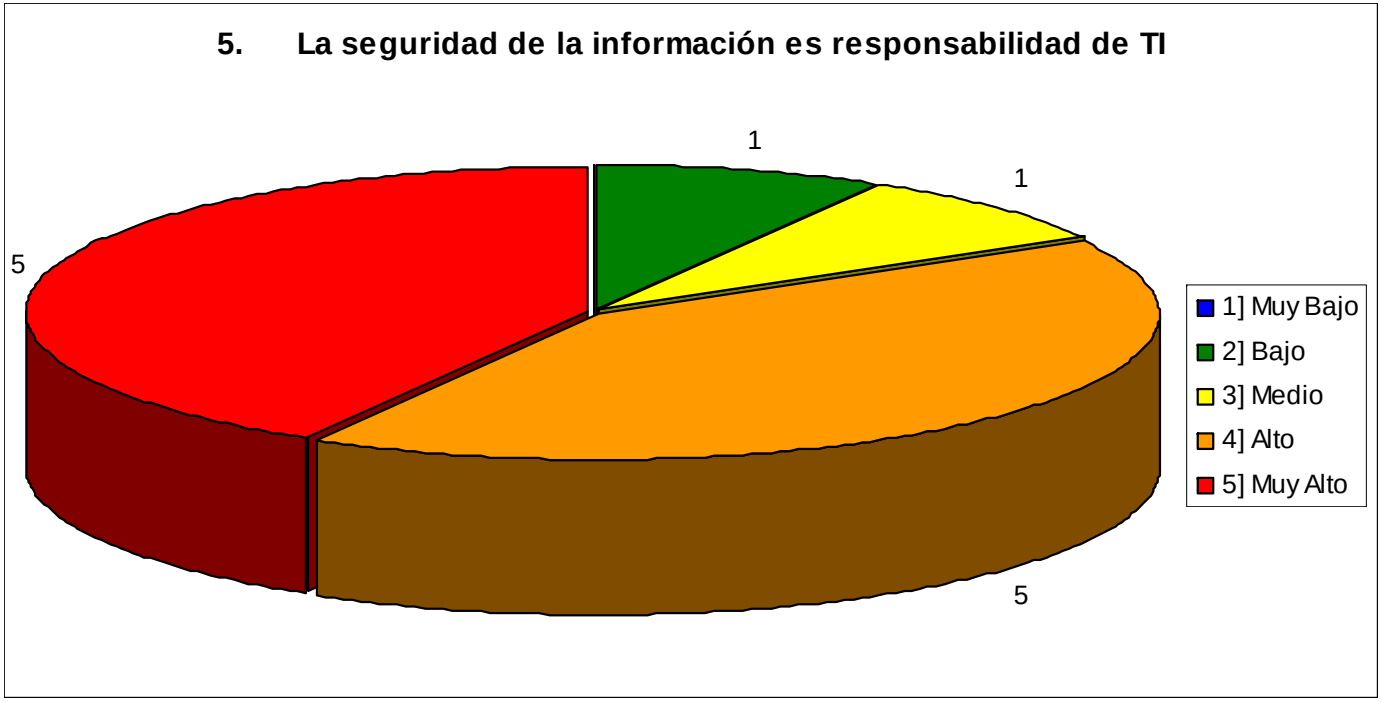
Situación actual – Identificación de atributos

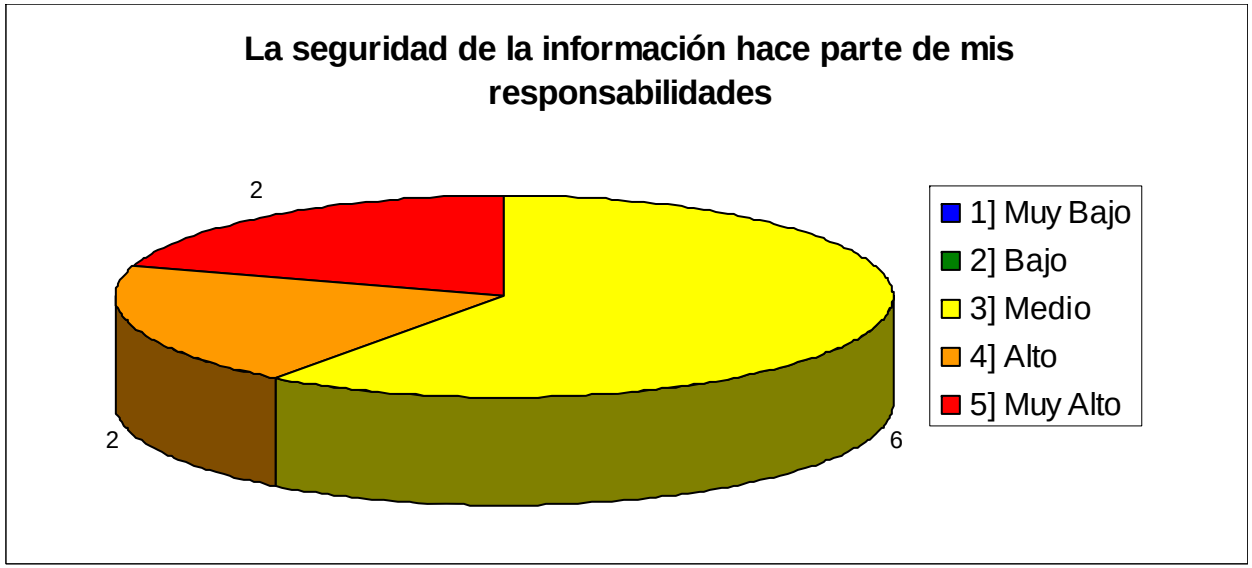
- Para identificar los atributos de negocio relevantes para la estrategia de la organización, se pueden utilizar técnicas como:
  - Sesiones de facilitación con accionistas, la junta, la gerencia ejecutiva, basado en su percepción de seguridad de la información.
  - Diagramas de espina de pescado u otras técnicas para el análisis de causas, a partir de los objetivos del negocio:
    - Lluvia de ideas
    - Diagramas de causa efecto
    - Diagramas de relación (causa-relación-efecto)

