Jornada

"La auditoría y el hacking ético como elementos de mejora continua en los sistemas de seguridad de la información"

Parque Tecnológico de Zamudio

27/04/2006

Enpresa Digitala

nesys

Descripción: durante la jornada se mostrará cómo las técnicas de hacking ético pueden ayudar en los procesos de mejora continua de los sistemas de gestión de la seguridad de la información

Objetivo: los asistentes obtendrán una visión del estado actual y de las tendencias futuras de la seguridad en los sistemas de información. Se presentarán metodologías y técnicas de hacking ético de gran ayuda a la hora de realizar auditorías de seguridad.

Dirigido a: administradores de sistemas, responsables de sistemas de información, responsables de seguridad, responsables de calidad, directores de departamentos de tecnologías de la información

Introducción

La seguridad informática es percibida en la actualidad como una "nueva moda" que se empieza a escuchar por todos lados y empieza a calar en las empresas y los usuarios.

La eclosión de las tecnologías de la información nos ha brindado un cambio considerable en la forma en la que vivimos y nos comunicamos diariamente tomando Internet como eje central. Nos vamos dando cuenta que para todo ello se van a necesitar unas garantías en cuanto a la seguridad de la información y lo que ésta acarrea planteandose un nuevo escenario.

Esto se produce en muchas ocasiones motivado por el "miedo" producido por las nuevas noticias de incidentes relacionados con la seguridad y el "desconocimiento" de la tecnología por parte del usuario medio. Las reacciones que provocan estos dos factores son dispares en las empresas: desde la implantación de sistemas excesivamente costosos en las redes con el fin de conseguir un falso sentido de la seguridad "*Caso: plan director de seguridad*" o la negación del problema no prestándole la importancia que requiere "*Caso: eso nunca me va a pasar a mi*"

Esta jornada tratará de dar una visión global del escenario actual y orientará sus conclusiones a dar a la problemática la respuesta adecuada con ayuda de profesionales y describir las metodologías y mecanismos de auditoría y "hacking ético"

Introducción

Todo esto nos sitúa en una nueva era en la que se debe considerar la seguridad de la información como un "proceso" más en la estructura de negocio y que por tanto habrá que planificar, implantar, controlar, optimizar y revisar cíclicamente.

Se trata, por tanto, de una jornada de concienciación por un lado y de exposición del camino a seguir a corto, medio y largo plazo. La jornada esta dividida en tres partes:

- La **primera** parte de la jornada nos dará una visión global de la situación actual en lo referente a la seguridad de los sistemas de información, y nos marcará las tendencias actuales en tres áreas diferentes:

    1. La situación actual en cuanto a las amenazas a las que estamos expuestos
    2. La búsqueda de profesionales con capacidad de abordar la problemática
    3. La seguridad como proceso de negocio

- La **segunda** parte nos describirá qué o quién nos amenaza, sus comportamientos y el riesgo que provoca en nuestras empresas

- La **tercera** parte nos describirá como funcionan las metodologías y los estándares a utilizar a la hora de llevar a cabo las auditorías y el "hacking ético" en los sistemas de información, describiéndo las diferentes áreas que analizan y tocan y los pasos a seguir en cada una de ellas.

Agenda

9:30 Estado actual y tendencias de la seguridad en los sistemas de información

10:30 Tipos de amenazas, perfiles de ataque y niveles de riesgo

11:30 **Descanso, café**

12:00 El hacking ético de redes y sistemas dentro de los procesos de mejora continua de las empresas

Agenda

9:30 Estado actual y tendencias de la seguridad en los sistemas de información

Tendencias de la seguridad en las TIC

1. Cada año aumenta el **número de amenazas**: virus, ataques, vulnerabilidades, exposición e incidentes de seguridad.

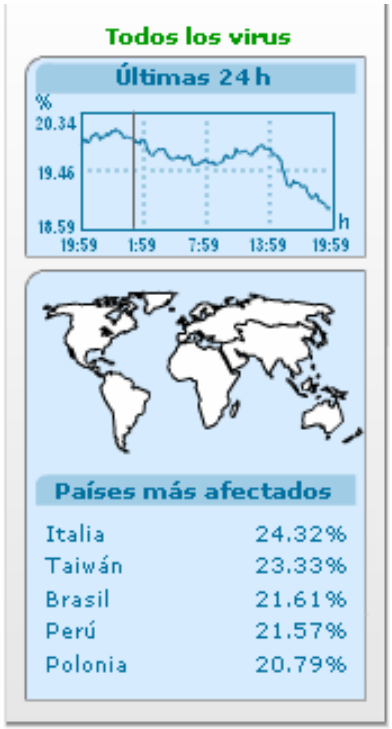
   Aparecen nuevos tipos de malware, mayor número de delitos, nuevas tecnologías y técnicas, herramientas de intrusión automatizadas, mayor acceso al conocimiento …

Estado actual vírico

Virus actuales e infecciones por paises:

Virus Top 10 en Marzo 2006	
1	W32/Zafi-B
2	W32/Netsky-P
3	W32/Nyxem-D
4	W32/MyDoom-AJ
5	W32/Mytob-EX
6	Troj/Clagger-I
7	W32/Mytob-BE
8	W32/Netsky-D
8	W32/Mytob-FO
10	W32/Mytob-Z
Fuente: Sophos	

Últimos 10 virus	
24 abr	W32/Bagle-GT
24 abr	Troj/Bdoor-AAB (en inglés)
24 abr	W32/Bagle-GY
24 abr	W32/Bagle-GN
24 abr	W32/Kassbot-O
23 abr	Troj/BankSnif-J
22 abr	W32/Forbot-GI
22 abr	W32/Bagle-GU
21 abr	Troj/Agent-BHO
21 abr	Troj/Dloadr-HAA
Fuente: Sophos	



Impacto económico de los virus

Pérdidas en millones de dólares:

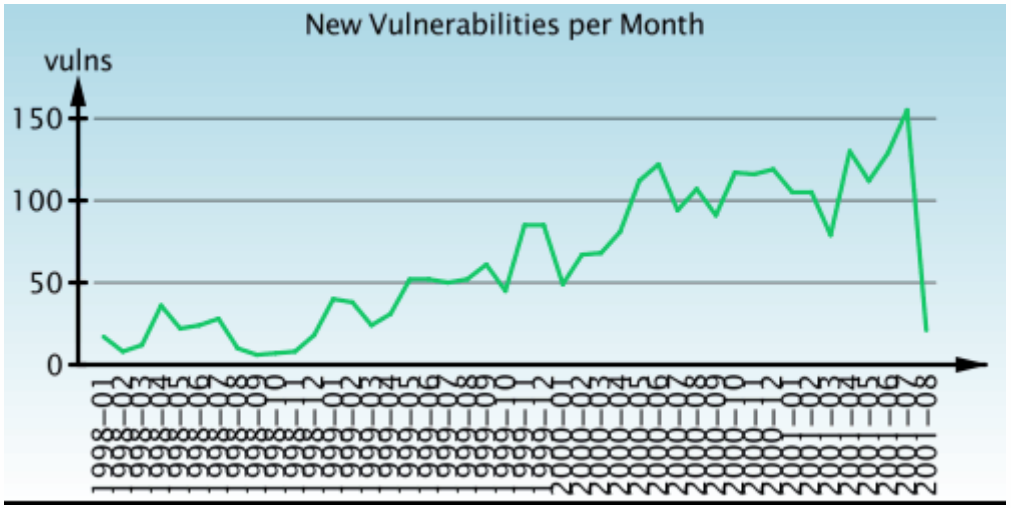
Financial Impact of Virus Attacks 1995—2005

	Worldwide Impact (US $)
2005	$14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion
1997	3.3 Billion
1996	1.8 Billion
1995	500 Million

Source: Computer Economics, 2006

Figure 1

Vulnerabilidades descubiertas



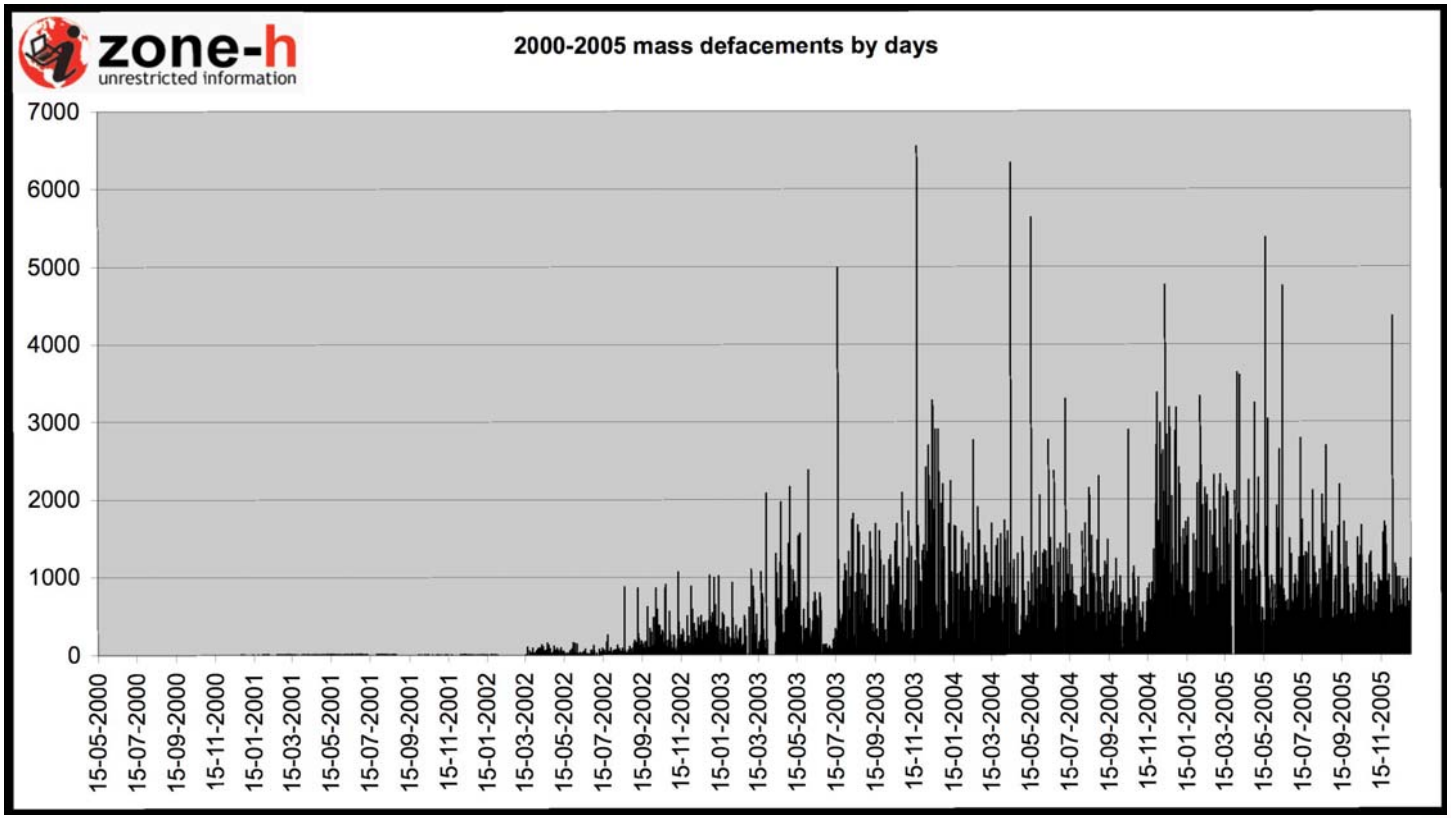
- Evolución del número de vulnerabilidades en el periodo (1998-2001)

Microsoft

- Microsoft publicó 51 security advisories en todos sus productos en 2003
  - ¡¡Una media de un parche por semana!!
- De todos, 30 correspondieron al SO Windows XP

Defacements de sitios Web

Fuente: www.zone-h.org

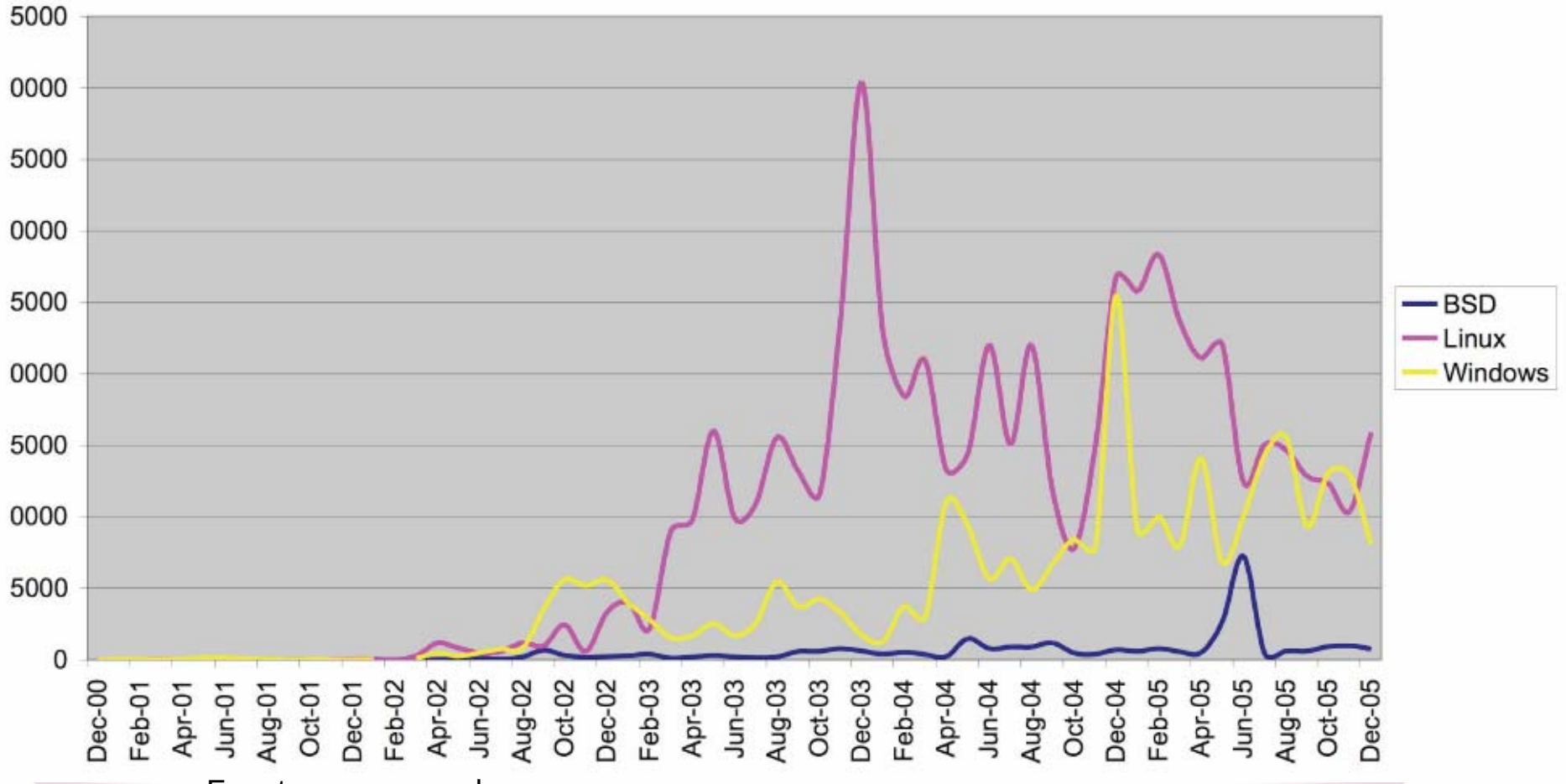


Ataques a sitios Web han incrementado de 20 al día a más de 1500/día en los últimos tres años

