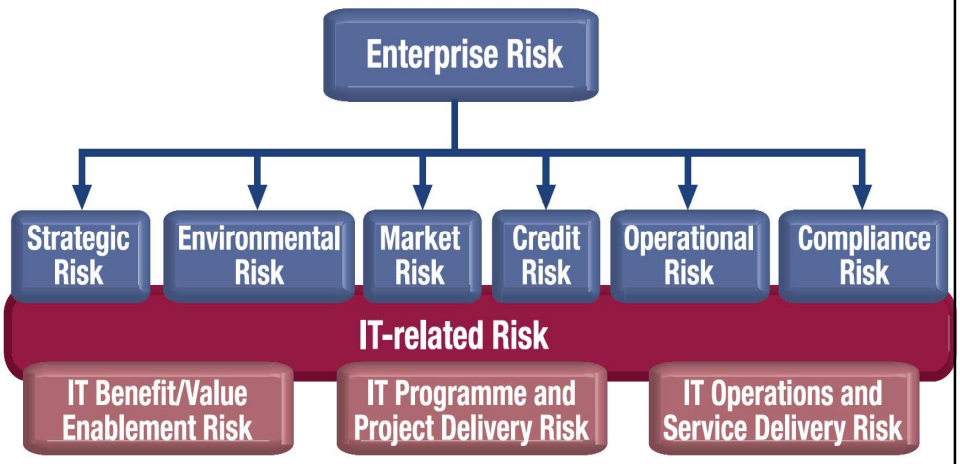
La privacidad en el marco de la prevención del delito en la empresa y las organizaciones: Riesgos Tecnológicos

***Antoni Bosch i Pujol*, CGEIT, CISA, CISM**

Director General Institute of Audit & IT-Governance (IAITG)
Director Data Privacy Institute (DPI-ISMS)
Presidente Fundador ISACA-Barcelona

antoni.bosch@iaitg.eu
http://es.linkedin.com/in/antonibosch

Risk IT. ISACA 2009



IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

IT Risk

(Font Westerman. MIT Sloan CISR,2005)

Enterprise IT Risks

Continuity	Access Management	Integrity	Strategic Change
• Availability • Business continuity • Disaster recovery	• Information protection • Knowledge sharing • Preventing malicious attacks	• Data accuracy, timeliness, and consistency • Regulatory compliance	• Ability to implement major strategic change

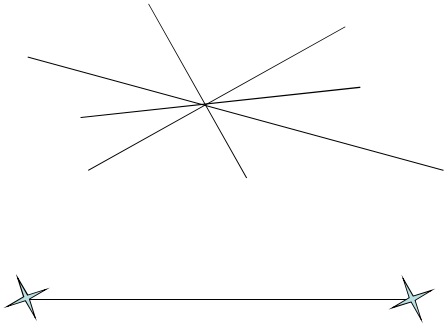
IT Risk Factors

Technology & Infrastructure	Applications & Information	People & Skills	Vendors & Other Partners	Policy & Process	Organizational
• Configuration management • Degree of standardization • Age of technology	• Architecture complexity • Redundancy • Data consistency • Degree of customization	• Turnover • Skills planning • Recruiting/ training • IT/Business Relationship	• SLAs • Use of firm's methods/standards • Sole source • Customer risk tolerance	• Controls architecture • Degree of standardization • Degree of accountability	• Cost cutting • Organizational Complexity • Funding processes

External Threats
New regulation
Virus
Geopolitical

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

De pequeños nos enseñaron:



