XIII Encuentro Iberoamericano de Protección de Datos

Lima, 6, 7 y 8 de mayo

Protección de datos personales y medidas de seguridad de la información

Antoni Bosch Pujol , CISA, CISM, CGEIT, ECPD

Director General del Institute of Audit & IT-Governance (IAITG)

Director del Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC de la Universidad Autónoma de Madrid (MASGDTIC)

Presidente Fundador ISACA-Barcelona

EL PAÍS

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

Peligro: ciberataques a empresas (7-03-2014)

De repente, McDonald's había comprado Burger King. De repente, Chrysler había vendido Jeep. Y de repente, todo era una gran mentira. Un fraude. Los últimos ataques que han sufrido las cuentas de Twitter de esos gigantes empresariales, publicando información falsa o directamente ultrajante, revelan la fragilidad de las marcas en las redes sociales.

Vodafone Egipto, Pfizer, USA Today, Reuters, Gizmodo, Fox News, NBC News, Cadillac, Bank of Melbourne... todas han sido atacadas por hackers entre 2011 y 2013. Hay más, muchas más, pero la discreción manda. Nadie quiere transmitir una imagen de flaqueza. Piensen en la credibilidad que comunica un banco cuya cuenta en Facebook o Twitter ha sido pirateada. Pero todas las compañías, "desde corporaciones bancarias hasta organizaciones de caridad locales, pueden ser un objetivo", advierte Andrew Rose, analista de la consultora Forrester Research. Mientras tanto, crece la sensación de peligro en el mundo digital.

LA VANGUARDIA

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

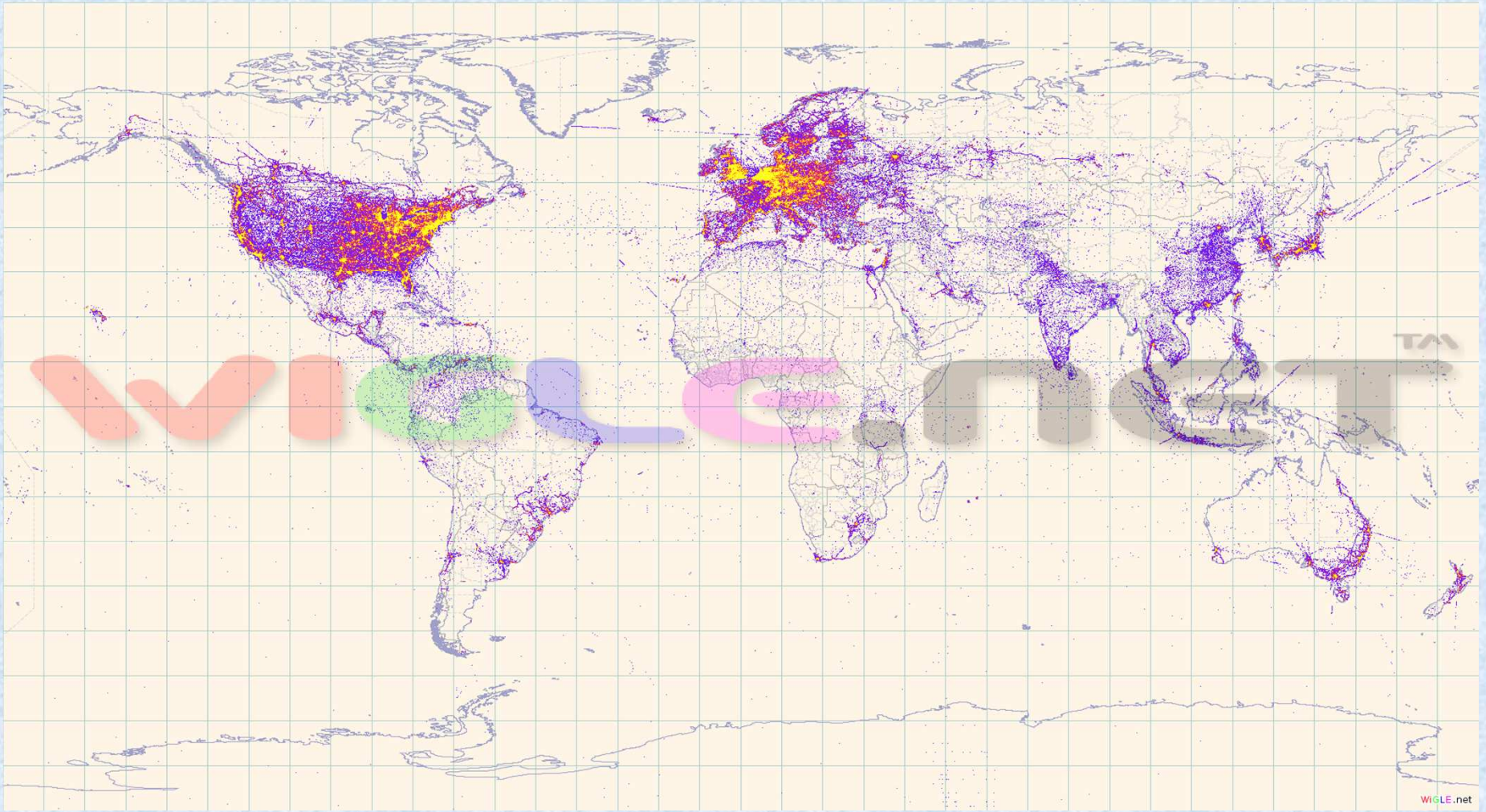
Mercados fuera del radar (6-10-2013)

Los algoritmos introducidos en los ordenadores dominan las transacciones financieras NYSE-Euronext gestiona órdenes en 37 microsegundos, 6.756 veces más rápido que un guiño Las operaciones de alta frecuencia y mayor velocidad se generalizan.

Lo que sigue es una demostración más de que la realidad supera la ficción hasta niveles estupefacientes. Se trata del peso ya preponderante –más del 50%– de las operaciones de alta frecuencia en las que la velocidad de las transacciones se hacen en microsegundos.

Culpar a los ordenadores ayer y a los complicadísimos algoritmos que hincharon y pincharon la última burbuja financiera equivale a olvidar que son los seres humanos quienes programan e introducen modelos estadísticos y financieros que son capaces de anticipar qué efecto tendrá una orden de compra o venta en los precios. A partir de ahí el programa analiza la información y las órdenes se producen de forma automática. Cuando más de la mitad de las operaciones en los mercados financieros se realiza mediante inverosímiles operaciones de alta frecuencia, el inversor minorista es, por supuesto, irremisiblemente lento.

http://wigle.net/



SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

- **Conjunto de sistemas y procedimientos que garantizan:**

  - CONFIDENCIALIDAD
  - INTEGRIDAD
  - DISPONIBILIDAD

  - AUTENTIFICACIÓN
  - NO REPUDIO

VALORACIÓN DE LOS REQUISITOS PROTECCIÓN

- Básico
  - Impacto limitado
- Moderado
  - Impacto considerable
- Alto
  - Impacto catastrófico

QUÉ PASA SI ... ?

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

QUE PASA SI HAY

- Pérdida de Confidencialidad
- Pérdida de Integridad
- Pérdida de Disponibilidad

- Incumplimiento leyes o contratos
- Atentado contra el honor y la intimidad
- Daños personales
- Incorrecta realización actividades
- Efectos negativos en relaciones externas
- Pérdidas económicas

La complejidad de la sencillez :

