

# **Servicios en seguridad de la información**

**Ing: Rodrigo Ferrer V.**  
CISSP, CISA, ABCP, COBIT f.c, CSSA, CST.

# Agenda

- Introducción a la seguridad**
- Evaluación de Riesgo.**
- Implementación de la seguridad**
- Planes para la continuidad**
- Auditorías en seguridad**
- Conclusiones**
- Comentarios**

Tiempo estimado: 60 min.

# **Introducción a la seguridad**

## **Para reflexionar.....**

The Forrester logo consists of the word "FORRESTER" in a white, serif, all-caps font, centered within a dark green, horizontally-oriented oval shape.

**FORRESTER®**

*Consumers will demand a safe Internet service, and if an ISP doesn't measure up on security, members will flee to a rival provider.*

*Customers will absolutely demand a clean pipe.*

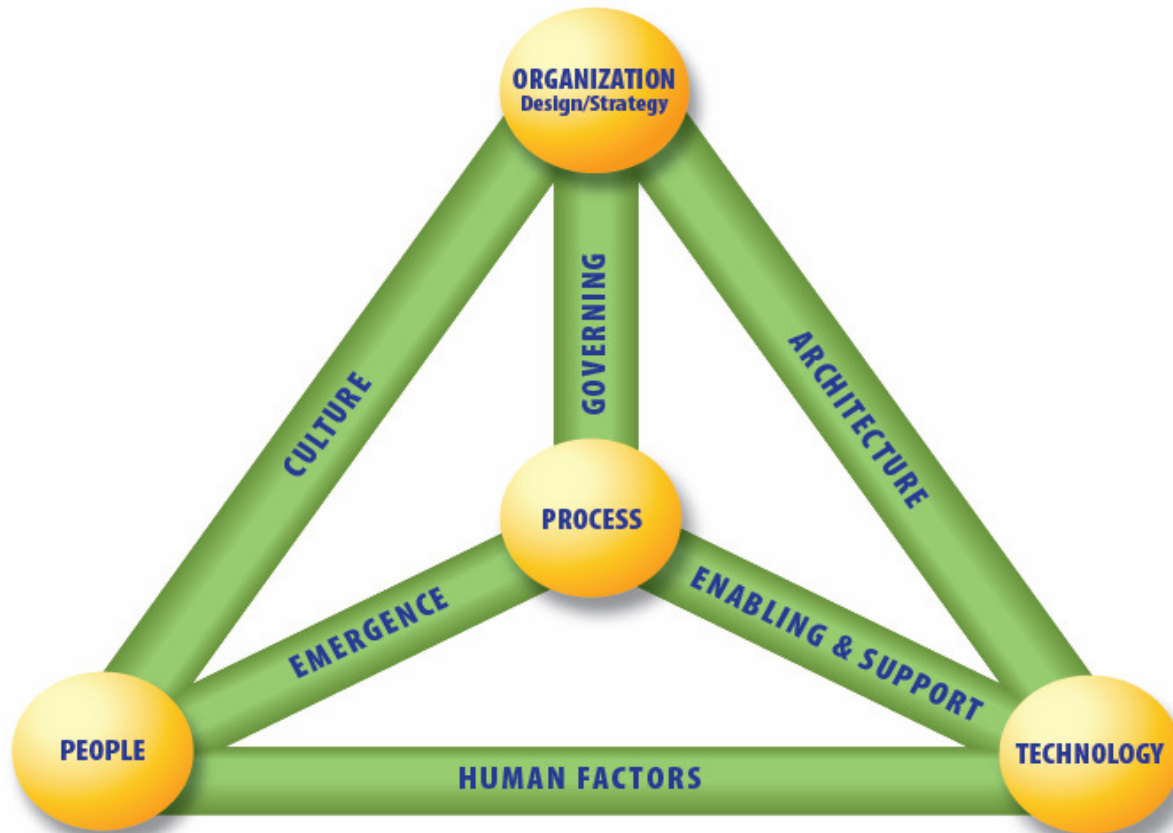
## Información...el activo

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.