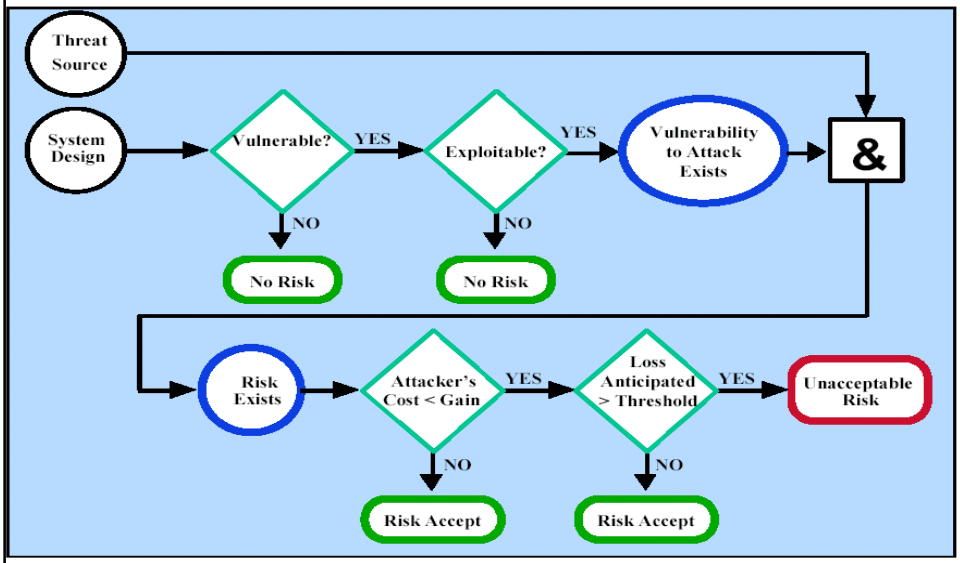
IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

El gran problema del consejo de administración

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque el atacante era muy listo y tenía muchos medios

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

(NIST SP 800-30)

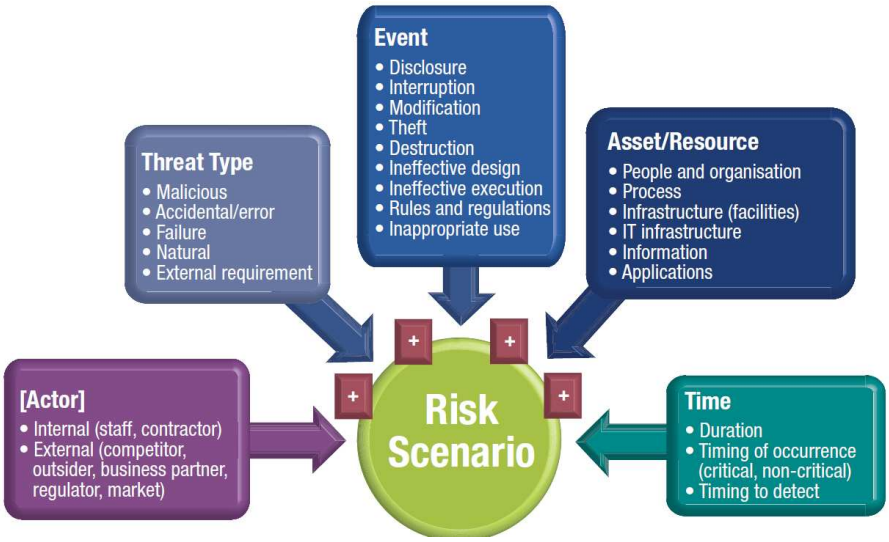


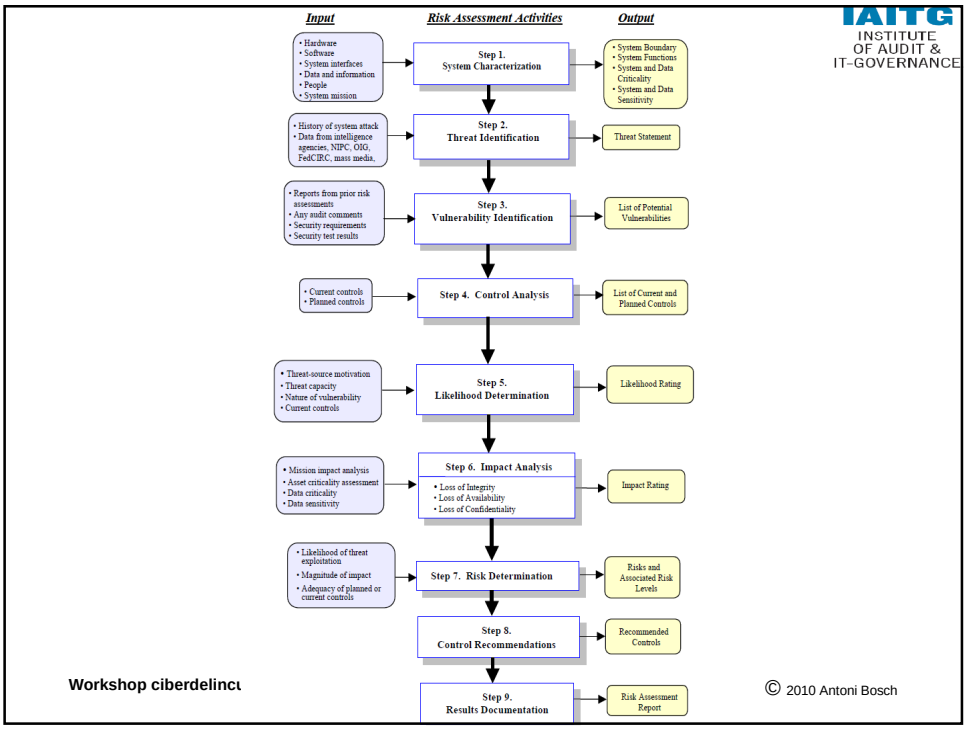
IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque no habíamos implantado un sistema de análisis de riesgos

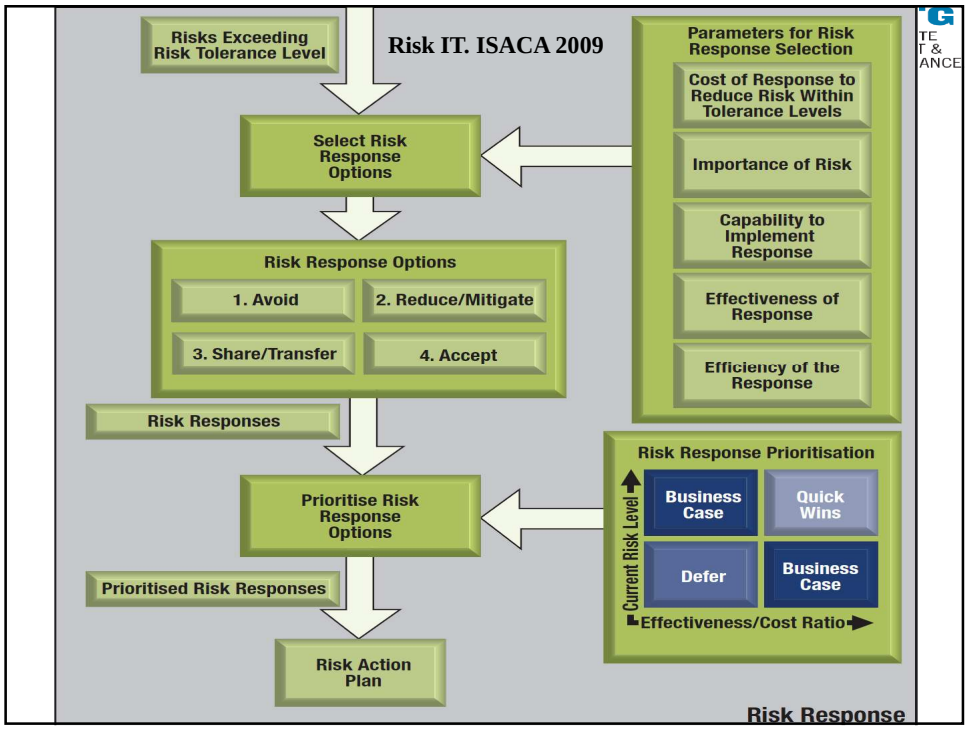
Risk IT. ISACA 2009

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE





- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque nos faltaba la gestión de riesgos

