



**VIII Jornada Nacional de
Seguridad Informática**



***ANALISIS Y GESTION DE RIESGOS,
BASE FUNDAMENTAL DEL SGSI
Caso: METODOLOGIA MAGERIT***



Armando Carvajal

Gerente Consultoría – Globaltek Security
armando.carvajal@globalteksecurity.com

Msc en seguridad informática de la Universidad Oberta de Catalunya - España
Especialista en construcción de software para redes Uniandes, Colombia
Ing. Sistemas – Universidad Incca de Colombia

Antecedentes

Por que medir el riesgo?

"La medición es el primer paso para el control y la mejora. Si algo no se puede medir, no se puede entender. Si no se entiende, no se puede controlar. Si no se puede controlar, no se puede mejorar."

H.James Harrington

Toda actividad para que logre los objetivos de manera eficiente debe ser planeada y debe tener unos beneficios claros

VIII Jornada Nacional de Seguridad Informática



UNA URBANIZACIÓN



VIII Jornada Nacional de Seguridad Informática



UN CENTRO VACACIONAL





VIII Jornada Nacional de
Seguridad Informática



UN CRUCE DE AUTOPISTAS ...





**VIII Jornada Nacional de
Seguridad Informática** ACIS

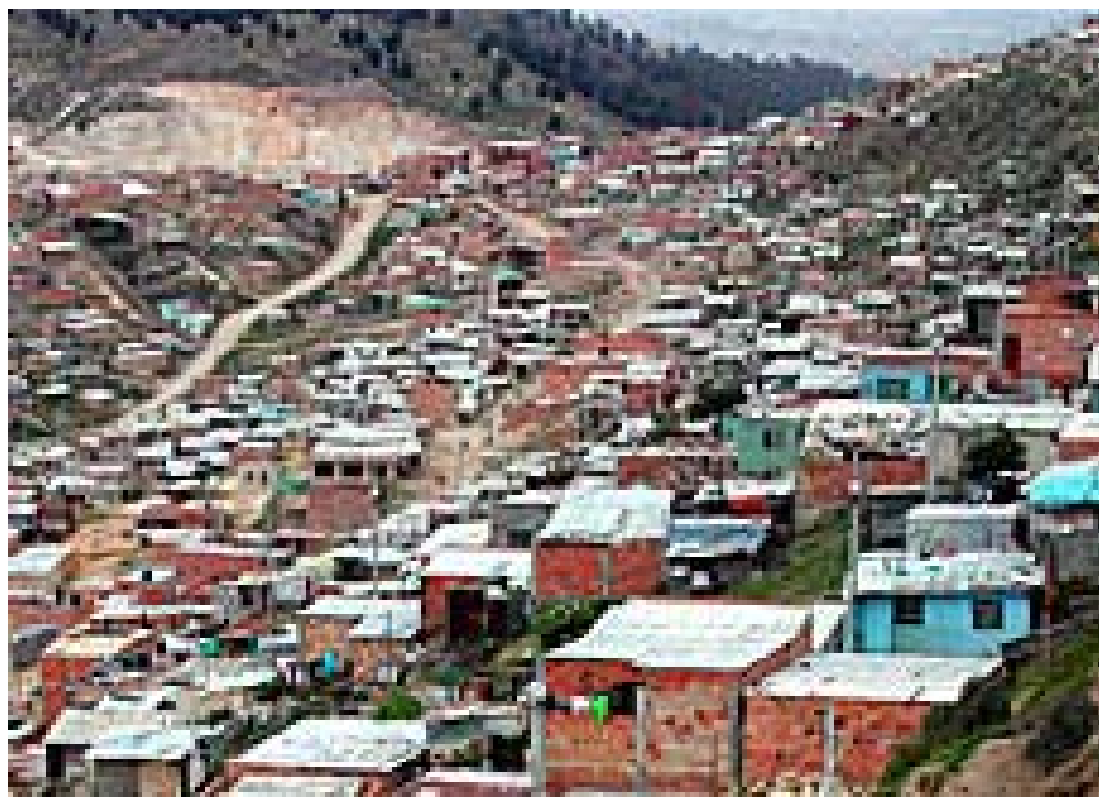
IMPROVISANDO TAMBIEN SE CRECE



VIII Jornada Nacional de Seguridad Informática



PERO LOS RESULTADOS NO SON LOS MEJORES



VIII Jornada Nacional de Seguridad Informática



Y LOS COSTOS SE ELEVAN EN FORMA EXPONENCIAL

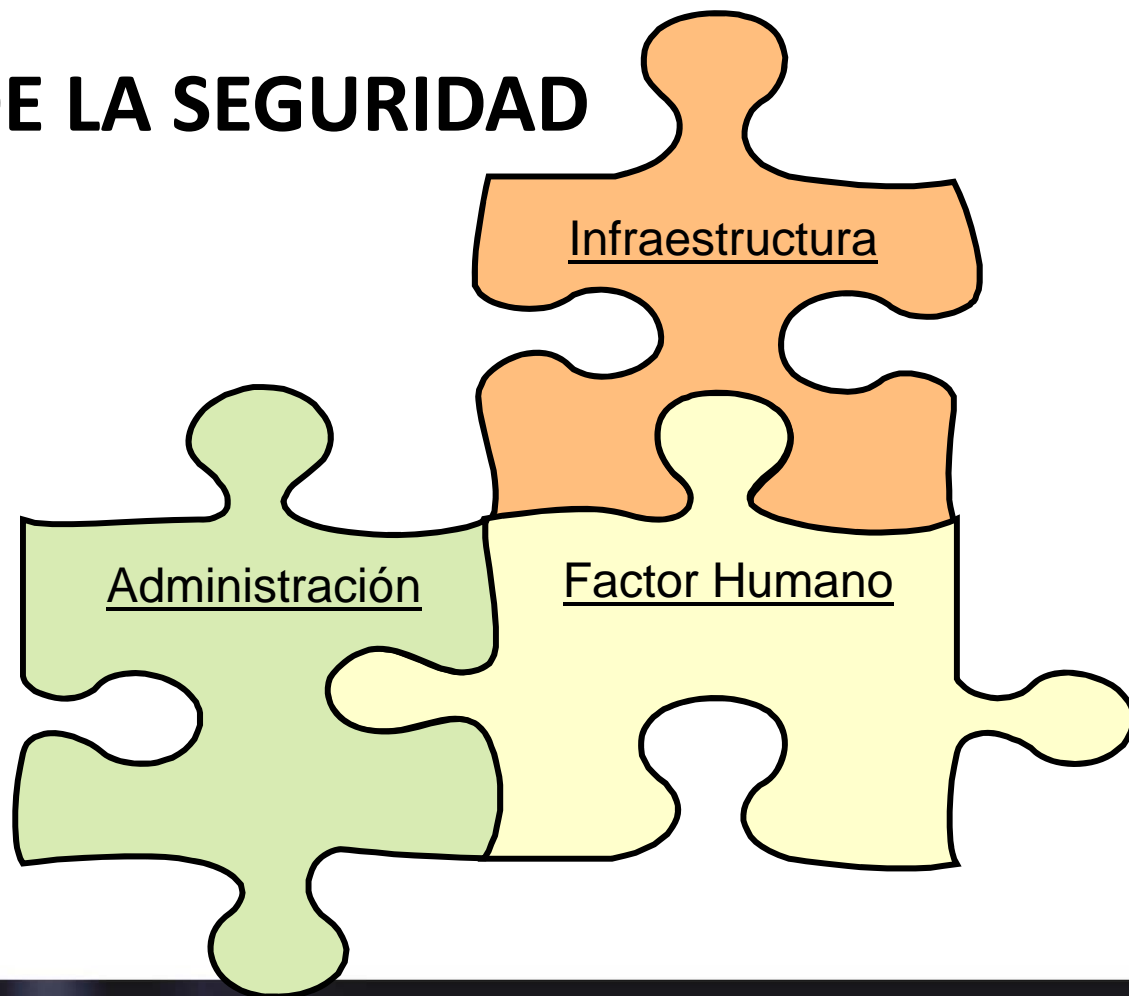


EL RIESGO OPERACIONAL

Es la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la Tecnología, la infraestructura o por la ocurrencia de acontecimientos externos

“Superfinanciera de Colombia”

ACTORES DE LA SEGURIDAD



Circulares Superfinanciera

La Circular Externa 041 de 2007, aprobó la implementación del Sistema de Administración de Riesgos Operativos...

QUE ES ANÁLISIS DE RIESGOS?