# Seguridad de la Información

Figure 1—The Business Model for Information Security

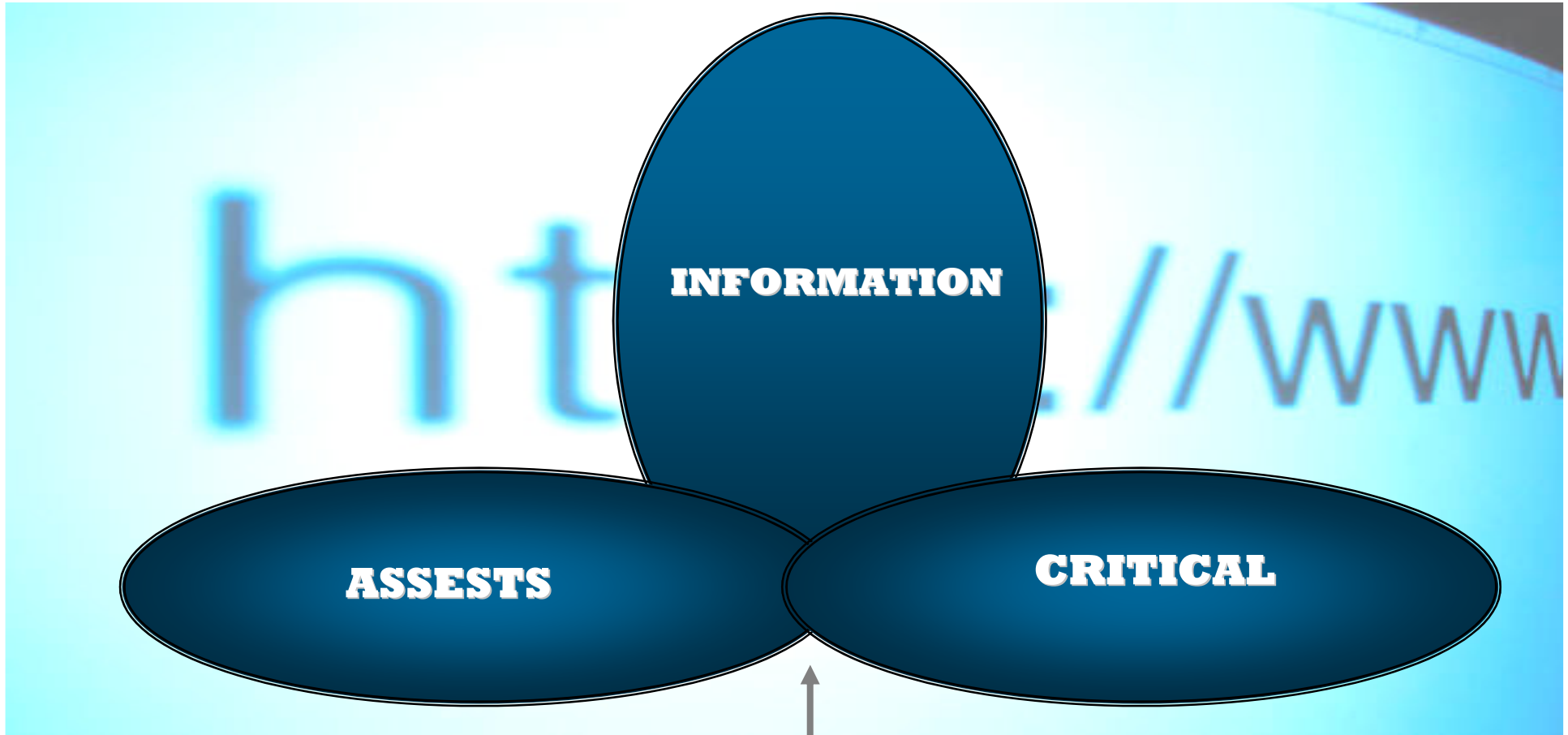


Source: Adapted from the USC Marshall School of Business Institute for Critical Information Infrastructure Protection