Enpresa Digitala

nesys

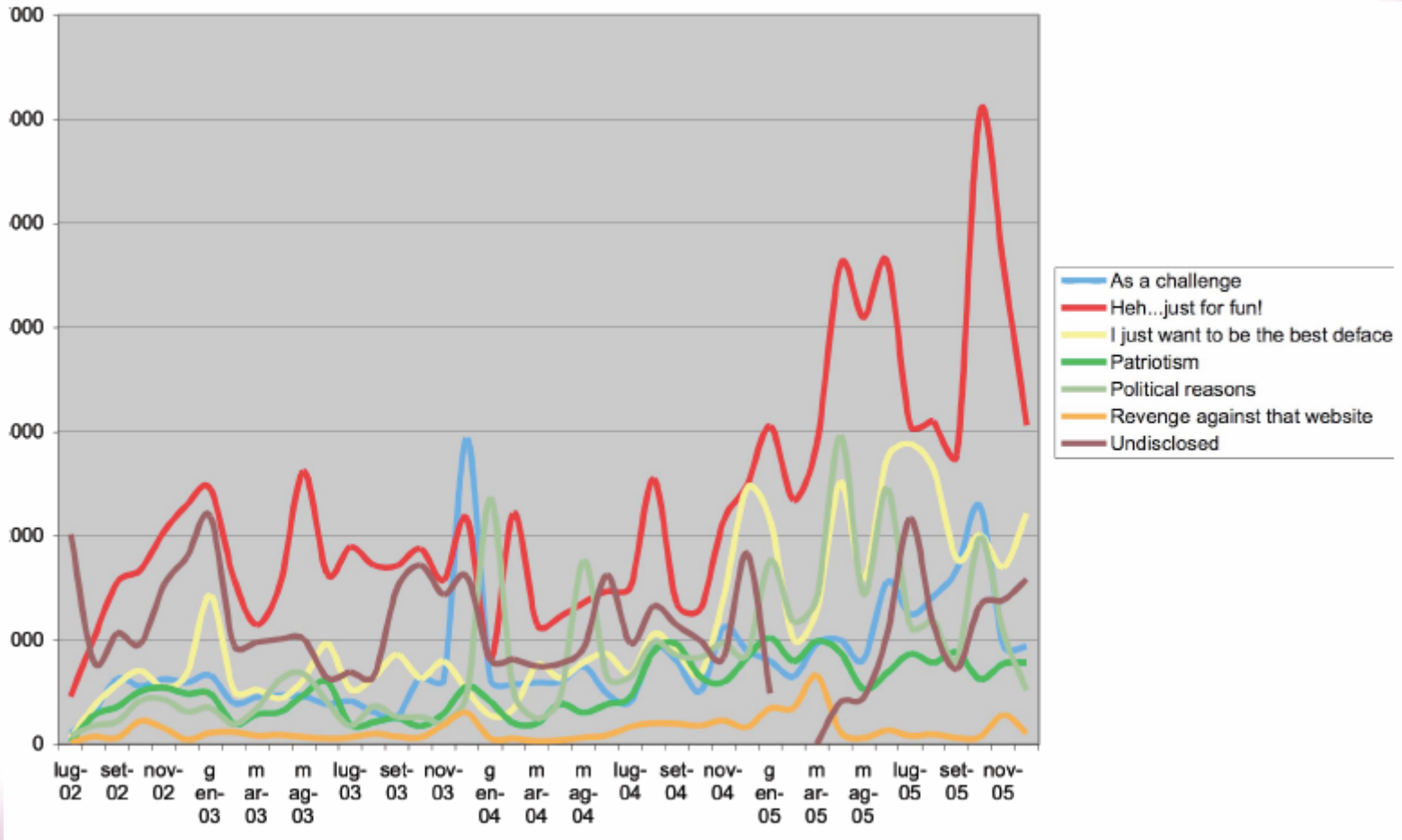
Ataques a servidores web



Fuente: www.zone-h.org

Motivos de los ataques

Fuente: www.zone-h.org



Ataques en Internet: Top 20

Rank	% of total	Type	Name	Advisory
1	32.21	probe	HTTP GET Generic	—
2	8.03	probe	Radmin	—
3	7.88	worm	Ditpnet_Probe	—
4	7.81	worm	Slammer.A	MS02-039
5	6.15	probe	Webdav	MS03-007
6	4.80	probe	MSSQL	—
7	3.43	exploit	Microsoft SQL Server 2000 Resolution Service	MS02-039
8	2.85	probe	SSH Bruteforce Password Crack	—
9	2.73	exploit	Microsoft ASN.1	MS04-007
10	2.29	exploit	Buffer Overrun in Microsoft RPC Interface	MS03-026
11	2.03	probe	Get HTTP Proxy Information	—
12	1.75	worm	Blaster	MS03-026
13	1.71	probe	Bagle Backdoor	—
14	1.54	exploit	Dameware_Netmaniak_40	VU#909678
15	1.53	probe	HTTP CONNECT	—
16	1.45	worm	Dabber	—
17	0.39	worm	Agobot via WebDAV exploit	MS03-007
18	0.38	exploit	WINS	MS04-045
19	0.31	probe	FTP	—
20	0.24	exploit	UPNP	MS01-059

Fuente: http://www.viruslist.com

Puertos usados en ataques

Rank	% of total	Port	
1	26.14	445	**SMB**
2	18.75	80	**WEB**
3	15.65	135	**NETBIOS**
4	12.71	1026 (UDP)	**Windows Messenger Popup**
5	5.13	1433	**Microsoft SQL Server**
6	4.23	1434 (UDP)	**Microsoft SQL Server**
7	4.19	1027 (UDP)	**Windows Messenger Popup**
8	2.68	4899	
9	2.57	15118	
10	1.03	5554	

Fuente: http://www.viruslist.com

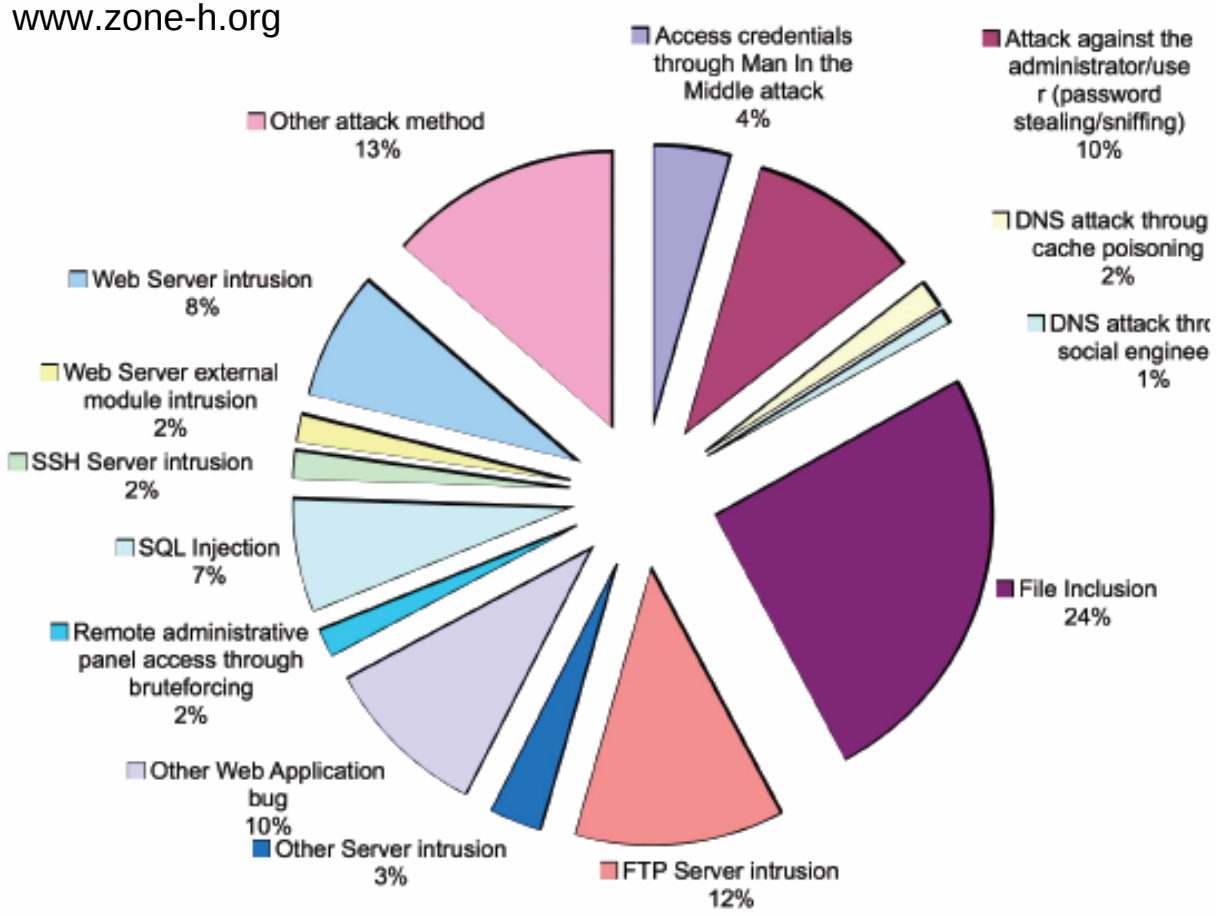
Vulnerabilidades usadas

Rank	Advisory	Description
1	MS02-039	Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)
2	MS03-007	Unchecked Buffer in Windows Component Could Cause Server Compromise (815021)
3	MS03-026	Buffer Overrun in RPC Interface Could Allow Code Execution (823980)
4	MS04-007	ASN.1 Could Allow Code Execution (828028)
5	VU#909678	DameWare Mini Remote Control vulnerable to buffer overflow
6	MS04-045	Vulnerability in WINS Could Allow Remote Code Execution (870763)
7	MS02-061	Escalation of Privilege in SQL Server Web Tasks (Q316333)
8	MS05-039	Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)
9	MS01-059	Unchecked Buffer in Universal Plug and Play Could Allow Remote Code Execution and Elevation of Privilege
10	—	AWStats Rawlog Plugin Logfile Parameter Input Validation Vulnerability

Fuente: http://www.viruslist.com

Métodos de ataques

Fuente: www.zone-h.org



Dist. geográfica de ataques

Rank	% of total	Country	Rank	% of total	Country
1	27.38	China	11	1.25	Germany
2	21.16	USA	12	1.25	the Netherlands
3	6.03	South Korea	13	1.13	United Kingdom
4	2.82	Canada	14	0.72	France
5	2.04	Hong Kong	15	0.41	Italy
6	2.00	Russia	16	0.39	Brazil
7	1.88	Spain	17	0.31	Switzerland
8	1.77	the Philippines	18	0.29	India
9	1.72	Japan	19	0.25	Poland
10	1.63	Taiwan	20	0.22	Uruguay

Fuente: http://www.viruslist.com

Phishing

Percentage of Corporate Phishing Victims

Company	% of Attacks
CitiBank	54.16%
Smith Barney	13.48%
SunTrust	10.02%
Paypal	7.57%
Wells Fargo	5.42%
HSBC	5.07%
eBay	4.15%
USBank	0.11%
CitizensBank	0.014%

Fuente: www.ciphertrust.com

Phishing

Country of Origin (by IP)

Country	% of Attacks
United States	27.74%
Republic of Korea	17.35%
China	8.00%
France	6.27%
Germany	4.85%
United Kingdom	3.95%
Spain	3.59%
Japan	3.49%
Italy	2.43%

Fuente: www.ciphertrust.com

Spam

The 10 Worst Spam Origin Countries		As at 24 April 2006
Rank	Country	Number of Current Known Spam Issues
1	United States	2291
2	China	344
3	Russia	295
4	Japan	273
5	Taiwan	180
6	Canada	173
7	South Korea	160
8	United Kingdom	136
9	Netherlands	133
10	Hong Kong	122

Source: Spamhaus Blocklist (SBL) database.

Spam

The 10 Worst Spam Service ISPs		As at 24 April 2006
Rank	Network	Number of Current Known Spam Issues
1	mci.com	214
2	sbc.com	91
3	comcast.net	71
4	hinet.net	51
5	nttpc.ne.jp	42
6	ocn.ne.jp	40
7	xo.com	39
8	level3.net	39
9	interbusiness.it	36
10	newworldtel.com	31

Source: Spamhaus Blocklist (SBL) database.

Spam

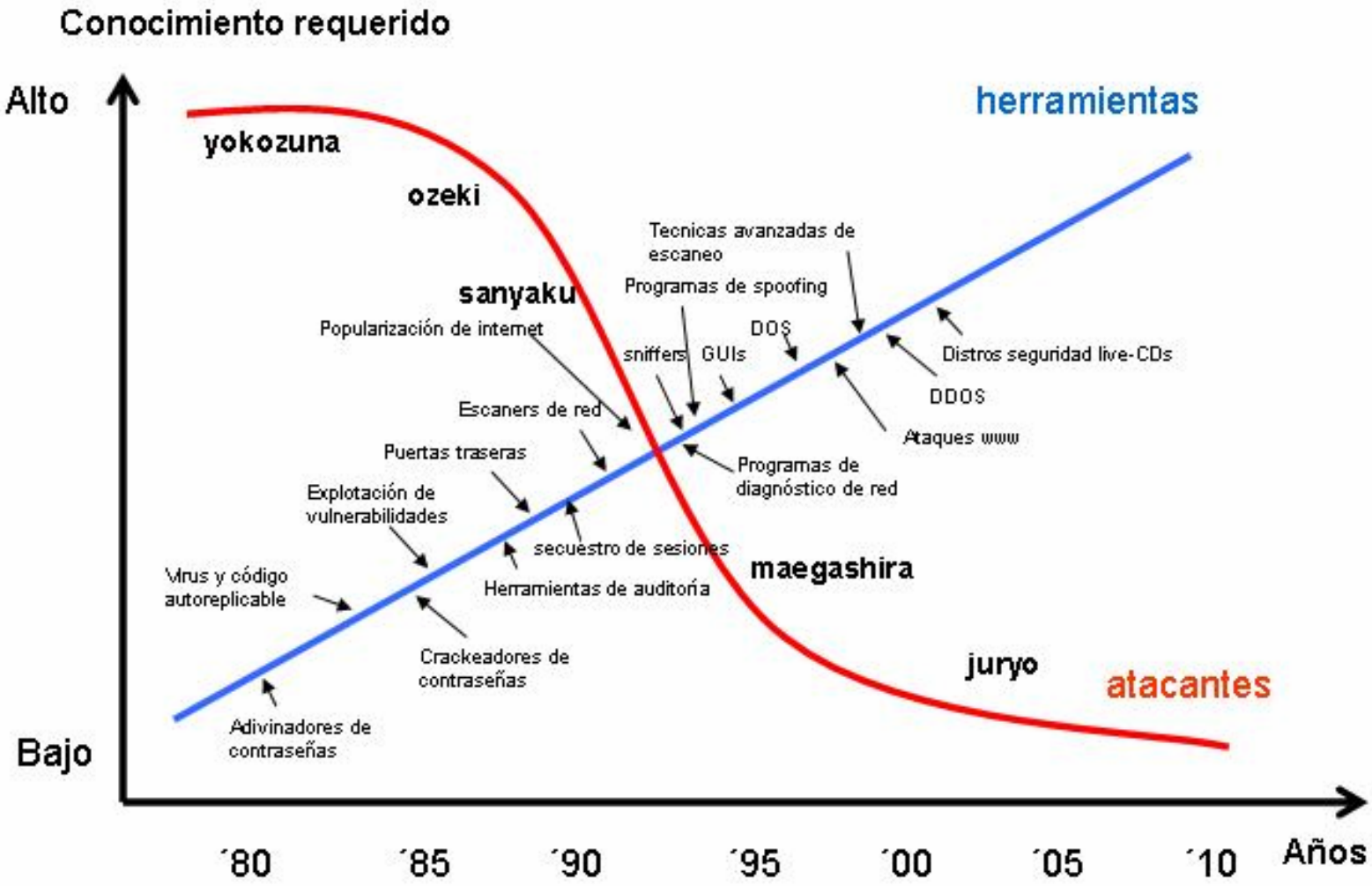
Email considerado Spam	**40% del total**
Spam diario enviado	**12.400 millones**
Spam Anual recibido por persona	**2,200**
usuarios non-corp Internet	**$255 millones**
Coste del Spam a las empresas US (2002)	**$8900 millones**
Cambios de dirs. Email debidas al Spam	**16%**
Crecimiento estimado del Spam para 2007	**63%**
Usuarios que responden a emails Spam	**28%**
Usuarios que compran por el Spam	**8%**
Email corporativo considerado Spam	**15-20%**
Tiempo perdido por email de Spam	**4-5 seconds**

¿Por qué a pesar de la mejora de la tecnología vamos a peor en lo referente a incidentes de seguridad?