- Es la consideración sistemática del daño probable que puede causar en el negocio un fallo en la seguridad de la información, con las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información



CUANTO INVERTIR EN SEGURIDAD DE LA INFORMACION?

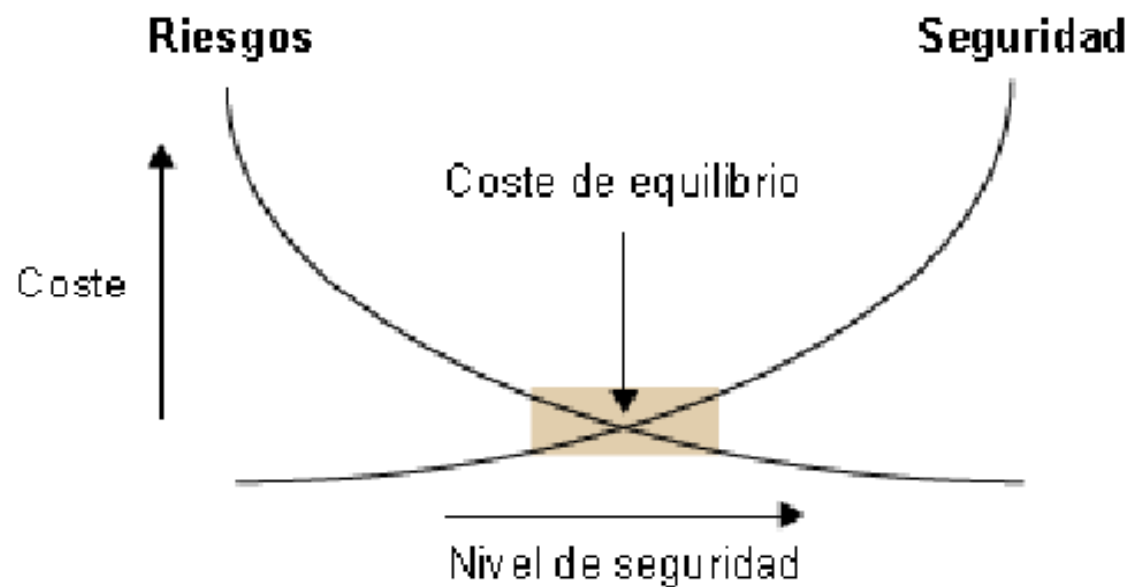
- La respuesta esta directamente relacionada con EL VALOR DEL ACTIVO A PROTEGER
- El valor de un activo depende de varios factores:
 - No solo de su costo de adquisición
 - La información contenida en los activos
 - Los procesos controlados
 - El impacto en la organización cuando falle



VIII Jornada Nacional de Seguridad Informática



Quando debo invertir?



VIII Jornada Nacional de Seguridad Informática



PROCESO DE EVALUACION DEL RIESGO



Juan Carlos Reyes, Seltika, 2007

Riesgo (1 de 2)

- Es la posibilidad de que se produzca un impacto sobre algún activo (Incurrir en pérdidas)



Riesgo (2 de 2)

- El control del riesgo como resultado del análisis de riesgos, es un proceso complejo que parte de la determinación de los activos y las amenazas



VIII Jornada Nacional de Seguridad Informática



PROCESO DE EVALUACION DEL RIESGO




Juan Carlos Reyes, Seltika, 2007

Amenazas (1 de 4)

- Las amenazas son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos

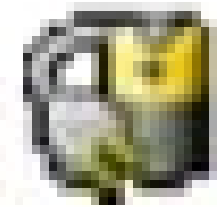


Amenazas (2 de 4)

- La consecuencia de la amenaza, si se materializa, es un incidente que modifica el estado de seguridad de los activos amenazados 
- Es decir, hace pasar el activo de un estado inicial anterior conocido a otro posterior, que puede ser no deseable

Amenazas (3 de 4)

- Los activos están expuestos a muchas clases de amenazas
- Las cuales pueden explotar sus vulnerabilidades



Amenazas (4 de 4)

- Los controles de seguridad que se implementen se seleccionarán teniendo en cuenta las vulnerabilidades, no las amenazas (*)