# Objetivo del sistema

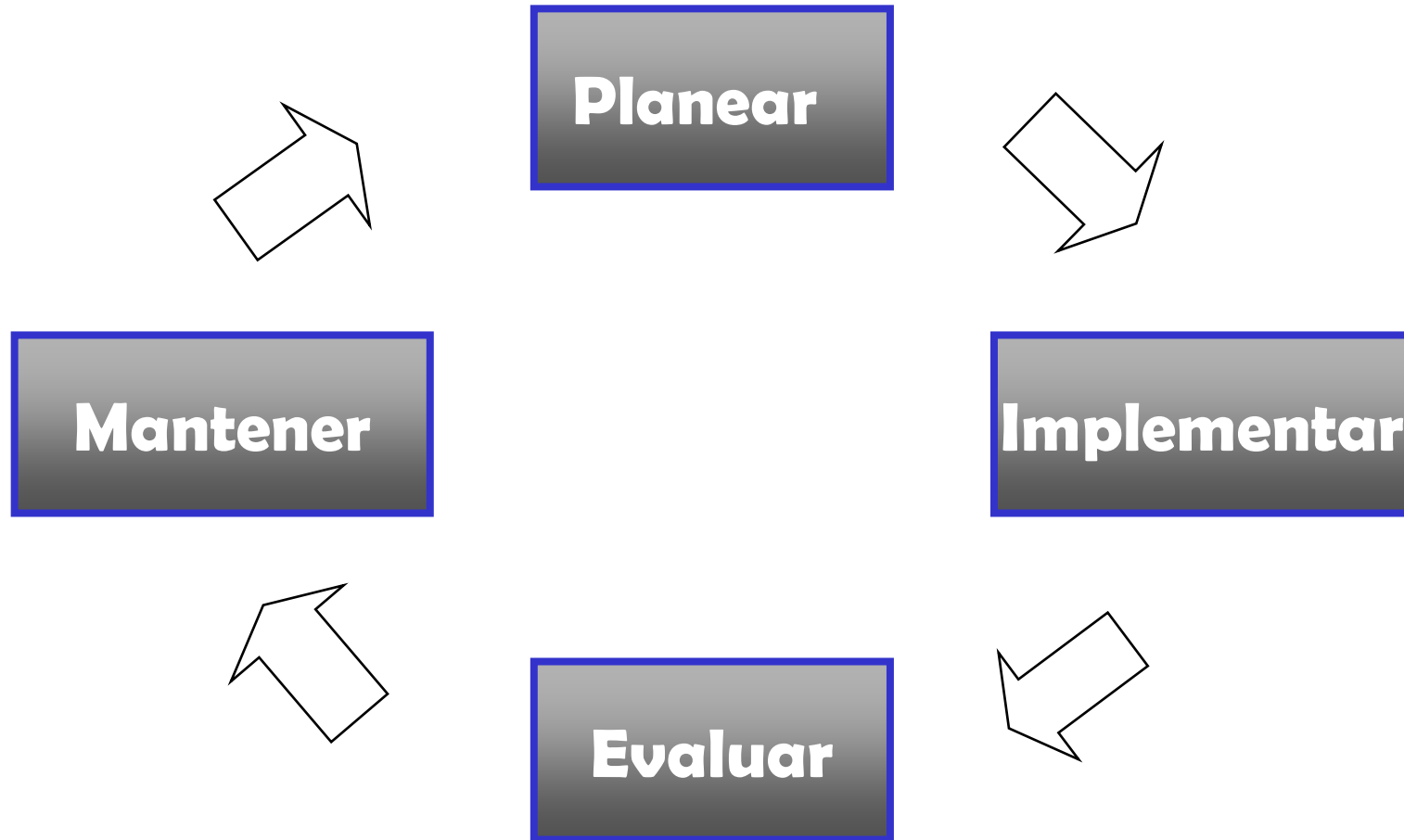


# Qué proteger?



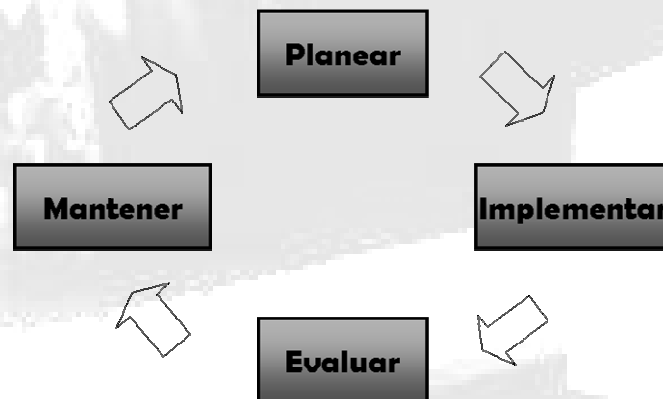
**Inventario+clasificación**

# El proceso SGSI



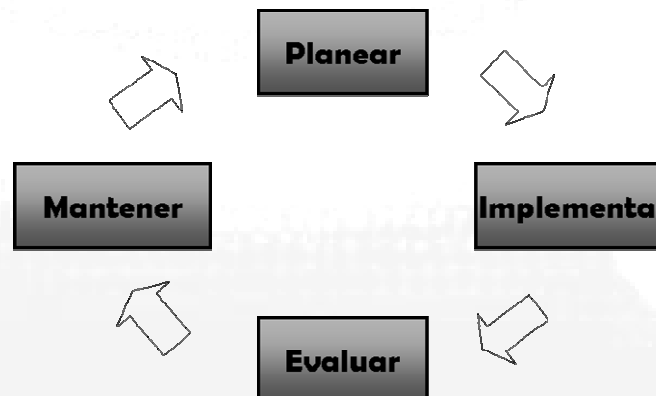
## Planear el SGSI

- ◆ Definir alcance
- ◆ Definir una política
- ◆ Definir metodología de valoración del riesgo
- ◆ Identificar riesgos
- ◆ Analizar y evaluar riesgos
- ◆ Gestión del riesgo
- ◆ Objetivos de control
- ◆ Obtener autorización para operar SGSI
- ◆ Elaborar una declaración de aplicabilidad



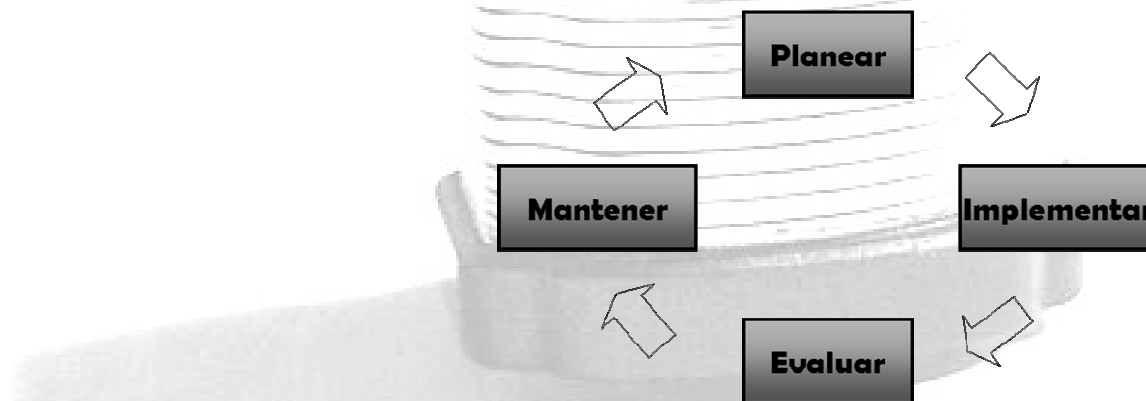
# Implementar el SGSI

- ◆ Plan de tratamiento del riesgo
- ◆ Implementar controles seleccionados
- ◆ Definir métrica de los controles establecidos
- ◆ Implementar programas de educación
- ◆ Gestionar la operación del SGSI
- ◆ Gestionar los recursos del SGSI
- ◆ Implementar procedimientos



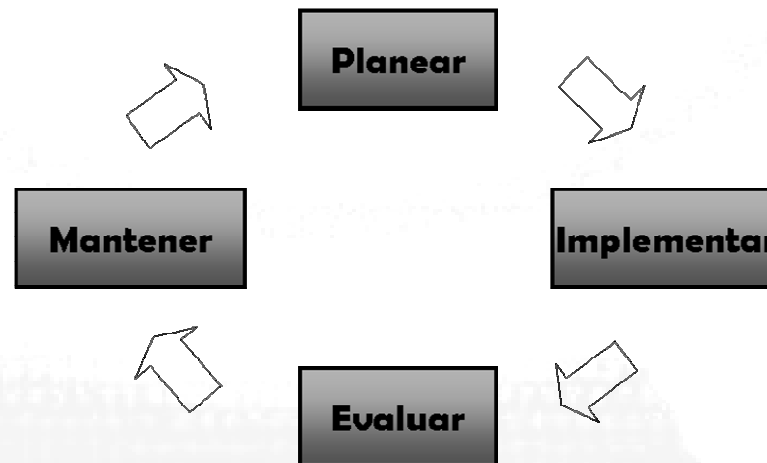
# Evaluar el SGSI

- ◆ Ejecutar procedimientos de revisión
- ◆ Empezar revisiones regulares
- ◆ Medir la eficacia de los controles
- ◆ Revisar las valoraciones de riesgos
- ◆ Realizar auditorías internas