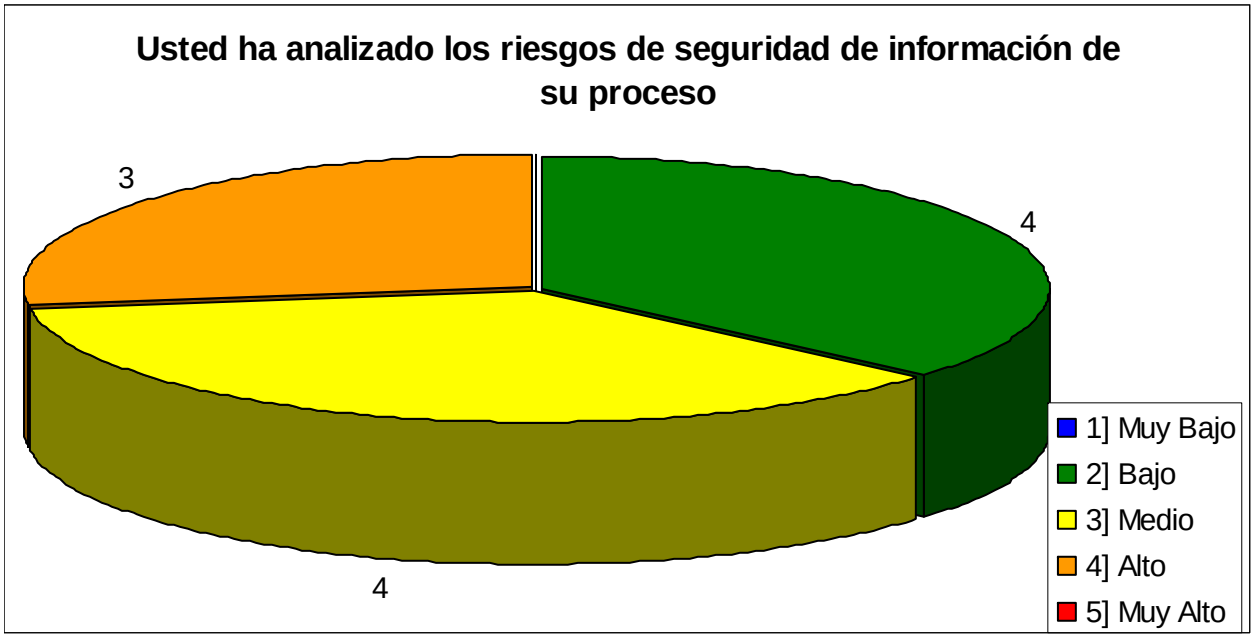
Situación actual – Identificación de atributos