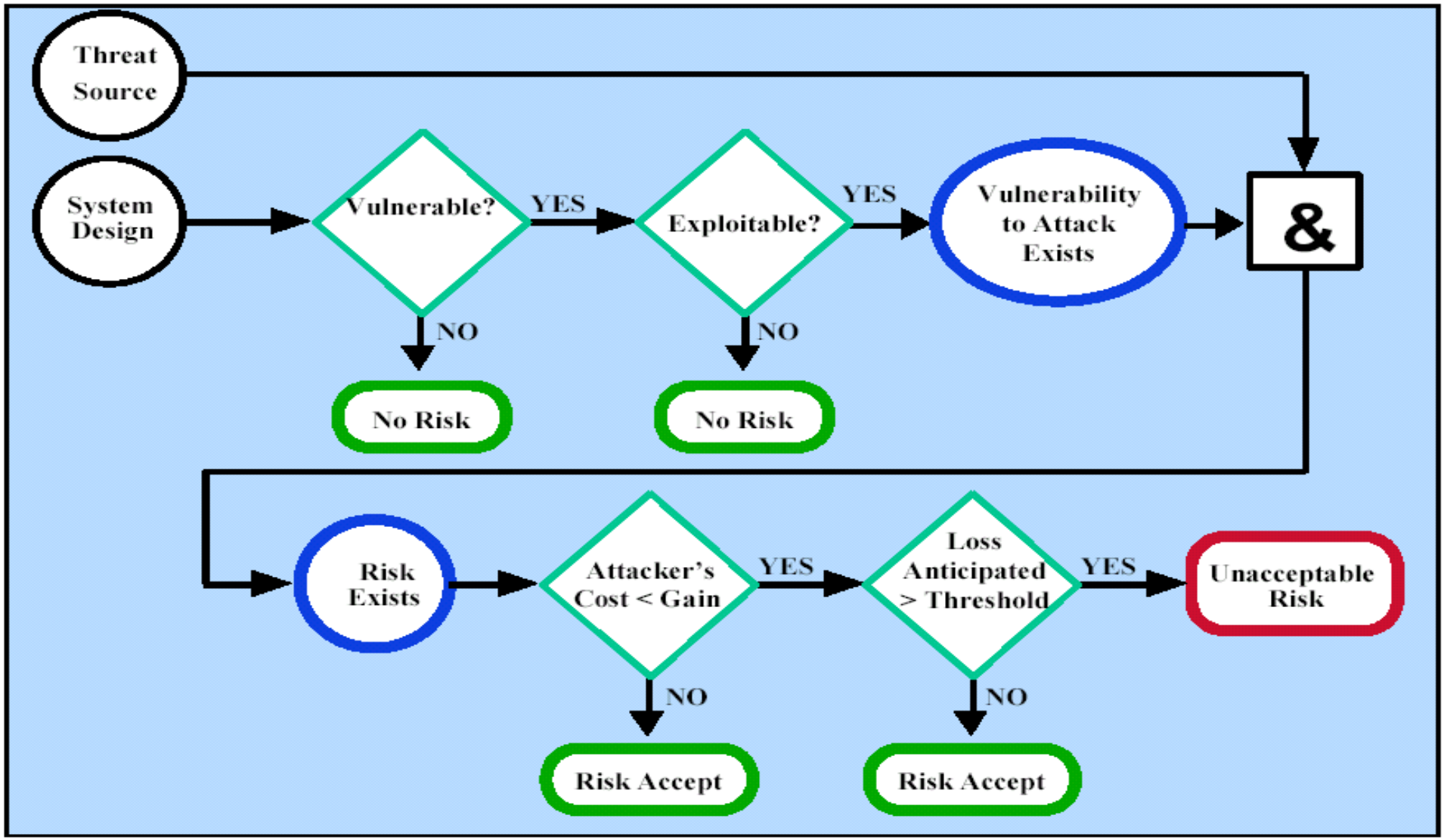
1º clase de matemática aplicada

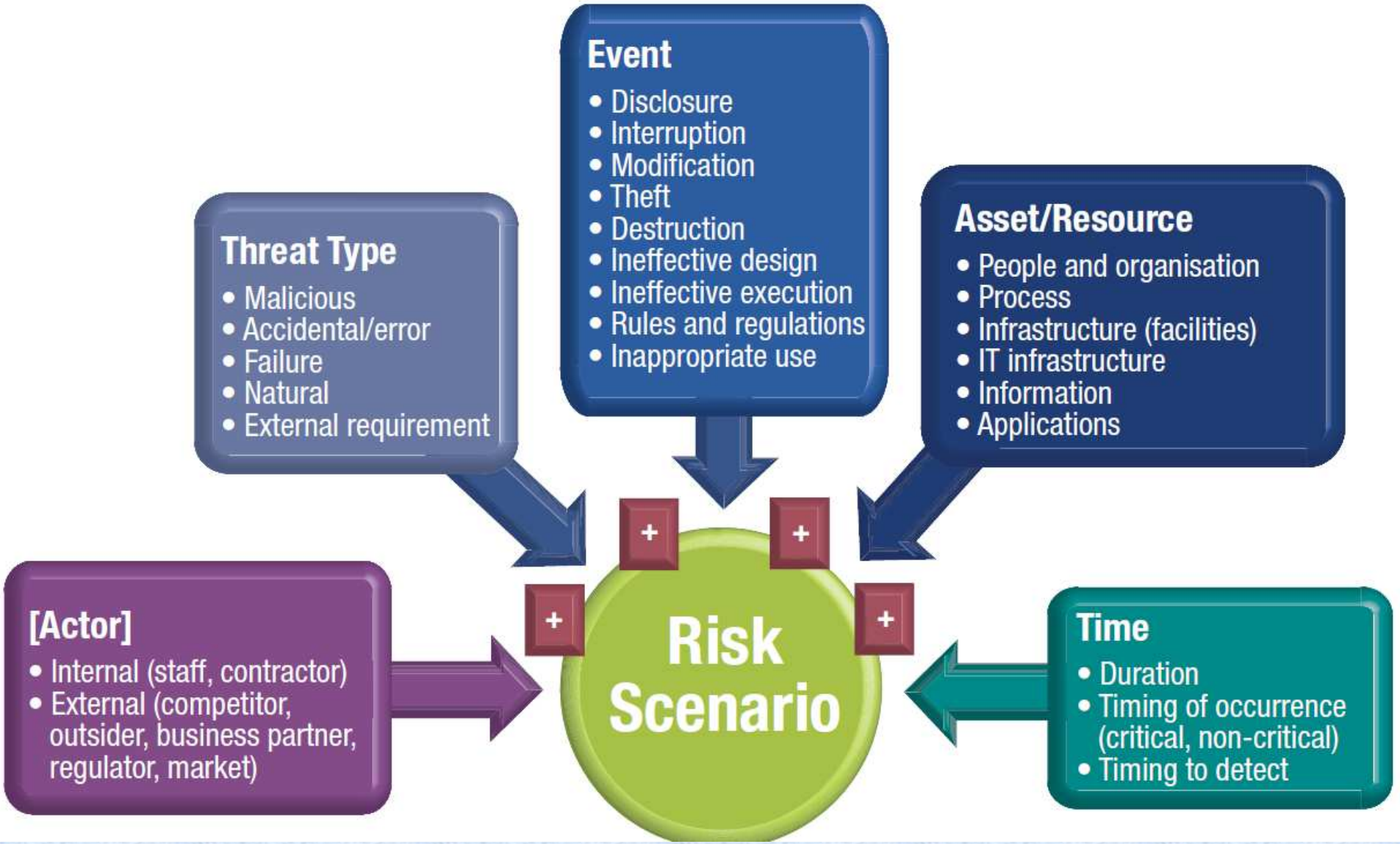
Cualquier futuro ingeniero aprende la notación matemática según la cual la suma de dos números reales, como por ejemplo

$$1+1=2$$

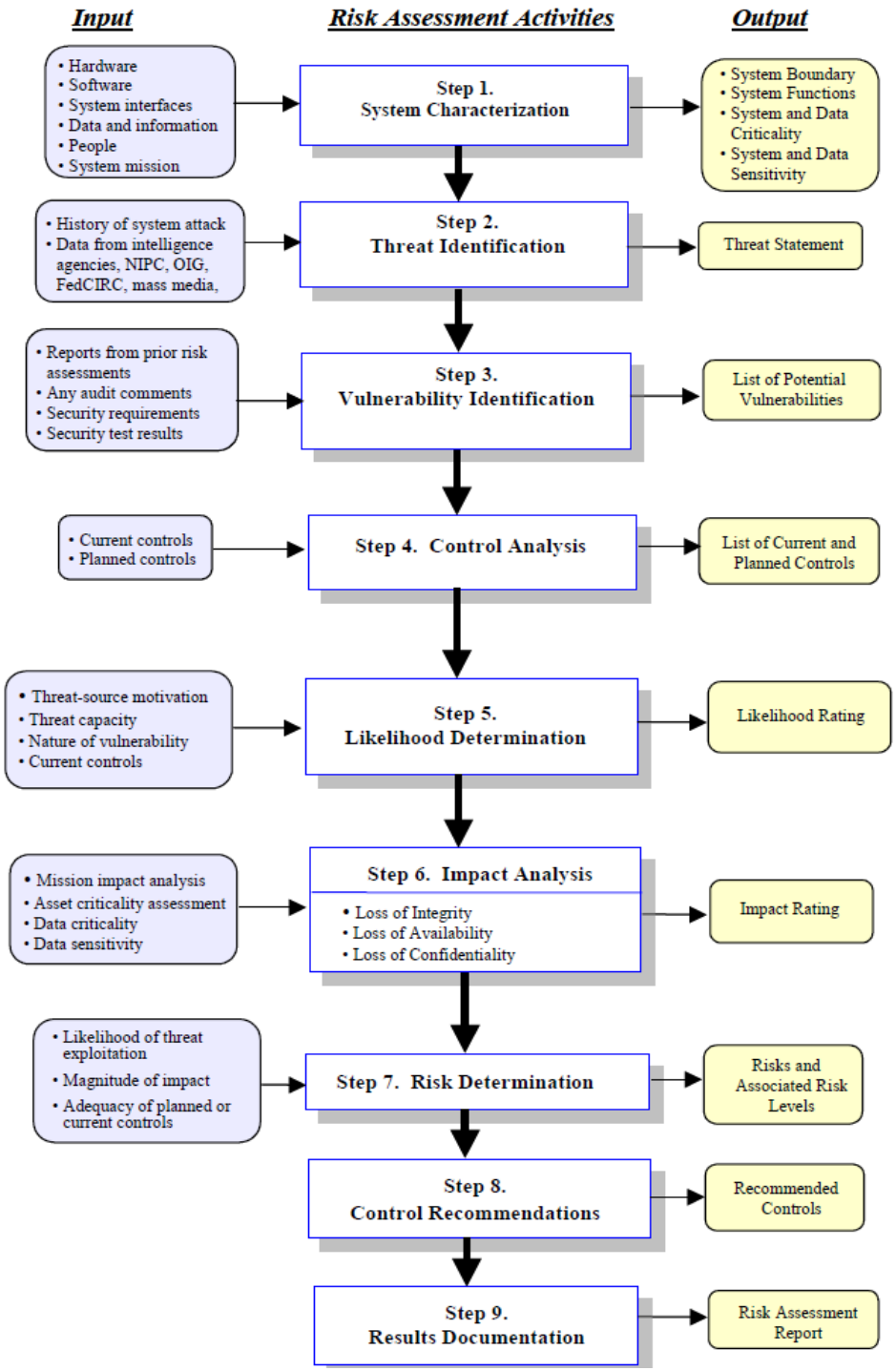
puede ser escrita de manera tan simple. Sin embargo esta forma es errónea debido a su banalidad y demuestra una falta total de estilo.

(NIST SP 800-30)

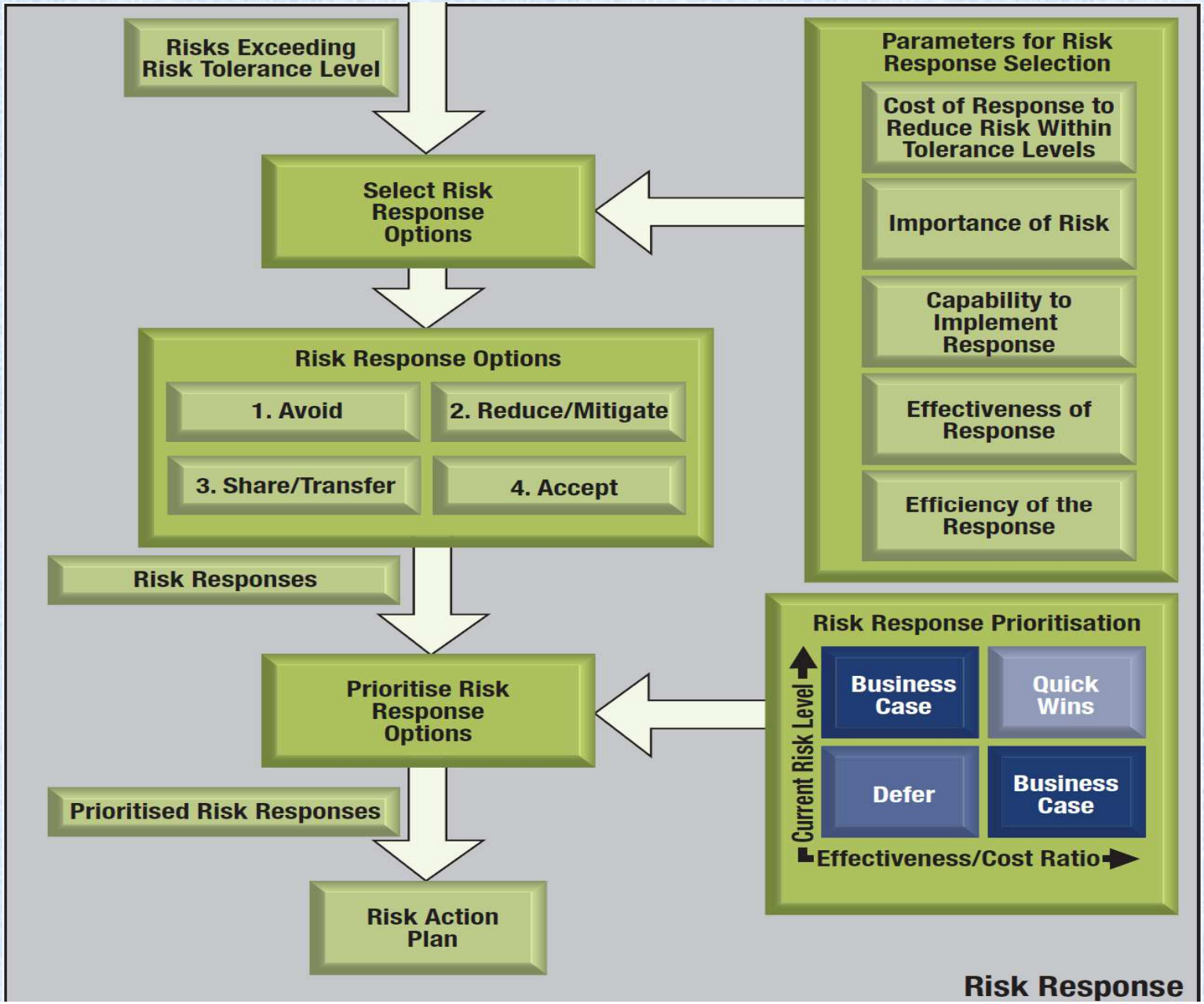



Event
• Disclosure
• Interruption
• Modification
• Theft
• Destruction
• Ineffective design
• Ineffective execution
• Rules and regulations
• Inappropriate use
Threat Type
• Malicious
• Accidental/error
• Failure
• Natural
• External requirement
Asset/Resource
• People and organisation
• Process
• Infrastructure (facilities)
• IT infrastructure
• Information
• Applications
[Actor]
• Internal (staff, contractor)
• External (competitor, outsider, business partner, regulator, market)
Risk Scenario
Time
• Duration
• Timing of occurrence (critical, non-critical)
• Timing to detect

NIST SP 800-30



Risk IT. ISACA



MACROPROCESOS EN LA GESTIÓN DE INCIDENTES

Los procesos de gestión y respuesta a incidentes se pueden resumir en:

- Detectar incidentes rápidamente.
- Diagnosticar incidentes con exactitud.
- Gestionarlos adecuadamente.
- Reducir y minimizar los daños.
- Restaurar los servicios afectados.
- Determinar las causas originales.
- Implementar mejoras para evitar que se repitan.