VIII Jornada Nacional de Seguridad Informática



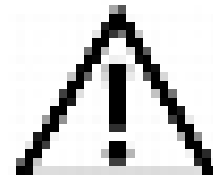
PROCESO DE EVALUACION DEL RIESGO



Juan Carlos Reyes, Seltika, 2007

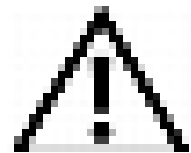
Vulnerabilidades (1 de 4)

- Falla,
- error,
- "causa"



Vulnerabilidades (2 de 4)

- También se le conoce a la vulnerabilidad como una debilidad
- Agujero, falla o error en la seguridad del sistema de información




Vulnerabilidades (3 de 4)

- En sí misma no causa daño, es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo



Vulnerabilidades (4 de 4)

- Una propiedad de la relación entre un activo y una amenaza, 
- Si no se gestiona adecuadamente permitirá a la amenaza materializarse

Impacto (1 de 2)

- Es la consecuencia sobre un activo de la materialización de una amenaza



Impacto (2 de 2)

- El impacto mide la diferencia entre el estado de seguridad de un activo
- Lo hace antes y después de la materialización de una amenaza



PROCESO DE EVALUACION DEL RIESGO



Riesgo Intrínseco

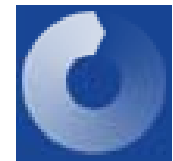
- Es el estudio que se realiza sin tener en consideración las diferentes medidas de seguridad que ya están implantadas en una organización

Riesgo Residual

- Es el estudio que se realiza teniendo en consideración las medidas de seguridad que la organización ya tiene implantadas

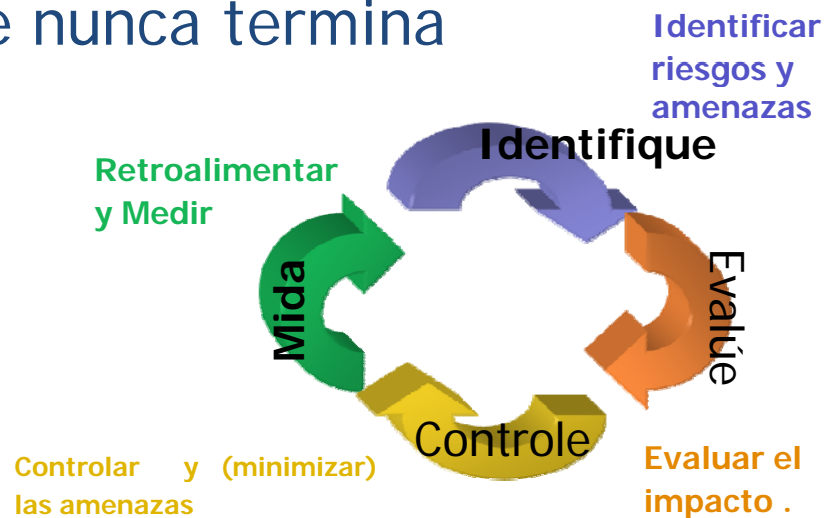
QUE HACER DESPUES DEL ANÁLISIS DE RIESGOS?

- Gestión de los riesgos detectados que soporta la identificación, selección y adopción de controles con base a los riesgos identificados y a la reducción de esos riesgos a un nivel aceptable definido por la ALTA dirección. ISO 27002:2005 (antes 17799:2005) ayuda en esta tarea