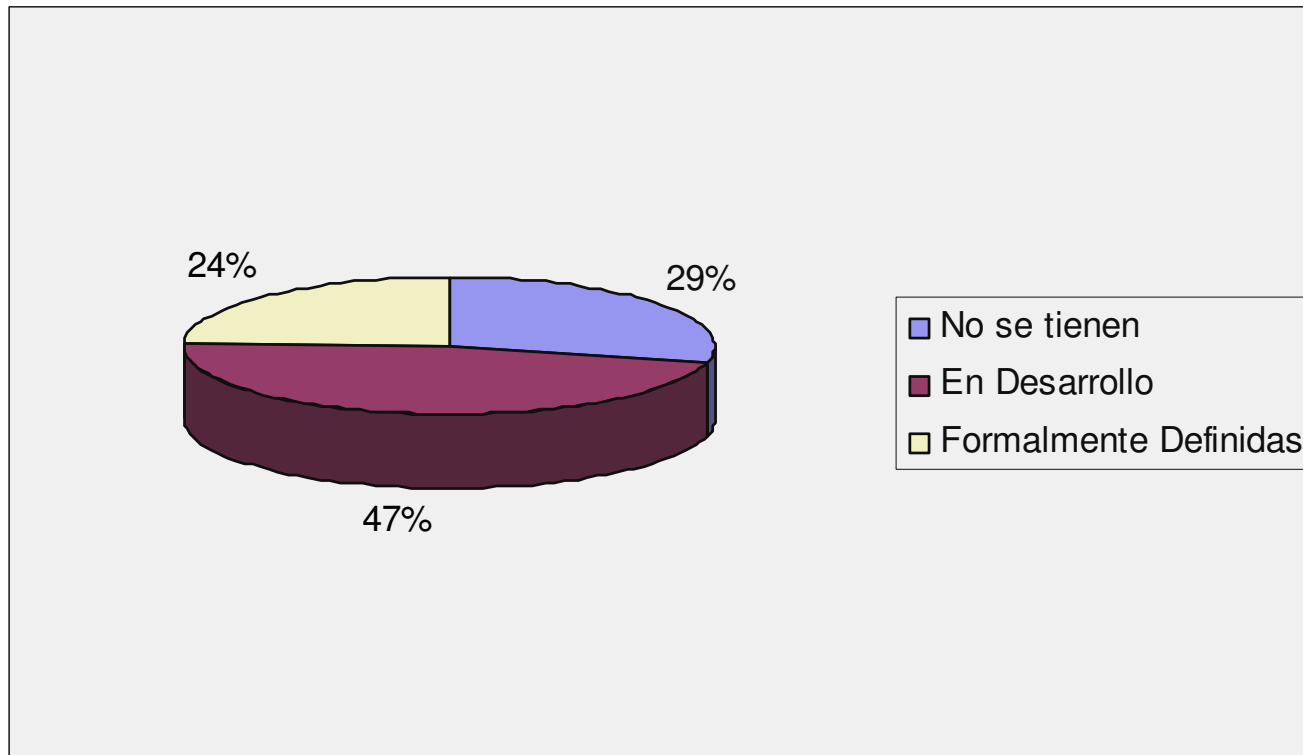


# Mantener el SGSI

- ◆ Implementar las mejoras identificadas en el SGSI
- ◆ Emprender acciones correctivas y preventivas
- ◆ Comunicar las acciones y mejoras a las partes interesadas
- ◆ Asegurarse que las mejoras logran los objetivos propuestos

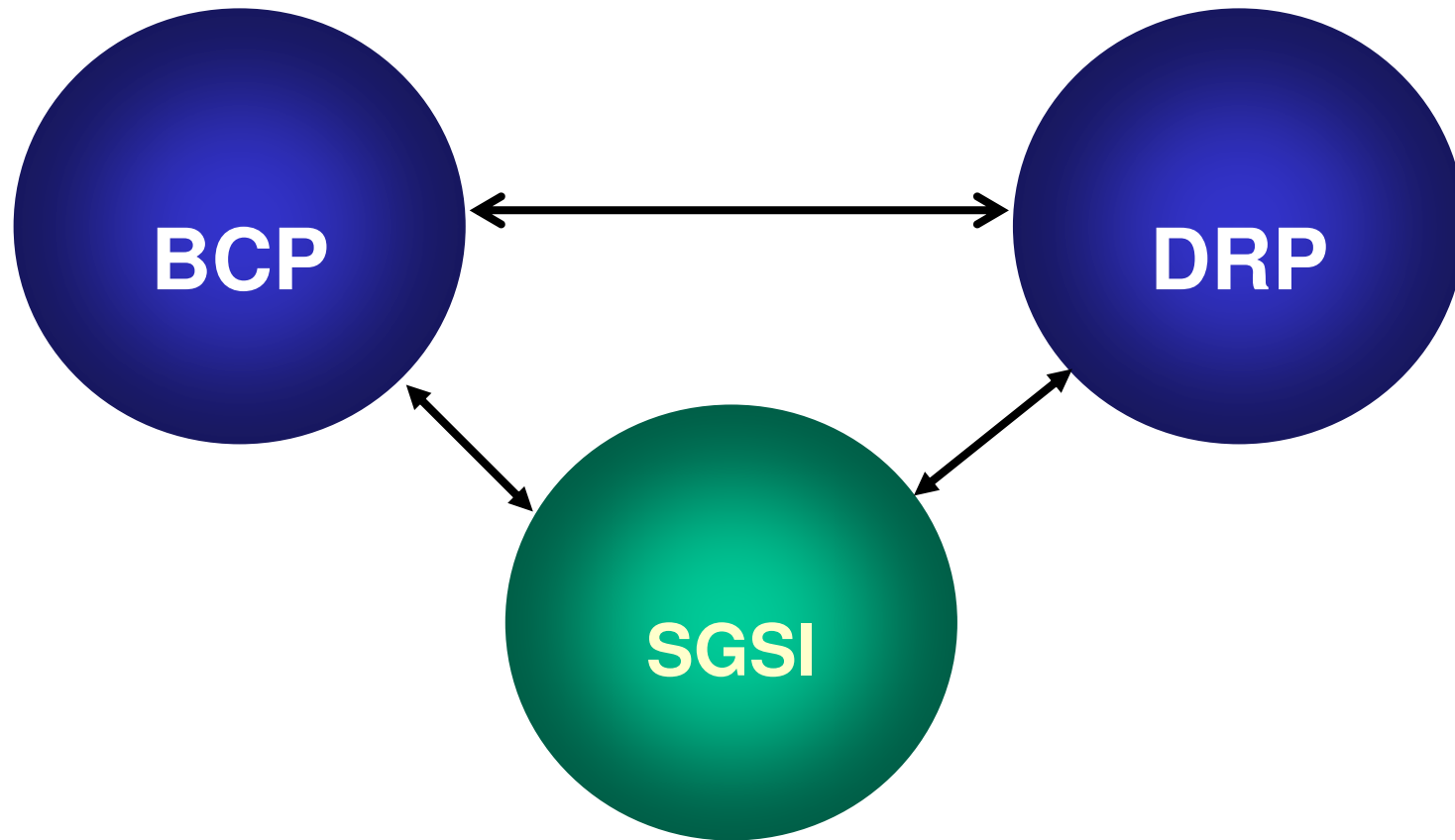


## Sin embargo...



Fuente: ACIS

# Integración BCP, DRP, SGSI



Mejores Prácticas: ITIL V3, COBIT, ISO 27001

# Mejores prácticas en la gestión del riesgo de la Información

- ◆ BS 7799 Parte2:2002
- ◆ COBIT: Control Objectives for Information and related Technology
- ◆ Systems Security Engineering-Capability Maturity Model (SSE-CMM) 3.0
- ◆ Generally Accepted Information Security Principles (GAISP)
- ◆ ISF-Standard of Good Practice for Information Security
- ◆ ISO 13335 – Guidelines for Management of IT Security
- ◆ ISO 13659:1997 – Banking and Related Financial Services
- ◆ ISO 15408:1999 Security Techniques-Evaluation Criteria for IT Security
- ◆ ISO 17799:2000
- ◆ NFPA 75
- ◆ ISO 27002