El nivel de conocimiento necesario para comprometer un sistema ha cambiado con el tiempo

1010101010101
1010101010101
1010101010101

Sofisticación VS Conocimiento



Distros Live-CD de seguridad

Tendencias de la seguridad en las TIC

2. Es difícil encontrar el personal con conocimientos de seguridad suficientes para gestionar el riesgo y más aún retenerlo en la empresa

   Para abordar la gestión de la seguridad es aconsejable recurrir a **empresas especializadas** en la materia,

La figura del *"administrador de sistemas"*

también conocido como:

"*el solucionador de problemas*",

"el informático" y/o

"brown manager"

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Técnico multiusos:

Linux, Unix, win32, Mac,XML, HTML, PHP, SQL, Perl, python, todo tipo de acrónimos…

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Cumple la legislación aplicable:

LOPD, LSSICE, Firma digital…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Técnico multiusos:

Linux, Unix, win32, Mac,XML, HTML, PHP, SQL, Perl, python, todo tipo de acrónimos…

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

Cumple la legislación aplicable:

LOPD, LSSICE, Firma digital…

Conoce las normas de calidad y los códigos de buenas prácticas:

ISOs, UNEs, NIST…

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

Técnico multiusos:

Linux, Unix, win32, Mac,XML, HTML, PHP, SQL, Perl, python, todo tipo de acrónimos…

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Cumple la legislación aplicable:

LOPD, LSSICE, Firma digital…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Conoce las normas de calidad y los códigos de buenas prácticas:

ISOs, UNEs, NIST…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Técnico multiusos:

Linux, Unix, win32, Mac,XML, HTML, PHP, SQL, Perl, python, todo tipo de acrónimos…

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

Experto en seguridad:

Capacidad para combatir, spam, malware, gestionar VPNs, firewalls…

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Cumple la legislación aplicable:

LOPD, LSSICE, Firma digital…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

¿SGSI?

Conoce las normas de calidad y los códigos de buenas prácticas:

ISOs, UNEs, NIST…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Técnico multiusos:

Linux, Unix, win32, Mac,XML, HTML, PHP, SQL, Perl, python, todo tipo de acrónimos…

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

Experto en seguridad:

Capacidad para combatir, spam, malware, gestionar VPNs, firewalls…

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

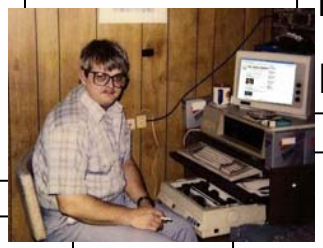
Help desk, soporte microinformático…

Cumple la legislación aplicable:

LOPD, LSSICE, Firma digital…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…



Conoce las normas de calidad y los códigos de buenas prácticas:

ISOs, UNEs, NIST…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

¿SGSI?

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Técnico multiusos:

Linux, Unix, win32, Mac,XML, HTML, PHP, SQL, Perl, python, todo tipo de acrónimos…

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

Experto en seguridad:

Capacidad para combatir, spam, malware, gestionar VPNs, firewalls…

El "papel" del administrador de sistemas en la empresa

Atención a usuarios:

Help desk, soporte microinformático…

Cumple la legislación aplicable:

LOPD, LSSICE, Firma digital…

Soporte de sistemas:

Backups, hostings, servidores, control de accesos, gestión de contraseñas, página web intranet/extranet…

Conoce las normas de calidad y los códigos de buenas prácticas:

ISOs, UNEs, NIST…

Soporte de red:

Salidas a Internet, accesos remotos, VLANs, proveedores, comunicaciones…

SGSI

Experto tecnólogo:

Experto en compras de PCs, impresoras, portátiles, móviles, GPSs y todo tipo de juguetes tecnológicos que van apareciendo

Apoyo a desarrollo y diseñadores:

Programación de tareas, scripts, parcheo de aplicaciones, administrador de BBDD

Técnico multiusos:

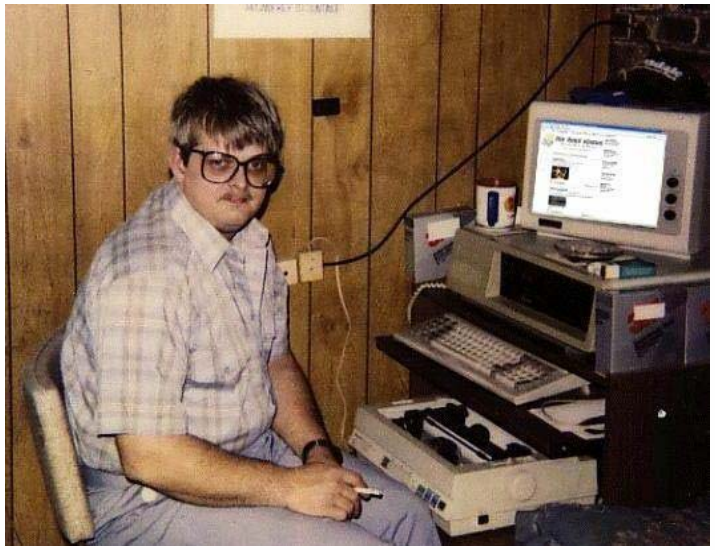
Linux, Unix, win32, Mac,XML, HTML, PHP, SQL, Perl, python, todo tipo de acrónimos…

Formador técnico:

Con capacidad de ser formado y formar en cualquier tecnología en cuestión de horas

Experto en seguridad:

Capacidad para combatir, spam, malware, gestionar VPNs, firewalls…



!=

Solución: Externalizar

- Nueva especie, expertos en seguridad informática
  - Auditores externos
- Existen varias formas de externalizar la **gestión de la seguridad:**

In-tasking

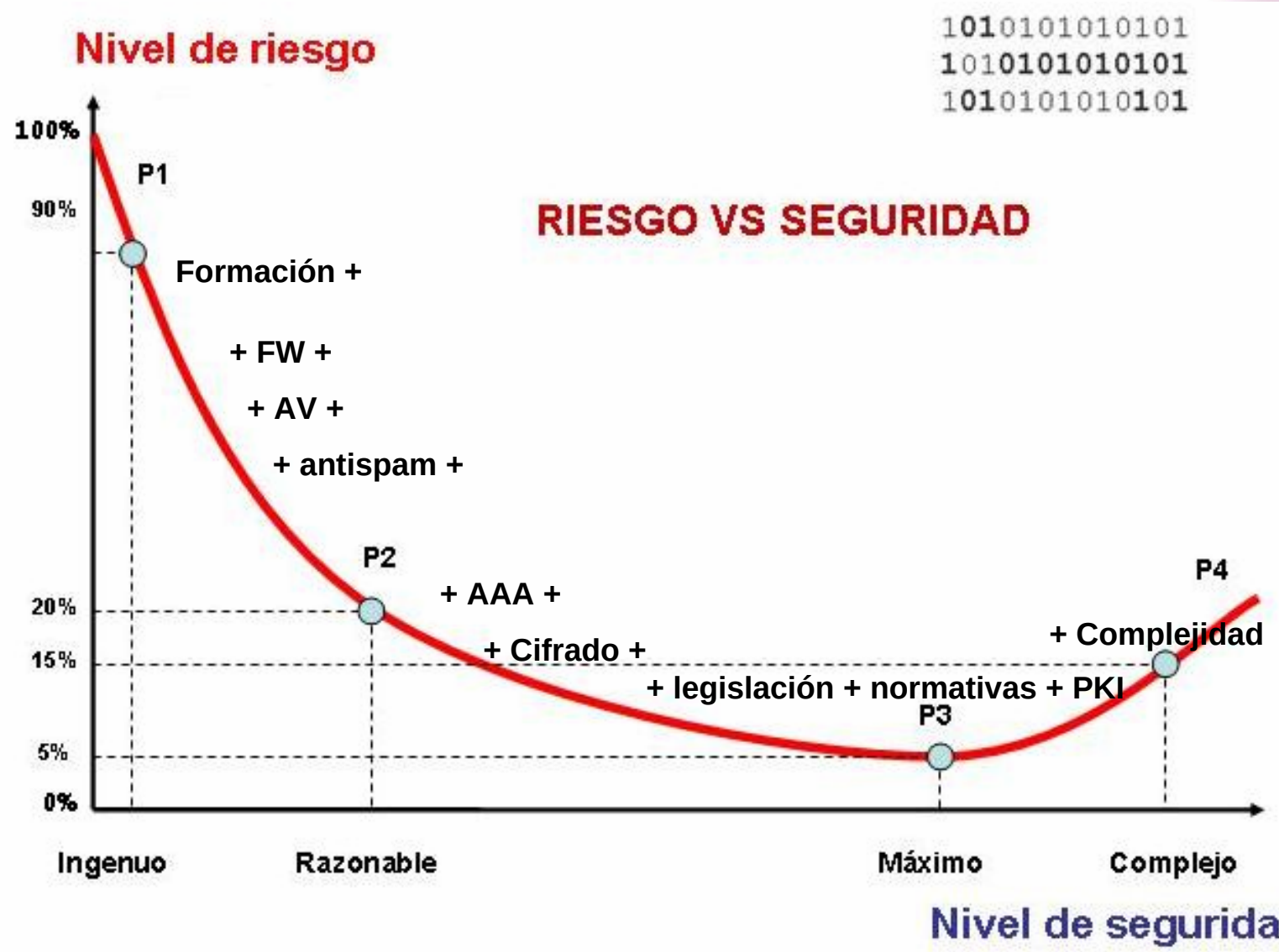
Out-tasking

Out-sourcing

Tendencias de la seguridad en las TIC

3. La seguridad hay que entenderla como una costumbre en la que intervienen, personas y tecnología y **se gestiona el riesgo de forma razonable**.

   Los "productos" de seguridad han demostrado no ser suficientes, no basta con tener el firewall GT+V5+iS9rc9



Objetivo de la seguridad

- La seguridad pretende garantizar la **confidencialidad**, **autenticidad**, **integridad**, **no repudio** de las comunicaciones, y el **control de acceso** y la **disponibilidad** de la información.

- En los últimos años se han vendido muchos "***productos"*** de seguridad pero esto está cambiando

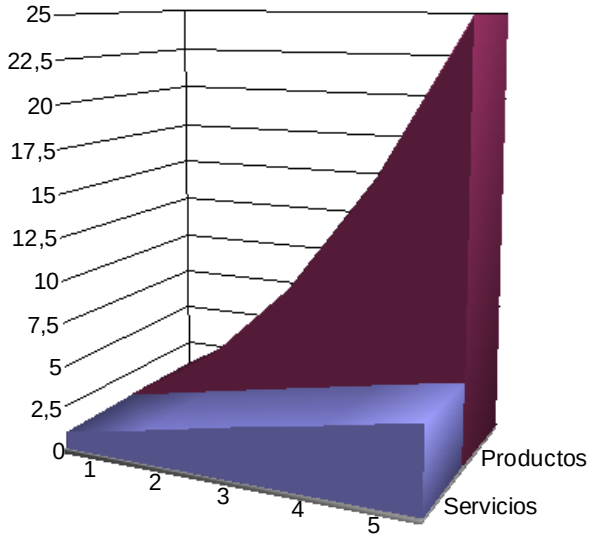
Producto vs Servicio

- Producto (similar a un “bien”): en contabilidad es un producto físico factible de ser entregado a un comprador e involucra la transferencia de propiedad del vendedor hacia el comprador.

- Servicio: es lo no-material equivalente a producto. La provisión de servicios es una actividad económica que no tiene consecuencias de propiedad.

¿Por qué se intenta vender como producto?

- "Economías de gran escala"
  - La relación de beneficios sobre los costes crece exponencialmente
  - Si además el coste marginal es cero los beneficios son aún mayores
- Los servicios escalan linealmente
  - La capacidad de comercialización es linealmente proporcional a los recursos humanos