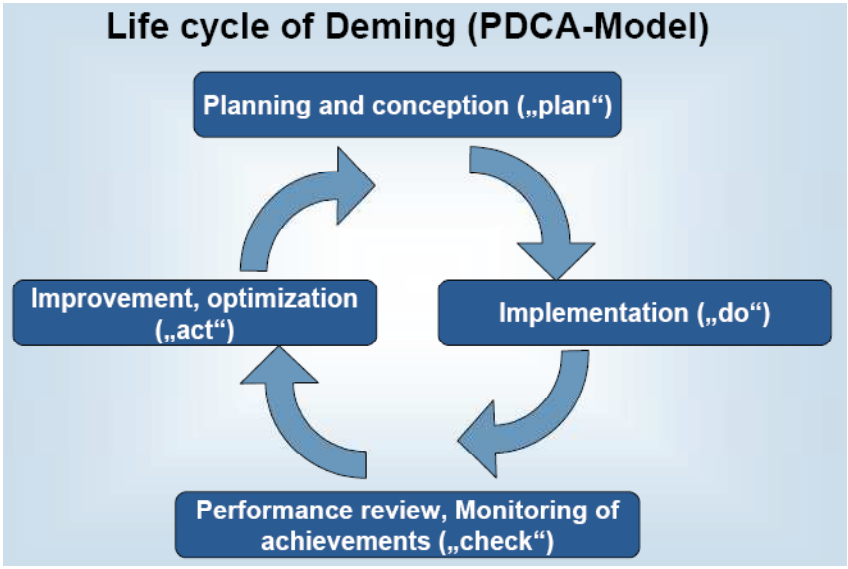


IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque no teníamos un sistema de gestión de seguridad

IT Baseline Protection Manual

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE



IT Baseline Protection Manual

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

The lifecycle of an IT security policy

P

IT security Conception
- Selecting a method for risk
- Classifying risks and
- Risk assessment
- Developing a strategy for dealing with
- Selecting IT security

D

Implementing
- Development an implementation plan for the IT security
- Implementation of IT security
- Supervising and controlling the
- Developing strategies for security
- Training and improving

C

Performance review
- Detection of IT security incidents during usual
- Checking if the requirements are being complied
- Checking the suitability and efficacy of IT security
- Checking the efficiency of the IT security
- Management

A

Improvement,
- Debugging
- Improving the IT security

ISO 27000

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

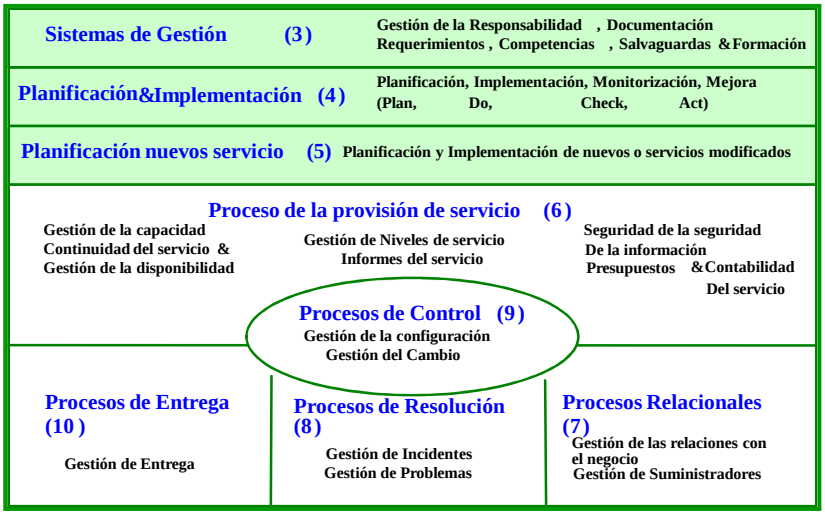
9-GESTIÓN DE INCIDENCIAS

10-GESTIÓN DE CONTINUIDAD DEL NEGOCIO

11-CUMPLIMIENTO

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque no habíamos implantado un sistema de gestión de servicios TI

ISO 20000



- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque nos faltaban más estándares que seguir

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 signatures
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

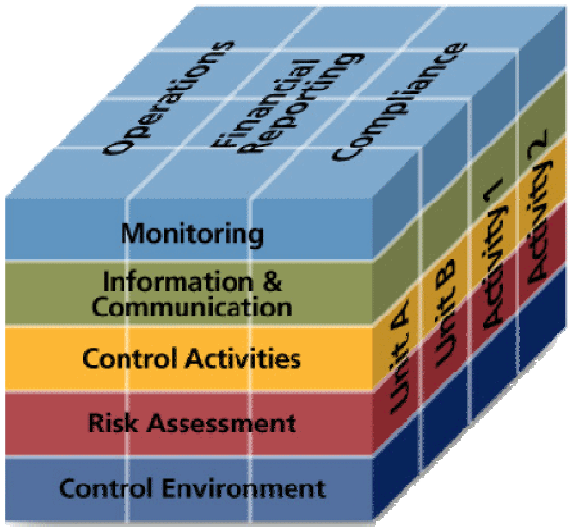
ISO/IEC 18031:2005	Information technology -- Security techniques -- Random bit generation
ISO/IEC 18032:2005	Information technology -- Security techniques -- Prime number generation
ISO/IEC 18033-1:2005	Information technology -- Security techniques -- Encryption algorithms -- Part 1: General
ISO/IEC 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

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque no definimos bien el control interno

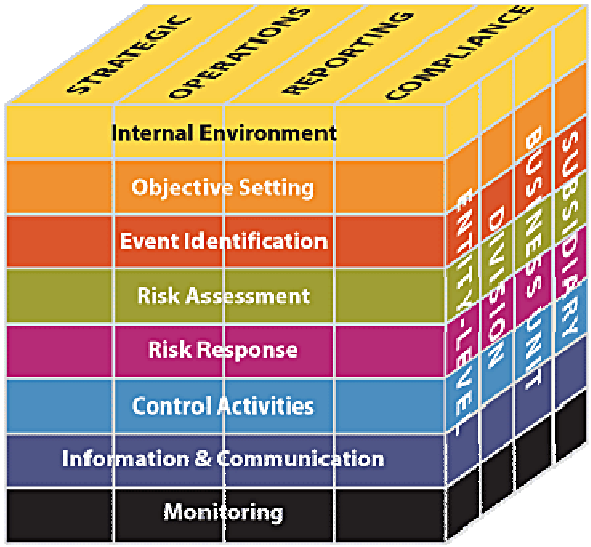
The COSO "Cube"

(Font COSO)



COSO-ERM "Cube"

(Font COSO)

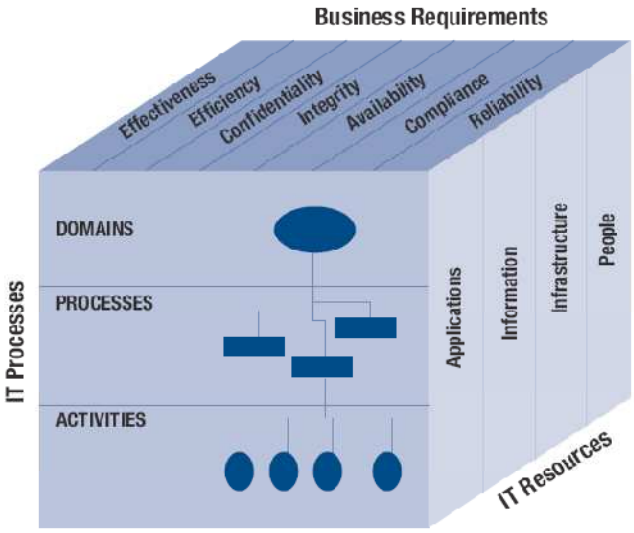


- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque nos faltaba añadir al control interno la parte de seguridad de TI

The CobiT "Cube"

(Font IT Governance Institute Cobit 4.0, USA 2005)

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE



ITGI Cobit 4.0, USA 2005

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure regulatory compliance.
ME4 Provide IT governance.