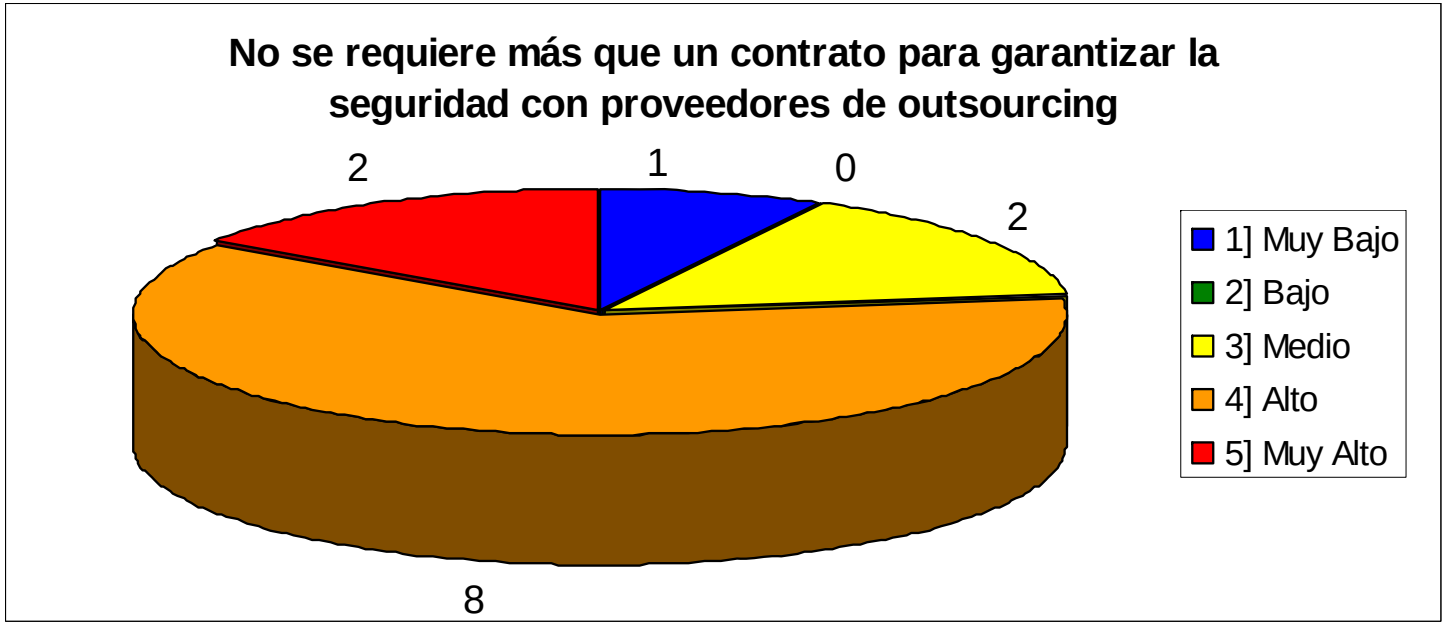
- ***Identificación de atributos de información clave en sesiones de facilitación***
  - Conocimiento de la estrategia del negocio
  - Entendimiento de proyectos en curso y prioridades
  - Elaboración de un cuestionario acorde con la cultura de la organización y sus circunstancias pasadas, actuales y futuras
  - Análisis de resultados

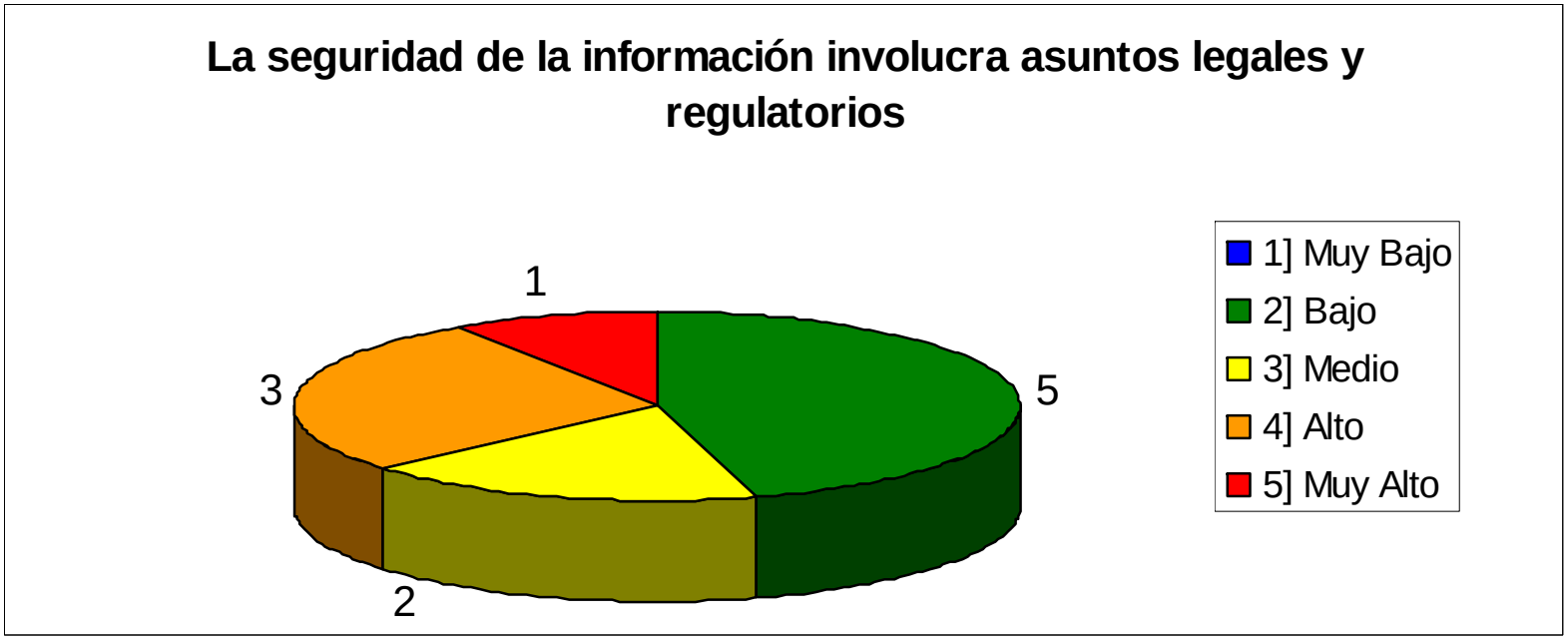

Percepción de impacto adverso
Confidencialidad
Integridad
Disponibilidad
1] Muy Bajo
2] Bajo
3] Medio
4] Alto
5] Muy Alto
1
1
1
1
3
2
5
7
8
4
0
2
4
6
8
10
12
14
16
18
20
Votos