ISO 27000/ NTP ISO/IEC 17799

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

1-POLÍTICA DE SEGURIDAD

2-ESTRUCTURA ORGANIZATIVA PARA LA SEGURIDAD

3-CLASIFICACIÓN Y CONTROL DE ACTIVOS

4-SEGURIDAD EN EL PERSONAL

5-SEGURIDAD FÍSICA Y DEL ENTORNO

6-GESTIÓN DE COMUNICACIONES Y OPERACIONES

8-DESARROLLO Y MANTENIMIENTO DE SISTEMAS

7-CONTROL DE ACCESOS

9-GESTIÓN DE INCIDENCIAS

10-GESTIÓN DE CONTINUIDAD DEL NEGOCIO

11-CUMPLIMIENTO

International Organization for Standardization

JTC 1/SC 27
IT Security techniques

ISO/IEC 7064:2003	Information technology -- Security techniques -- Check character systems
ISO/IEC 9796-2:2002	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:2000	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797-1:1999	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:2002	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9798-1:1997	Information technology -- Security techniques -- Entity authentication -- Part 1: General
ISO/IEC 9798-2:1999	Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms
ISO/IEC 9798-2:1999/Cor 1:2004	
ISO/IEC 9798-3:1998	Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques
ISO/IEC 9798-4:1999	Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function
ISO/IEC 9798-5:2004	Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques
ISO/IEC 9798-6:2005	Information technology -- Security techniques -- Entity authentication -- Part 6: Mechanisms using manual data transfer

International Organization for Standardization

JTC 1/SC 27
IT Security techniques

ISO/IEC 9979:1999	Information technology -- Security techniques -- Procedures for the registration of cryptographic algorithms
ISO/IEC 10116:1997	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO/IEC 10118-1:2000	Information technology -- Security techniques -- Hash-functions -- Part 1: General
ISO/IEC 10118-2:2000	Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
ISO/IEC 10118-3:2004	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 10118-4:1998	Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic
ISO/IEC 11770-1:1996	Information technology -- Security techniques -- Key management -- Part 1: Framework
ISO/IEC 11770-2:1996	Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
ISO/IEC 11770-2:1996/Cor 1:2005	
ISO/IEC 11770-3:1999	Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques

International Organization for Standardization

JTC 1/SC 27
IT Security techniques

ISO/IEC 13335-1:2004	Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
ISO/IEC TR 13335-3:1998	Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
ISO/IEC TR 13335-4:2000	Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
ISO/IEC TR 13335-5:2001	Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security
ISO/IEC 13888-1:2004	IT security techniques -- Non-repudiation -- Part 1: General
ISO/IEC 13888-2:1998	Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques
ISO/IEC 13888-3:1997	Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques
ISO/IEC TR 14516:2002	Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services
ISO/IEC 14888-1:1998	Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General
ISO/IEC 14888-2:1999	Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Identity-based mechanisms
ISO/IEC 14888-3:1998	Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Certificate-based mechanisms
ISO/IEC 14888-3:1998/Cor 1:2001	

International Organization for Standardization

JTC 1/SC 27
IT Security techniques

ISO/IEC 15292:2001	Information technology - Security techniques - Protection Profile registration procedures
ISO/IEC 15408-1:2005	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
ISO/IEC 15408-2:2005	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
ISO/IEC 15408-3:2005	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements
ISO/IEC TR 15443-1:2005	Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework
ISO/IEC TR 15443-2:2005	Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods
ISO/IEC TR 15446:2004	Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets
ISO/IEC 15816:2002	Information technology -- Security techniques -- Security information objects for access control
ISO/IEC 15945:2002	Information technology -- Security techniques -- Specification of TTP services to support the application of digital signature
ISO/IEC 15946-1:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General
ISO/IEC 15946-2:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures
ISO/IEC 15946-3:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 3: Key establishment
ISO/IEC 15946-4:2004	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 4: Digital signatures giving message recovery

International Organization for Standardization

JTC 1/SC 27
IT Security techniques

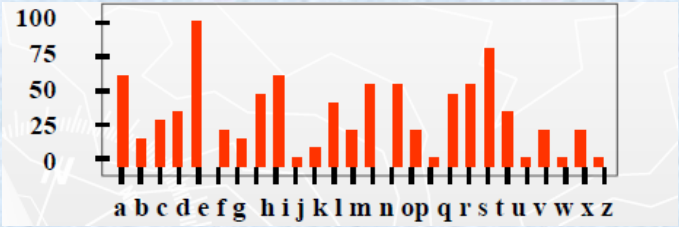
ISO/IEC TR 15947:2002	Information technology -- Security techniques -- IT intrusion detection framework
ISO/IEC 17799:2005	Information technology -- Security techniques -- Code of practice for information security management
ISO/IEC 18014-1:2002	Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework
ISO/IEC 18014-2:2002	Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens
ISO/IEC 18014-3:2004	Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens
ISO/IEC 18028-3:2005	Information technology -- Security techniques -- IT network security -- Part 3: Securing communications between networks using security gateways
ISO/IEC 18028-4:2005	Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access

International Organization for Standardization

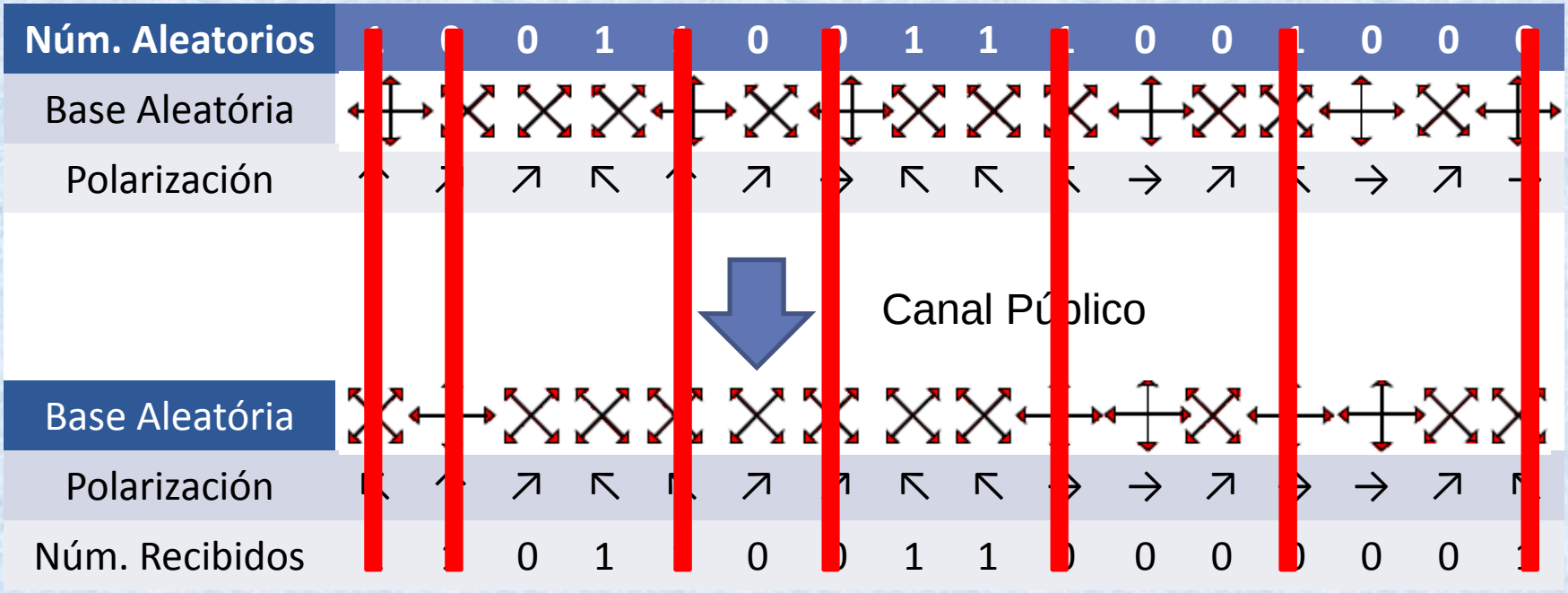
JTC 1/SC 27
IT Security techniques

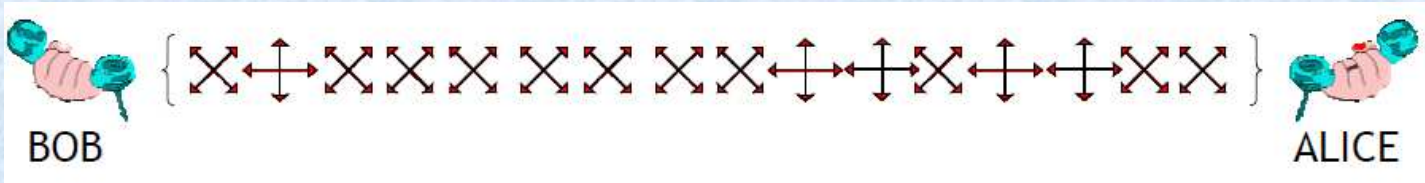
ISO/IEC 18031:2005	Information technology -- Security techniques -- Random bit generation
ISO/IEC 18032:2005	Information technology -- Security techniques -- Prime number generation
ISO/IEC 18033-1:2005	Information technology -- Security techniques -- Encryption algorithms -- Part 1: General
ISO/IEC 18033-3:2005	Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
ISO/IEC 18033-4:2005	Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers
ISO/IEC TR 18044:2004	Information technology -- Security techniques -- Information security incident management
ISO/IEC 18045:2005	Information technology -- Security techniques -- Methodology for IT security evaluation
ISO/IEC 21827:2002	Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM®)
ISO/IEC 27001:2005	Information technology -- Security techniques -- Information security management systems -- Requirements