- ◆ ITIL – Security Management
- ◆ NIST 800-12 An Introduction to Computer Security
- ◆ NIST 800-14 Generally Accepted Principles and Practices for Securing IT Systems
- ◆ NIST 800-18 Guide for Developing Security Plans for Information Technology
- ◆ NIST 800-53 Recommended Security Control for Federal IS
- ◆ OCTAVE - Operationally Critical Threat, Asset and Vulnerability Evaluation
- ◆ OEDC – Guidelines for Security of IS and Networks
- ◆ Open Group's Manager's Guide to Information Security
- ◆ BS 25999

¿Cuánta Seguridad requiere o desea ?

# Análisis de Brecha ISO 27001

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

# **Evaluación de Riesgo de TI**

# Entorno Complejo



Extranet Clientes y  
Proveedores



Portales



Redes Privadas  
Virtuales



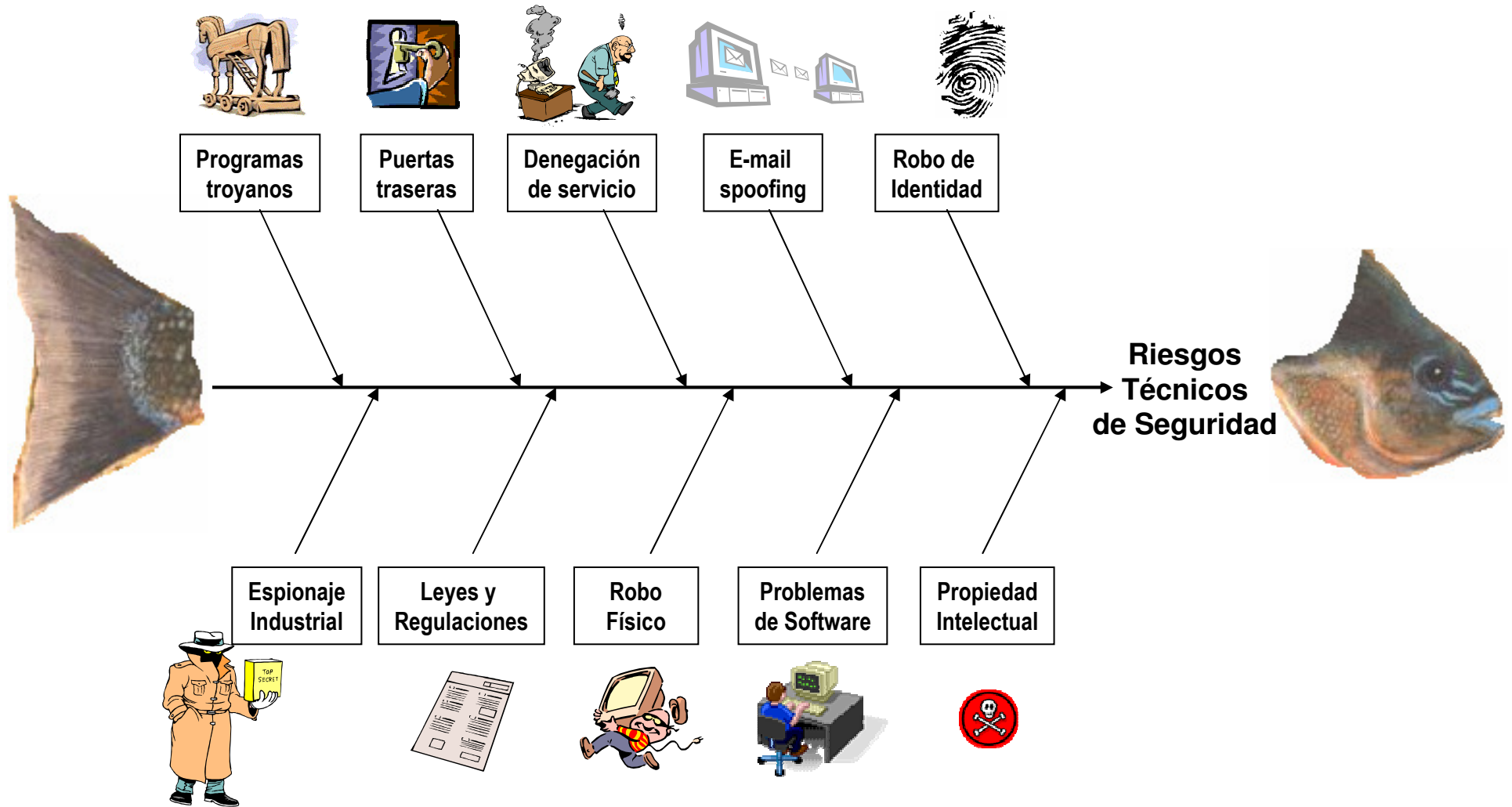
E-mail /  
Mensajería



Intranets y Procesos  
Corporativos

- ◆ Seguridad de mis clientes o socios
- ◆ Seguridad en mi red
- ◆ Quién accede a mis aplicaciones
- ◆ Configuraciones de seguridad tengo que actualmente
- ◆ Respuesta a incidentes

# ¿Dónde está el peligro?



# Output

## MAPA DE RIESGOS

Riesgo

010101 - 03

Pérdida financiera (demandas), pérdida de imagen y/o daño a la comunidad ocasionada por la degradación en la prestación del servicio debido a *fallas en los cables de la red* causadas por daño intencional, daño físico debido a roedores o deterioro natural.

### Riesgo Inherente

(PF:	10	+	PI:	10	+	DC10:	10	)X	PR:	3	=	RIESGO:	150
------	----	---	-----	----	---	-------	----	----	-----	---	---	---------	-----

### Controles Existentes

- Se monitorea y gestiona la red mediante software 7x24x365.
- Se dispone de enlaces redundantes.
- Existencia de canaletas para la protección de cables.