5. La seguridad de la información es responsabilidad de TI
1
1
5
5
1] Muy Bajo
2] Bajo
3] Medio
4] Alto
5] Muy Alto


La seguridad de la información hace parte de mis responsabilidades
2
2
6
1] Muy Bajo
2] Bajo
3] Medio
4] Alto
5] Muy Alto


Usted ha analizado los riesgos de seguridad de información de su proceso
3
4
4
1] Muy Bajo
2] Bajo
3] Medio
4] Alto
5] Muy Alto

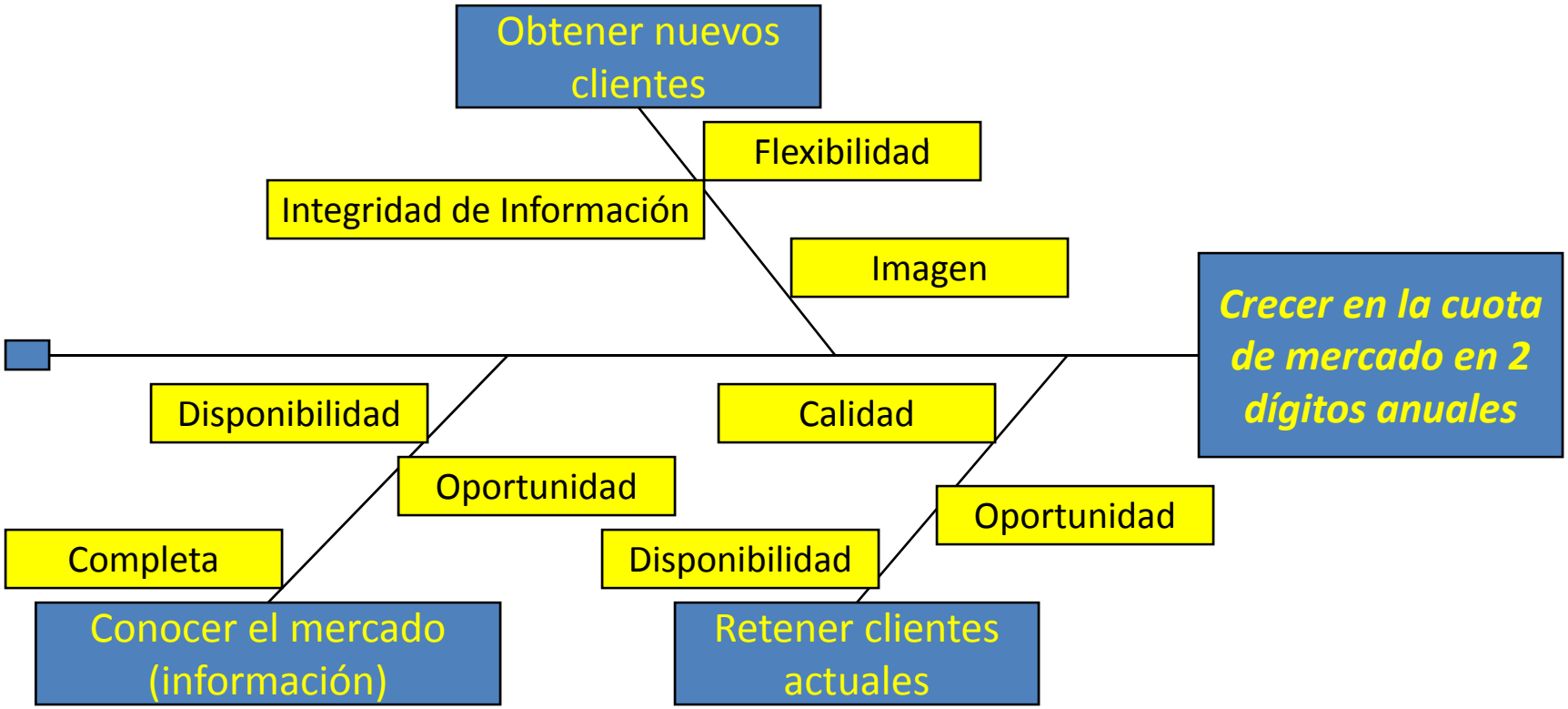

No se requiere más que un contrato para garantizar la seguridad con proveedores de outsourcing
2
1
0
2
8
1] Muy Bajo
2] Bajo
3] Medio
4] Alto
5] Muy Alto


La seguridad de la información involucra asuntos legales y regulatorios
1
2
3
5
1] Muy Bajo
2] Bajo
3] Medio
4] Alto
5] Muy Alto