Criptografía

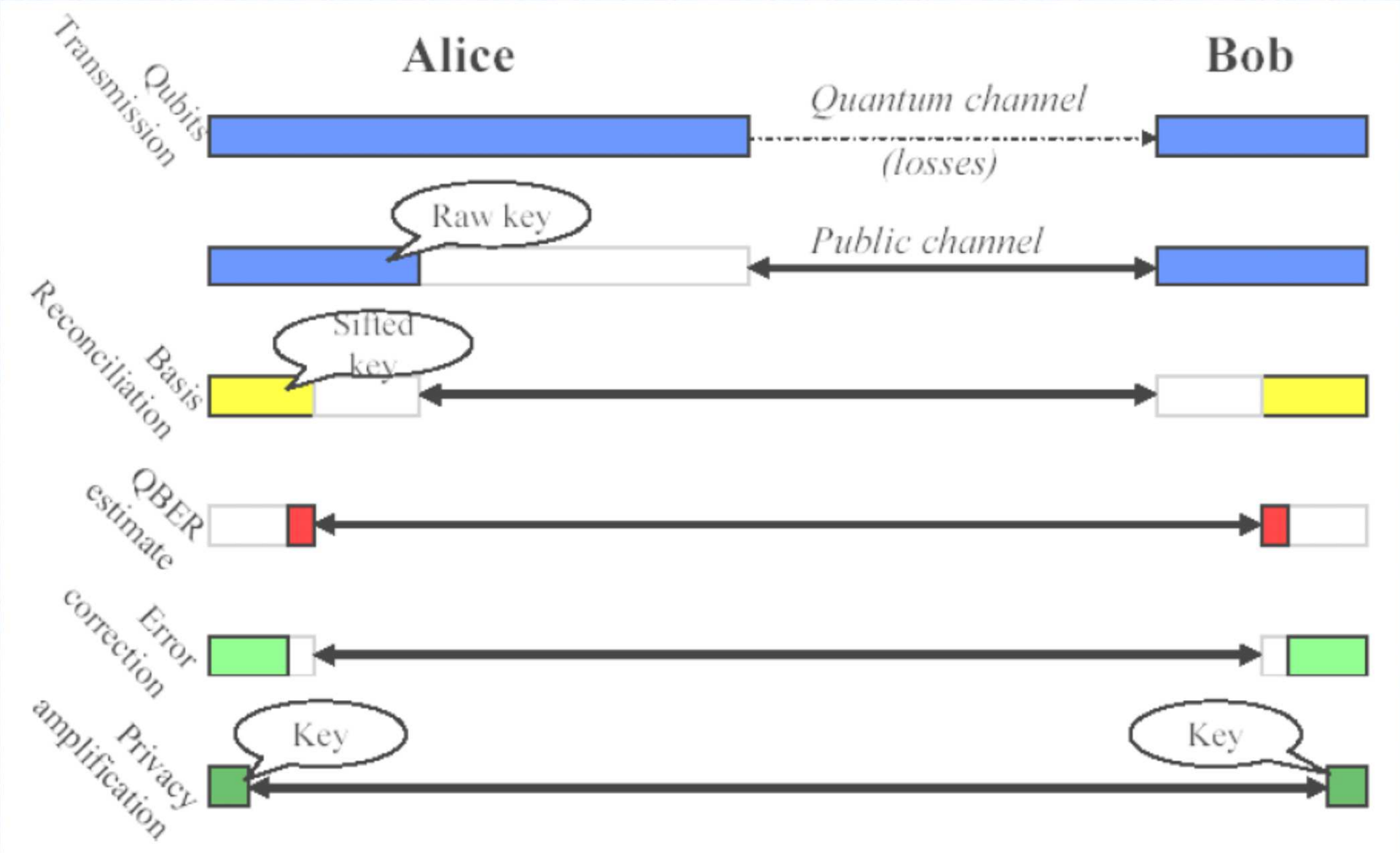


Criptografía Cuántica





Criptografía Cuántica



Computación Cuántica

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

Bit	Qubit

• Unidad información Clásica
• Reglas Mecánica Clásica
• Discreto: 2 posibles valores
  • 0 / 1
  • Verdadero / Falso
  • Arriba / Abajo
• Descripción matemática:
  • 0 1
• Computación Clásica:
  • Factorización en tiempo exponencial
  • Factorización número subprimo de 768 bit tardaría 2000 años aprox.
	• Unidad Información Cuántica
	• Reglas Mecánica Cuántica
	• Continuo: Superposición de los posibles estados.
	  • 0 y 1
	  • Verdadero y Falso
	  • Arriba y Abajo
	• Descripción matemática:
	  • $\|\phi\rangle = \alpha\|0\rangle + \beta\|1\rangle$
	• Computación Cuántica:
	  • Algoritmo de Shor
	  • Factorización en tiempo polinómico.
	  • Factorización número subprimo de 768 bit en tiempo factible (horas) en condiciones ideales.

GOBERNAR  TOMAR DECISIONES

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

IT-GOVERNANCE
PRIVACY GOVERNANCE

- ¿Qué decisiones se han de tomar?
- ¿Quién las ha de tomar?
- ¿Quién provee la información?
- ¿Cómo se han de tomar?
- ¿Cuándo se han de tomar?
- ¿Cómo se han de monitorizar y controlar?

Qué y Quien ?

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

		Principios IT		Arquitectura IT		Infraestructura		Aplicaciones de negocio		Inversión y Prioridades	
		Input	Decisión	Input	Decisión	Input	Decisión	Input	Decisión	Input	Decisión
1. Director ejecutivo (CEO) 2. Director financiero (CFO) 3. Directores áreas funcionales (CxO) 4. Director de S.I. (CIO) 5. Director de Seguridad (CISO) 6. Propietario del proceso de negocio 7. Director de Operaciones 8. Encargado de tratamiento 9. Director de Arquitectura 10. Director de Desarrollo 11. Director de Administración de TI. 12. Director Oficina de proyectos 13. Responsables de control. 14. Auditores de SI (externos o internos) 15. Consultores externos (outsourcing)	**Monarquía Negocios**										
	Monarquia IT										
	Federal										
	Duoplio IT										
	Feudal										

RACI CHART *(Font ITGI,USA 2007)*

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

RACI Chart

Functions

Activities	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Establish executive and board oversight and facilitation over IT activities.	A	R	C	C	C							C
Review, endorse, align and communicate IT performance, IT strategy, and resource and risk management with business strategy.	A	R	I	I	R							C
Obtain periodic independent assessment of performance and compliance with policies, plans and procedures.	A	R	C	I	C		I	I	I	I	I	R
Resolve findings of independent assessments, and ensure management's implementation of agreed-upon recommendations.	A	R	C	I	C		I	I	I	I	I	R
Generate an IT governance report.	A	C	C	C	R	C	I	I	I	I	I	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

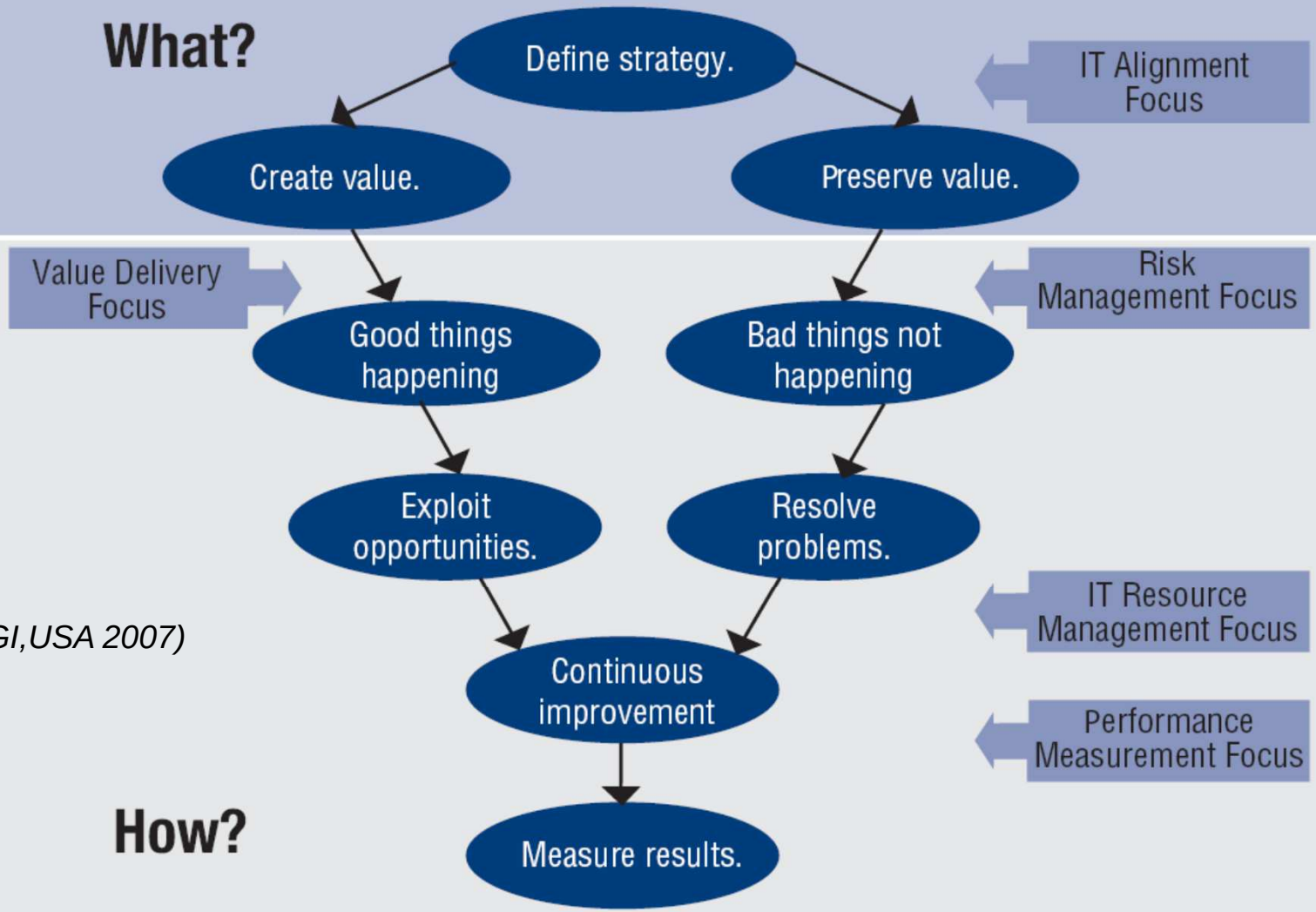
IT-GOVERNANCE

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

- **¿Cómo se han de tomar?**

CREACIÓN O CONSERVACIÓN DE VALOR

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE



(Font ITGI,USA 2007)