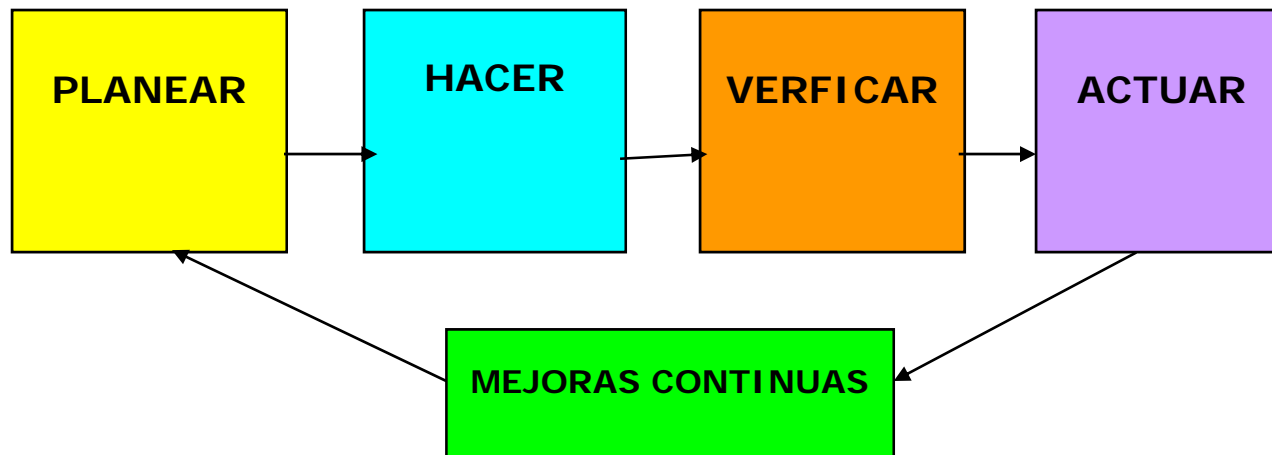
SGSI

- La organización debe entender la seguridad como un proceso que nunca termina



SGSI

- La organización debe entender la seguridad como un proceso que nunca termina
- La inseguridad es una propiedad inherente a los recursos informáticos y la gestión es la única forma de medirla y aminorarla



Metodología Magerit

VIII Jornada Nacional de Seguridad Informática



METODOLOGIAS/HERRAMIENTAS

@Risk

LAVA (Los Alamos Vulnerability Analysis)

Analyze des Risques Programmes LRAM&ALRAM ([Automated] Livermore Risk

AnalyZ

Analysis)

AROME+

MAGERIT

BDS Risk Assesor

MINIRISK

BDSS (Bayesian Decision Support System)

PREDICT

Buddy System

PSICHE

COBRA

RANK-IT

CONTROL-IT

RISAN

CRITI_CALC

RiskCALC

CRAMM

RiskWatch

CCTA Risk Analysis and Management Methods

SBA (Security by Analysis)

DDIS (Datenschutz-und-datensicherheits

SISSI

Informations System)

XRM (eXpert Risk Management)

Magerit

- Una metodología exitosa muy probada es la creada por el “Consejo Superior de Informática” de España sobre el Análisis y Gestión de Riesgos de los sistemas de Información
- La primera versión se hizo en 1997, actualmente existe la versión II

Magerit

- MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
- El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos

Objetivos Magerit

- 1. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo
- 2. Ofrecer un método sistemático para analizar tales riesgos

Objetivos Magerit

- 3. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control
- 4. Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Ventajas de magerit

- Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles

Desventajas de magerit

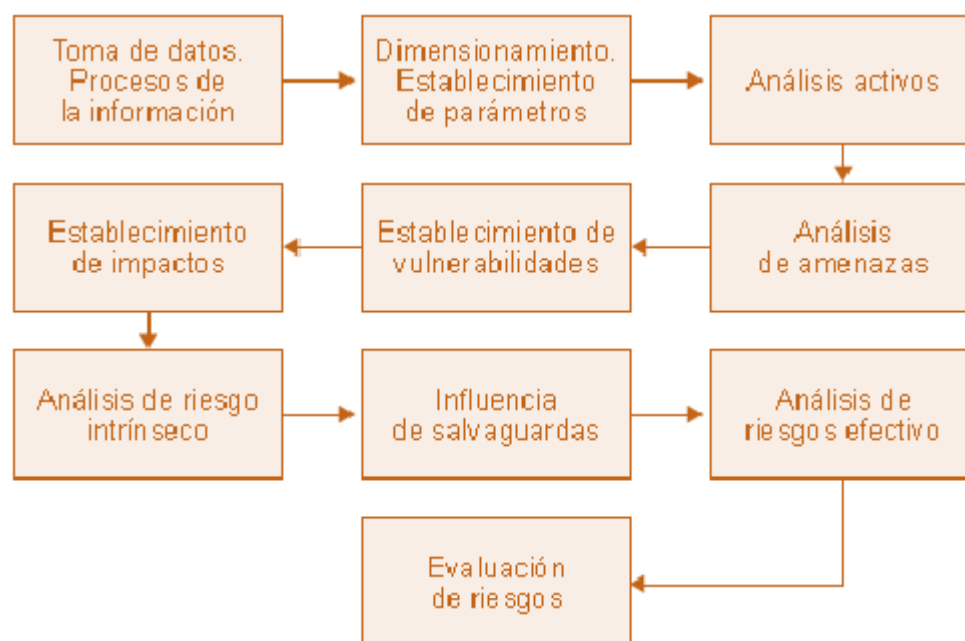
- Por el contrario, el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa

Donde consigo la metodología
versión II?