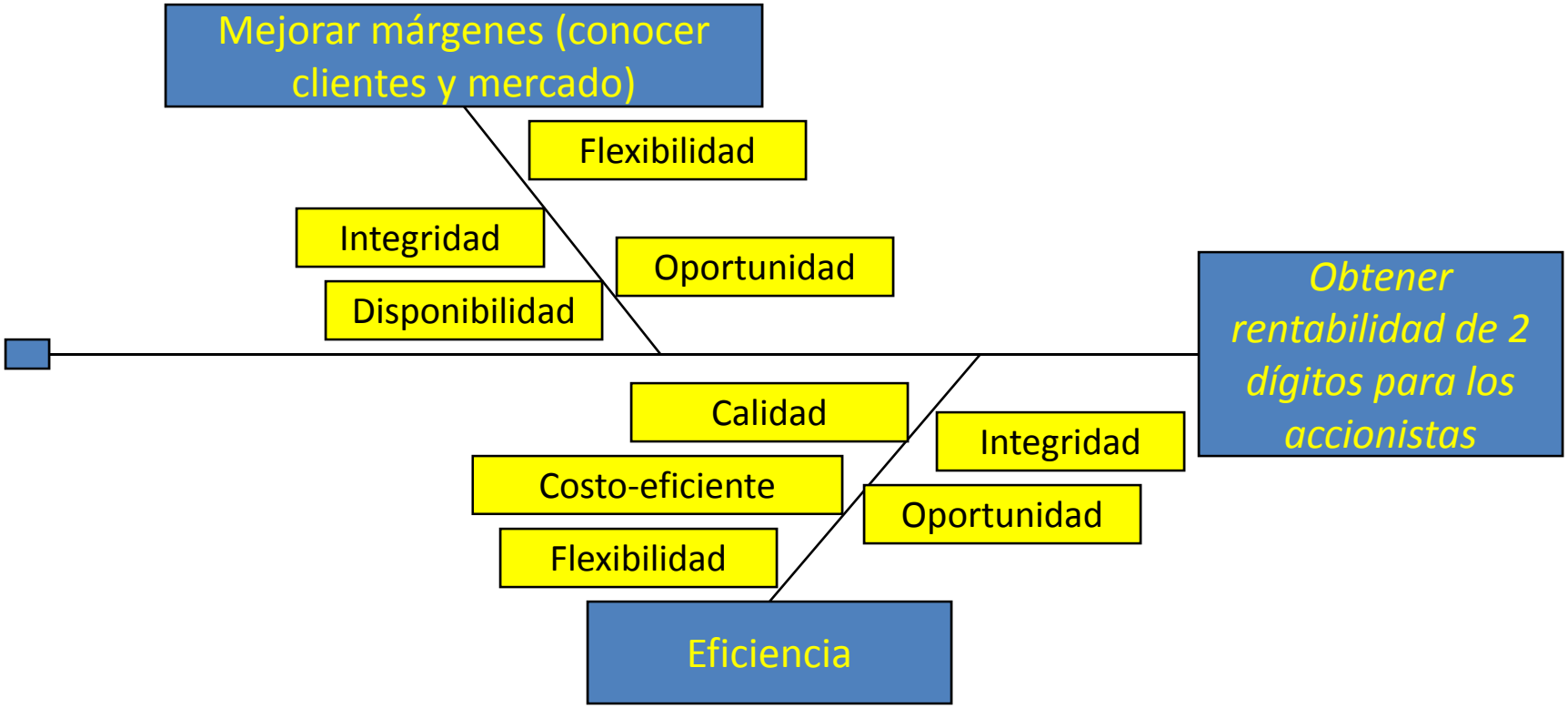
Situación actual – Identificación de atributos

- ***Identificación de atributos de información clave con base en los objetivos del negocio***
- Objetivos de negocio. Ejemplo
  - ***Objetivo 1:*** *Crecer en la cuota de mercado en 2 dígitos anuales*
  - ***Objetivo 2:*** *Obtener rentabilidad de 2 dígitos para los accionistas*
  - ***Objetivo 3:*** *Desarrollar 2 nuevos productos para el mercado anualmente*