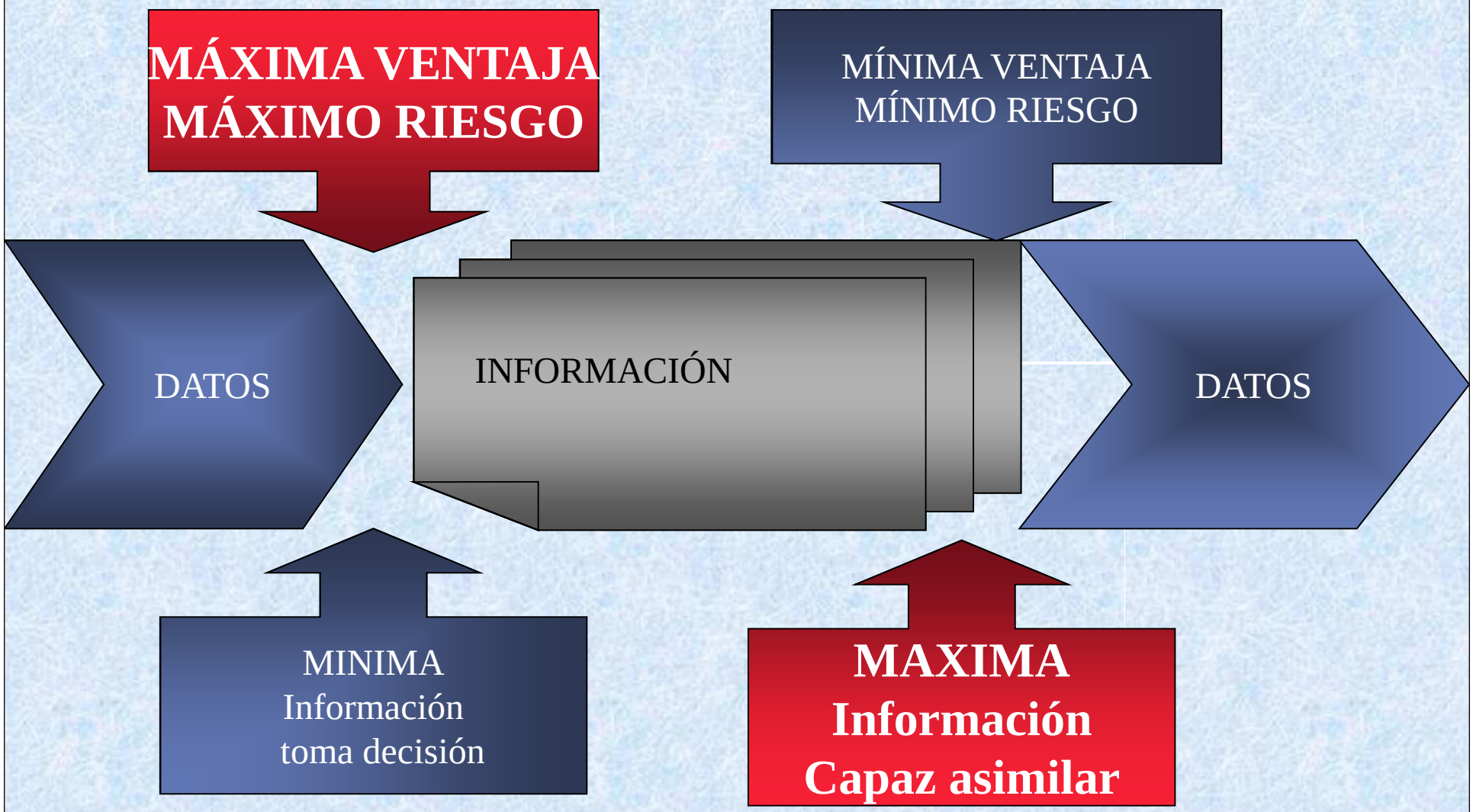
IT-GOVERNANCE

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

- **¿Cuándo se han de tomar?**

¿Cuándo se han de tomar ?

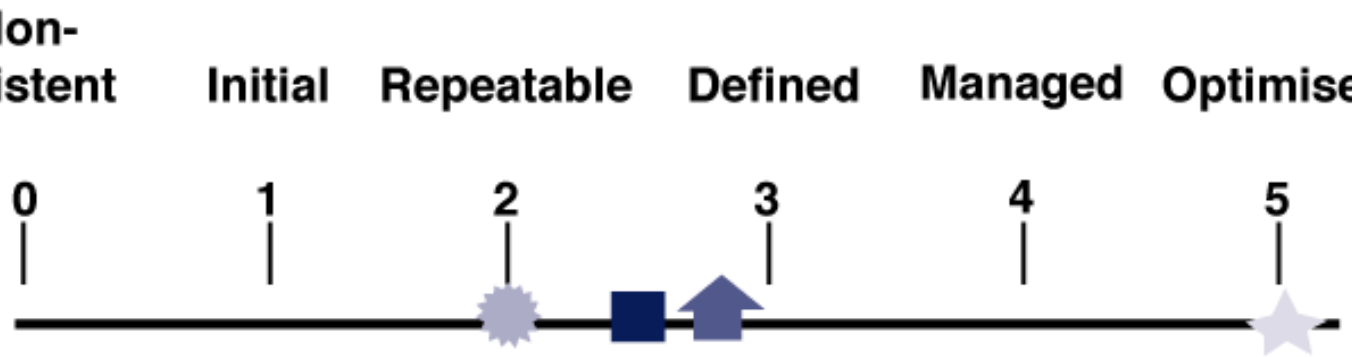
IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE



Modelos de Madurez

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

(Font IT Governance Institute Cobit 4.0, USA 2005)



LEGEND FOR SYMBOLS USED

- Enterprise Current Status
- International Standard Guidelines
- Industry Best Practice
- Enterprise Strategy

LEGEND FOR RANKINGS USED

0	Non-Existent	– Management processes are not applied at all
1	Initial	– Processes are ad hoc and disorganised
2	Repeatable	– Processes follow a regular pattern
3	Defined	– Processes are documented and communicated
4	Managed	– Processes are monitored and measured
5	Optimised	– Best practices are followed and automated

IT-GOVERNANCE

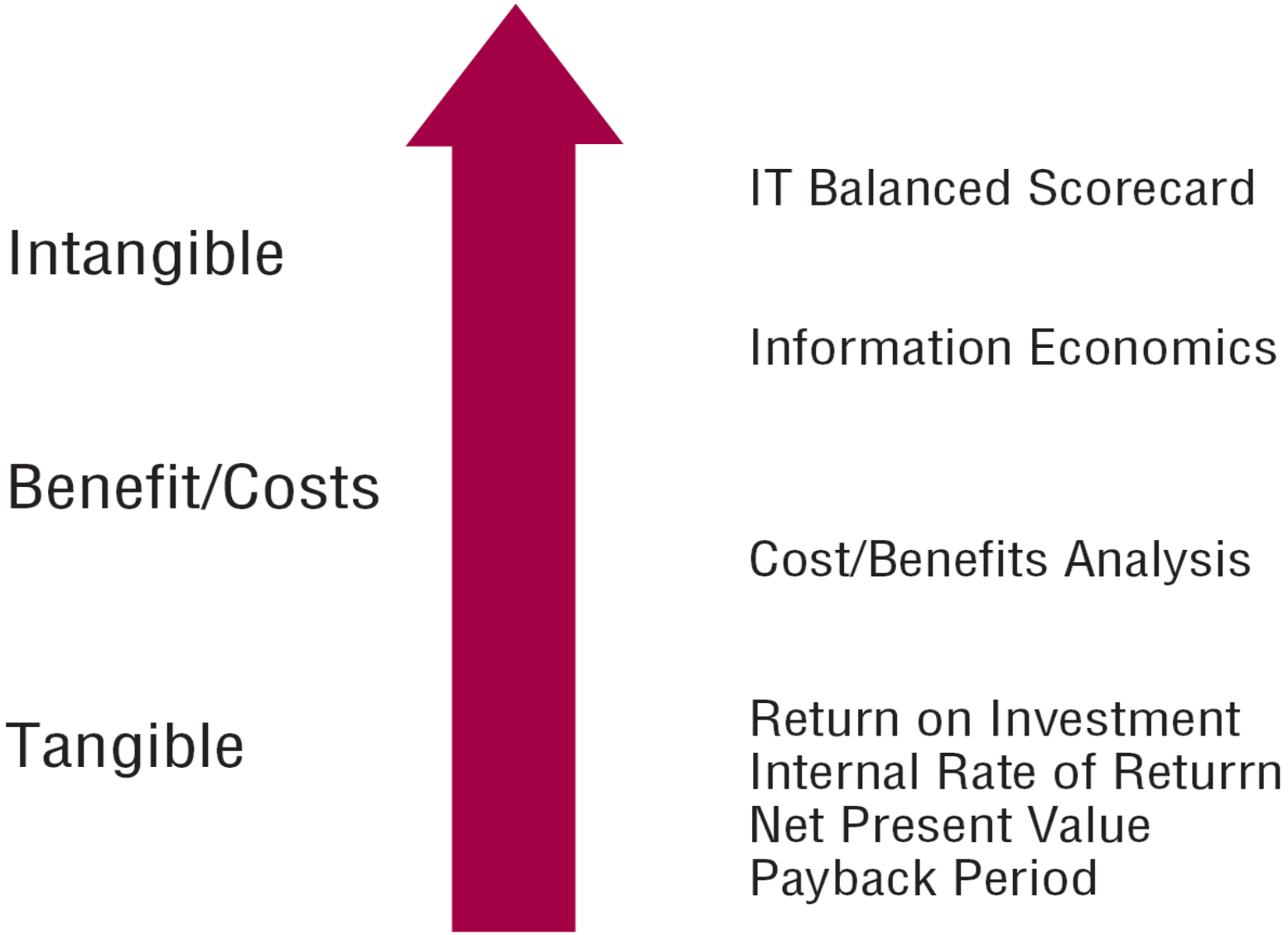
IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

- **¿Cómo se han de monitorizar**

y controlar?

Performance Measurement Approaches (ITGI-2005)

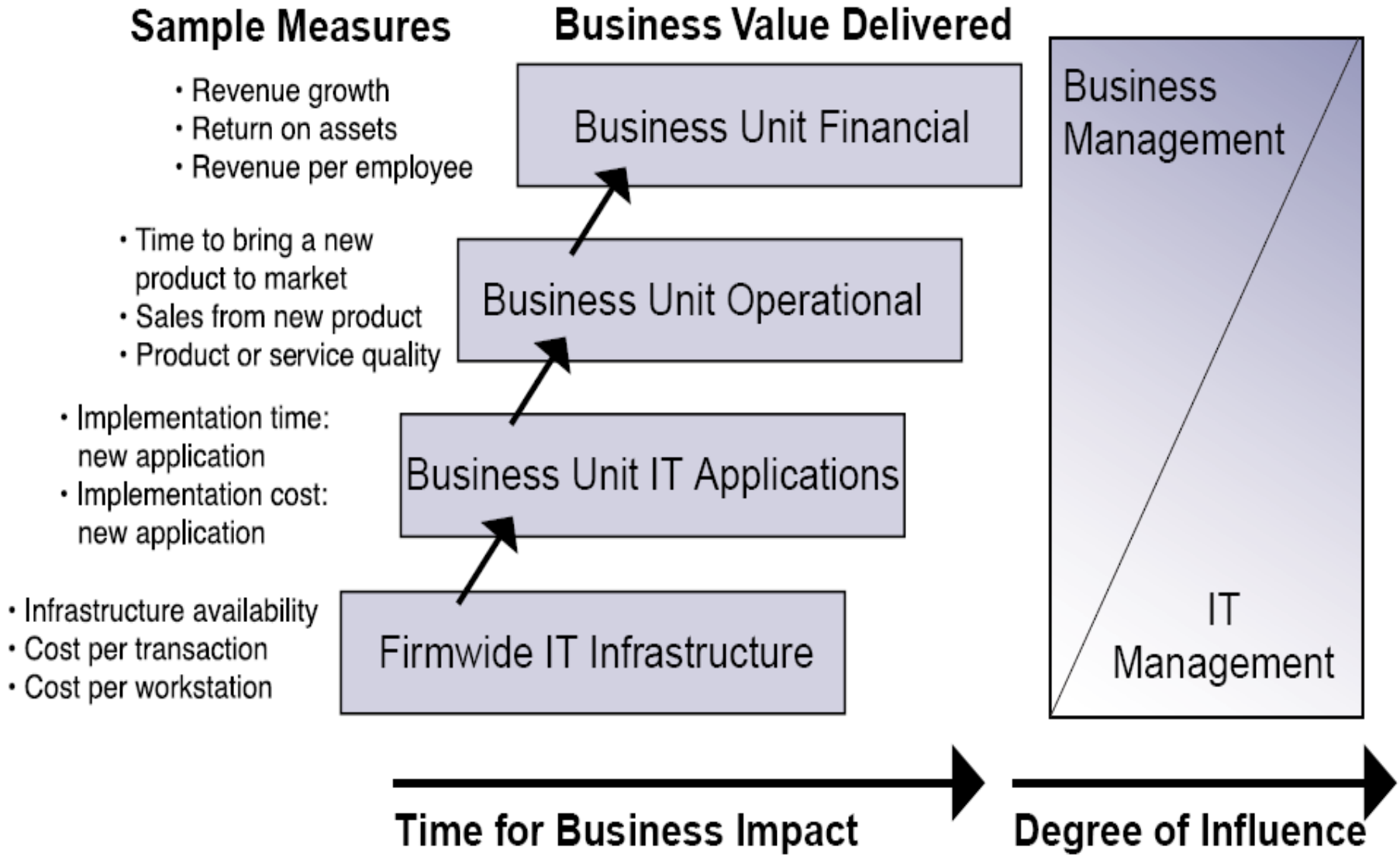
IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE



Business Value Hierarchy

(Font Weill & Broadbent. Leveraging the New Infrastructure. HBSP,1998)

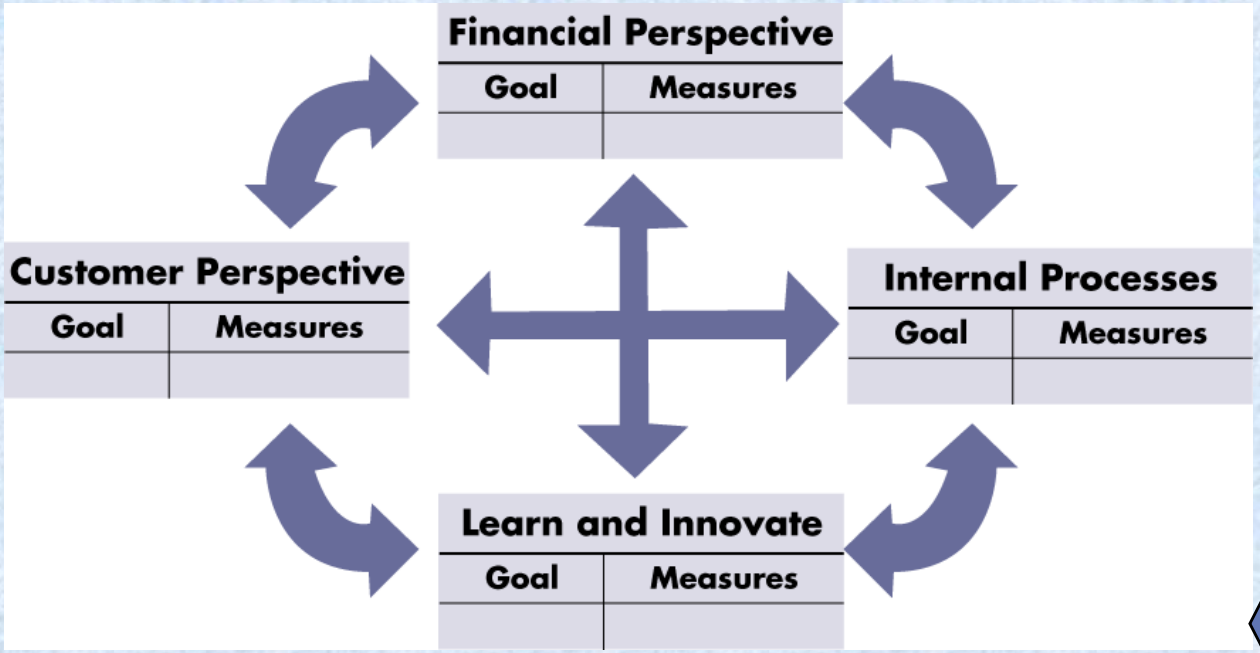
IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE



Indicadores de Objetivos(KGI)
Indicadores de Rendimiento (KPI)

(Font IT Governance Institute Cobit 4.0, USA 2005)

KGI



KPI

LA DIRECTIVA DE SEGURIDAD DE LA INFORMACIÓN

¿ Por qué ?

Ley N° 29733: DISPOSICIONES COMPLEMENTARIAS FINA

SEGUNDA. Directiva de seguridad

La Autoridad Nacional de Protección de Datos Personales elabora la directiva de seguridad de la información administrada por los bancos de datos personales en un plazo no mayor de ciento veinte días hábiles, contado a partir del día siguiente de la publicación de la presente Ley.

Medidas de Seguridad

Medidas de seguridad

El titular del Banco de Datos Personales debe de tomar medidas que garanticen la seguridad, eviten la alteración, pérdida o acceso no autorizado.

Medidas de Seguridad

(i) Seguridad para el tratamiento de la información digital.

Las bases de datos que utilicen un sistema de información digital deberán contar con medios de gestión por los cuales sea posible identificar al usuario que accede al sistema (se incluye las horas de inicio y cierre de sesión de los usuarios) como también las facultades con las que cuenta el usuario en la base de datos. También se deberán integrar mecanismos que restrinjan el acceso a la base de datos, como por ejemplo el uso de contraseñas o tokens.

(ii) Conservación respaldo y recuperación de los DP

Los ambientes y medios por los cuales se transmite, almacene o procese la información deben de estar acorde a las recomendaciones “NTP ISO/IEC 17799 EDI” vigentes.

(iii) Transferencia lógica y electrónica de DP.

La transferencia de la información sólo procederá con la autorización del titular del banco de datos personales. En el transporte del mismo se debe de evitar en todo momento el acceso no autorizado o corrupción de los datos personales implementando medidas de seguridad para tal fin.

Medidas de Seguridad

(i) Almacenamiento de información no automatizada.

Los armarios o archivadores donde se encuentren documentos no automatizados con datos personales deben de encontrarse en áreas en las que el acceso esté protegido por algún sistema de seguridad (automatizado o no). Las áreas donde se encuentren los datos personales deberán permanecer cerradas. En caso no sea posible contar con la infraestructura antes comentada se deberán de tomar medidas igualmente idóneas para la preservación de la información.

(ii) Copia o reproducción de la documentación.

Las copias a la información deberán ser realizadas únicamente por el personal autorizado. Las copias que sean desechadas deberán ser descartadas para evitar un indebido acceso a esta información.

(iii) Acceso a la documentación.

El acceso a los documentos que contienen datos personales será exclusivamente por el personal autorizado. De este modo también se implementarán mecanismos con la finalidad de poder reconocer al personal que tuvo acceso a la base de datos. Por último se añade que las personas no incluidas anteriormente y que tengan acceso deben de estar debidamente registradas.

(iv) Traslado de documentación no automatizada.

Se deberá evitar en todo momento el acceso o manipulación del material materia del traslado.

LA DIRECTIVA DE SEGURIDAD DE LA INFORMACIÓN

¿Para qué ?

Orientar sobre las condiciones, los requisitos, y las medidas técnicas que se deben tomar en cuenta para el cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales y su reglamento, aprobado a través del Decreto Supremo N° 003-2013-JUS, en materia de medidas de seguridad de los bancos de datos.

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

ESTRUCTURA

CONDICIONES

Constituyen recomendaciones que facilitan o generan impacto favorable para la implementación de los requisitos, habilitando un entorno apropiado para la comprensión y desarrollo de las actividades necesarias.

REQUISITOS

Corresponden a condiciones que deben ser demostrables, para considerar que se ha cumplido la presente directiva

MEDIDAS TÉCNICAS

Son aquellas que se consideran coherentes para cumplir con los requisitos.

LA DIRECTIVA DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVOS GENERALES

Garantizar la seguridad de los datos personales contenidos o destinados a ser contenidos en bancos de datos personales, mediante medidas de seguridad que protejan a los bancos de datos personales, en conformidad con la Ley N° 29733 y su reglamento

OBJETIVOS ESPECÍFICOS

Brindar lineamientos en el tratamiento de datos personales a cumplir por el titular del banco de datos personales para determinar:

- Las condiciones de seguridad.
- Las medidas organizativas.
- Las medidas legales.
- Las medidas técnicas.
- Las medidas de seguridad que resulten apropiadas, en función a las características de cada caso concreto, a partir de considerar criterios de diferenciación basados en las características del tratamiento de datos personales que se vaya a efectuar y en las características de datos personales que se tratan.

Condiciones de Seguridad

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

Condiciones de Seguridad Externas:

- Marco legal apropiado (leyes, reglamentos o similares

- Conocimiento y conciencia (conocer la importancia de la protección de los datos personales, la Ley Nº29733, Ley de Protección de Datos Personales, y su reglamento.

Condiciones de Seguridad Internas:

- Compromiso del titular del banco de datos personales (para brindar los recursos y dirección en la protección de los datos personales).

- Comprender el contexto institucional en el tratamiento y protección de los datos personales.

- Determinar claramente las responsabilidades y roles organizacionales con la suficiente autoridad y recursos.

- Enfoque de gestión del riesgo de los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales.

Requisitos de Seguridad

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

Determinar y dar a conocer una política de protección de datos personales :

Declaración breve que demuestre el compromiso.

Mantener la gobernabilidad completa de los procesos involucrados en el tratamiento de los datos personales; conocer procesos y procedimientos.

Implementación de las medidas de seguridad.

Implementar y mantener los procedimientos documentados.

Adoptar un enfoque de riesgos y basar las decisiones en el plan de tratamiento de riesgos del banco de datos personales.

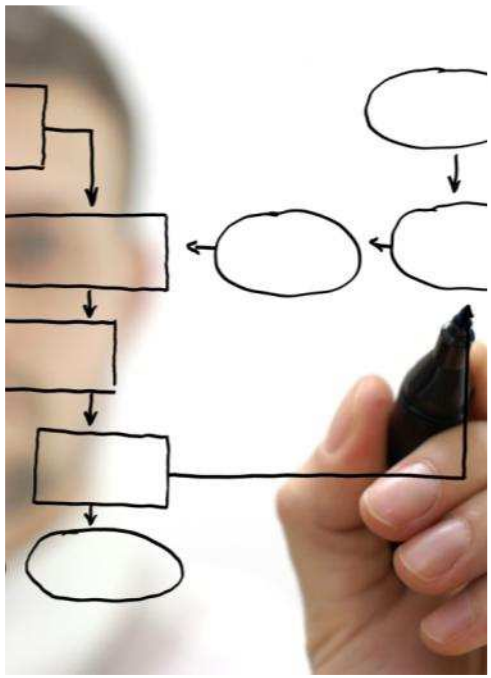
Alineamiento a los requisitos según ISO/IEC 27001 en su edición vigente, incorporando dentro del alcance del SGSI los bancos de datos personales.

Desarrollar y mantener un documento maestro de seguridad de la información del banco de datos personales.

LA LPDP

Obligaciones de las Organizaciones

Obligaciones Legales



Obligaciones Organizativas

Obligaciones Técnicas

Medidas de Seguridad Jurídicas

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

Mantener los formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para la cual son acopiados

Adecuación de los contratos del personal relacionado con el tratamiento de datos personales y de los contratos con terceros.

Desarrollar y mantener actualizado un documento de compromiso de confidencialidad en el tratamiento de datos personales.

Medidas de Seguridad Organizativas

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

Desarrollar una estructura organizacional con roles y responsabilidades de acuerdo a la proporcionalidad de los datos a proteger.

Adecuación de los sistemas de gestión, aplicaciones existentes y procesos de negocio que intervengan en el tratamiento de datos personales a los requisitos establecidos en la Ley Nº29733 y su reglamento.

Compromiso documentado de respeto a los principios de la ley.
Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación.

Llevar un control de registro de los operadores con acceso al banco de datos personales (Trazabilidad).