<http://www.csi.map.es/>



Ejemplo metodología Magerit



Toma de datos y procesos de información

VIII Jornada Nacional de Seguridad Informática



Establecimiento de Parámetros

Tabla Costo de Activos		
MA	Muy alto	2.100.000
A	Alto	300.000
M	Medio	72.000
B	Bajo	4.000

Explicación:

De acuerdo a los activos se les da una categoría

Tabla Vulnerabilidad de los activos		
EF	Extremadamente frecuente	1
MF	Muy Frecuente	0,071
F	Frecuente	0,016
FN	Frecuencia Normal	0,005
PF	Poco Frecuente	0,003

Clasificación numérica de la vulnerabilidad que puede presentar el activo

Tabla Degradación de los activos (Impacto)		
A	Alta	90
M	Media	50
B	Baja	10

Clasificación del nivel de impacto que puede tener un activo

Valoración de activos

Código	Nombre	valor
90	Imagen Organizacional	2.100.000
51	Bases de datos	72.000
22	Desarrollo	300.000
68	Servidor WEB	4.000



2.476.000

Estos son los cuatro activos elegidos del archivo excel: Imagen Organizacional, Bases de datos, Desarrollo y servidor web

Amenazas globales

Código	Amenaza	Vulnerabilidad		Impacto		Activos	Riesgo
							Intrínseco
A1	Incendio oficinas	PF	0,003	A	90	2.476.000	6.685
A2	Danio de Hardware	EF	1	M	50	2.476.000	1.238.000
A4	Acceso a oficinas no autorizado	MF	0,071	B	10	2.476.000	17.580
A3	No disponibilidad del Personal	FN	0,005	B	10	2.476.000	1.238
TOTAL						9.904.000	1.263.503



Aca se hace el análisis de amenazas y la formula utilizada para calcular el Riesgo Intrínseco seria:
Valor de los activos * Vulnerabilidad * (Impacto/100) = Riesgo Intrínseco

Controles por amenazas

Amenaza	Control	Dism. Vulnerabilidad		Dism. Impacto	
A1	S12	A	90	M	60
A2	S14	M	60	A	90
A4	S02	A	90	M	60
	S04	M	60	M	60
	S06	M	60	M	60
	S08	A	90	A	90
A3	S10	A	90	M	60

Ahora relacionamos cada amenaza con su respectivo control/salvaguardas y asignamos un valor de disminución de la vulnerabilidad como disminución del impacto por cada control/salvaguarda asignado

Riesgo efectivo x activo

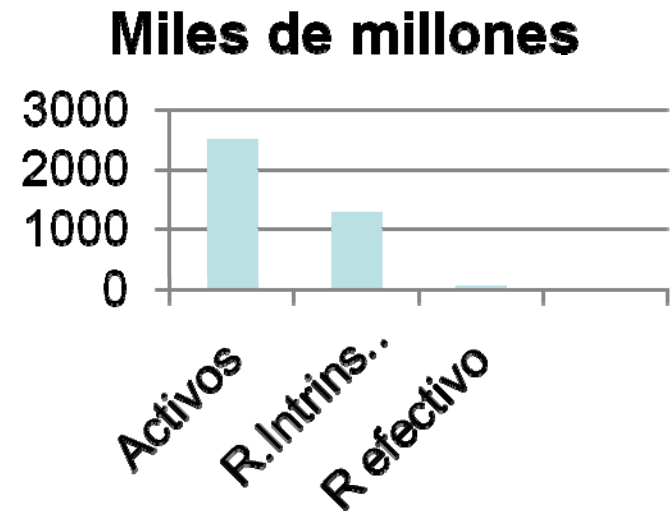
RIESGO EFECTIVO								
ACTIVOS			AMENAZAS					
Código	Valor del Activo	Descripción del Activo	Amenazas	A1	A2	A4	A3	RIESGO EFECTIVO POR ACTIVO
				Incidio Oficinas	Danio en Hardware	Acceso a Oficinas no autorizado	No disponibilidad de Personal	
			Vulnerabilidad	0,003	1	0,071	0,005	
			Impacto (%)	90	50	10	10	
			Disminución de Vulnerabilidad (%)	90	60	99,84	90	
			Disminución de Impacto (%)	60	90	99,36	60	
90	2.100.000	Imagen Organizacional		227	42.000	0,1527	42	42.269
51	72.000	Bases de datos		8	1.440	0,0052	1	1.449
22	300.000	Desarrollo		32	6.000	0,0218	6	6.038
68	4.000	Servidor web		0	80,0000	0,0003	0	81
RIESGO EFECTIVO POR AMENAZA				267	49.520	0,1800	50	49.837