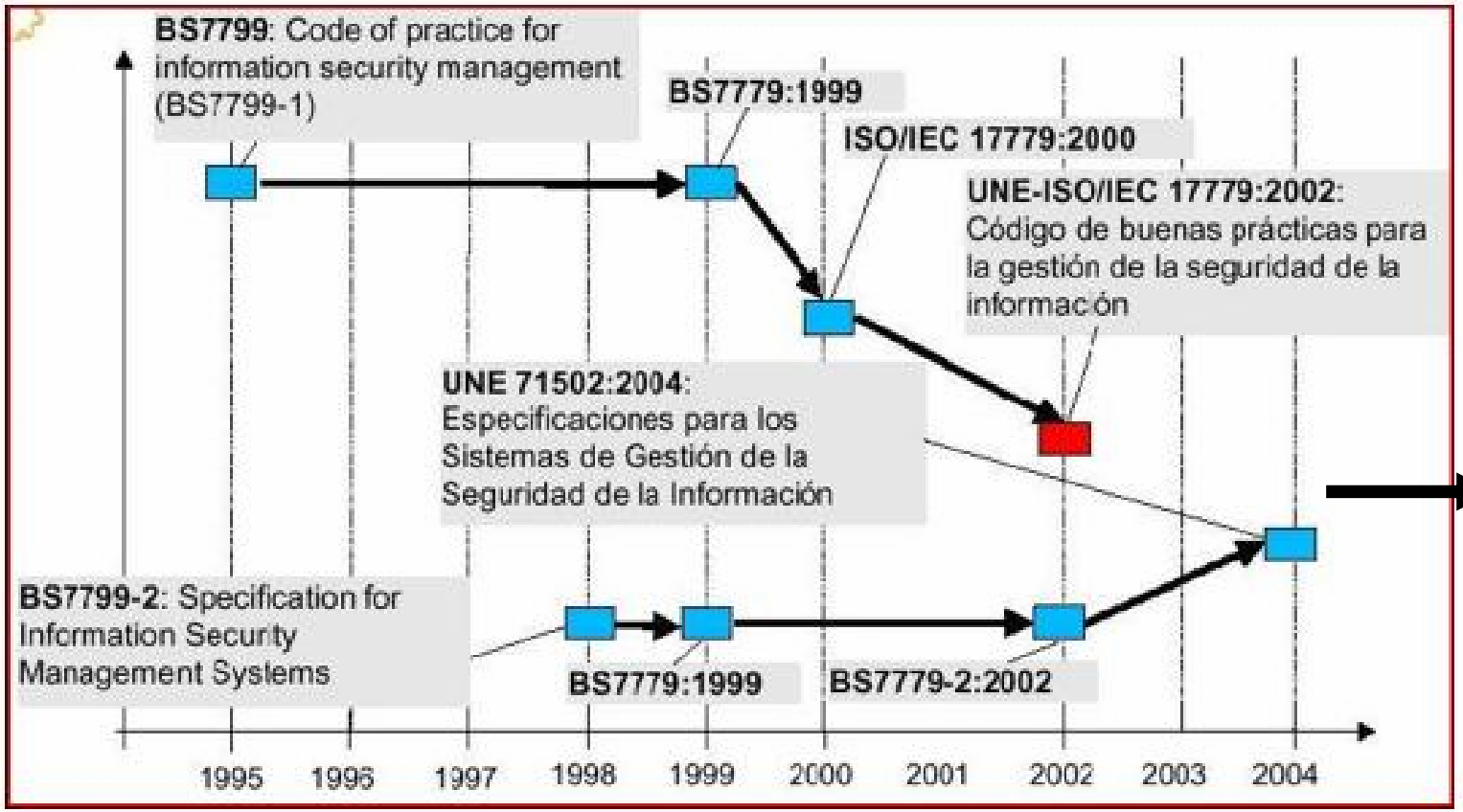


Mercado establecido alrededor del producto

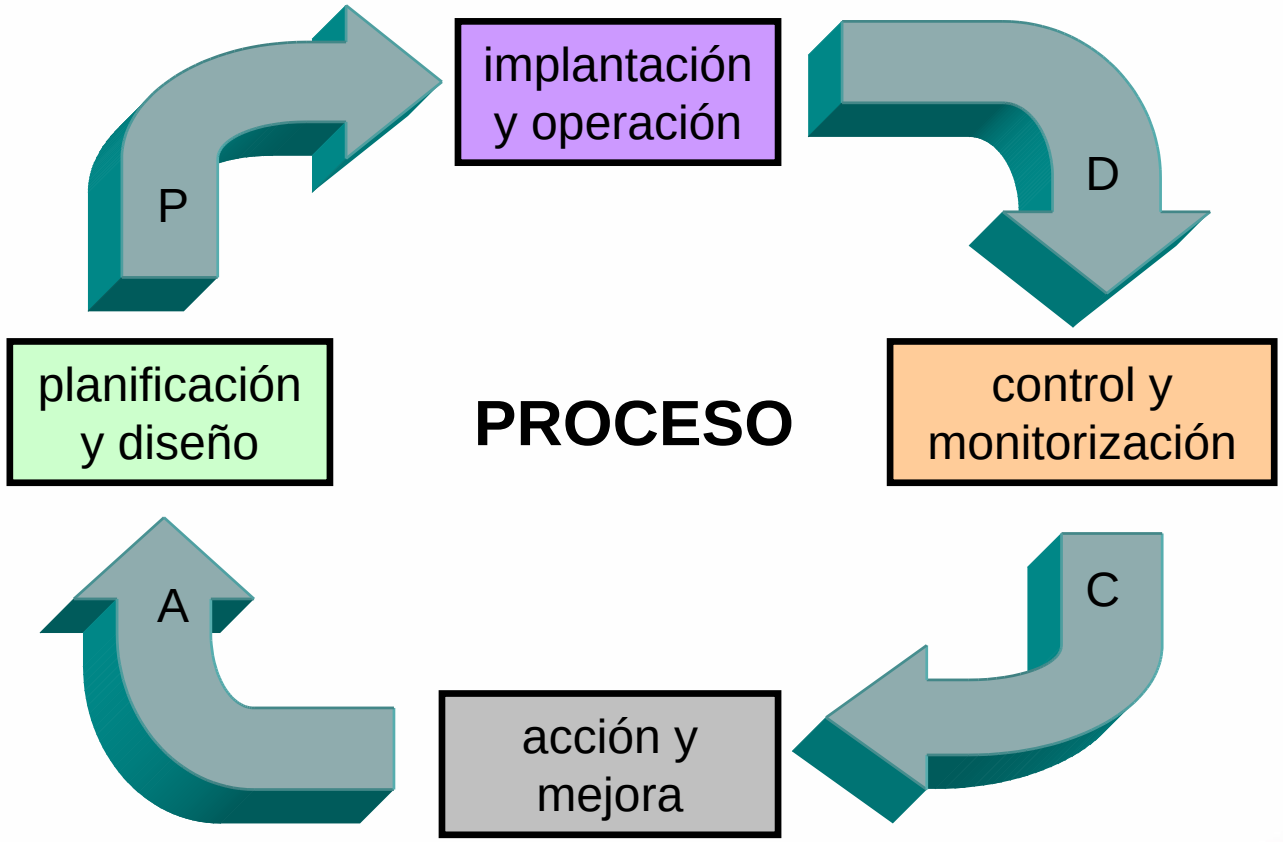
- Empresas que han vendido producto
  - Cisco, Microsoft, Oracle, Sun, IBM…
- Facilidad para el mercadeo:
  - Comerciales vendiendo licencias
  - Facilidad de implantación
  - Mercado cerrado a nuevas empresas (si no pasan por el aro del *partner*-ismo)
- Oportunidad del Sofware Libre – Venta de servicio!!
  - Se iguala la competencia, **prima la profesionalidad**

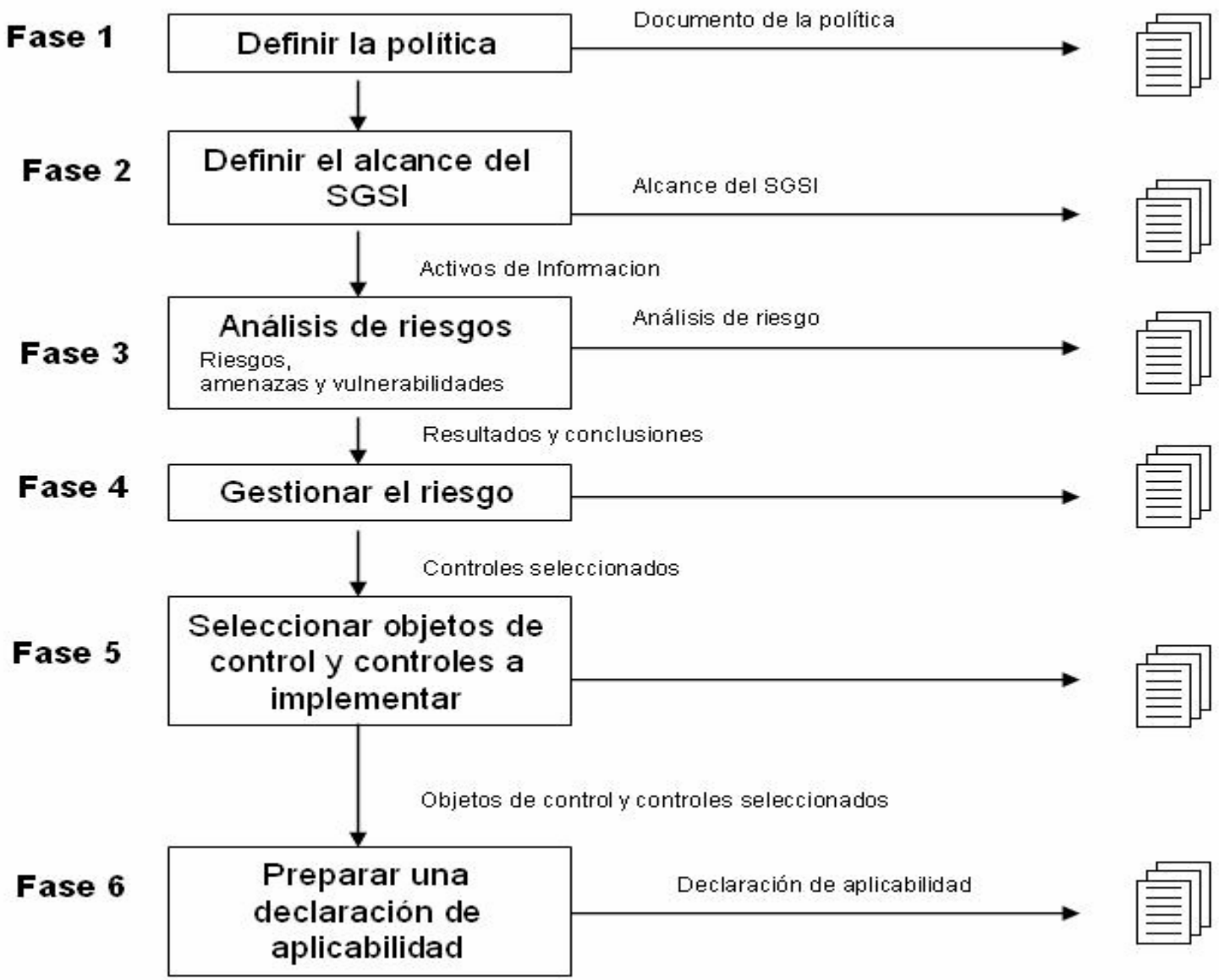
S.G.S.I.

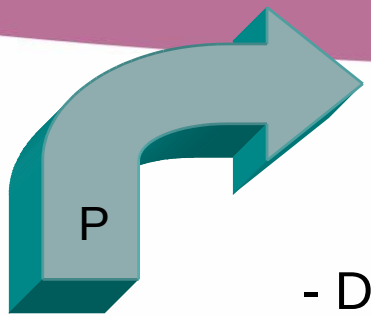
Sistema de **G**estión de la **S**eguridad de la **I**nformación



SGSI (**S**istema de **G**estión de la **S**eguridad de la **I**nformación)



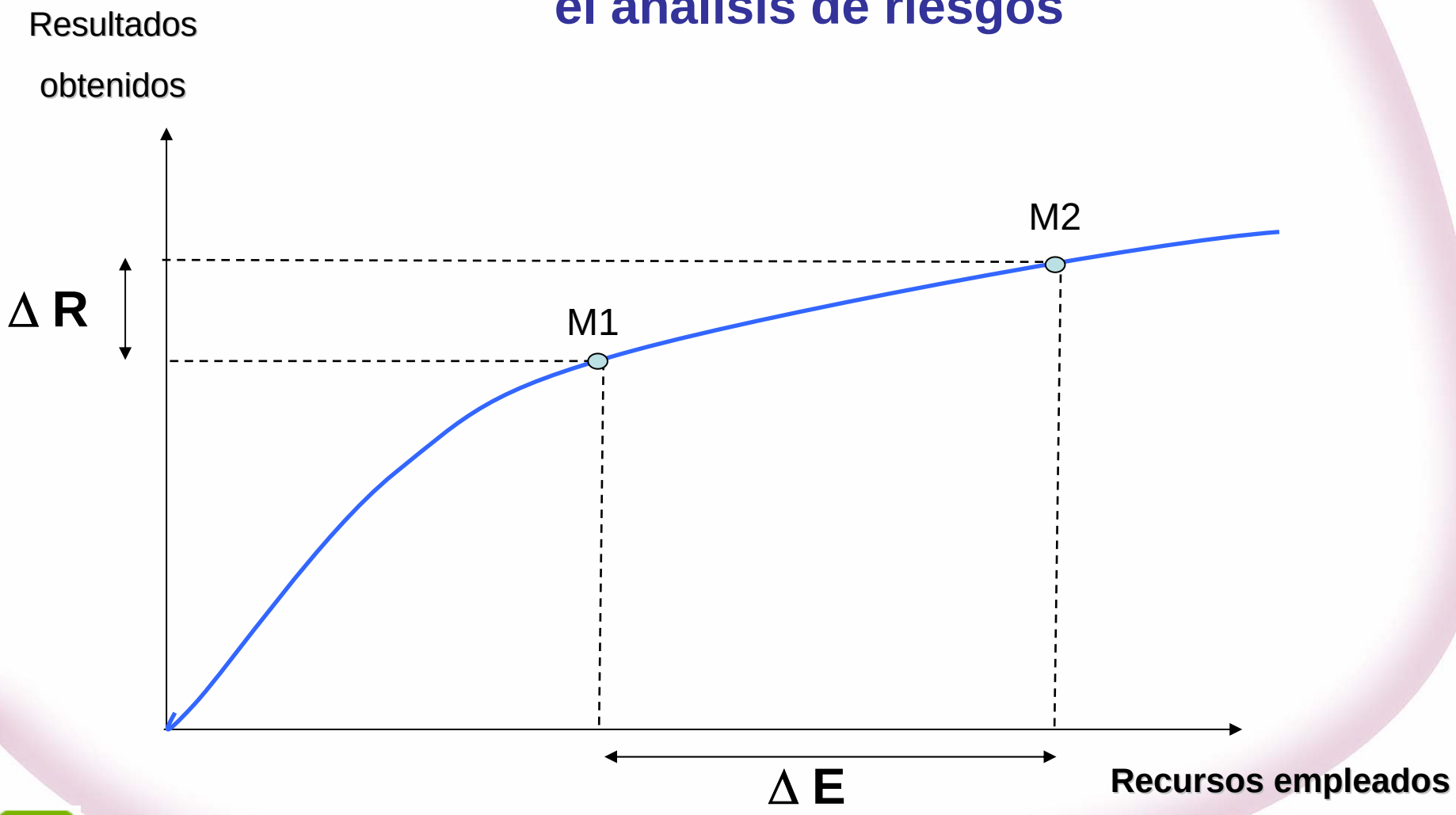




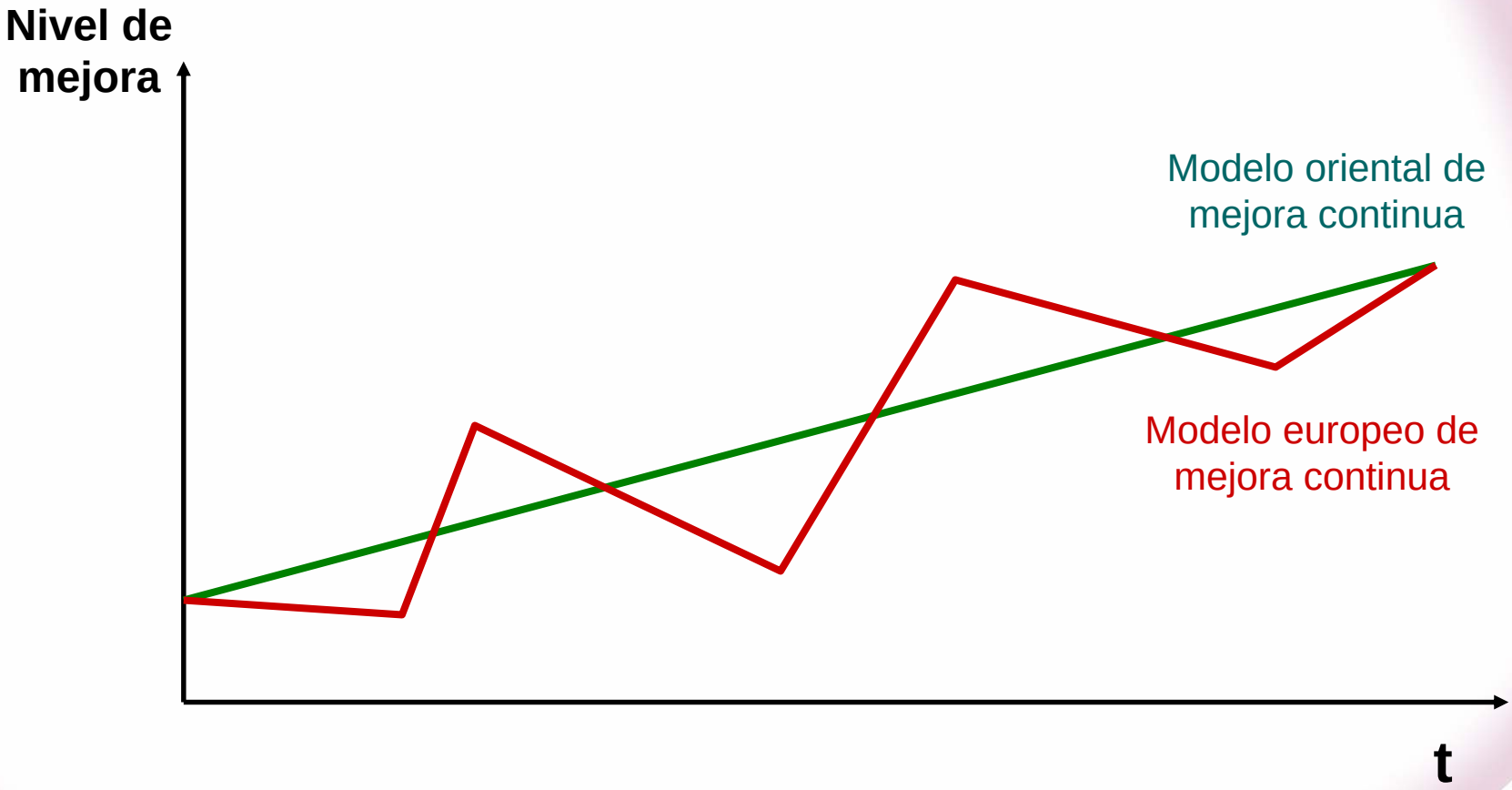
planificación y diseño

- Determinar el alcance del SGSI y el grado de compromiso
- Realizar un inventario de activos
- Clasificar los activos de información
- Realizar un análisis de riesgos identificando amenazas y vulnerabilidades
- Definir responsables y responsabilidades
- Tener en cuenta la legislación vigente
- Planificar reuniones periódicas y formación
- Utilizar como guías los códigos de buenas prácticas y normas ya existentes (ISO 17799, UNE 71502)