Desarrollar:
-Procedimientos documentados adecuados para el tratamiento de datos personales
- Un programa de creación de conciencia y entrenamiento en materia de protección de datos.
-Un procedimiento de auditoría respecto de las medidas de seguridad implementadas, teniendo como mínimo una auditoría anual.
-Un procedimiento de gestión de incidentes para la protección de datos.
-Un procedimiento de asignación de privilegios de acceso al banco de datos personales y su correspondiente registro de acceso.

Medidas de Seguridad Técnicas

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

Gestión y uso de contraseñas cuando el tratamiento se realice con medios informáticos

Revisión y registro de los privilegios de acceso.

Proteger el banco de datos personales contra acceso físico no autorizado mediante mecanismo de bloqueo físico.

Cuando se utilicen mecanismos informáticos para el tratamiento, se debe proteger el banco de datos personales contra acceso lógico no autorizado mediante algún mecanismo de bloqueo lógico, limitando el acceso solo a los involucrados

El titular del banco de datos personales, o quien este designe, debe autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales.
Dicha autorización debe registrarse.

Identificar los accesos realizados a los datos personales para su tratamiento.

Autorización para el retiro de datos personales.

Eliminación de la información contenida en medios informáticos removibles.

Seguridad de la copia o reproducción de documentos.

Se deben realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción.

SECCIÓN	CONTROL ISO 27001:2013		DIRECTIVA DE SEGURIDAD	SISTEMA
A5	**Políticas de seguridad de la información**			
A5.1	**Orientación de administración para la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	1.3.1.1	Determinar y dar a conocer una política de protección de datos personales	**No Implementado**
A5.1.2	Revisión de las políticas para la seguridad de la información	2.1.4	Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento	**No Implementado**
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Revisiones de los roles y responsabilidades de la seguridad en la información	2.1.1	Desarrollar una estructura organizacional con roles y responsabilidades de acuerdo a la proporcionalidad de los datos a	**No Implementado**
A6.1.2	Segregación de deberes			**No Implementado**
A6.1.3	Contacto con las autoridades			**No Implementado**
A6.1.4	Contacto con grupos de interés especiales			**No Implementado**
A6.1.5	Seguridad de la información en la administración de proyectos			**No Implementado**
A6.2	**Dispositivos móviles y teletrabajo**			
A6.2.1	Política de dispositivos móviles			**No Implementado**
A6.2.2	Teletrabajo			**No Implementado**
A7	**Seguridad de Recursos Humanos**			
A7.1	**Antes del empleo**			
A7.1.1	Selección	2.2.1	Mantener los formatos de consentimiento para el tratamiento de datos personales.	**No Implementado**
A7.1.2	Términos y condiciones de empleo	2.2.2	Adecuación de los contratos del personal relacionado con el tratamiento de datos personales	**No Implementado**
A7.2	**Responsabilidades de la dirección**			
A7.2.1	Responsabilidades de la dirección			**No Implementado**
A7.2.2	Concientización, educación y capacitación sobre la seguridad de la información	2.1.8	Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.	**No Implementado**
A7.2.3	Proceso disciplinario			**No Implementado**
A7.3	**Cese o cambio de puesto de trabajo**			
A7.3.1	Cese o cambio de puesto de trabajo			**No Implementado**

SECCIÓN	CONTROL ISO 27001:2013		DIRECTIVA DE SEGURIDAD	SISTEMA
A5	**Políticas de seguridad de la información**			
A5.1	**Orientación de administración para la seguridad de la información**			
A5.1.1	Políticas para la seguridad de la información	1.3.1.1	Determinar y dar a conocer una política de protección de datos personales	**No Implementado**
A5.1.2	Revisión de las políticas para la seguridad de la información	2.1.4	Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales.	**No Implementado**
A6	**Organización de la seguridad de la información**			
A6.1	**Organización interna**			
A6.1.1	Revisiones de los roles y responsabilidades de la seguridad en la información	2.1.1	Desarrollar una estructura organizacional con roles y responsabilidades de acuerdo a la proporcionalidad de los datos a proteger.	**No Implementado**
A6.1.2	Segregación de deberes			**No Implementado**
A6.1.3	Contacto con las autoridades			**No Implementado**
A6.1.4	Contacto con grupos de interés especiales			**No Implementado**
A6.1.5	Seguridad de la información en la administración de proyectos			**No Implementado**
A6.2	**Dispositivos móviles y teletrabajo**			
A6.2.1	Política de dispositivos móviles			**No Implementado**
A6.2.2	Teletrabajo			**No Implementado**

A7	Seguridad de Recursos Humanos			
A7.1	**Antes del empleo**			
A7.1.1	Selección	2.2.1	Mantener los formatos de consentimiento para el tratamiento de datos personales.	**No Implementado**
A7.1.2	Términos y condiciones de empleo	2.2.2	Adecuación de los contratos del personal relacionado con el tratamiento de datos personales	**No Implementado**
A7.2	**Responsabilidades de la dirección**			
A7.2.1	Responsabilidades de la dirección			**No Implementado**
A7.2.2	Concientización, educación y capacitación sobre la seguridad de la información	2.1.8	Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.	**No Implementado**
A7.2.3	Proceso disciplinario			**No Implementado**
A7.3	**Cese o cambio de puesto de trabajo**			
A7.3.1	Cese o cambio de puesto de trabajo			**No Implementado**

A8	Administración de activos			
A8.1	**Responsabilidad por los activos**			
A8.1.1	Inventario de activos			**No Implementado**
A8.1.2	Propiedad de los activos			**No Implementado**
A8.1.3	Uso aceptable de activos			**No Implementado**
A8.1.4	Devolución de activos			**No Implementado**
A8.2	**Clasificación de la información**	**1.1**	**Categoría**	
A8.2.1	Clasificación de información	1.1.1	Para efectos de la presente directiva, se debe considerar la siguiente clasificación de categorías en el tratamiento de datos personales y el principio de proporcionalidad descrito en el artículo 7 de la Ley N° 29733 cuando no exista coincidencia exacta.	**No Implementado**
A8.2.2	Etiquetado de información	1.1.3	Matriz de apoyo para la selección de categoría en el tratamiento de datos personales.	**No Implementado**
A8.2.3	Manejo de activos			**No Implementado**
A8.3	**Manejo de medios**			
A8.3.1	Administración de medios extraíbles	2.3.2.1/2.3.2.2	Autorización para el retiro o traslado de datos personales.	**No Implementado**
A8.3.2	Eliminación de medios	2.3.2.3	Eliminación de la información contenida en medios informáticos removibles	**No Implementado**
A8.3.3	Soportes físicos en tránsito			**No Implementado**

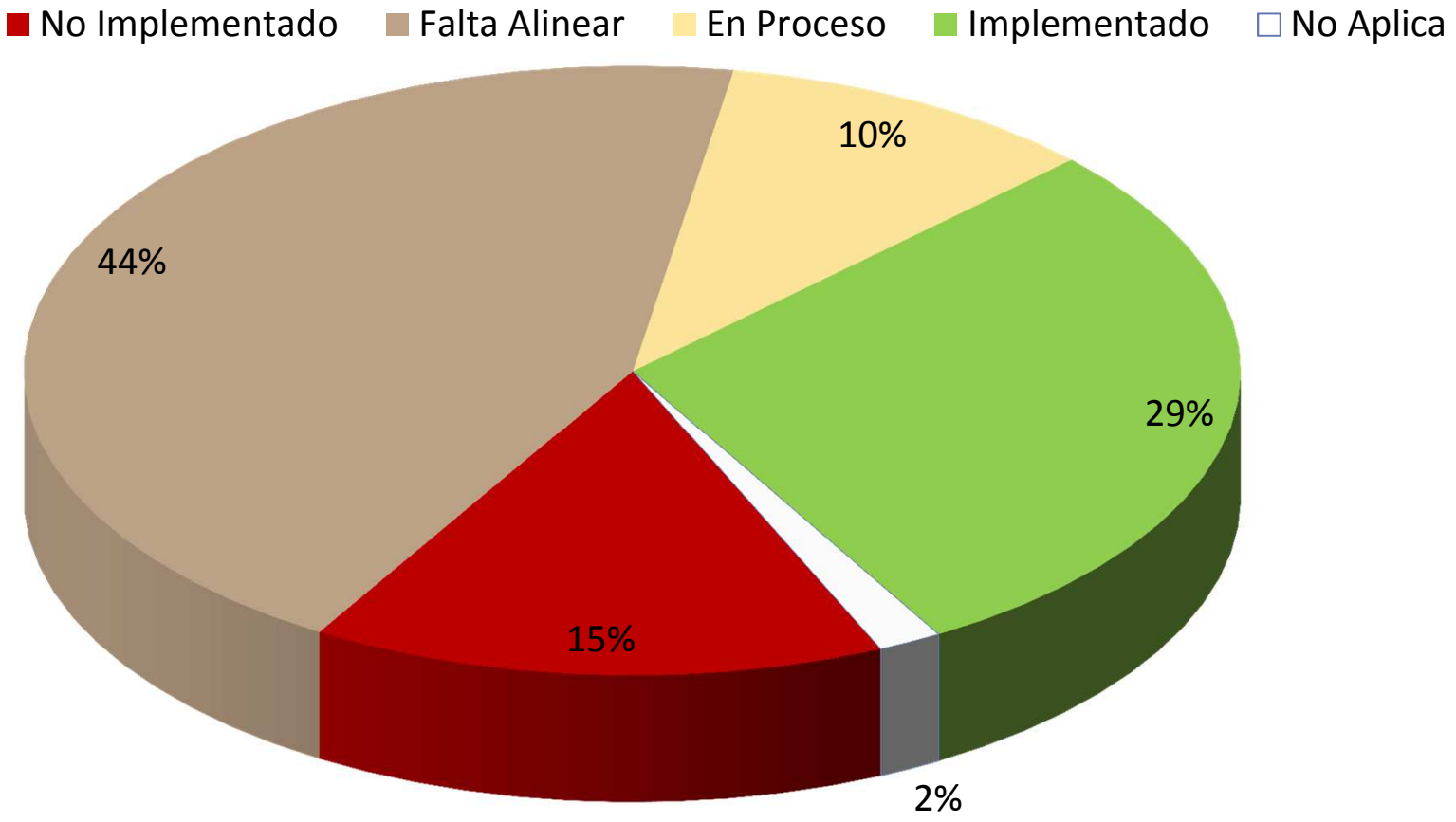
A9	Control de acceso			
A9.1	**Requisitos comerciales del control de acceso**			
A9.1.1	Política de control de acceso	2.3.1.2	Revisión y registro de los privilegios de acceso.	**No Implementado**
A9.1.2	Control de acceso a las redes y servicios asociados			**No Implementado**
A9.2	**Administración de acceso a los usuarios**			
A9.2.1	Gestión de altas/bajas en el registro de usuarios	2.3.1.5	El titular del banco de datos personales, o quien este designe, debe autorizar o retirar el acceso de usuarios que realicen tratamiento de datos personales. Dicha autorización debe registrarse.	**No Implementado**
A9.2.2	Gestión de los derechos de acceso asignados a usuarios			**No Implementado**
A9.2.3	Gestión de los derechos de acceso con privilegios especiales	2.3.2.5	El titular del banco de datos personales, o quien éste designe, debe asignar o retirar el privilegio o privilegios (datos a tratar o tarea a realizar) para el tratamiento de datos personales a usuarios autorizados.	**No Implementado**
A9.2.4	Gestión de información confidencial de autenticación de usuarios			**No Implementado**
A9.2.5	Revisión de los derechos de acceso de usuarios	2.3.1.2	Revisión y registro de los privilegios de acceso.	**No Implementado**
A9.2.6	Eliminación o ajuste de los derechos de acceso			**No Implementado**
A9.3	**Responsabilidades de los usuarios**			
A9.3.1	Uso de información confidencial para la autenticación.			**No Implementado**
A9.4	**Control de acceso de sistemas y aplicaciones**			
A9.4.1	Restricción de acceso a la información	2.3.1.6	Identificar los accesos realizados a los datos personales para su tratamiento.	**No Implementado**
A9.4.2	Procedimientos de inicio de sesión seguros			**No Implementado**
A9.4.3	Sistema de administración de contraseñas	2.3.1.1	Gestión y uso de contraseñas cuando el tratamiento se realice con medios informáticos.	**No Implementado**
A9.4.4	Uso de programas de utilidad privilegiados			**No Implementado**
A9.4.5	Control de acceso al código de fuente del programa			**No Implementado**