Ahora calculamos el riesgo efectivo por amenaza y por activo:

$$\text{Riesgo Efectivo} = \text{Riesgo Intrínseco} * (1 - \text{Disminución de la vulnerabilidad}) * (1 - \text{Disminución del impacto})$$

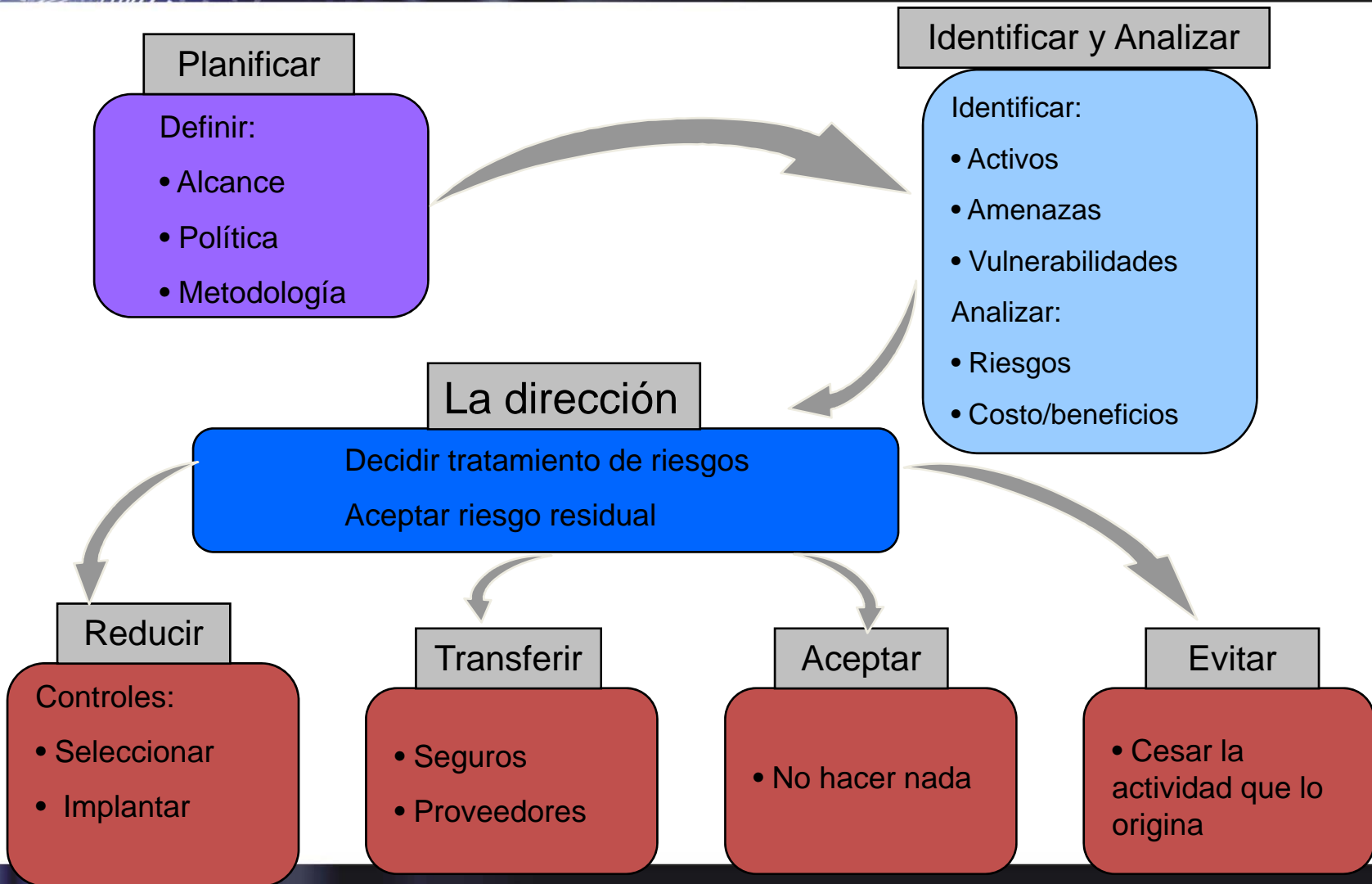
Que mira la alta gerencia?