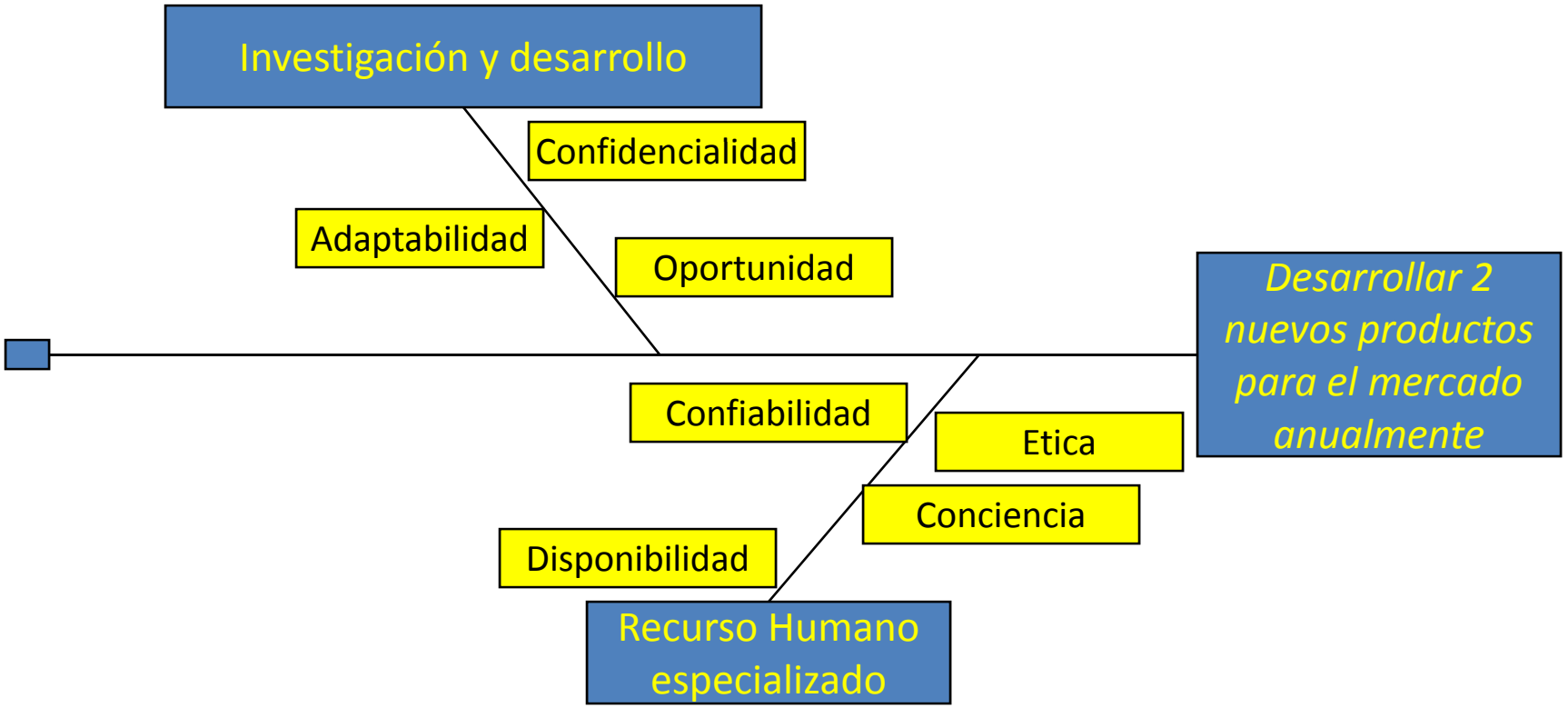
Situación actual – Identificación de atributos



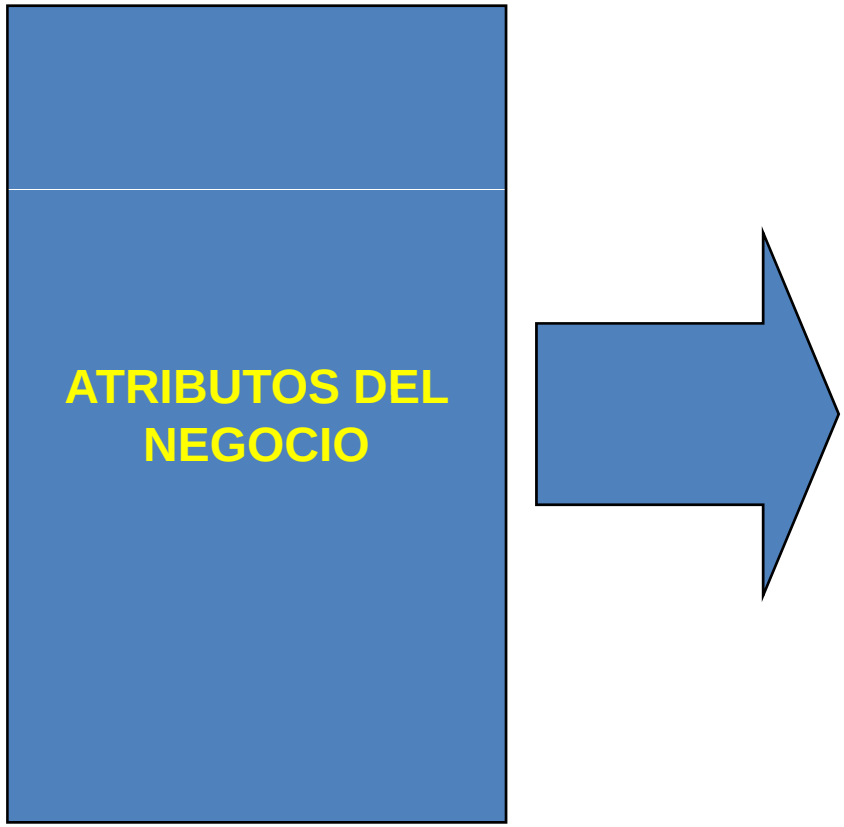
Situación actual – Identificación de atributos



Situación actual – Identificación de atributos



Situación actual – Aplicación de los atributos



- Objetivos estratégicos de seguridad de la información
- Priorización de procesos
- Clasificación de los activos de información

Situación actual – Atributos e información

- ***Atributos y Clasificación de activos de información***
- Obtener un inventario de activos de información por proceso
- Impacto de la pérdida de CUALIDAD DE LA INFORMACIÓN de este activo en ATRIBUTO DEL NEGOCIO

Situación actual – Atributos e información

- ***Ejemplo:***
  - ¿Cuál es el impacto en IMAGEN si esta información se revela de manera no autorizada a personas no autorizadas?