A11	Seguridad física y ambiental			
A11.1	**Areas seguras**			
A11.1.1	Perímetro de seguridad física			No Implementado
A11.1.2	Controles de entrada física	2.3.1.3	Proteger el banco de datos personales contra acceso físico no autorizado mediante algún mecanismo de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados (en caso de banco de datos personales no autorizado).	No Implementado
A11.1.3	Protección de oficinas, salas e instalaciones			No Implementado
A11.1.4	Protección contra las amenazas externas y ambientales			No Implementado
A11.1.5	Trabajo en áreas seguras			No Implementado
A11.1.6	Áreas de acceso público, carga y descarga.			No Implementado
A11.2	**Equipos**			
A11.2.1	Emplazamiento y protección de equipos			No Implementado
A11.2.2	Instalaciones de suministro			No Implementado
A11.2.3	Seguridad del cableado			No Implementado
A11.2.4	Mantenimiento de equipos	2.3.4.3	Los equipos utilizados para el tratamiento de los datos personales deben recibir mantenimiento preventivo y correctivo de acuerdo a las recomendaciones y especificaciones del proveedor para asegurar su disponibilidad e integridad. El mantenimiento de los equipos debe ser realizado por personal autorizado.	No Implementado
A11.2.5	Salida de activos fuera de las dependencias de la empresa			No Implementado
A11.2.6	Seguridad de los equipos y activos fuera de las instalaciones			No Implementado
A11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento			No Implementado
A11.2.8	Equipo informático de usuario desatendido			No Implementado
A11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.			No Implementado

A12	Seguridad de las operaciones			
A12.1	**Procedimientos y responsabilidades operacionales**			
A12.1.1	Documentación de procedimientos de operación			No Implementado
A12.1.2	Gestión de cambios			No Implementado
A12.1.3	Gestión de capacidades			No Implementado
A12.1.4	Separación de entornos de desarrollo, prueba y producción			No Implementado
A12.2	**Protección contra código malicioso**			
A12.2.1	Controles contra el código malicioso	2.3.4.4	Los equipos utilizados para el tratamiento de los datos personales deben contar con software de protección contra software malicioso (virus, troyanos, spyware, etc.), para proteger la integridad de los datos personales. El software de protección debe ser actualizado frecuentemente de acuerdo a las recomendaciones y especificaciones del proveedor.	No Implementado
A12.3	**Copias de seguridad**			
A12.3.1	Copias de seguridad de la información	2.3.2.4	Seguridad en la copia o reproducción de documentos.	No Implementado
A12.3	**Registro de actividad y monitoreo .**			
A12.4.1	Registro de eventos	2.3.4.9	Todo evento identificado que afecte la confidencialidad, integridad y disponibilidad de los datos personales, o que indique un posible incumplimiento de las medidas de seguridad establecidas, debe ser reportado inmediatamente al encargado del banco de datos personales.	No Implementado
A12.4.2	Protección del registro de información			No Implementado
A12.4.3	Registros de actividad del administrador y operador del sistema			No Implementado
A12.4.4	Sincronización con relojes			No Implementado
A12.5	**Control de software operacional**			
A12.5.1	Instalación del software en sistemas en producción			No Implementado
A12.6	**Administración de vulnerabilidades técnicas**			
A12.6.1	Gestión de la vulnerabilidad técnica			No Implementado
A12.6.2	Restricciones en la instalación de software			No Implementado
A12.7	**Consideraciones sobre la auditoría de los sistemas de información**			
A12.7.1	Controles de auditoría de los sistemas de información	2.3.4.11	Se debe realizar una auditoría sobre el cumplimiento de la presente directiva, bajo responsabilidad del titular del banco de datos personales.	No Implementado

A13	Seguridad en las comunicaciones			
A13.1	**Administración de la seguridad de redes**			
A13.1.1	Controles de red			**No Implementado**
A13.1.2	Seguridad de los servicios de redes	2.3.4.6	La información de datos personales que se transmite electrónicamente debe ser protegida para preservar su confidencialidad e integridad.	**No Implementado**
A13.1.3	Segregación en las redes			**No Implementado**
A13.2	**Transferencia de información**			
A13.2.1	Políticas y procedimientos sobre la transferencia de información			**No Implementado**
A13.2.2	Acuerdos sobre la transferencia de información			**No Implementado**
A13.2.3	Mensajería electrónica	2.3.5.3	a) Transporte electrónico de datos personales en forma cifrada, lo cual puede realizarse mediante el cifrado de la información antes de su transmisión o mediante el uso de protocolos de comunicación cifrados (Ejemplo: VPN, correo electrónico cifrado, FTP seguro, entre otros). b) Uso de firmas digitales para validar la identidad del emisor de la información.	**No Implementado**
A13.2.4	Confidencialidad de los acuerdos de no divulgación			**No Implementado**

Resultados de Evaluación Directiva de Seguridad



- ¿ Hasta dónde queremos llegar?
- ¿El beneficio justifica el coste ?
- ¿Cuál es el nivel de Control para mis Sistemas de Información?

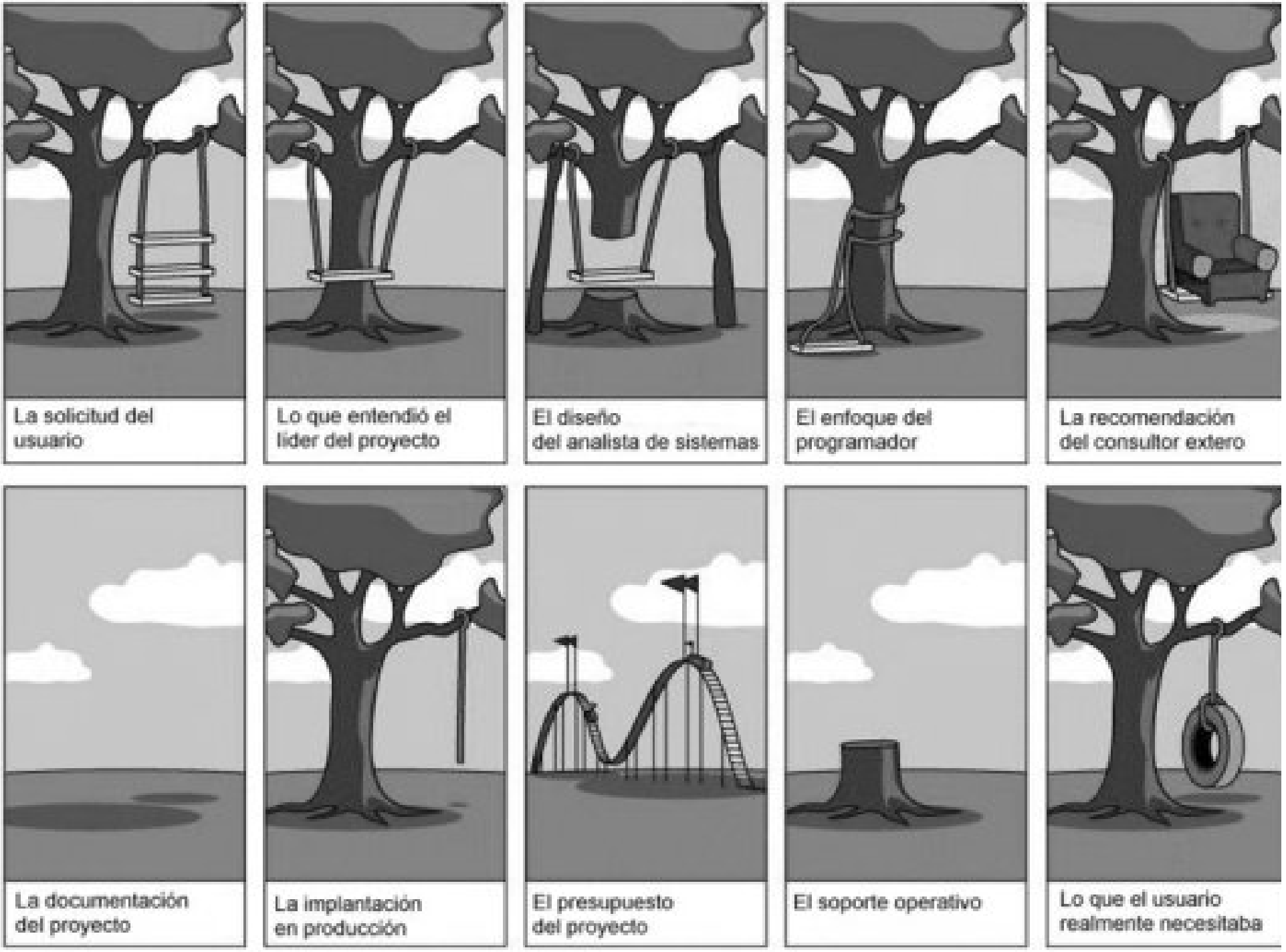
RETO ESTRATÉGICO

1. Sea Proactivo, no reactivo
2. Sepa cuando rediseñar
3. Involucre a todos los altos directivos
4. Tome decisiones
5. Clarifique el manejo de las Excepciones
6. Incentive adecuadamente
7. Asigne propiedad y responsabilidades
8. Considere diferentes niveles
9. Sea Transparente y eduque
10. Implemente mecanismos comunes

RETO TÁCTICO

Paso a la acción: Implementación

- 1.- Priorizar acciones
  - Especial énfasis matriz de riesgo ALTO
- 2.- Evaluar recomendaciones
  - No siempre los controles o procesos recomendados son los adecuados a nuestra organización
- 3.- Analizar coste-beneficio
  - Descripción del coste y beneficio de implementar o no
- 4.- Seleccionar controles y procesos
  - Deben combinarse controles de gestión, operacionales y técnicos
  - Medidas organizativas y técnicas
- 5.- Asignar responsabilidades
  - Personal interno y externo
- 6.- Desarrollar un plan de acción
  - Equipo responsable, fechas, costes, …
- 7.- Implementar los controles y procesos seleccionados
  - Reduciremos el riesgo pero no lo eliminaremos


La solicitud del usuario
Lo que entendió el líder del proyecto
El diseño del analista de sistemas
El enfoque del programador
La recomendación del consultor extero
La documentación del proyecto
La implantación en producción
El presupuesto del proyecto
El soporte operativo
Lo que el usuario realmente necesitaba

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

Antoni Bosch Pujol, CISA, CISM, CGEIT, ECPD

Director General Institute of Audit & IT-Governance.

www.iaitg.eu

Director Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC de la Universidad Autónoma de Madrid.

www.uam.es/masgdtic

www.privacyperu.com