### Nivel de Exposición

(PF:	10	+	PI:	10	+	DC10:	10	)X	PR:	2	=	RIESGO:	90
------	----	---	-----	----	---	-------	----	----	-----	---	---	---------	----

### Controles Recomendados

- 01 Analizar la viabilidad de implementar los controles recomendados en las normas ISO-27001, NFPA-75 y EIA/TIA-942 para seguridad física.

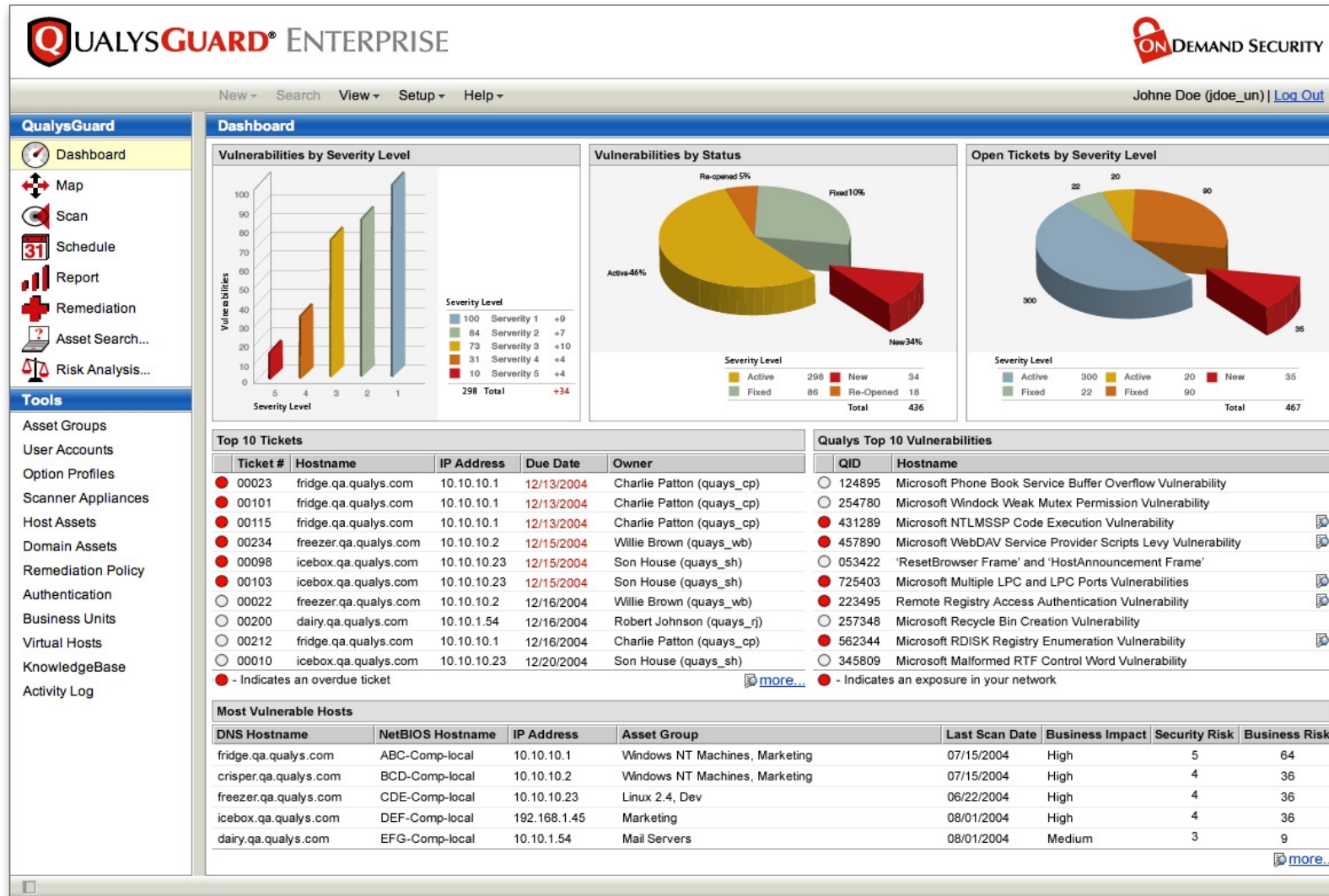
### Riesgo Residual

(PF:	10	+	PI:	10	+	DC10:	10	)X	PR:	1	=	RIESGO:	60
------	----	---	-----	----	---	-------	----	----	-----	---	---	---------	----