Análisis de las metodologías empleadas en el análisis de riesgos



Modelo europeo VS modelo oriental



- **Modelo europeo**

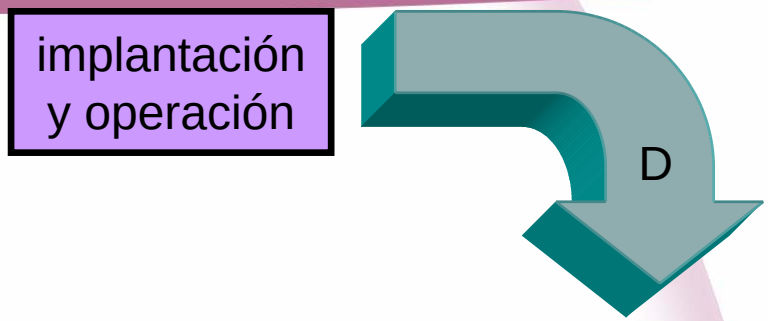
  Grandes saltos de mejora a base de grandes esfuerzos en el tiempo, mejora base de picos con inyección de recursos

- **Modelo oriental**

  Pequeños cambios continuos en el tiempo con pocos recursos pero de forma constante

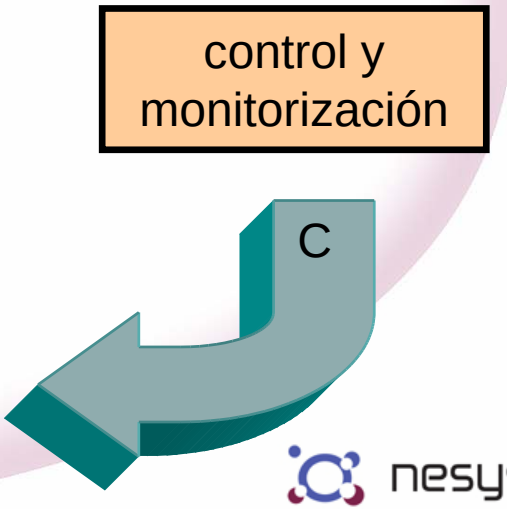
  Por el tipo de problemática que presenta la seguridad en las tecnologías de la información el modelo oriental encaja mejor como modelo de mejora ya que se optimizan las energías y recursos con menores esfuerzos.

Ej. Monitorización de sistemas de información 24x7 y pequeños ajustes corrigiendo los problemas que van surgiendo



- Gestionar el riesgo
- Procedimientos de respuesta a incidentes
- Formación y valoración de RRHH
- Planes de contingencia y continuidad de negocio
- Control de accesos y privilegios
- Homologación de aplicaciones
- Aplicación de medidas de seguridad

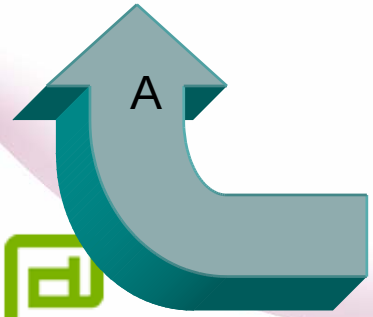
- Logear y dejar trazas en los sistemas
- Revisar y controlar las trazas
- Generar eventos de control y alerta sin falsos positivos
- Planificar auditorías periódicas internas y externas
- Evaluar el nivel de riesgo residual asumido
- Detectar acciones preventivas y correctivas



- Corregir desviaciones detectadas en procedimientos, responsabilidades, responsables, medidas de seguridad, controles y demás elementos del SGSI

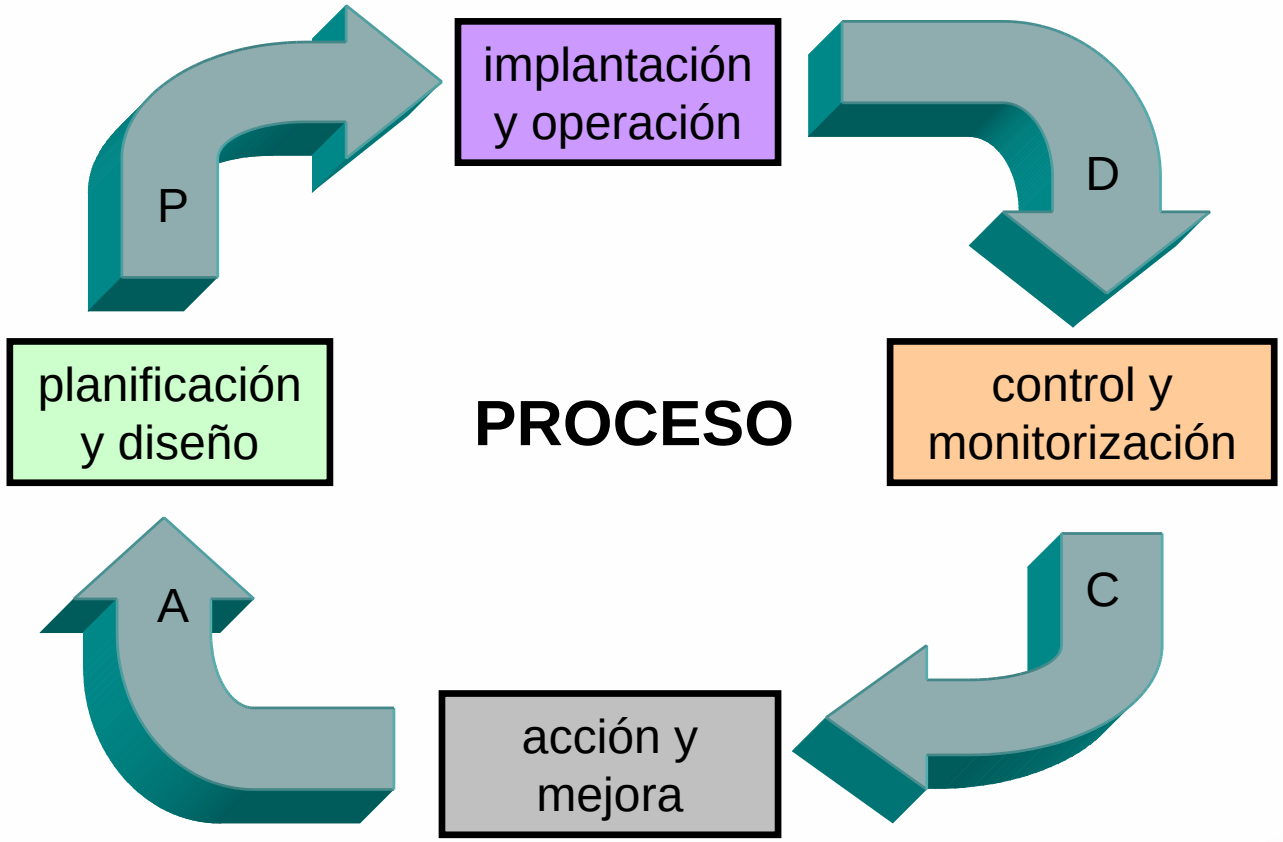
- Cada vez que se pasa por este punto se debe poder apreciar la mejora obtenida con respecto a etapas anteriores y la madurez del SGSI

- Consultar a profesionales expertos en la materia

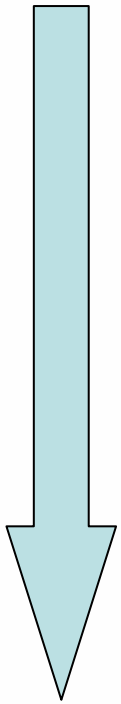


acción y mejora

SGSI (**S**istema de **G**estión de la **S**eguridad de la **I**nformación)



Evolución de los sistemas de gestión



Sistemas Propietarios

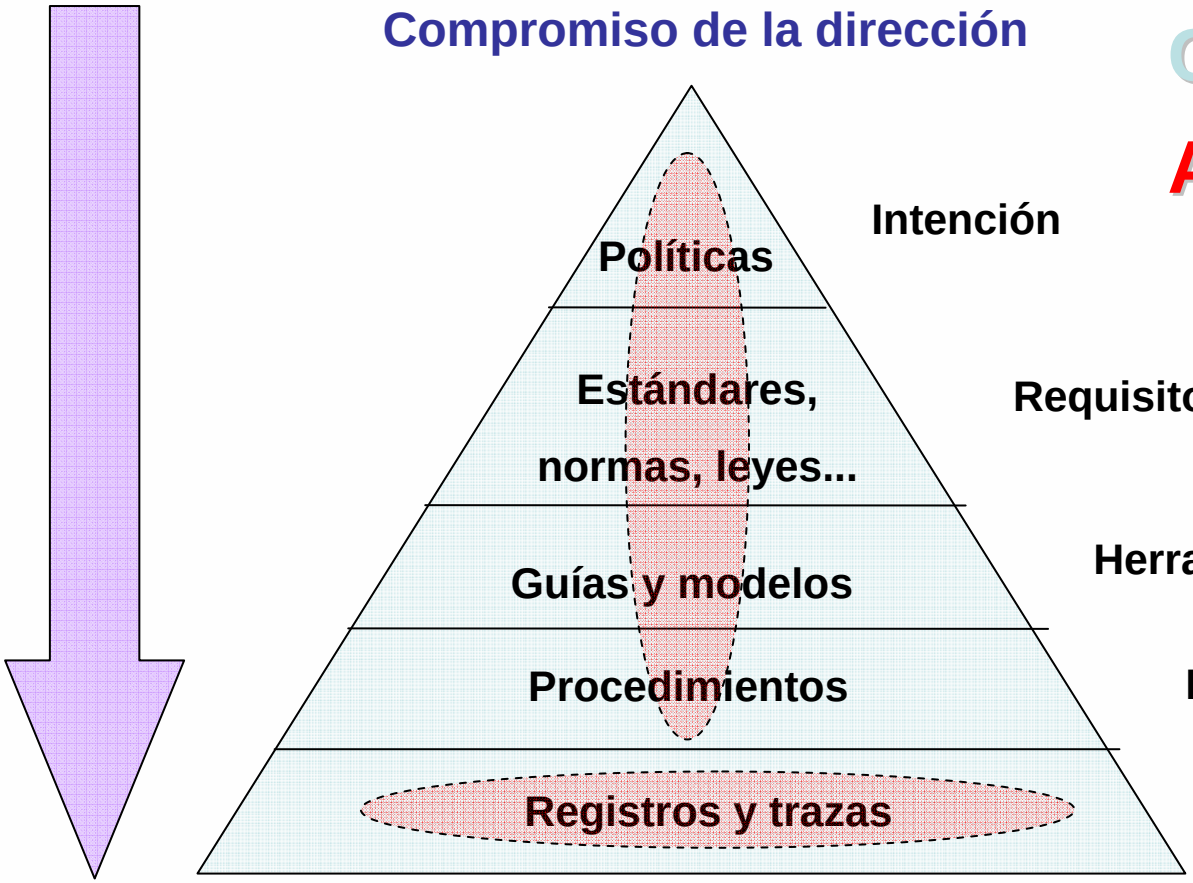
- Sistemas únicos y personalizados

Sistemas "normalizados"

- Sistemas que tienen en cuenta ciertas normas y que se orientan a estándares

Sistemas certificados

- Sistemas auditados y certificados que se rigen por estándares aprobados y reconocidos



Intención

Requisitos

Herramientas y técnicas

Metodología

Evidencias

Consultoría

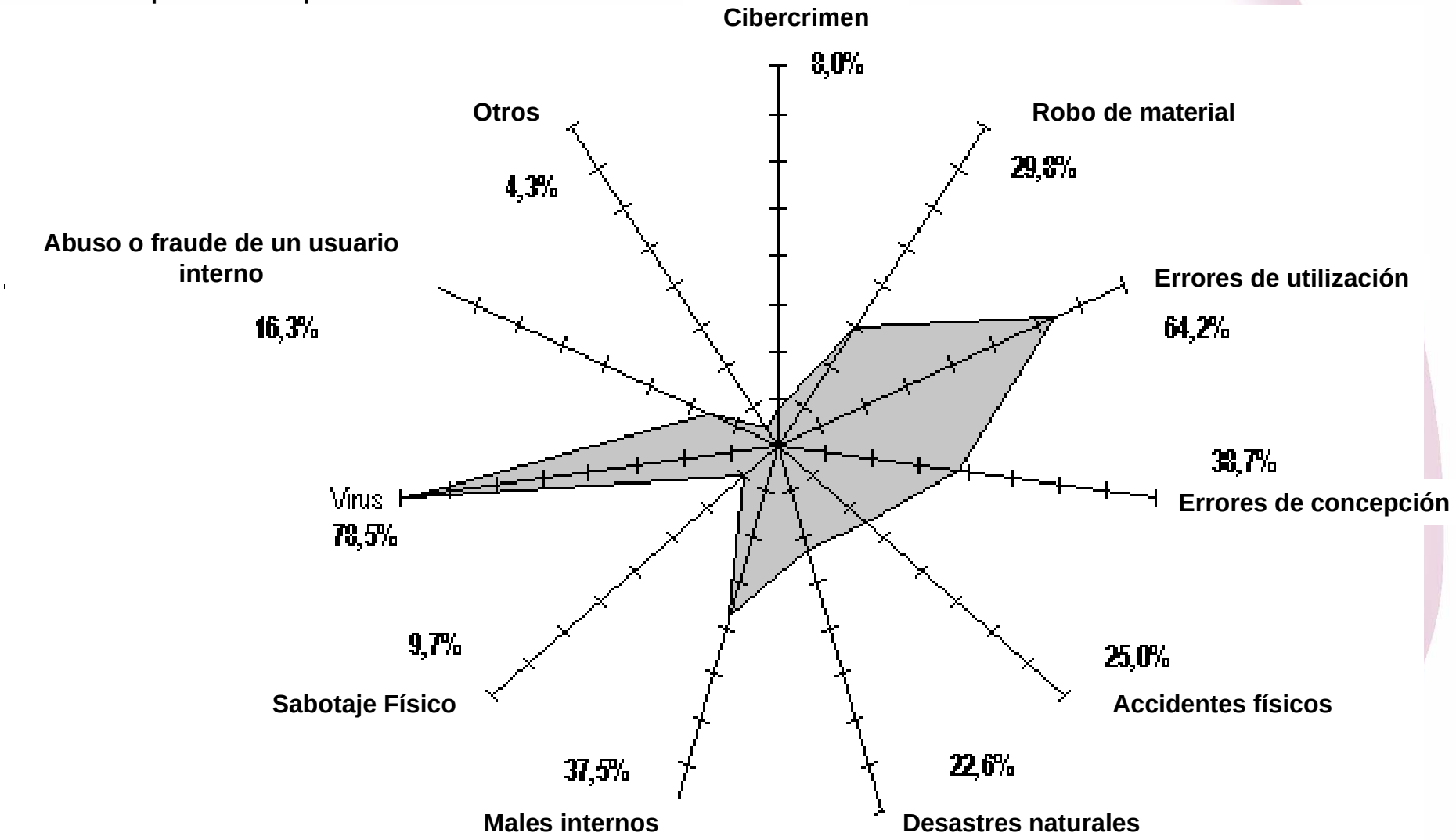
Auditoría

Agenda

10:30 Tipos de amenazas, perfiles de ataque y niveles de riesgo

¿ Quién o qué es la amenaza ?