Situación actual – Atributos e información

Proceso	Activo de Información	Atributos									Atributos			Valor del activo
		C			I			D						
		Atributo 1	Atributo 2	Atributo 3	Atributo 1	Atributo 2	Atributo 3	Atributo 1	Atributo 2	Atributo 3	C	I	D	
Proceso 1	Activo 1	5	3	1	3	4	2	3	1	4	3.0	3.0	2.7	2.89
	Activo 2	4	5	4	3	4	3	5	5	4	4.3	3.3	4.7	4.11
	Activo 3	2	3	1	5	3	3	5	3	3	2.0	3.7	3.7	3.11
	Activo 4	3	1	3	1	3	2	3	2	5	2.3	2.0	3.3	2.56
	Activo 5	3	2	1	3	1	3	4	3	4	2.0	2.3	3.7	2.67
	Activo 6	3	3	3	3	3	3	3	3	3	3.0	3.0	3.0	3.00
	Activo 7	1	5	5	3	4	4	5	1	3	3.7	3.7	3.0	3.44

Situación actual – Atributos y procesos

	Atributos / Principios						
Proceso	Integración	Impacto Financiero	Confidencialidad	Integridad	Disponibilidad	Automatización	**Promedio**
Proceso 1	3	3	2	3	3	5	3.16666667
Proceso 2	3	2	3	5	3	4	3.33333333
Proceso 3	3	5	2	3	3	5	3.5
Proceso 4	5	3	2	5	3	3	3.5
Proceso 5	3	2	2	3	3	5	3
Proceso 6	3	3	2	3	2	3	2.66666667
Proceso 7	4	3	4	3	4	5	3.83333333
Proceso 8	3	2	2	2	2	2	2.16666667
Proceso 9	1	2	1	2	3	3	2

Situación futura

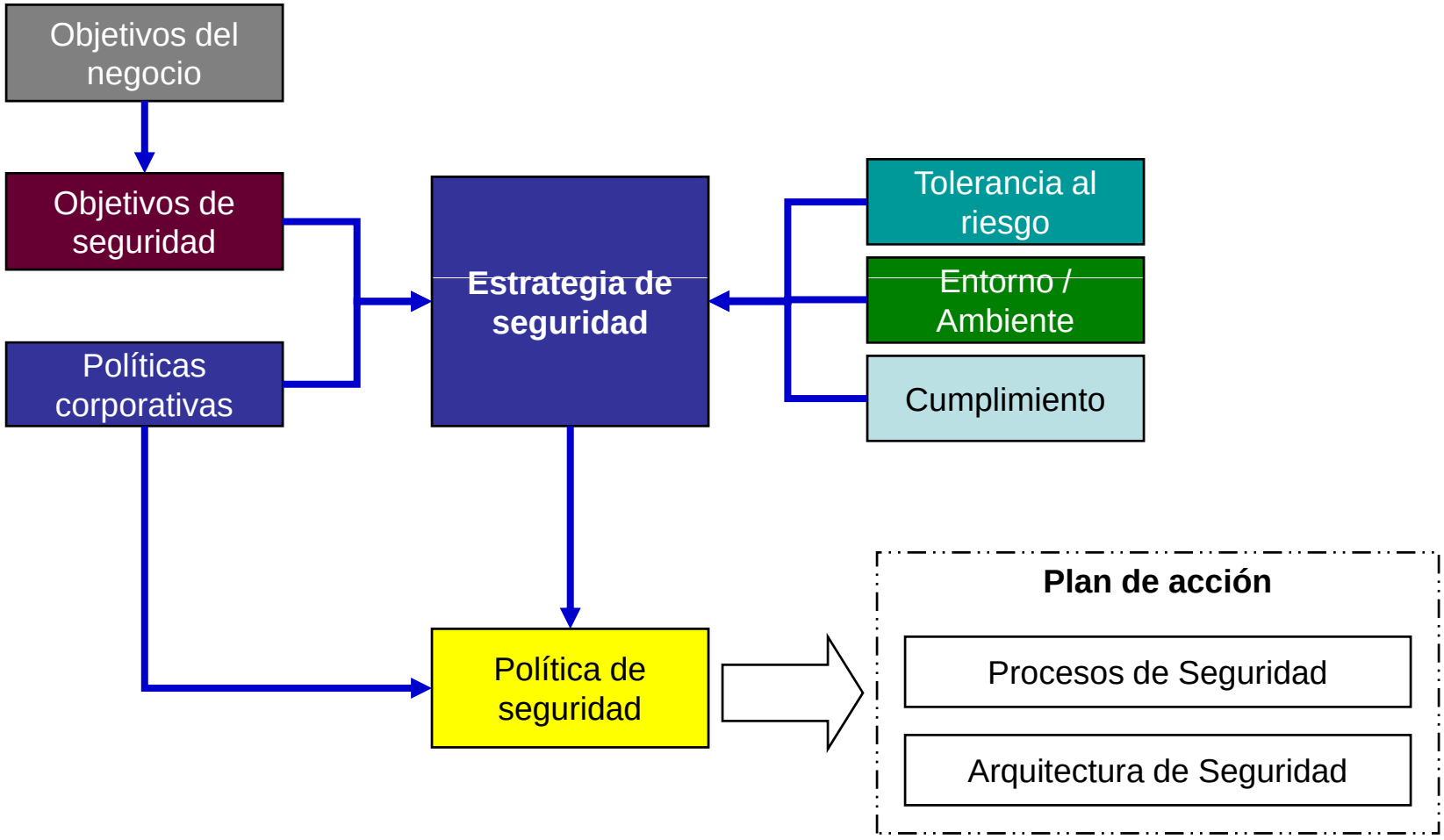
- La relevancia de los atributos para los procesos del negocio permite determinar:
  - La **Misión** y **Visión** de seguridad.
  - La **prioridad** de las diferentes iniciativas estratégicas que se definan posteriormente y su contribución al logro de los objetivos estratégicos (**necesidades de seguridad**)

- **Política de seguridad**

  Define el la intención de los accionistas, la junta y la gerencia ejecutiva frente a la seguridad. Establece un marco de actuación y los principios de seguridad

Plan de Acción

- **Necesidades de seguridad**
  - En el marco de la política de seguridad y con base en la información obtenida de atributos y su relevancia para cada proceso se puede determinar:
    - Necesidades comunes
    - Necesidades particulares
  - Las necesidades pueden generar diferentes tipos de iniciativas de acuerdo con el marco de referencia utilizado
  - Las necesidades son **Objetivos de Control** que deben ser cubiertas con base en uno o varios marcos de referencia (p. e. ISO27002, COBIT, ITIL, PMI)


Objetivos del negocio
Objetivos de seguridad
Políticas corporativas
Estrategia de seguridad
Tolerancia al riesgo
Entorno / Ambiente
Cumplimiento
Política de seguridad
Plan de acción
Procesos de Seguridad
Arquitectura de Seguridad

Plan de acción - Necesidades de seguridad en el marco de referencia SABSA

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

Plan de acción - Necesidades de seguridad en el marco de referencia SABSA

- Las necesidades se traducen en:
  - **Servicios de seguridad (Arquitectura Orientada a Servicios)**
  - **Procesos de seguridad**
    - Gestión de roles e identidades
    - Modelos de confianza, dominios de seguridad
    - Ciclos de vida de seguridad
    - Conciencia, entrenamiento y educación

Plan de acción - Necesidades de seguridad en el marco de referencia SABSA

- **Estrategia de seguridad**
  - Iniciativas de seguridad – con base en las necesidades identificadas
  - Plan estratégico

Iniciativa n: Proceso de gestión de usuarios y acceso

Objetivo: Contar con un proceso uniforme de control de acceso que …..

Alcance: los sistemas de información que soportan …

Beneficios:
- Tener un proceso uniforme de control de acceso
- Tener un ciclo de vida …
- Contar con una arquitectura de …
- Centralizar labores de …
- Dar a los usuarios la posibilidad de …
- Controlar el proceso y sus actividades a través de …

Costos:
- Recursos internos US$
- Recursos externos US$
- Gastos US$

Complejidad: 

Impacto: 

Plazo:
10 MESES

Principales Actividades:
- Determinar …
  - Integración de …
  - Gestión de …
  - Implementar …
  - Gestión de …
- Diseñar …
- Analizar …

Recursos:
- Hw
- Sw
- Servicios
- Gerentes funcionales (x%)
- Jefe de sección (x%)
- Gerente de RRHH (x%)

Prerrequisitos:
- Unificación de …
- Aseguramiento de …
- Participación de …

No	Iniciativa	Tiempo (Meses)	Costo (Miles de USD)	Complejidad (5=alto, 0=bajo)	Impacto (5=alto, 0=bajo)
14	Asegurar … activos de información				
15	Actualizar… los procedimientos de seguridad				
16	Actualizar e implementar estándares de seguridad …				
17	Implementar el proceso de gestión de acceso				
18	… definición y establecimiento de acuerdos de servicio ..				
19	… implementación del monitoreo y medición del cumplimiento de la seguridad de la información..				

INICIATIVAS	Año 1												Año 2												Año 3											
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
Iniciativa 1																																				
Iniciativa 2																																				
Iniciativa 3																																				
Iniciativa 4																																				
Iniciativa 5																																				
Iniciativa 6																																				
Iniciativa 7																																				
Iniciativa 8																																				
Iniciativa 9																																				
Iniciativa 10																																				
Iniciativa 11																																				
Iniciativa 12																																				
Iniciativa 13																																				
Iniciativa 14																																				
Iniciativa 15																																				
Iniciativa 16																																				
Iniciativa 17																																				
Iniciativa 18																																				
Iniciativa 19																																				
Iniciativa 20																																				

Más de un US$1 millón
Entre US$500 mil y US$1 millón
Menos de US$500 mil

- Referencias
  - Deloitte – Experiencia en proyectos
  - Material público existente sobre el modelo SABSA
  - IT Governance Institute
  - ISACA
  - CISM Review Manual
  - ISO27002:2005
  - OECD - Organisation for Economic Co-operation and Development
  - www.gaisp.org

GRACIAS …!

Wilmar Arturo Castellanos

wcastellanos@deloitte.com