# **Análisis de la Infraestructura por aplicación crítica.**

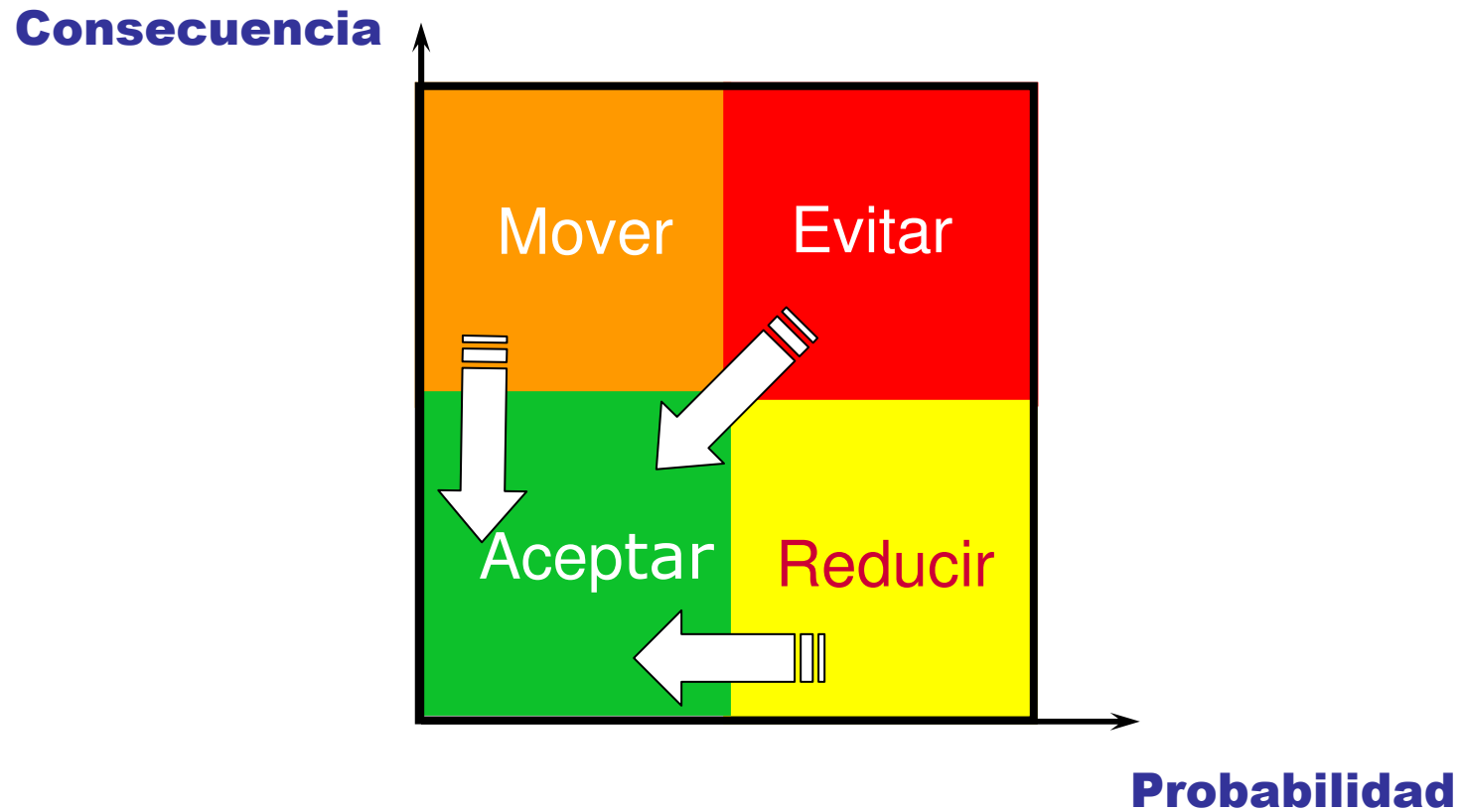
- ◆ **Seguridad Física.**
  - ▶ Monitoreo ambiental
  - ▶ Control de acceso
  - ▶ Desastres naturales
  - ▶ Control de incendios
  - ▶ Inundaciones
- ◆ **Seguridad en las conexiones a Internet.**
  - ▶ Políticas en el Firewall
  - ▶ VPN
  - ▶ Detección de intrusos
- ◆ **Seguridad en la infraestructura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

# Vulnerabilidades en la red



Ejemplo informe

# Evaluación del riesgo y su administración

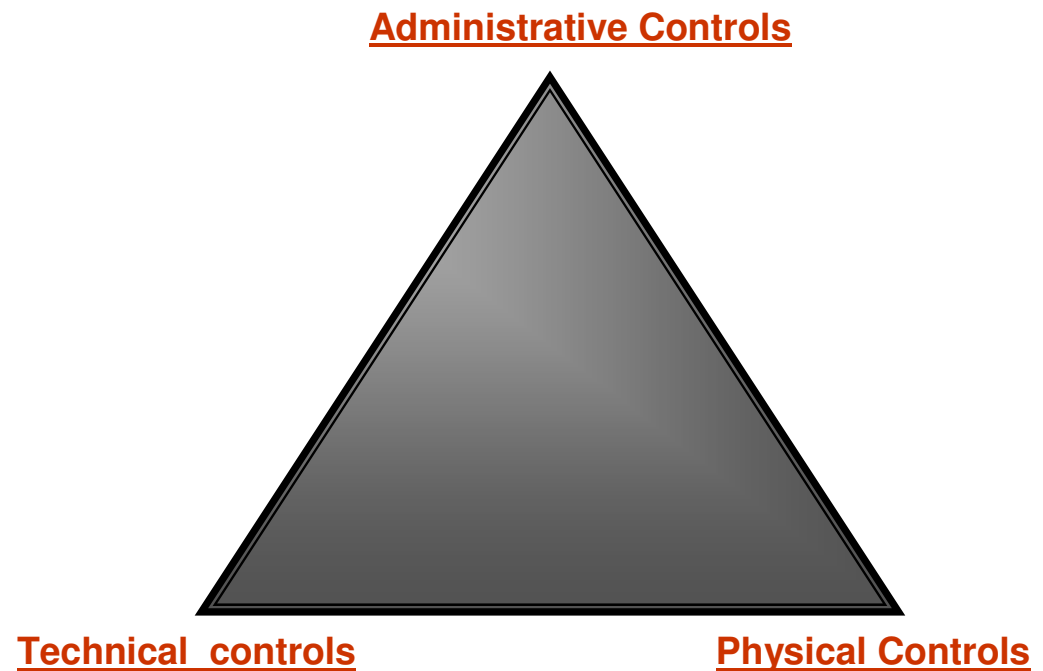


# Tipo de controles en el manejo del riesgo



# Tipos de Controles

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



# **Implementación del SGSI**

# **SGSI**



# **Políticas seguridad de la información**

Una política de seguridad de la información, 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.

[Documento General SGSI](#)

# **Procedimientos seguridad de la información**

Los procedimientos de seguridad de la información 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.

[Ejemplo de procedimiento](#)

# Estándares seguridad de la información

- 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).
- [Ejemplo de estándar de configuración Firewall.](#)

# Formatos del SGSI

- ◆ Documentos utilizados para formalizar, legalizar y verificar la realización o no de ciertas actividades.
- ◆ [Ejemplo de formato.](#)

# Plan de Entrenamiento en Seguridad.

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



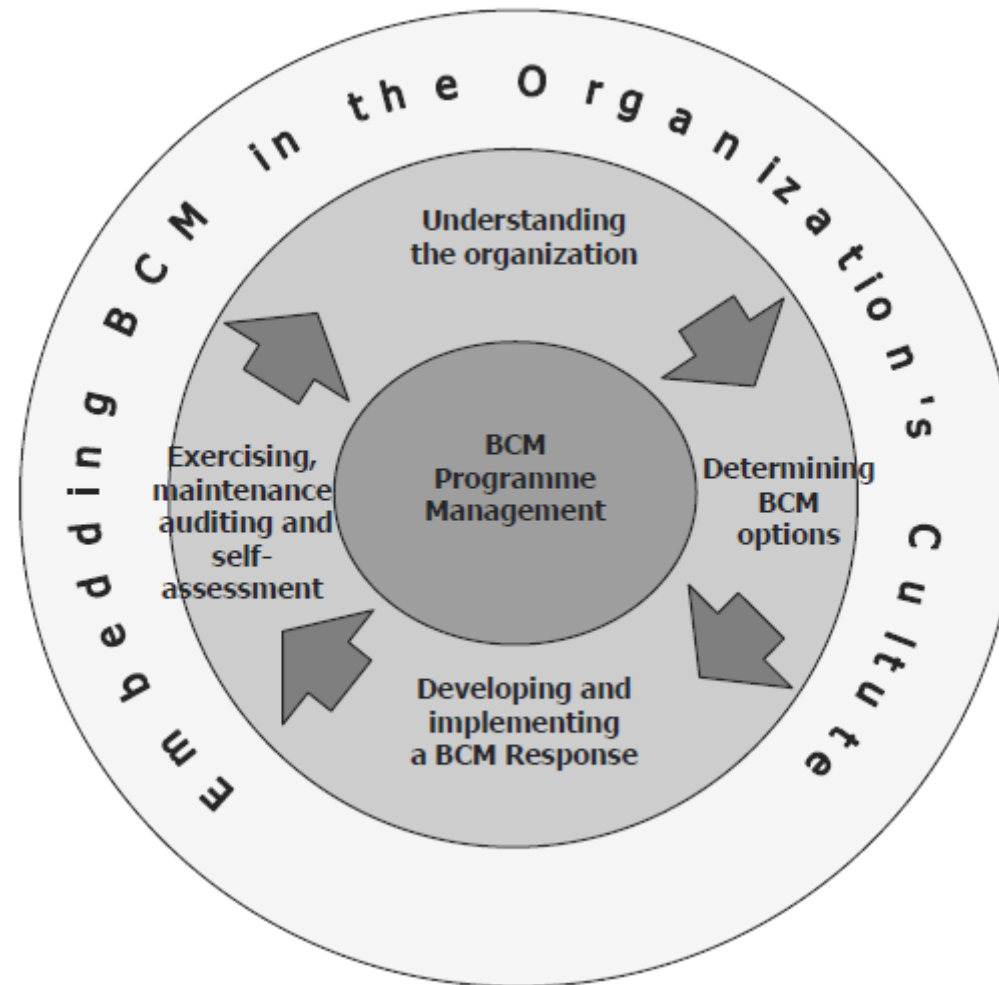
# **Planes para la continuidad**

## **Qué es Continuidad del servicio?**

**La continuidad del servicio involucra capacidades tácticas y estratégicas preaprobadas por la dirección de una entidad para responder a incidentes e interrupciones del servicio con el fin de poder continuar con sus operaciones a un nivel aceptable previamente definido.**

Business continuity strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to incidents and business interruptions in order to continue business operations at an acceptable pre-defined level (BSI, BS-25999,p.6.)

# Gestión de la continuidad del servicio (BCP, DRP)



# **Productos que componen el BCP, DRP**

- ◆ **Business Impact Analysis (Impacto de Análisis del Negocio).**
- ◆ **Risk Assesment (Evaluación o Valoración de Riesgos).**
- ◆ **Estrategias de Continuidad.**
- ◆ **Estructura Organizacional para la Continuidad (Roles, responsabilidades y procedimientos).**
- ◆ **Procesos de Continuidad.**
- ◆ **Plan de Pruebas del Plan de Continuidad.**

# **Auditorías**

# **Auditorías ISO 27001**

- ◆ Evaluar el cumplimiento con respecto a la norma
- ◆ Definir plan de remediación
- ◆ Apoyar procesos de certificación
- ◆ Declaración de aplicabilidad
- ◆ Revisión sobre todos los dominios de la norma

# Auditorías Circular 052

2. Definiciones y criterios de seguridad y calidad
  - 2.1. Criterios de Seguridad de la información
  - 2.2. Criterios de Calidad de la información
3. Obligaciones Generales
  - 3.1. Seguridad y Calidad
  - 3.3. Documentación
  - 3.4. Divulgación de Información
4. Obligaciones Adicionales por Tipo de Canal
  - 4.1. Oficinas
  - 4.2. Cajeros Automáticos (ATM)
  - 4.3. Receptores de Cheques
  - 4.4. Receptores de Dinero en Efectivo
  - 4.5. POS (incluye PIN Pad)
  - 4.6. Sistemas de Audio Respuesta (IVR)
  - 4.7. Centro de Atención Telefónica (Call Center, Contact Center)
  - 4.8. Sistemas de Acceso Remoto para Clientes
  - 4.9. Internet
  - 4.10. Prestación de Servicios a través de Nuevos Canales
5. Reglas sobre Actualización de Software
6. Obligaciones Específicas por Tipo de Medio – Tarjetas débito y crédito
7. Análisis de Vulnerabilidades

# Pre-Auditoría PCI

- ◆ Construir y mantener una red segura.
  - Instalar y mantener un Firewall
  - No usar contraseñas por defecto
- ◆ Proteger información del tarjeta habiente
  - Proteger datos de la tarjeta
  - Cifrar la información
- ◆ Mantener una gestión de vulnerabilidad
  - Mantener un software anti-virus
  - Desarrollar y mantener sistemas y aplicaciones seguras
- ◆ Implementar mecanismos fuertes de control de acceso
  - Mantener un estrategia de *need-to-know*
  - Asignar únicos ID
  - Medidas de control del acceso físico
- ◆ Monitorear y probar (test) la red
  - Monitorear todos los acceso a la red
  - Regularmente pruebe los sistemas y procesos
- ◆ Mantenga una política de seguridad
  - Mantener un política de seguridad de la información

# **Nuestra propuesta**

## Servicios a ofrecer

- “GaP Analysis” en relación al ISO 27001
- Análisis de riesgo (risk assessment) orientado a aplicaciones e Infraestructura de red.
- Análisis de vulnerabilidades.
- Plan de remediación de vulnerabilidades ciertamente explotadas
- Análisis de la Seguridad Física en el Centro de Computo.
- Definición de Políticas, Procedimientos, Estándares, formatos para las aplicaciones definidas como críticas (SGSI).
- Diseño de la Arquitectura de Seguridad para conectividad hacia Internet.
- Plan de educación en Seguridad de la información.
- Planes para la continuidad del negocio (BCP, DRP).
- Auditorías Circular 052, Auditoria ISO 27001, Pre-auditoría PCI.

**FIN**