Estadística publicada por IDC/EDS



Clasificación del universo hacker

Spammer

Persona que roba o compra direcciones de correo electrónico sustraídas y remite e-mails no solicitados

Exploiter

Son personas que aprovechan un error en la programación de un programa para obtener diversos privilegios sobre el software

Guru

Son los expertos en algún área, entiéndase por experto conocer "TODO". Encargados de formar a futuros hackers

CopyHackers

Falsificadores que comercializan todo lo copiado

Clasificación del universo hacker

Bucaneros
Personas con escaso conocimiento informático que se dedican a la venta de productos comprados a los copyhackers

Newbie
Son los novatos del hacker

Wannaber
Newbie que desea ser hacker pero estos consideran que su nivel no da para tal fin (Wannaber= wanna be =quiero ser)

Samurai
Son los llamados "hackers a sueldo" trabajan solos y saben que todo puede ser tumbado si se tiene dinero suficiente para pagarlo

Clasificación del universo hacker

Creador de virus

Aquí se ha de diferenciar entre el programador del virus y el propagador, sienten un gran placer al ver que su "software" ha sido ampliamente "adquirido" por el publico

Cracker

Proviene del termino "*Criminal hacker*", es aquel que viola la seguridad de un sistema informático, con la diferencia de que lo hace con fines de beneficio personal. También es así llamado a quien diseña cracks informáticos para modificar el comportamiento del software o hardware original sin que pueda ser dañino para el usuario del mismo

Clasificación del universo hacker

Lamer
Proviene del ingles "incompetente", "falto de inteligencia", personas con una boca mas grande que sus habilidades. Suelen ser personas que alardean de ser hackers cuando en realidad utilizan programas de fácil manejo creado por los auténticos hackers sin obtener los resultados que ellos pretendían.

Script kiddie
Es aquella persona que presume de hacker o cracker cuando en realidad no posee un grado de conocimientos suficientes. Se podría decir que es la siguiente fase del lamer.

Phreaker
Es una persona que mediante el uso de la tecnología es capaz de interferir en los sistemas telefónicos de forma ilegal

Clasificación del universo hacker

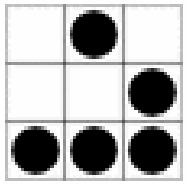
Geek
Es una persona que comparte una fascinación obsesiva por la tecnología y la imaginación. Se trata de una persona extravagante y extrovertida, tanto en el estilo de vida como en la forma de ser, que hace las cosas por el reconocimiento y la diversión.

Nerd
Es una persona con gran inteligencia y pasión con el conocimiento que tiende a apartarse de la corriente social. Menos extravagante que un *Geek*

Hacker

Hacker (del inglés hack, recortar) es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.

Su entendimiento es más sofisticado y profundo respecto a los sistemas informáticos, ya sea de tipo hardware o software. Se suele llamar hackeo y hackear a las obras propias de un hacker.



Una persona inteligente que tiene una curiosidad natural, le gusta aprender como funcionan las cosas, y le interesa conocer técnicas de evasión o abusar de procesos para ver qué sucede.

Hacker

El término "Hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

En palabras de Richard Stallman,

"Hacker, quiere decir divertirse con el ingenio [cleverness], usar la inteligencia para hacer algo difícil. No implica trabajar sólo ni con otros necesariamente. Es posible en cualquier proyecto. No implica tampoco hacerlo con computadoras. Es posible ser un hacker de las bicicletas. Por ejemplo, una fiesta sorpresa tiene el espíritu del hack, usa el ingenio para sorprender al homenajeado, no para molestarle"

Hacker

Para entender la mentalidad de un hacker hay que conocer sus motivaciones. Los resultados de una encuesta realizada dentro de varias comunidades de hackers dejó claro que por lo general los principales factores de motivación suelen ser:

1. La curiosidad y el reto intelectual
2. Diversión y entretenimiento
3. Convicciones políticas y/o religiosas
4. Deseo de obtener información y conocimiento
5. Control y dominio sobre redes y sistemas
6. Reconocimiento en la escena y notoriedad
7. Ánimo de lucro
8. Causar caos y destrucción
9. Otros

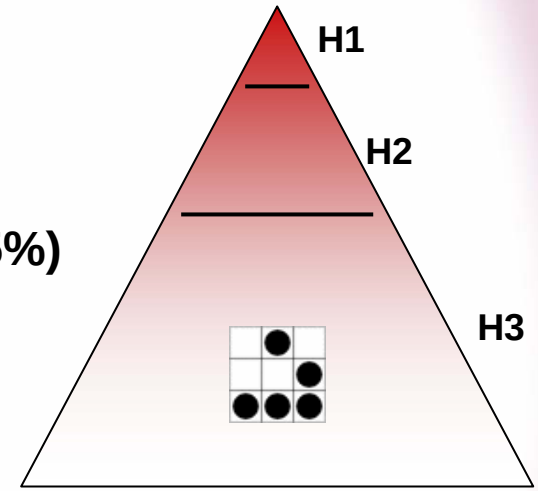
Perfiles

Dentro del amplio espectro del universo "hacker" establecemos tres grupos :

H1. Maestros y gurús (2%)
- Capaces de descubrir y explotar vulnerabilidades, programar exploits y desarrollar herramientas.

H2. Profesionales y fanáticos de las tecnologías (15%)
- Capaces de programar y escribir scripts, conocen la tecnología y son capaces de utilizarlas con precisión

H3. Aficionados y script kiddies (83%)
- Inexpertos, capaces de bajarse y ejecutar los últimos exploits y herramientas sin entender la tecnología, suelen ejecutar y probar hasta que algo funciona, el método click & forget es muy utilizado en sus ataques y se centran en blancos fáciles y probabilísticos



Vulnerabilidades

Vulnerabilidades

- Def: Wikipedia
  - Debilidad en un sistema que permite a un atacante violar la integridad, confidencialidad, control de acceso, disponibilidad o consistencia en un sistema o datos y aplicaciones que aloja
  - Errores en la programación o configuración
- Tipos de vulnerabilidades:
  - De protocolo: Múltiples fabricantes/desarrolladores implicados
  - De aplicación: De una aplicación o del sistema operativo. Normalmente un solo fabricante/desarrollador implicado

Búsqueda de vuln.

- La realizan tres grandes grupos:
  - Empresas de seguridad: Tienen productos relacionados con la seguridad
    - ISS → http://www.**iss**.net
    - eEye → http://www.**eeye**.com/
  - Empresas de programación: La propia evolución y mejora de sus productos
  - **La "comunidad":** Investigadores independientes y programadores libres, los propios usuarios, etc…

Solución, parches

- Soluciones propias
  - Antes del parche oficial
  - Quitar exposición (filtrar puertos, apagar servicios…)
- Solución del fabricante/desarrollador
  - Parcheo de la aplicación y corrección de la vulnerabilidad
  - A veces el parche trae una nueva (¡¡o vieja!!) vulnerabilidad

Exploits

- Herramientas que aprovechan las mencionadas vulnerabilidades para atacar sistemas
- A partir de ser conocida la vulnerabilidad
- ¡¡Pueden salir antes o después que el parche!!

Publicación de parches

- Mecanismo
  - Archivo binario que corrige otros archivos
  - Nueva versión
  - Patch de los fuentes
  - Nuevos fuentes
- Según fabricante/desarrollador:
  - Comunidad OS: Según se publican, se empieza a trabajar, sistema de actualizaciones
  - Empresas privativas: MS, Adobe….
    - Ej: Segundo martes de cada mes, ¡¡no depende de cuándo se descubren!!

Ejemplo

- Microsoft Windows WMF "SETABORTPROC" Arbitrary Code Execution
  - Secunia Advisory:SA18255
  - Release Date:2005-12-28
  - Last Update:2006-02-28
- http://secunia.com/advisories/18255/
  - Explotable mediante la apertura de un archivo .wmf trucado

SW LIBRE vs PRIVATIVO

- http://www.kriptopolis.org/node/2034
- Análisis a 32 proyectos de SW libre
- Índice de fallos por línea de código:
  - *Software libre: 0.434 errores por cada 1,000 líneas de código*
  - *Privativo: de 20 a 30 errores por cada 1,000 líneas de código*
- Los errores se corrigen antes en el Software Libre que en el privativo

Lugares de publicación

- Diferentes *bugtracks* en Internet
  - Infosyssec
  - CERT
  - SANS
  - PacketStorm etc…
  - Secunia
- Listas de correo de diferentes productos

Métodos de publicación

- Cómo difundir el hallazgo:
  - Full disclosure process: Publicación abierta en listas dedicadas a la seguridad
  - Responsible disclosure: Establecido por la industria y los fabricantes…
    - Supone la cooperación entre investigadores y fabricantes.
    - Puede considerarse el método “correcto” (para no tener “guerras”)

Full-Disclosure

- Puede ser bueno, ya que se extiende rápidamente por la comunidad de seguridad. Pero también la comunidad underground – blackhat
- Puede ser la mejor manera de que los fabricantes tomen conciencia ya que provoca la creación de exploits más rapidamente
- La no colaboración con fabricantes puede llevar a que los fabricantes no den crédito a los descubridores

Responsible-Disclosure

- Ponerse en contacto con el fabricante y comunicarle la vulnerabilidad
- Mantenerla confidencial hasta que se publique el parche → Acordar una fecha de publicación
- El fabricante gratificará con reconocimiento al descubridor
- ¿¿Todos contentos??

Responsible-Disclosure

- Y si hay más de un fabricante?? Como acordar la fecha de publicación??
  - Los que no tengan parche, o lo tengan pronto resuelto querrán prontitud (fama). El resto lentitud
- Temas de patentes: En La comunicación con un fabricante → Puede patentar las contramedidas!! Cómo demostrar la autoría del descubrimiento??
  - Ej: Cisco “Ataques ICMP contra TCP” con una información semi-pública (Internet Draft del IETF)
- Utilización del crédito como elemento de negociación por parte de fabricantes

Ejemplo

- ISS con Michael Lynn → Disclosure de vulnerabilidades IOS Cisco
  - 3 meses antes Cisco había sido avisada
  - Cisco y ISS boicotearon su presentación y amenazaron con denuncias a los sitios que lo publicaron
  - En la Black Hat de Las Vegas 2005 arrancaron las páginas de su presentación de la documentación a entregar a los asistentes
- http://jopi.seriousworks.net/files/cisco.mov
- http://jopi.seriousworks.net/files/Cisco_Lynn_blackhat_presentation.pdf

Ciclo de vida de una vulnerabilidad

Cada vez que aparece una nueva vulnerabilidad el ciclo se repite y se crea una ventana abierta al riesgo.

Se trata de hacer dicha ventana lo más “cerrada” posible

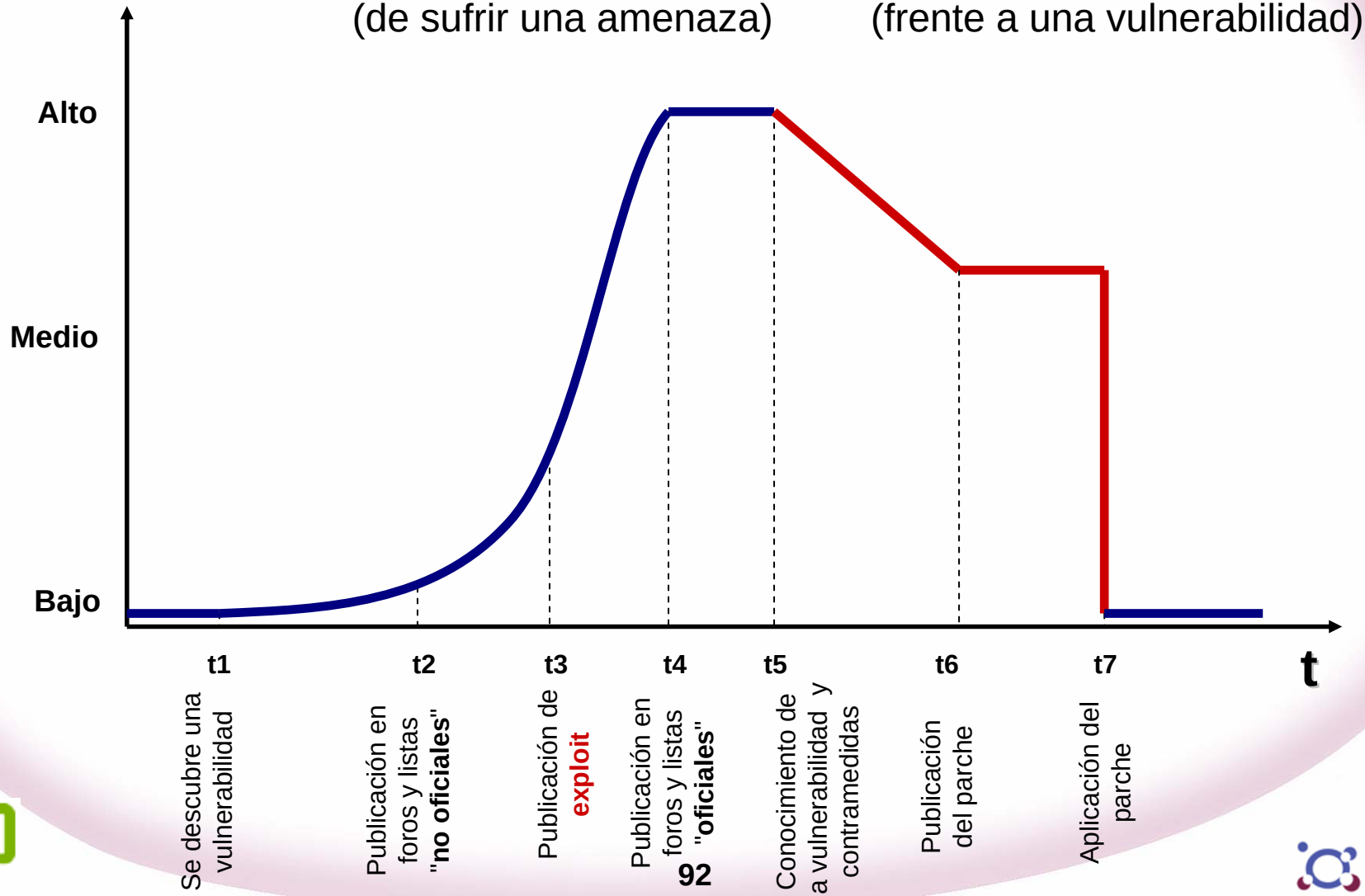
Pueden cambiar los tiempos el escenario y los personajes pero el patrón se repite en el tiempo

