

# Servicios en Seguridad de la información.

Ing: Rodrigo Ferrer V.

**CISSP**

**CISA**

**BS (British Standard) lead Auditor 27001**

ASIS Member 262546

ISACA Member

IEEE Member

rodrigo.ferrer@sisteseg.com

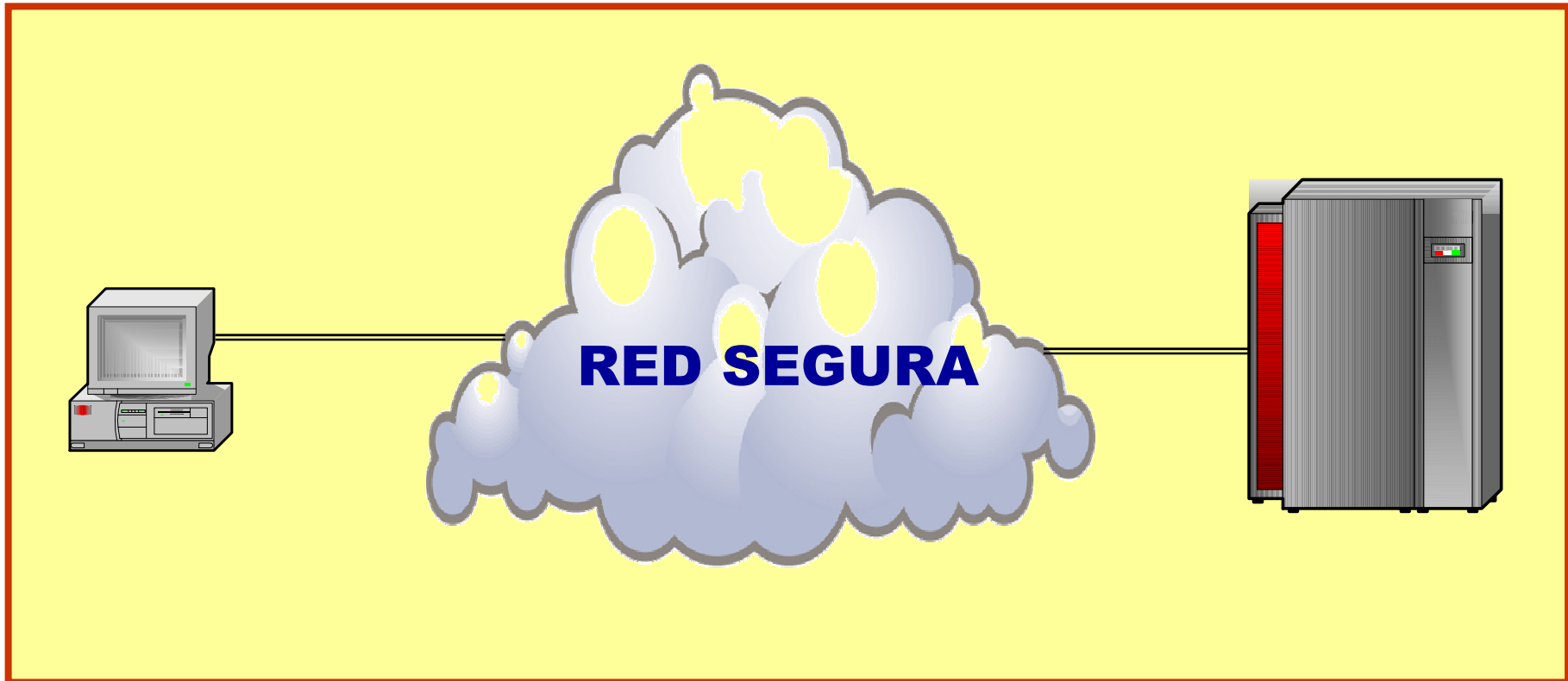
# Agenda

- ✓ **Introducción.**
- ✓ **Marco de Referencia**
  - ✓ **BS ISO/IEC 17799.**
- ✓ **Evaluación de Riesgo.**
- ✓ **Matrices de Riesgo.**
- ✓ **Definición de Políticas, procedimientos y Estándares**
- ✓ **Conclusiones**
  - ✓ **Servicios en Seguridad.**

Tiempo estimado: 60 min.