IT RESOURCES
- Applications
- Information
- Infrastructure
- People

PLANNING AND ORGANISATION

MONITORING

AQUISITION AND IMPLEMENTATION

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations

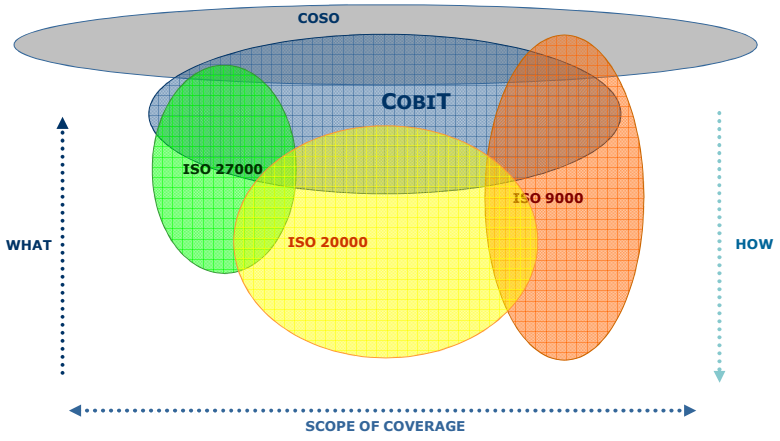
DELIVERY AND SUPPORT

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque nos faltaba integrar los sistemas con calidad

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE



IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque no tenemos un modelo de governanza del riesgo

Risk IT.
ISACA 2009

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

- Por qué el firewall no bloqueó la entrada no autorizada?
- Porque no tenemos un modelo de buen gobierno TIC

¿Modelos IT-Governance?

MIT-CISR LAS 5 PRINCIPALES DECISIONES *(Weill & Ross. IT-Governance. HBSP,2004)*	COBIT IT-GOVERNANCE Las 5 AREAS *(IT Governance Institute Cobit 4.1, USA 2007)*	ISO 38500 LOS 6 PRINCIPIOS *(ISO 38500 ISO/IEC JTC1/SC7,2008)*
Principios IT	**Alineamiento estratégico**	**Responsabilidad**
Arquitectura IT	**Entrega de Valor**	**Estrategia**
Infraestructura IT	**Gestión de Recursos**	**Adquisición**
Aplicaciones de negocio	**Gestión de Riesgos**	**Performance**
Inversiones y prioridades	**Medida del Performance**	**Cumplimiento**
		Factor Humano

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

Después de mil explicaciones

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

Principio de Parkinson

Ley del Trabajo:

Todo trabajo tiende a incrementarse hasta llegar al límite máximo del tiempo disponible.

Hipótesis de la demora-patrón:

Se fija un tiempo mínimo para la ejecución de un trabajo, e inferior a este tiempo es imposible ejecutarlo.

Ley de Banalidad:

El tiempo dedicado a la dirección de un tema es inversamente proporcional a su importancia.

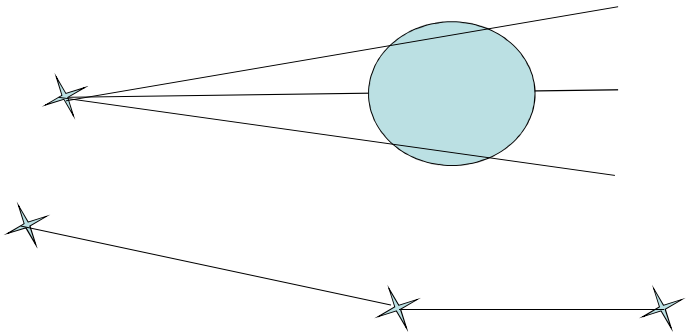
Principio de la comisión:

Las comisiones nacen, crecen, se reproducen y se reproducen muchísimo.

Principio del bloqueo de la administración:

Las organizaciones sólo trabajan de forma eficiente hasta que están a punto de desaparecer.

Teorema del punto gordo y la recta astuta



IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

La cruda realidad

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

LOS POR QUÉs

- **Por qué el firewall no bloqueo la entrada no autorizada?**
- **Porque el atacante tenía el password**
- **Por qué el atacante tenía el password?**
- **Porque se lo dió un empleado**
- **Por qué se lo dió un empleado?**
- **Porque no era consciente del peligro.**
- **Por qué no era consciente del peligro?**
- **Porque nadie se lo explicó**
- **Por qué nadie se lo explicó?**
- **Porque la formación no es importante y**
- **muy compleja, y muy costosa y muy …….**

IAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

¿Qué podemos hacer?

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

ITAITG INSTITUTE OF AUDIT & IT-GOVERNANCE

- 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
    - RIESGO CERO = COSTE INFINITO

IAITG
INSTITUTE
OF AUDIT &
IT-GOVERNANCE

MOLTES GRÀCIES