… aunque hay variantes

Ciclo V

Nivel de riesgo = probabilidad X exposición

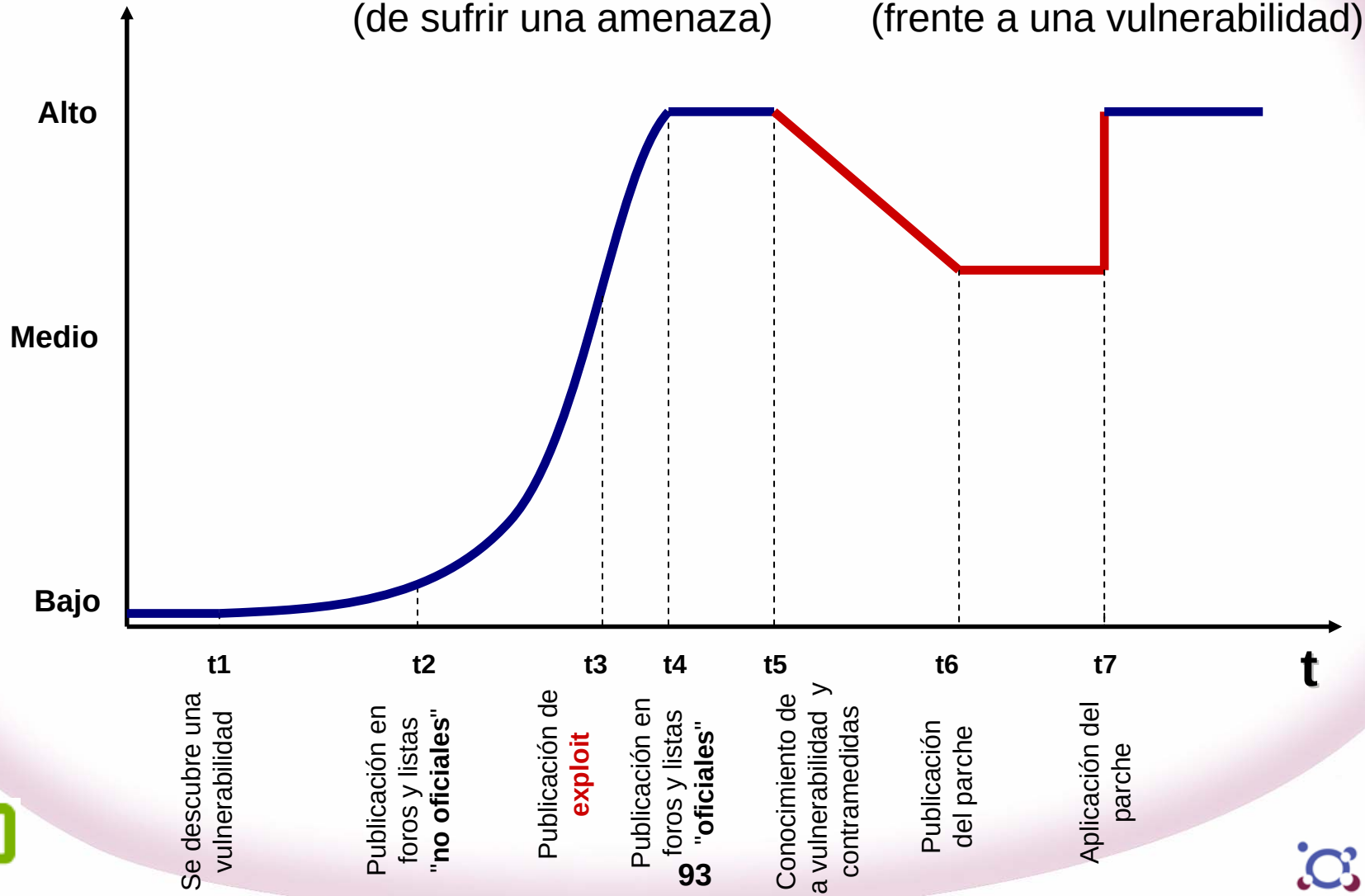
(de sufrir una amenaza) (frente a una vulnerabilidad)



Variante "parche inadecuado"

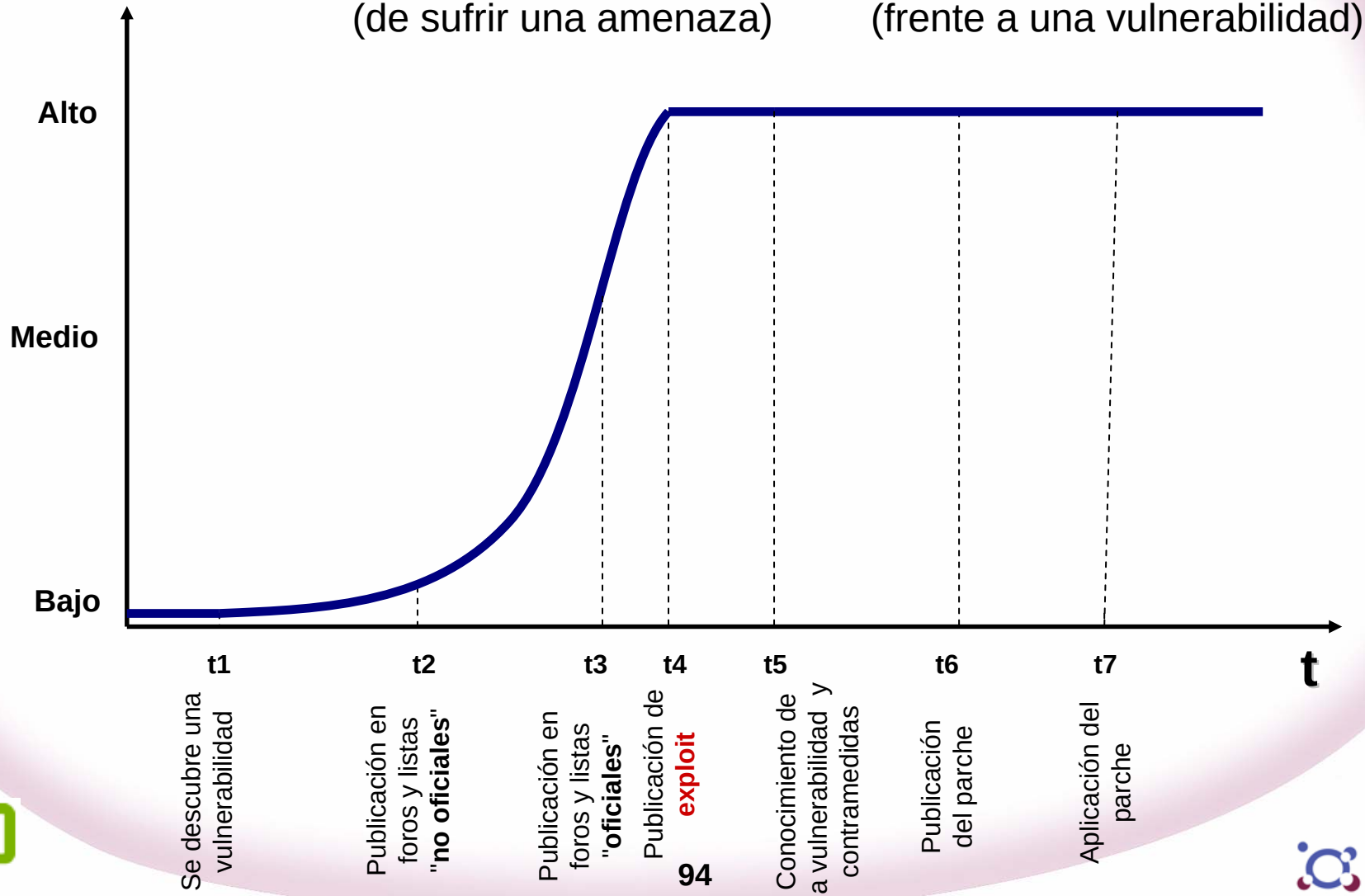
Nivel de riesgo = probabilidad X exposición

(de sufrir una amenaza) (frente a una vulnerabilidad)



Variante "¿qué es una vulnerabilidad?"

Nivel de riesgo = **probabilidad** (de sufrir una amenaza) **X** **exposición** (frente a una vulnerabilidad)



Desconocimiento

El desconocimiento y la negación del problema suelen ser las principales causas que intervienen en los incidentes de seguridad

Para evitar los problemas de seguridad lo primero que hay que tener es ***conocimiento***, ***motivación*** y ***recursos*** para solucionarlos.

¿Quién es la victima?

Individuos: virus, troyanos, phising…

Empresas e Instituciones: virus, troyanos, intrusiones…

Todos podemos ser el blanco de un ataque (no hay grandes ni pequeños)

¿Puedo ser yo una víctima?

Todos podemos ser el blanco de un ataque (no hay grandes ni pequeños)

La estadística es favorable al hacker (el tiempo y el número)

El navegador es hoy por hoy la herramienta de ataque más utilizada

Los mega-productos de seguridad no son la panacea

Citas…

"La seguridad es un viaje no un destino" (Hacking exposed)

"La seguridad es un proceso no un producto" (Bruce Schneier)

"Hay que entender la seguridad como una forma de hacer las cosas" (Dpto. Calidad)

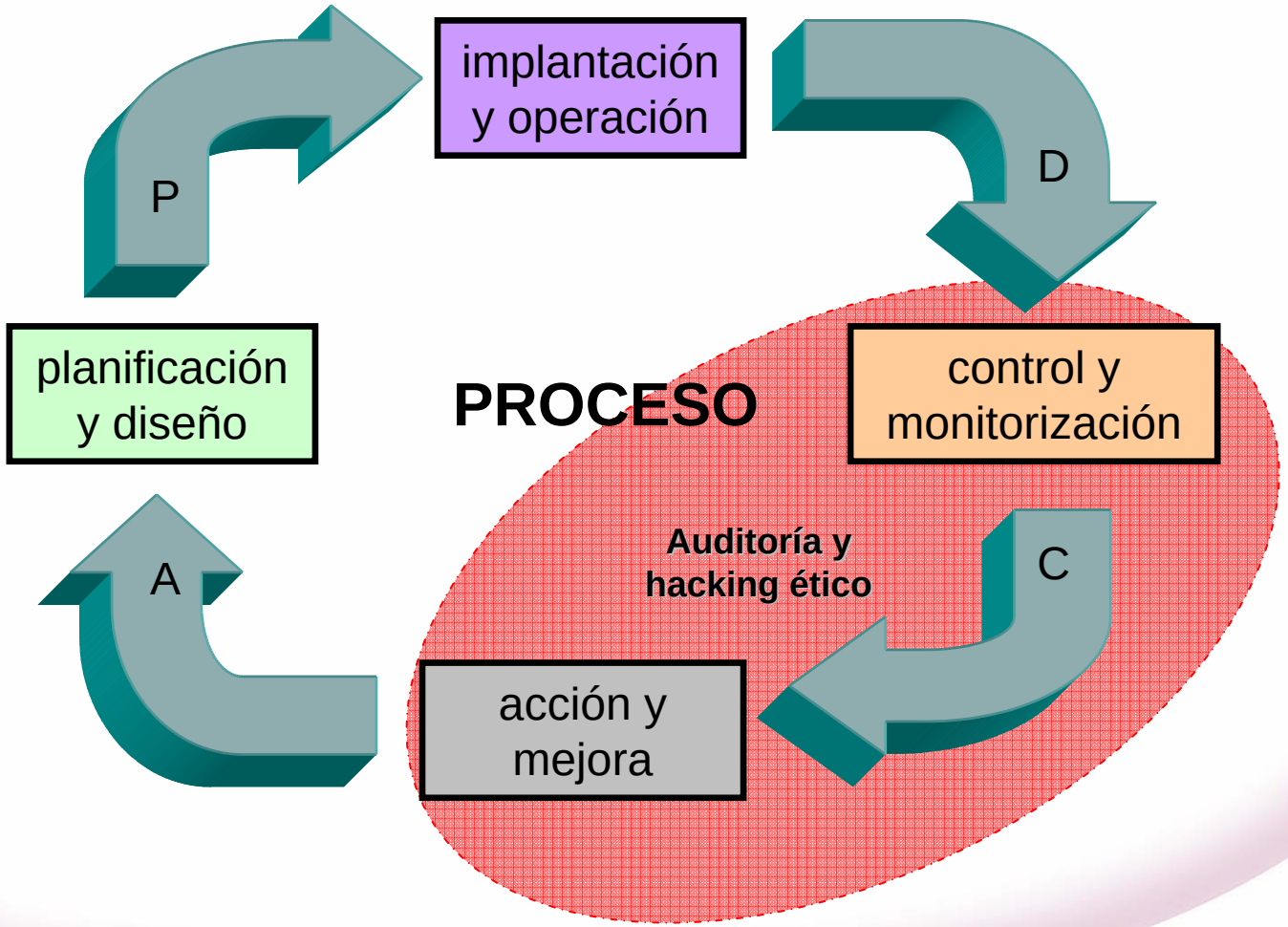
Agenda

11:30 **Descanso, café**

Agenda

12:00 El hacking ético de redes y sistemas dentro de los procesos de mejora continua de las empresas

SGSI (**S**istema de **G**estión de la **S**eguridad de la **I**nformación)



Cómo ser proactivo

- Profesionales de la seguridad: **hacking ético**
  - Procesos para detectar vulnerabilidades e identificar riesgos tomando la perspectiva de un atacante → ayudará a definir medidas de prevención
- Requerirán: entrevistas, revisión de políticas, inspecciones técnicas y físicas
- Uso de herramientas específicas

Hacking ético

- Confidencialidad, discreción y claridad
- Asesoramiento imparcial
- Previas consideraciones legales.
  - **Permiso explícito**
  - Con repercusiones en caso de desastre
  - Debe presentar el plan **detallado** a priori
    - Métodos y herramientas a usar
  - Respeto a los derechos sobre los datos a tratar
- A veces, sin avisar a responsables de sistemas
  - Con la autorización correspondiente
    - ¿Responsable de seguridad?
    - ¿Dirección?

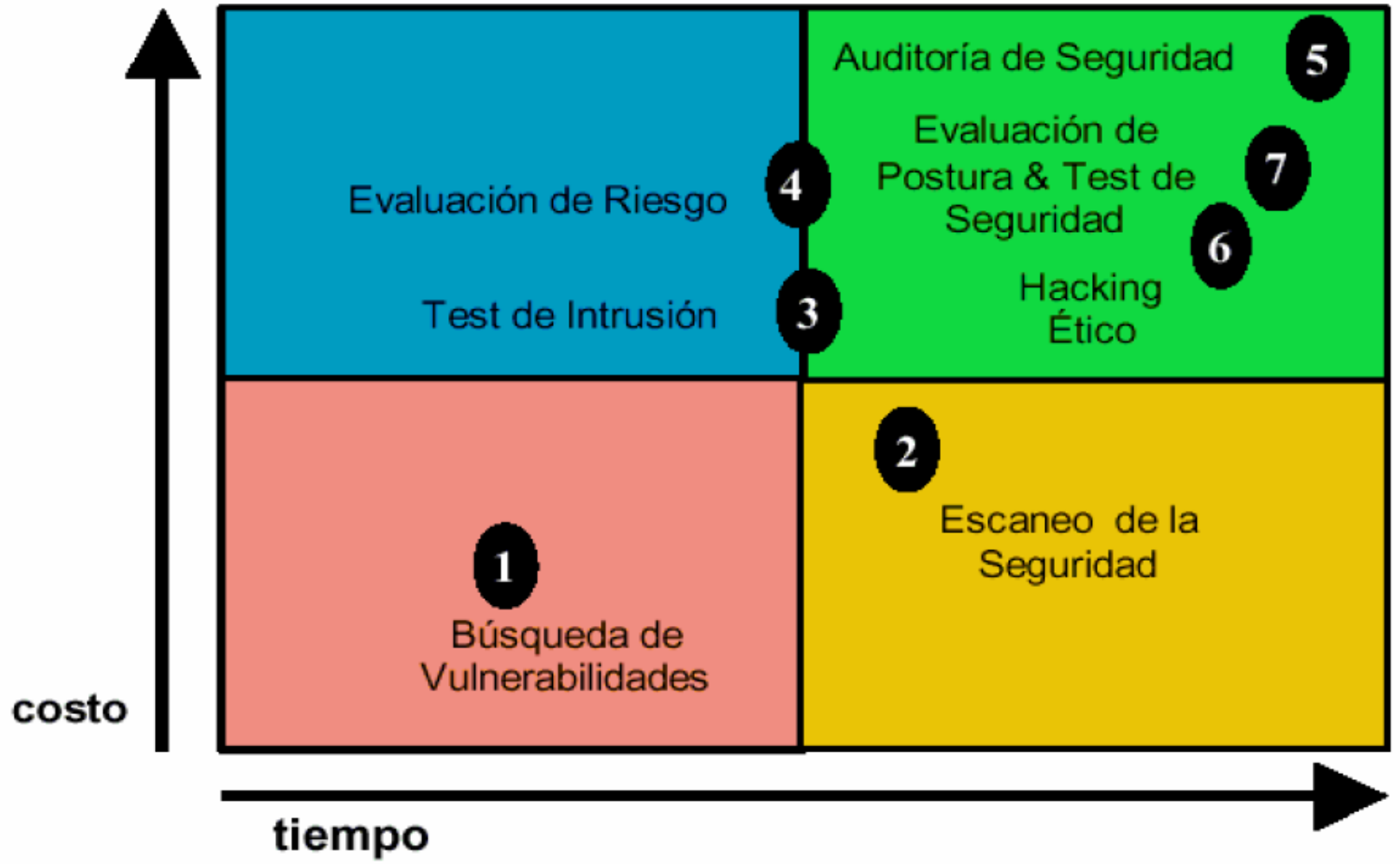
¿Qué se le pide a un profesional de seguridad?