# **Introducción**

# Red Segura

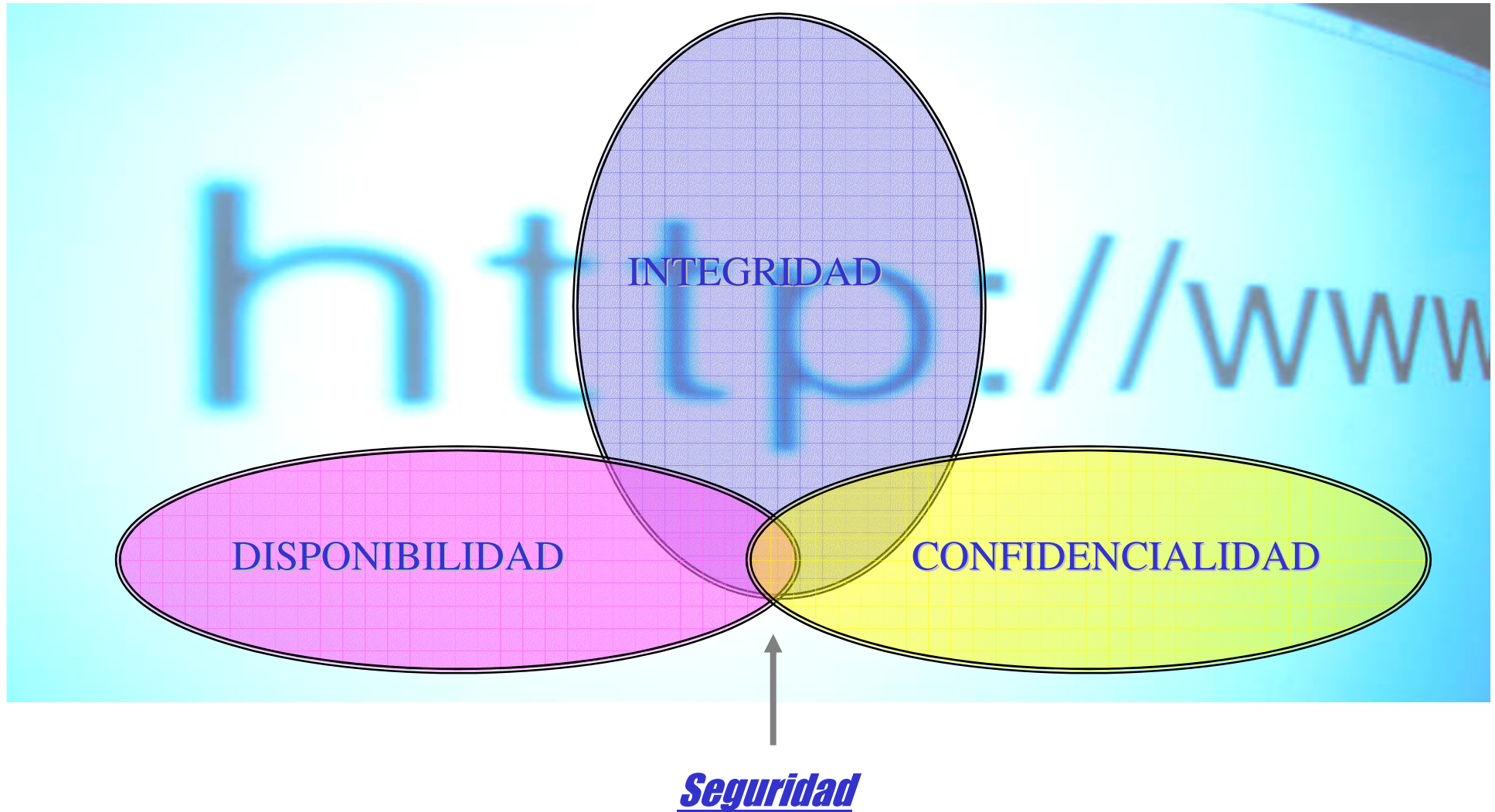


# Información

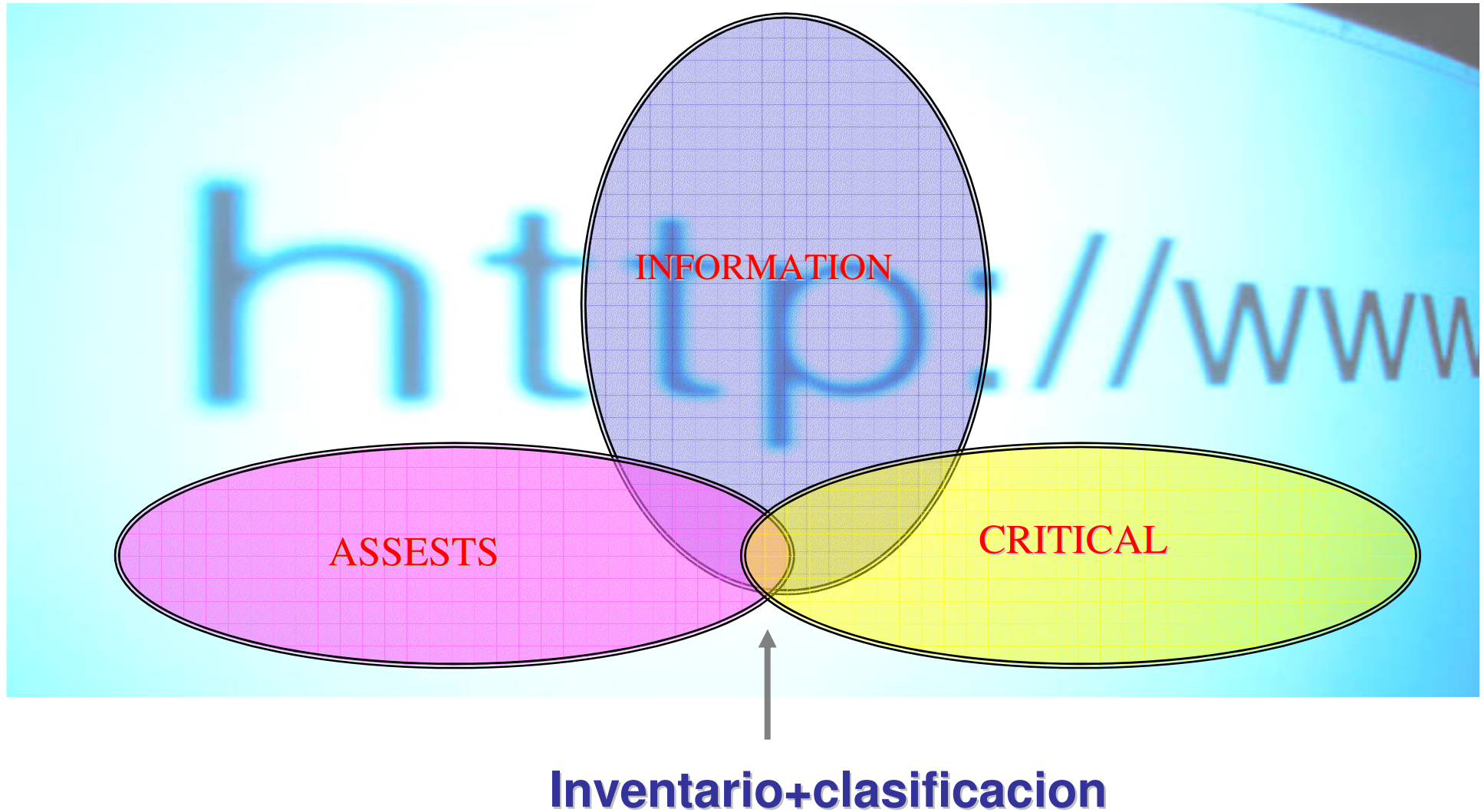
Es el conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que debemos proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando diferentes tecnologías lógicas, físicas o procedimentales.



## Objetivo en Seguridad (Costo)

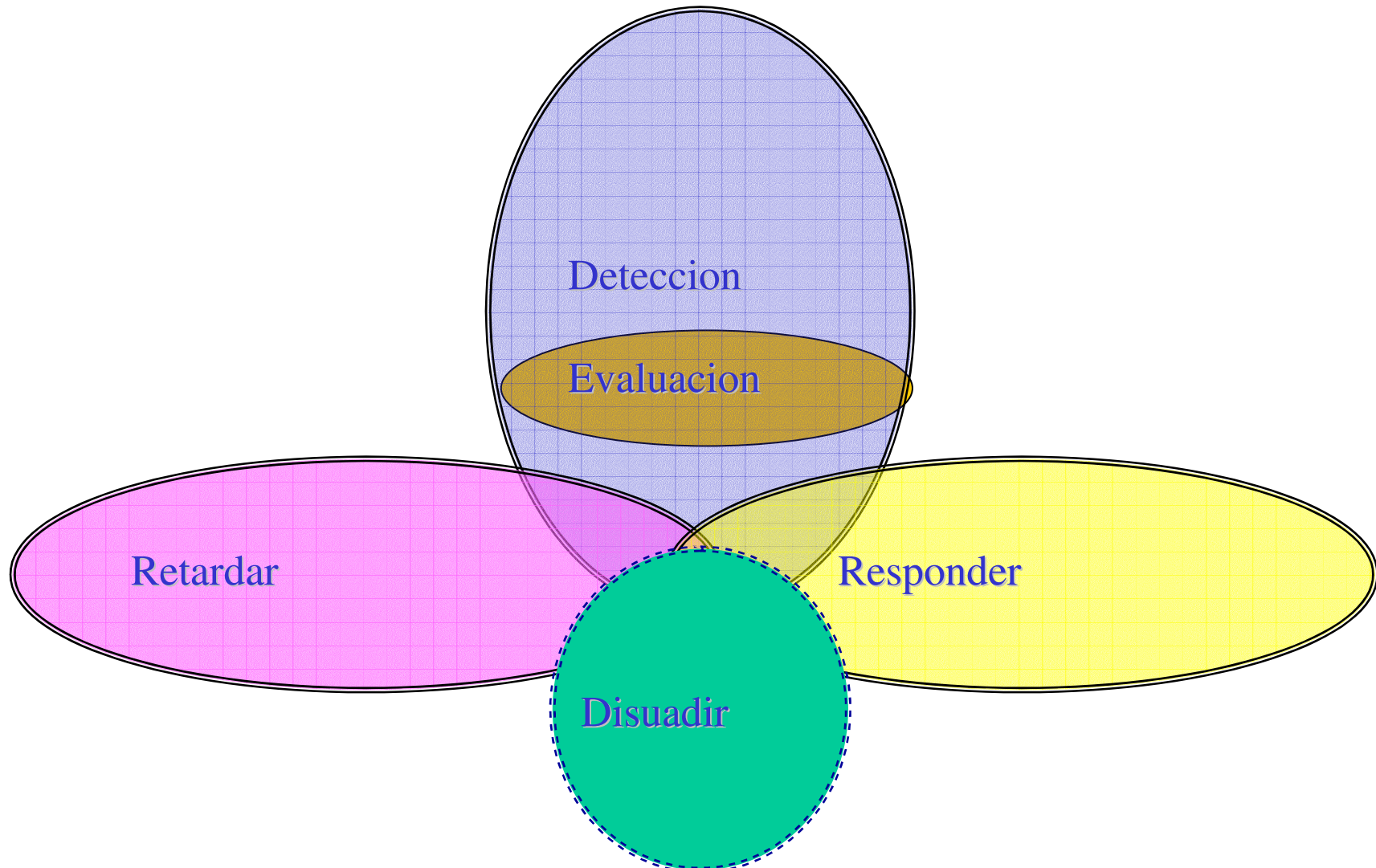


# Qué ayudar a proteger?: C.I.A

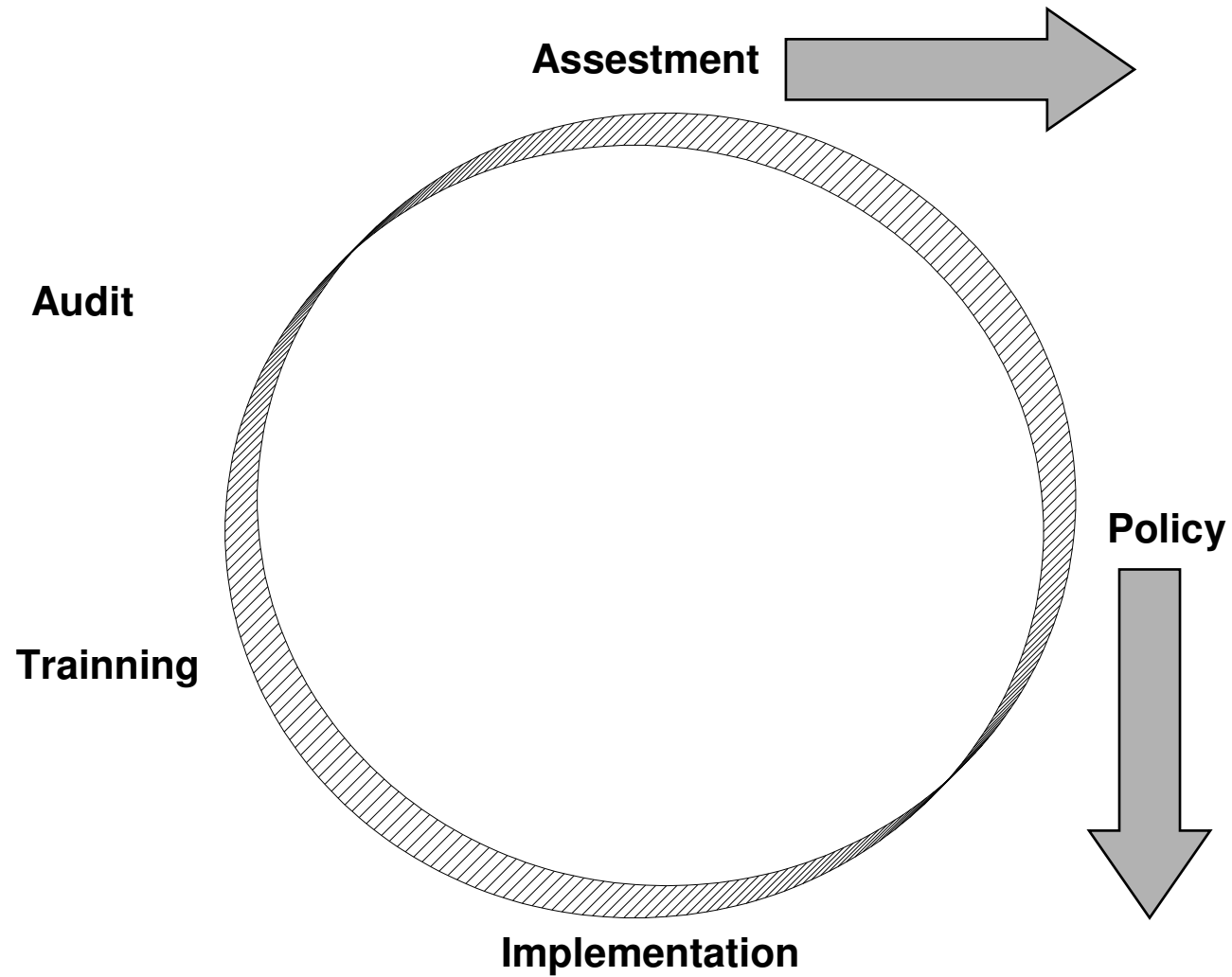


**Inventario+clasificacion**

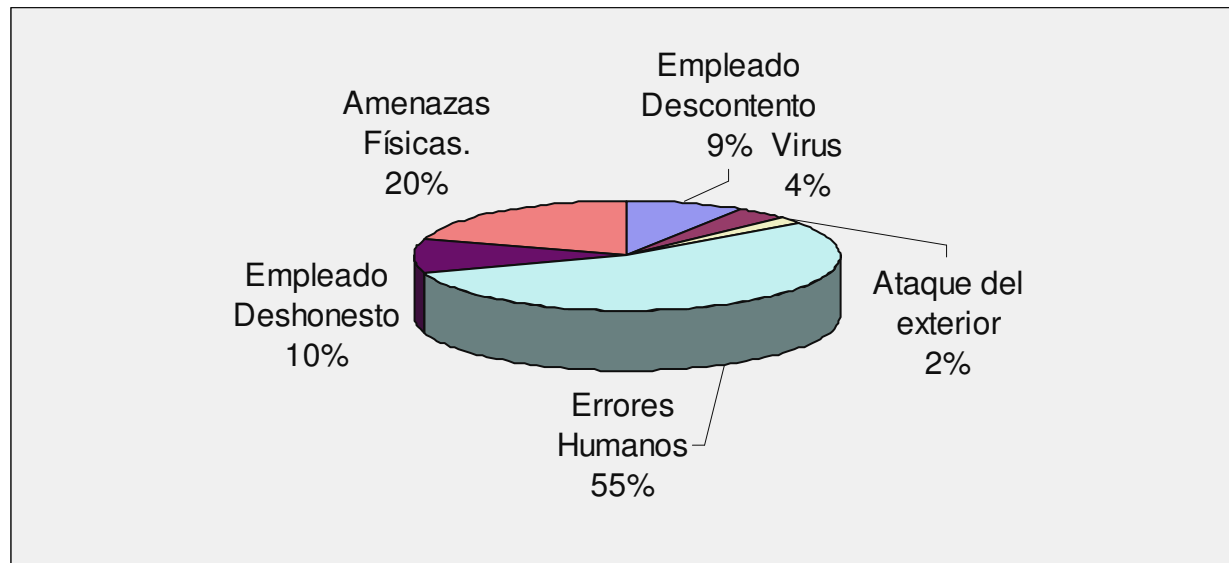
# Los controles y procedimientos buscan:



# La seguridad como Proceso

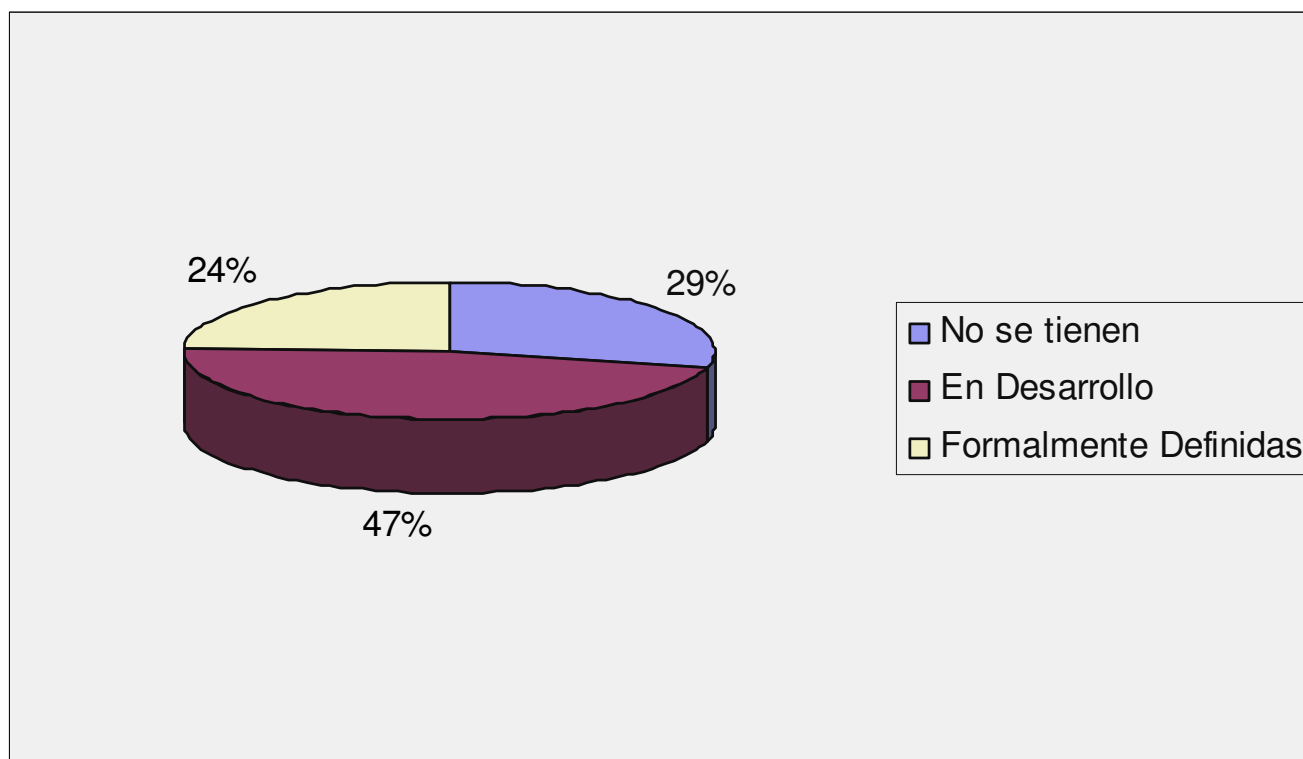


# Fuentes de los problemas de seguridad en las Empresas.



Fuente: Computer Security Institute

# Estado de las Políticas de Seguridad en las Empresas Colombianas



Fuente: ACIS 2004

# **Marco de Referencia**

# **Evaluación de Riesgo de TI**

# El Riesgo

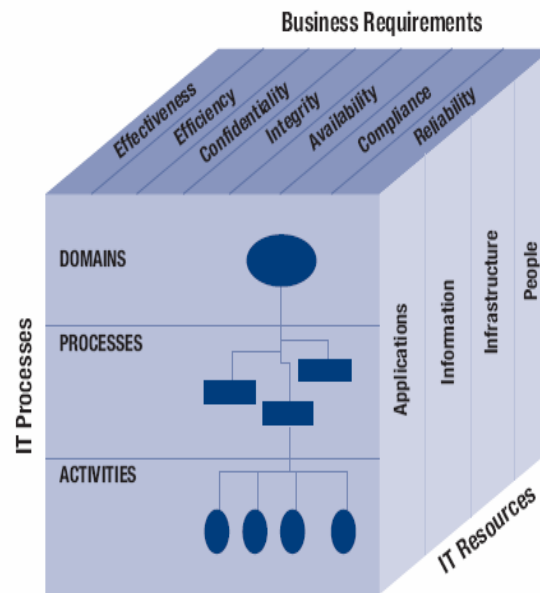
La falta de Políticas de Seguridad en cualquier organización puede tener como consecuencia:

- ▶ Pérdida de Dinero.
- ▶ Pérdida de tiempo.
- ▶ Pérdida de productividad
- ▶ Pérdida de información confidencial.
- ▶ Pérdida de clientes.
- ▶ Pérdida de imagen.
- ▶ Pérdida de ingresos por beneficios.
- ▶ Pérdida de ingresos por ventas y cobros.
- ▶ Pérdida de ingresos por producción.
- ▶ Pérdida de competitividad en el mercado.
- ▶ Pérdida de credibilidad en el sector.

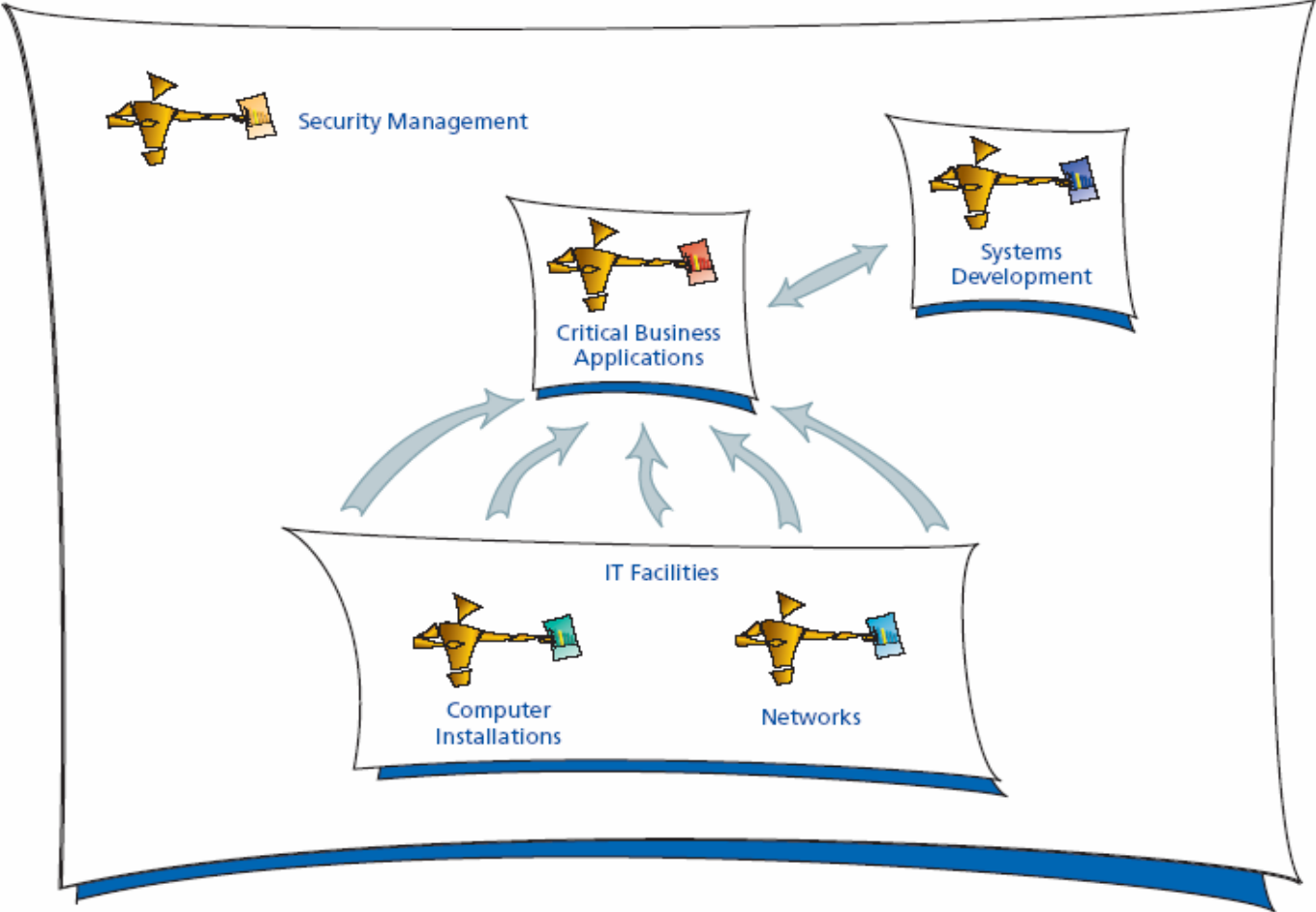


# COBIT

Figure 22—The COBIT Cube

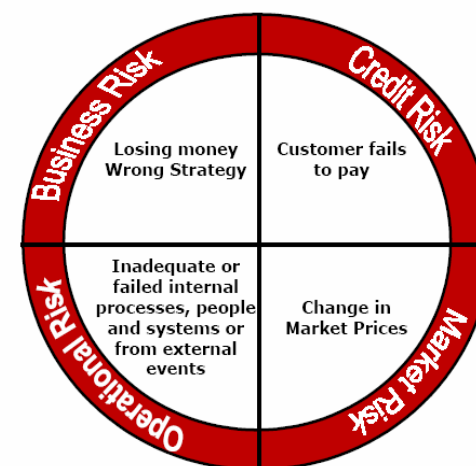


# Procesos y Aplicaciones Críticas



# Por qué realizar una Evaluación de Riesgo.

- Identificar, Analizar, y evaluar.
- Conocer los riesgos
- Ejercicio de entendimiento de toda la organización.
- Identificar los procesos críticos del negocio y las aplicaciones que los soportan.
- Presentar un diagnóstico de la Situación Actual.
- Identificar los puntos de mayor atención y focalizar el esfuerzo.



- ✓ **Risk** is a function of the **likelihood** of a given **threat-source.s** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization.

# Identificar amenazas

Es importante considerar todas las amenazas posibles, sin importar que tan probables sean o no.

- ▶ Acceso no autorizados
- ▶ Fraude
- ▶ Perdida de Confidencialidad
- ▶ Uso inapropiado de recursos
- ▶ Fallas de Hardware
- ▶ Fallas de canales de comunicaciones
- ▶ Virus
- ▶ Negación de Servicio.
- ▶ Incumplimiento de Normas.
- ▶ Perdida de Laptops
- ▶ Fallas de Potencia
- ▶ Incendio

# Resultados ISO 17799-ISO 27001

<b>Dominio</b>	<b>Cumplimiento</b>
<i>Política de Seguridad</i>	<b>0%</b>
<i>Seguridad en la Organización.</i>	<b>20%</b>
<i>Control y Clasificación de Activos.</i>	<b>33%</b>
<i>Aspectos de Seguridad relacionados con el recurso humano.</i>	<b>40%</b>
<i>Seguridad Física</i>	<b>60%</b>
<i>Administración de la operación de cómputo y comunicaciones.</i>	<b>28%</b>
<i>Control de Acceso (falta sistemas)</i>	<b>40%</b>
<i>Desarrollo y mantenimiento de Sistemas</i>	<b>45%</b>
<i>Continuidad del Negocio</i>	<b>30%</b>
<i>Cumplimiento de Leyes</i>	<b>20%</b>
<b>Promedio</b>	<b>31.6%</b>

# Analisis de la Infraestructura

- ◆ Seguridad Física.
  - ▶ *Monitoreo ambiental*
  - ▶ *Control de acceso*
  - ▶ *Desastres naturales*
  - ▶ *Control de incendios*
  - ▶ *Inundaciones*
- ◆ Seguridad en las conexiones a Internet.
  - ▶ *Políticas en el Firewall*
  - ▶ *VPN*
  - ▶ *Detección de intrusos*
- ◆ Seguridad en la infraestructura de comunicaciones.
  - ▶ *Routers*
  - ▶ *Switches*
  - ▶ *Firewall*
  - ▶ *Hubs*
  - ▶ *RAS*
- ◆ Seguridad en Sistema Operacionales(Unix, Windows)
- ◆ Correo Electrónico
- ◆ Seguridad en las aplicaciones.

# Evaluación en Seguridad Física

El objetivo es prevenir accesos no autorizados, daños, robos a los activos del negocio y la organización.

La evaluación de riesgo permite identificar las áreas más críticas y definir los controles requeridos.

- Perímetros de seguridad.
- Seguridad de equipos.( medio ambiente).
- Escritorios limpios.

# Seguridad Física Centro de Computo

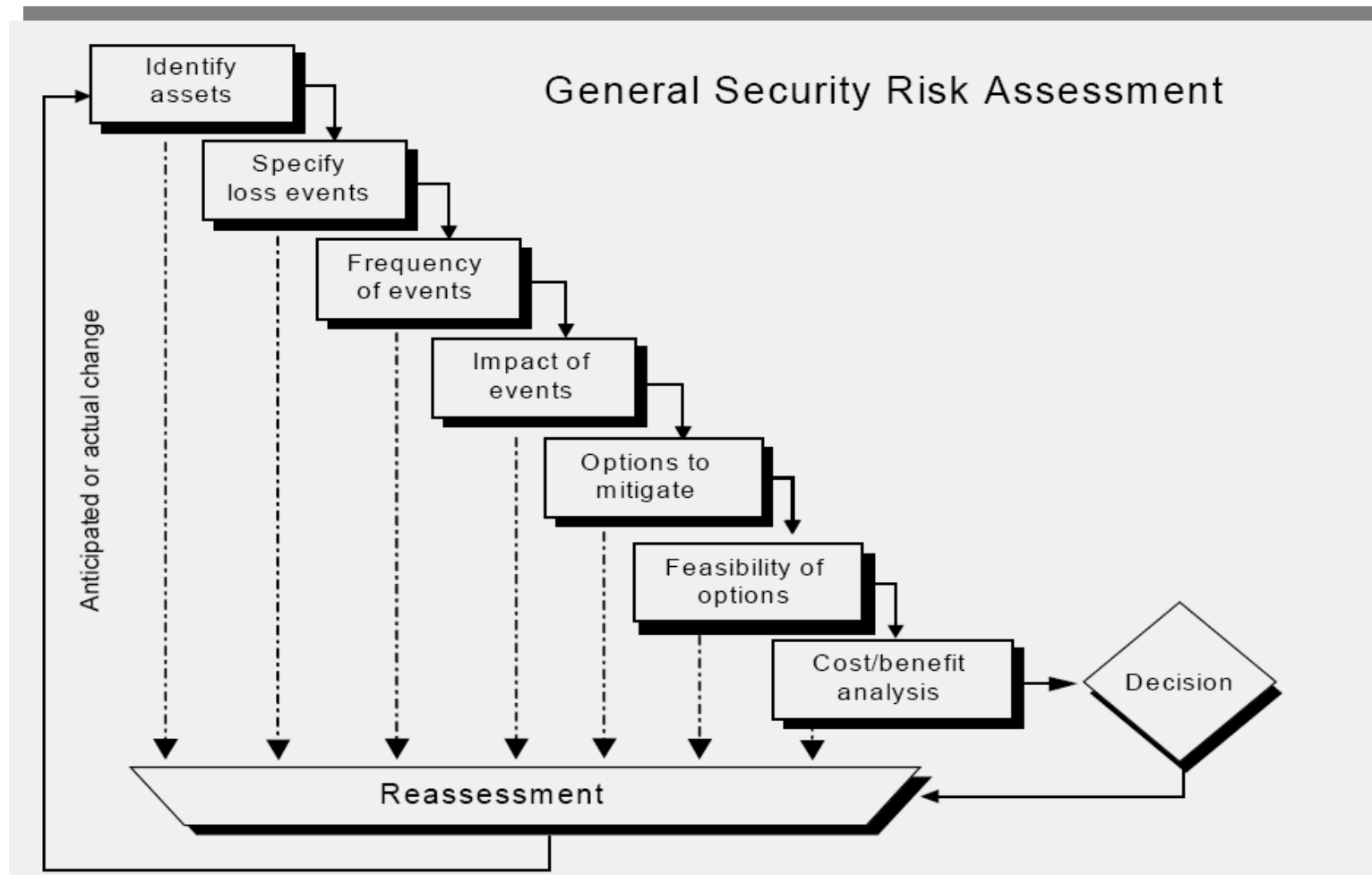


# **Matrices de Riesgo**

# Ejemplo Matriz de Riesgo

Amenazas	Vulnerabilidades	Ocurrencia del evento anualizada (1-5)	Impacto (1-5)	Factor de Riesgo (1-10)	Control	Costo Control	FR/CC
Falla de switch principal de la red LAN	<p>No hay procedimientos de contingencia.</p> <p>No hay procedimiento formal de almacenamiento de la configuración de los switches.</p> <p>No hay inventario actualizado</p>	1	3	4	<p>Procedimientos de Contingencia.</p> <p><b>Contrato de mantenimiento</b></p> <p>Gestión de red.</p> <p>Procedimientos de cambio de configuraciones</p>	1	4

# Metodología Análisis de Riesgo



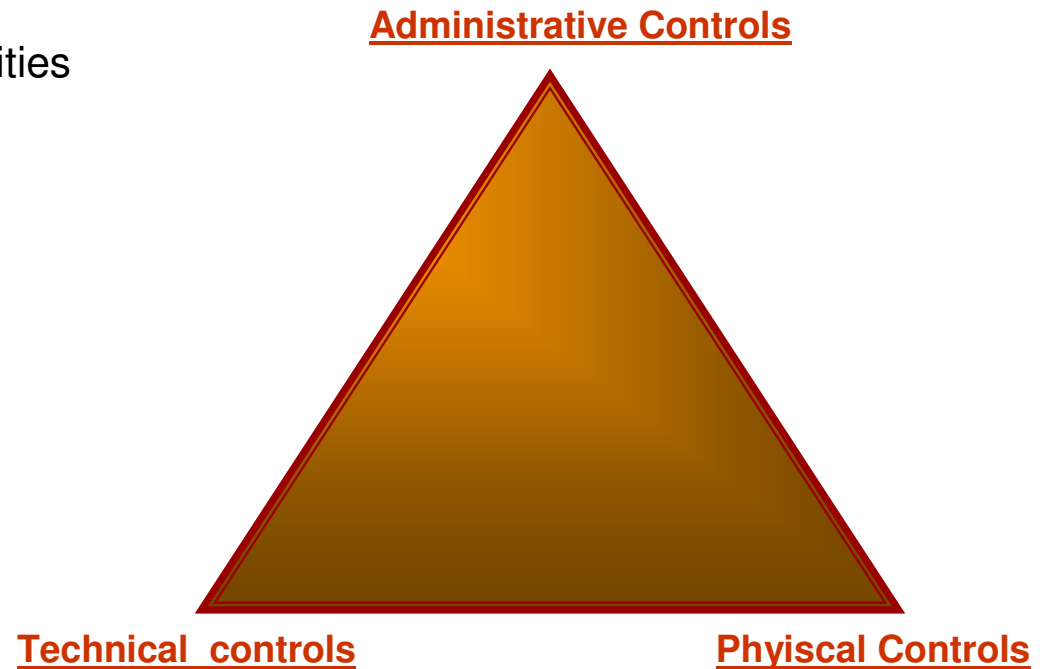
# Opciones para el tratamiento del riesgo

- ◆ Controlar el riesgo
- ◆ Aceptarlo
- ◆ Evitarlo
- ◆ Transferirlo



# Tipos de Controles

- ◆ Administrative Controls
  - Management responsibilities
    - Security Policies
    - Procedures
    - Screening Personal
    - Classifying data
    - BCP,DRP.
    - Change Control
- ◆ Technical Controls
  - IDS
  - Encryption
- ◆ Physical Control
  - Security Guards
  - Perimeters fences
  - Locks
  - Removal of CD-ROM



# **Definición de Políticas, procedimientos y estándares**

# La seguridad de la información



# **Políticas.**

Una política de seguridad, es una declaración formal de las reglas que deben seguir las personas con acceso a los activos de tecnología e información, dentro de una organización.

# Procedimientos.

Los procedimientos son la descripción detallada de la manera como se implanta una Política. El procedimiento incluye todas las actividades requeridas y los roles y responsabilidades de las personas encargadas de llevarlos a cabo.

# Estándares

- Es la definición cuantitativa o cualitativa de un valor o parámetro determinado que puede estar incluido en una norma o procedimiento.
- Los estándares pueden estar ligados a una plataforma específica (parámetros de configuración) o pueden ser independientes de esta (longitud de passwords).

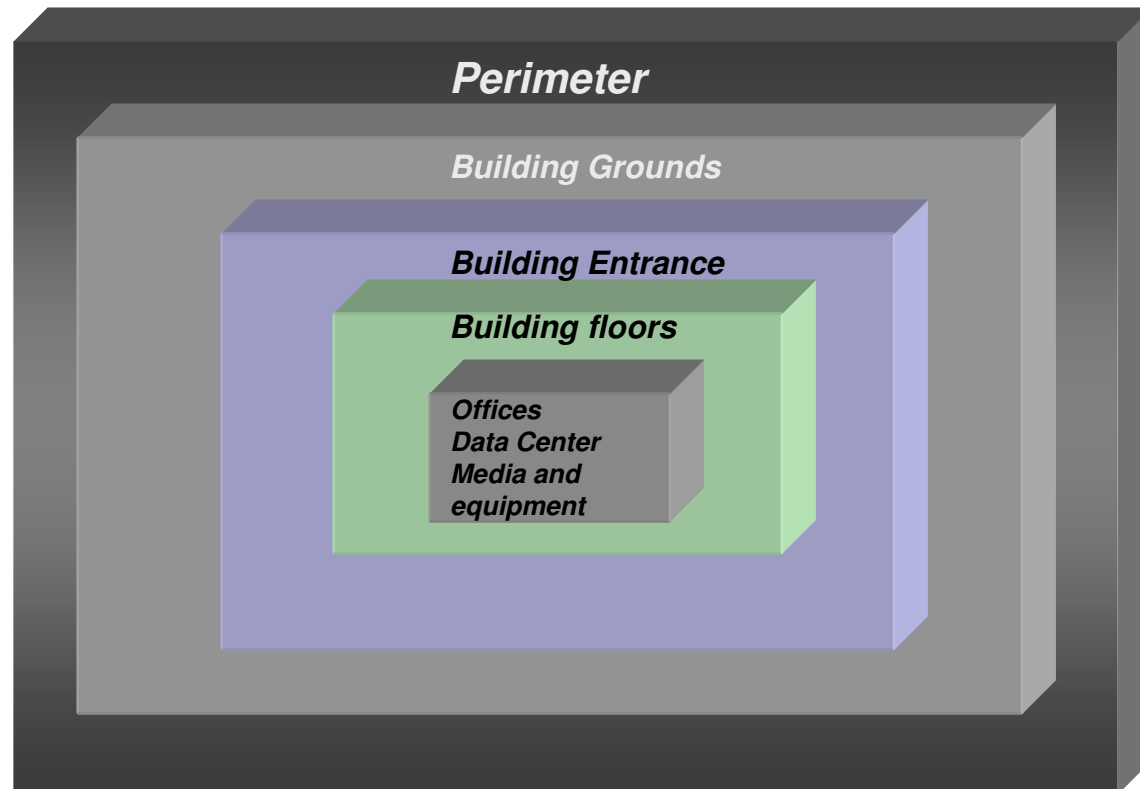
# Plan de Entrenamiento en Seguridad.

- ◆ El aspecto humano se debe considerar en cualquier proyecto de seguridad, sea esta física, lógica, informática o industrial.
- ◆ Debe ser corto pero continuo
- ◆ A veces es la única solución a ciertos problemas de seguridad como instalación de troyanos.
- ◆ Debe ser apoyado por campanas publicitarias, Email, objetos etc.



# **Conclusiones**

# Estrategia Niveles de Seguridad

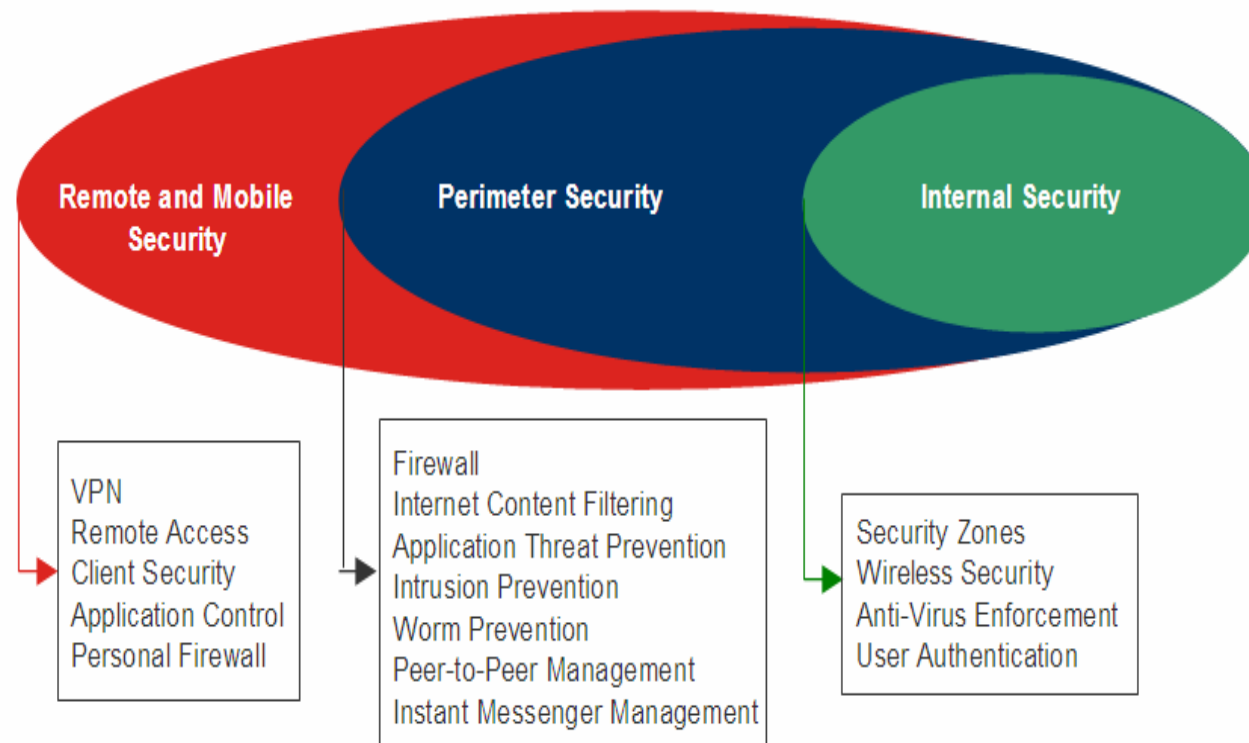


# Perímetro Lógico

▷ Dynamic

▷ Continuous

▷ Distributed

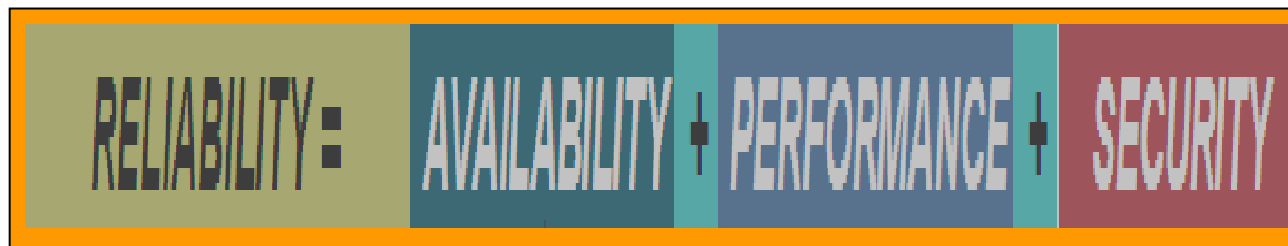
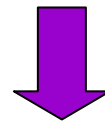


## Servicios a ofrecer

- GaP Analysis en relación al ISO 17799/27001
- Análisis de riesgo (risk assessment) orientado a aplicaciones e Infraestructura de red.
- Análisis de la Seguridad Física en el Centro de Computo.
- Definición de Políticas, Procedimientos y Estándares para los clientes.(SMB)
- Diseño de la Arquitectura de Seguridad para conectividad hacia Internet.
- Auditoría de seguridad ISO 27001.
- Plan de concientización en Seguridad de la información.
- Elaboración Plan de Contingencia para IT.
- Configuración y optimización sistema Firewall.
- Mejoramiento seguridad red Voz IP.
- Mejoramiento seguridad red Wireless.
- Optimización desempeño de red y Conectividad hacia Internet.

# Conclusiones

- ◆ Seguridad y desempeño.
- ◆ Seguridad y disponibilidad.
- ◆ Seguridad y productividad.(flexibilidad)
- ◆ Seguridad distribuida.
- ◆ Seguridad en el sistema operativo de la red.



# Conclusiones

- ❖ Alrededor de la evaluación de riesgo gira todo el proceso.
- ❖ Las políticas de seguridad habilitan el desarrollo de una arquitectura de seguridad de la información.
- ❖ Este proceso –análisis de riesgo- genera un plan de inversión en tecnología en general.(redes, servidores, software, servicios, IPS, Ciframiento, desarrollo aplicaciones, conectividad VPN, Velocidad hacia Internet. etc)
- ❖ Seguridad y desempeño a un costo razonable, sin afectar la flexibilidad.

En conclusión los proyectos de seguridad son un sub-conjunto de los proyectos de continuidad y el logro de objetivos empresariales.

**FIN**