Conclusiones Finales			
	Valor de Activos	Riesgo Intrínseco	Riesgo Efectivo
	2.476.000	1.263.503	49.837
TOT	2.476.000	1.263.503	49.837



El riesgo intrínseco para este estudio es de 51.03% del valor de los activos y el riesgo efectivo es de 2.01%

VIII Jornada Nacional de Seguridad Informática



CONCLUSIONES

- La **forma** de conseguir el mayor beneficio en seguridad de la información es contar con una adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en casos de incidentes
- No importa la metodología que se seleccione

CONCLUSIONES

- La seguridad de la información no es una responsabilidad únicamente del área de tecnología debe fluir desde la alta gerencia hacia todos los procesos de negocios

CONCLUSIONES

- Un comité de seguridad de la información compuesto por cada jefe de área genera más compromiso para hacer cumplir las políticas de seguridad de la información

CONCLUSIONES

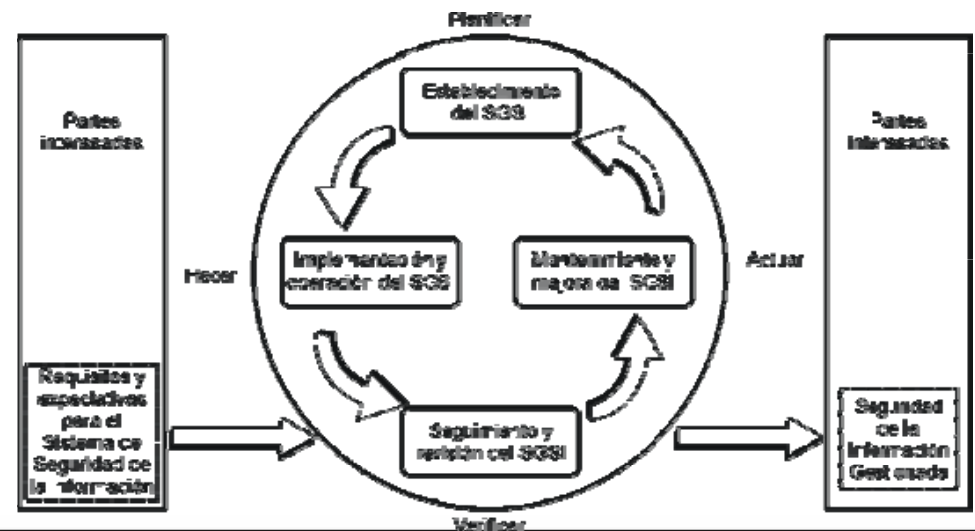
- Si la seguridad de la información depende únicamente de IT entonces la probabilidad es del 100% de que no se implemente

CONCLUSIONES

- Los recursos financieros de una organización deben invertirse de la mejor manera mirando siempre el retorno de inversión

CONCLUSIONES

- La organización debe entender la seguridad como un proceso que nunca termina
- La inseguridad es una propiedad inherente a los recursos informáticos y la gestión es la única forma de medirla y aminorarla



BIBLIOGRAFÍA

- [Maestria en seguridad informatica \(http://www.uoc.edu\)](http://www.uoc.edu), Daniel Cruz Allende
- [Creadores de la metodologia \(http://www.csi.map.es\)](http://www.csi.map.es) BCI (The Bussiness Continuity Institute) www.thebci.org
- CRAMM www.cramm.com
- esCERT <http://escert.upc.edu>
- FIRST <http://www.first.org/>
- ISO www.iso.org
- ITIL <http://www.ital.co.uk/>
- MAGERIT www.csi.map.es/csi/pg5m20.htm



Preguntas y aportes