1. Soluciones
2. Garantías
3. Métricas

Si no, perjuicios:

1. **No se pueden plantear umbrales a cumplir**
2. **No hay posibilidad de obtener ROI (dirección de empresa)**

Grados de auditoría



Auditorías de seguridad

- Se pueden clasificar en tres grupos
  - Test de penetración: Sin información, técnicas de “caja negra” desde el exterior al interior
  - Diagnóstico de seguridad: Más amplio. Tanto desde fuera como desde dentro. Análisis técnico. Con información
  - Auditoría de seguridad: Todo lo anterior + planes, políticas, normas, leyes…

Metodologías

Matriz de estado de seguridad

Métrica de seguridad definida por Alejandro Corletti

¿Es posible caracterizar el nivel de seguridad de un sistema informático?

- Deja de lado toda subjetividad
- Uso de herramientas

http://www.slackar.com.ar/MATRIZ_DE_ESTADO_DE_SEGURIDAD_v03.pdf

OSSTMM

Open Source Security Testing Methodology Manual

Esta metodología es una referencia abierta y gratuita que respeta la mayoría de los estándares estando en plena conformidad con los mismos (ISO-17799 o BS-7799, GAO y FISCAM, NIST, CVE de Mitre, etc.)

Estándar profesional para el testeo desde el exterior hasta el interior. Incluye,

- **Líneas de acción del testeador**
- **Ética del testeador**
- **Problemas de legislación**
- **Conjunto de tests a aplicar**

Se obtienen valores de evaluación de riesgo (RAVs) sobre un ciclo de vida: Métrica cíclica

OSSTMM

- El testeador debe cumplir una serie de reglas. Entre otras:
  - Reglas éticas en cuanto a la profesionalidad
  - Mantener la confidencialidad de los datos
  - Asumir responsabilidad sobre sus resultados
  - El ámbito, plan de trabajo, herramientas y limitaciones deben estar prefijadas
  - No provocar la explotación de vulnerabilidades, sino detectarlas y probar su existencia
  - Se deben incluir soluciones prácticas a los problemas encontrados

OSSTMM

- **Propone un proceso de evaluación de una serie de áreas que reflejan los niveles de seguridad que posee la infraestructura a auditar, a éstas las denominará "Dimensiones de seguridad", y son:**

  - **Visibilidad.**
  - **Confianza.**
  - **No repudio.**
  - **Privacidad.**
  - **Integridad.**
  - **Alarma**
  - **Acceso.**
  - **Autenticación.**
  - **Confidencialidad.**
  - **Autorización.**
  - **Seguridad.**

OSSTMM

Para un trabajo metódico y secuencial, describe seis secciones que abarcan el conjunto de los elementos que componen todo sistema actual, ellas son:

1 Seguridad de la Información
2 Seguridad de los Procesos
3 Seguridad en las tecnologías de Internet
4 Seguridad en las Comunicaciones
5 Seguridad Inalámbrica
6 Seguridad Física

Seguridad de la información

- Información recolectada de la presencia en Internet
  - No invasiva
  - Google hacking, whois, grupos de noticias…
- Revisión de privacidad desde el punto de vista legal
- Recopilación de documentos: emails, páginas personales, bbdd, redes P2P...

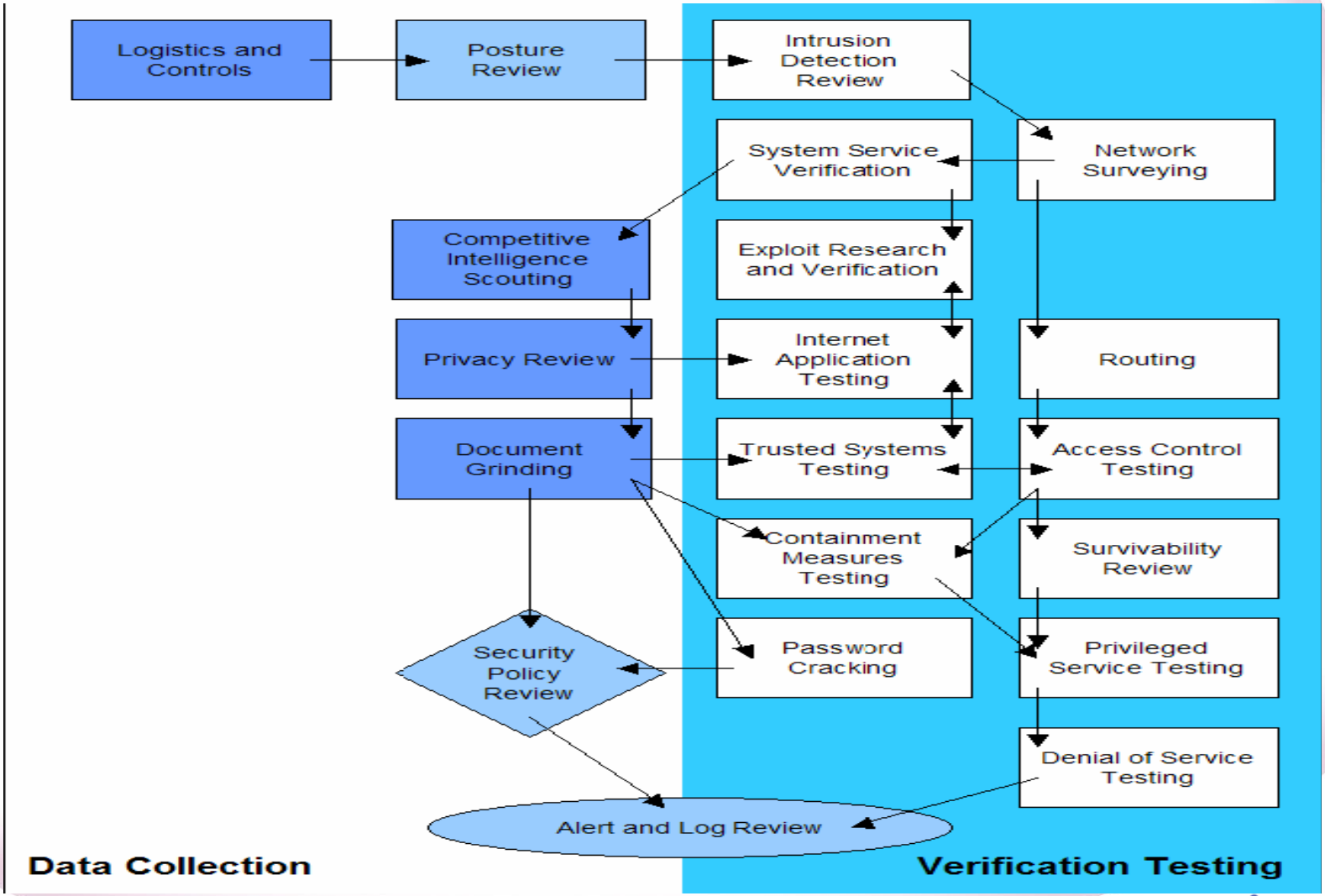
Seguridad de los procesos

- Ingeniería social
- Contacto fraudulento o no con la personas de entrada para obtener datos:
  - Puntos de acceso, IPs, personas, códigos,…

Seguridad en Internet

- Verdadero análisis de la infraestructura IT
  - Análisis de calidad de tráfico,
  - sondeo de red (dominios, IPs,…)
  - Identificación de servicios (enumeraciones)
  - Búsqueda de vulnerabilidades
  - Testeo de aplicaciones
  - Testeo del control de acceso
  - Encaminamiento
  - Testeo de IDSs
  - …

Seguridad en Internet



Seguridad en las comunicaciones

- Testeos de:
  - centralitas,
  - correo de voz,
  - faxes
  - modems
  - …

Seguridad Inalámbrica

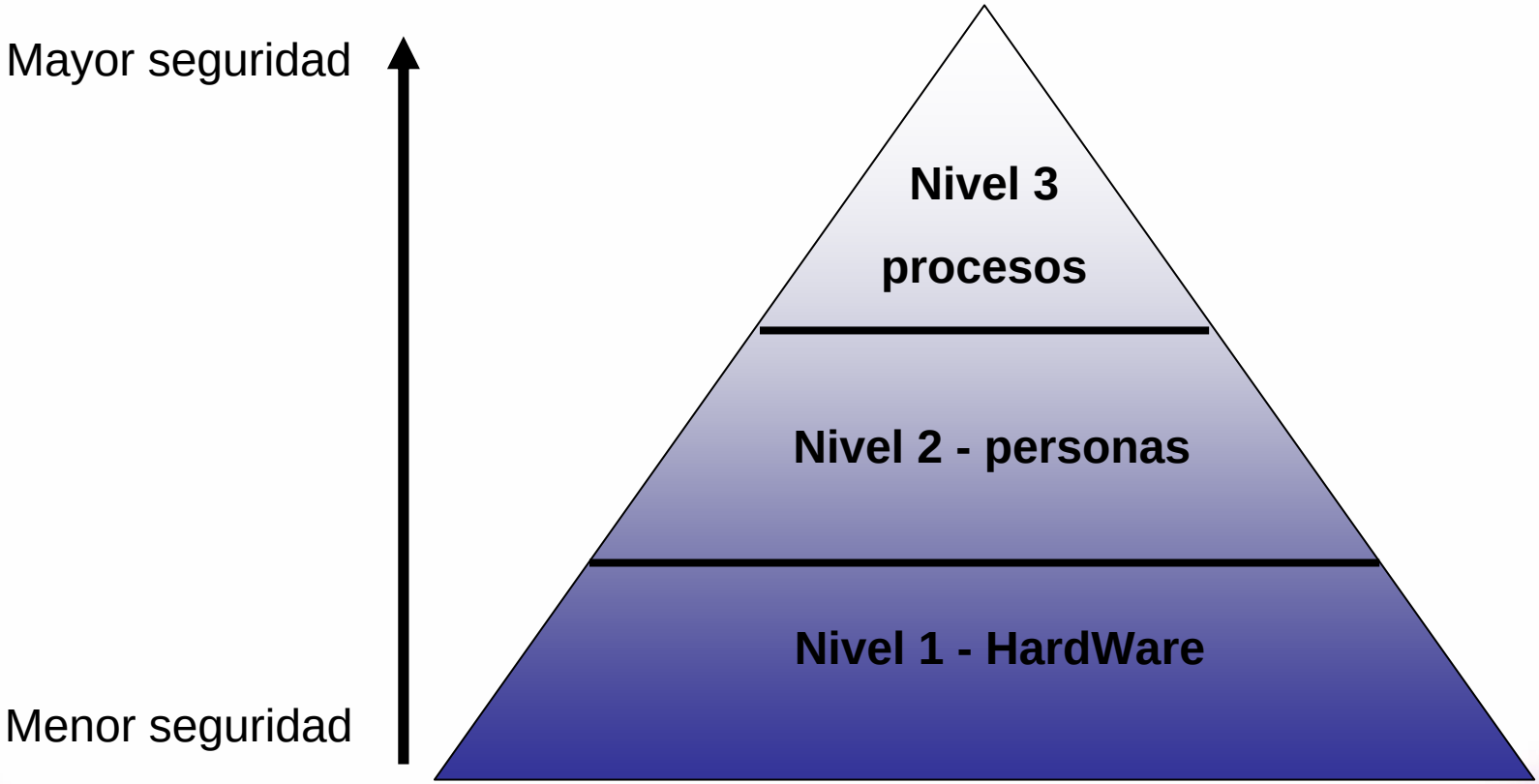
- Medidas de radiaciones EM
- Verificación de:
  - redes 802.11,
  - bluetooth,
  - infrarrojos,
  - RFID
  - …

Seguridad física

- Revisión del perímetro
- Puntos de acceso y controles
- Revisión de la vigilancia
- Alarmas
- Ubicación de los bienes
- ...

Gestionando la seguridad (Ej. proceso básico)

¿Por qué es importante la seguridad como proceso?



CONCLUSIONES

1. La seguridad hay que entenderla como un proceso
2. Auditoría y el hacking ético son parte del proceso
3. Si no se tienen conocimientos y recursos es conveniente consultar a profesionales en la materia
4. Las amenazas y las vulnerabilidades existen, es importante gestionar el riesgo

¿Preguntas ?

REFERENCIAS

Documentación relacionada:

ISO. International Standard Organitation
ISO 2859-4 Procedures for assessment of declared quality levels
ISO. International Standard Organitation
ISO GUIDE 73. Risk Management. Vocabulary. Guidelines for use in standards
ISO. International Standard Organitation
ISO GUIDE 73. Risk Management. Vocabulary. Guidelines for use in standards

STANDARDS AUSTRALIA AS 4360 Risk Management
STANDARDS AUSTRALIA HB 231 Information Security Risk Management Guidelines

AENOR. UNE ISO 17799 Código buenas practicas
AENOR. UNE 71501-1 Conceptos y modelos para la Seguridad de TI
AENOR. UNE 71501-2 Gestión y Planificación de la Seguridad de TI
AENOR. UNE 71501-3 Técnicas para la gestión de le Seguridad de TI

BSI. BS 7799-2 Information Security Management Systems.
BSI. BS 15000-2 IT Service Management. Part. 2
BSI. PD 3001 Preparing for BS 7799-2 Certification
BSI. PD 3002 Guide to BS 7799 Risk Assessment
BSI. PD 3003 Are you ready for a BS 7799-2 Audit ?
BSI. PD 3004 Guide to the implementation and auditing of BS 7799 controls
BSI. PD 3005 Guide on the selection of BS 7799-2 Controls

REFERENCIAS

Free Software Foundation

Ricardo Galli, Richard Stallman y Alejandro Corletti

seguridaddigital.info

pipers, inmolatus, nm0

OSSTMM - ISECOM

Wikipedia

Spamhaus, ciphertrust, viruslist, zone-h, sophos

Bizkaia Enpresa Digitala

NESYS - Seguridad y Tecnologías de la información

Contacto: info@nesys-st.com

LICENCIA

creative commons

COMMONS DEED

Reconocimiento-NoComercial 2.0

Usted es libre de:

- copiar, distribuir y comunicar públicamente la obra
- hacer obras derivadas

Bajo las condiciones siguientes:

Reconocimiento. Debe reconocer y citar al autor original.

No comercial. No puede utilizar esta obra para fines comerciales.

- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior.