



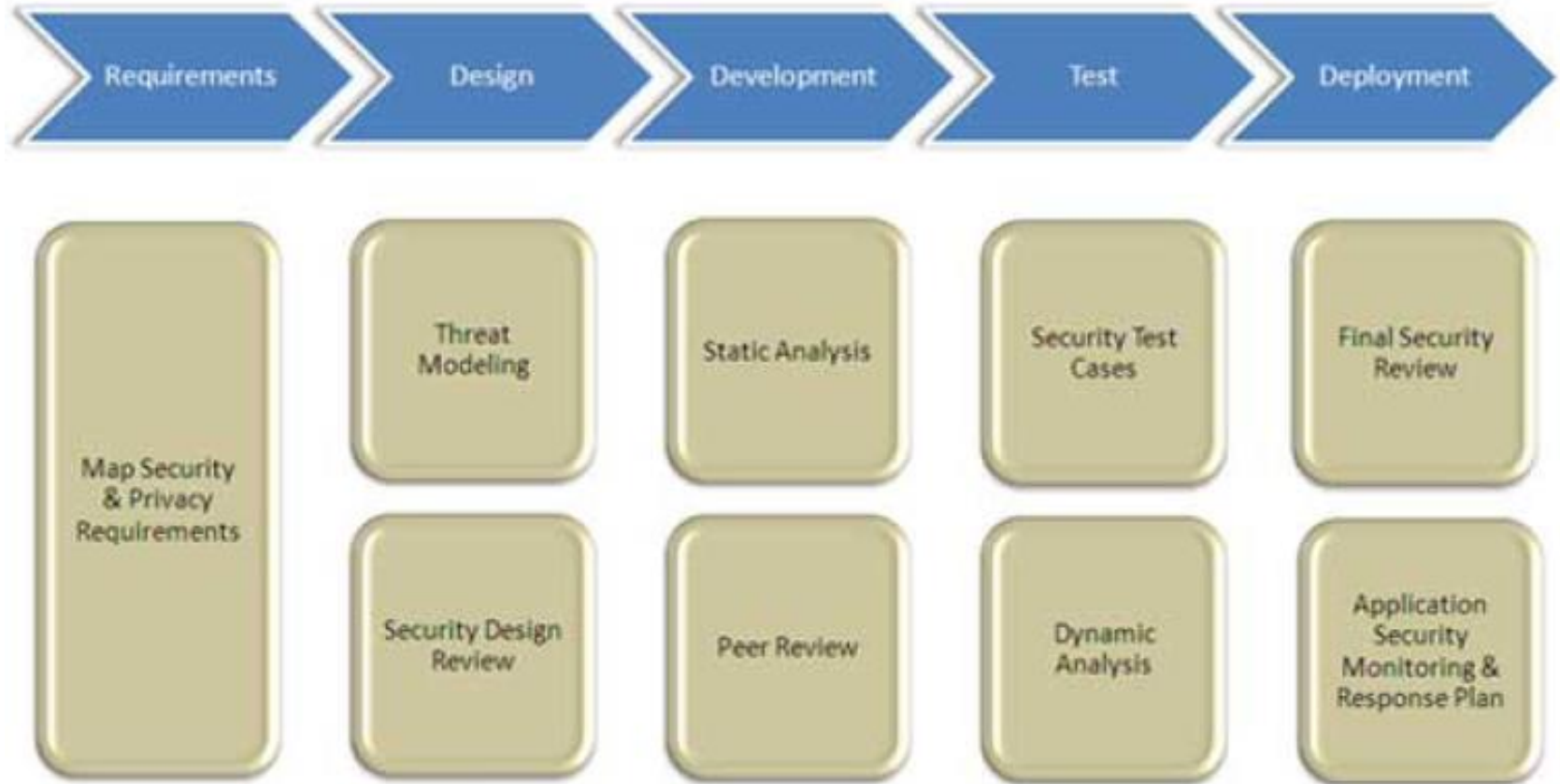
# Gestión de la Seguridad del Software

---

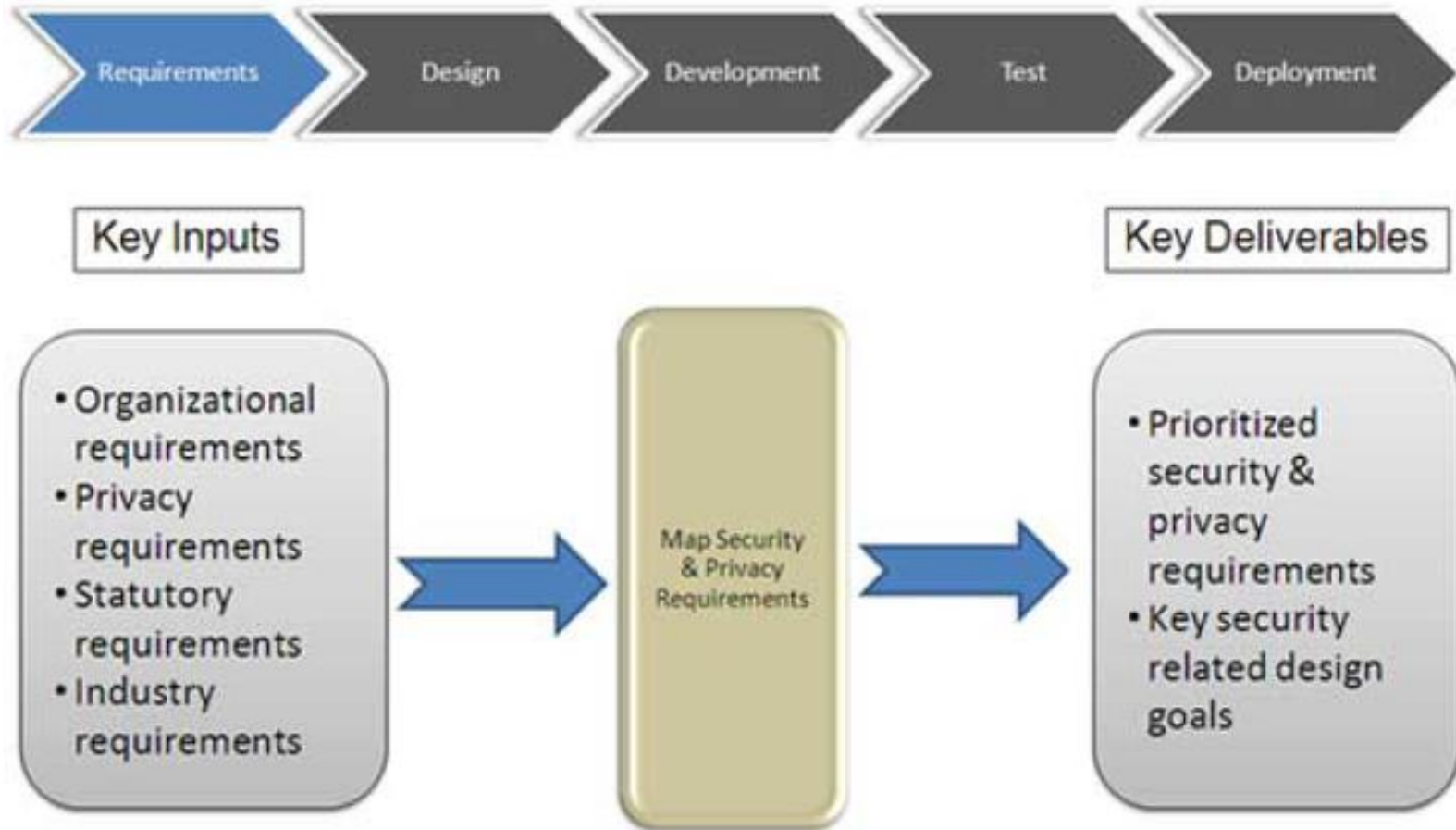
PhD. Félix Oscar Fernández Peña.  
[ffernandez1@utmatch.edu.ec](mailto:ffernandez1@utmatch.edu.ec)

# Seguridad en el desarrollo de aplicaciones

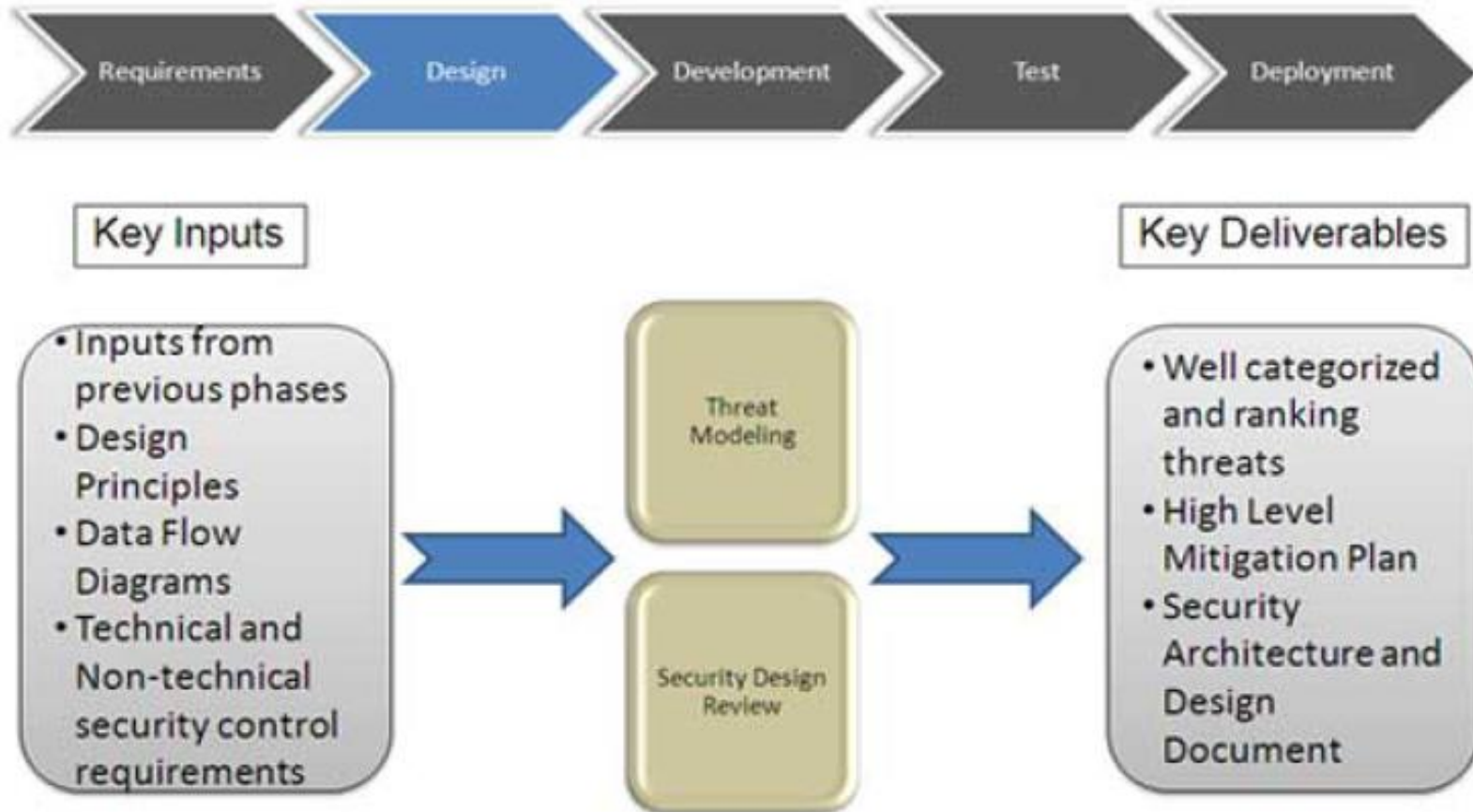
# Seguridad en el SDLC



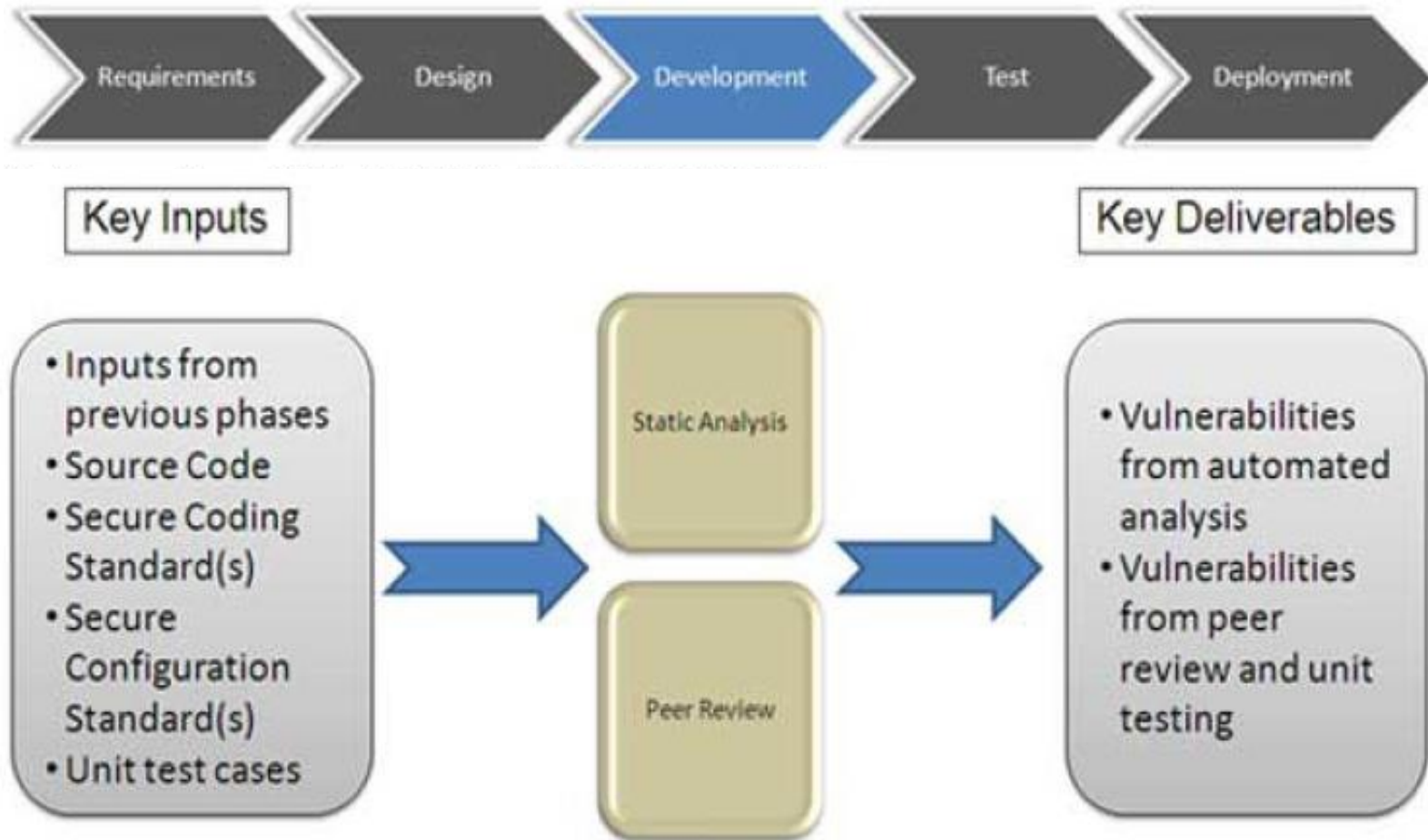
# Seguridad en el SDLC



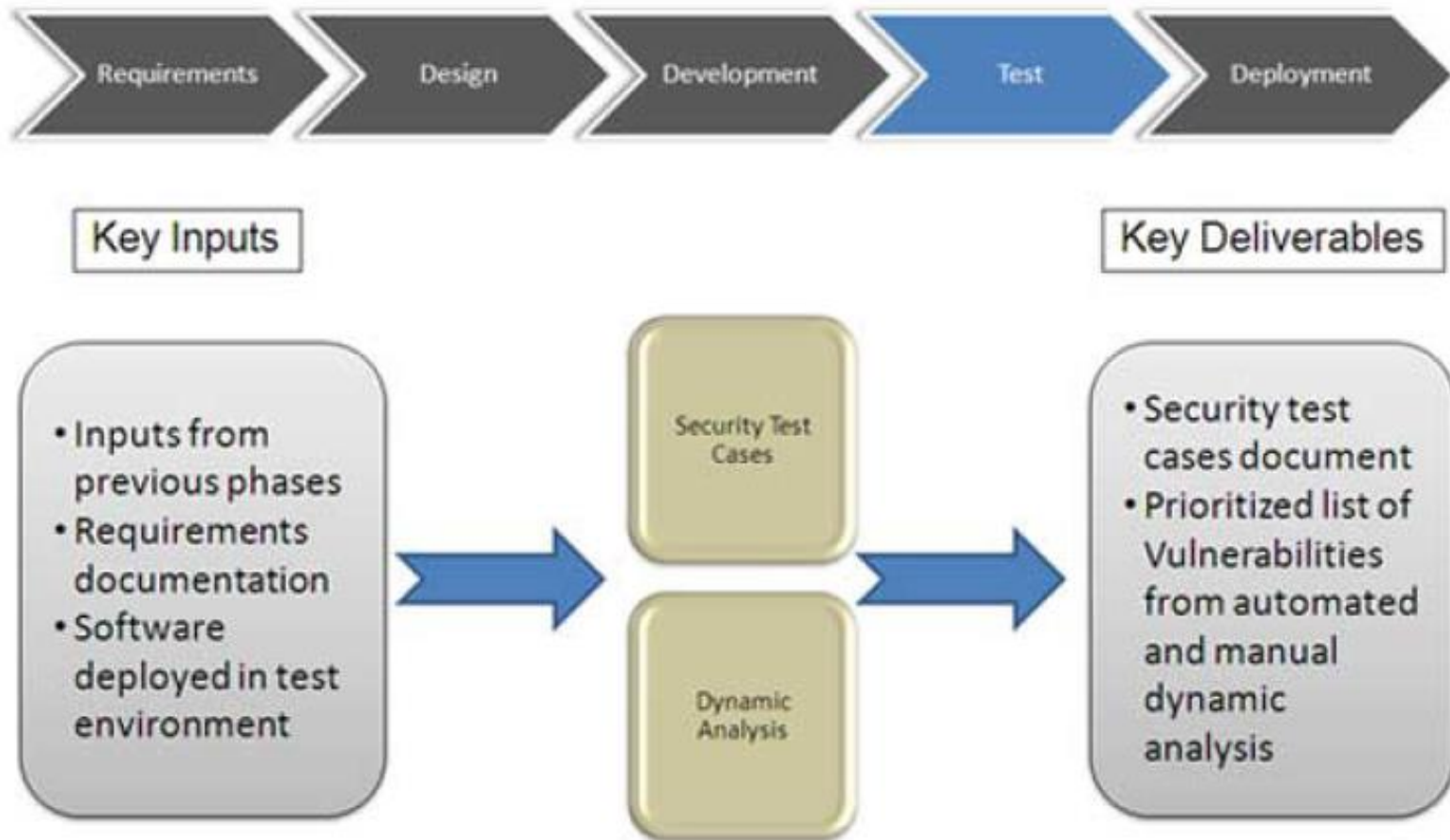
# Seguridad en el SDLC



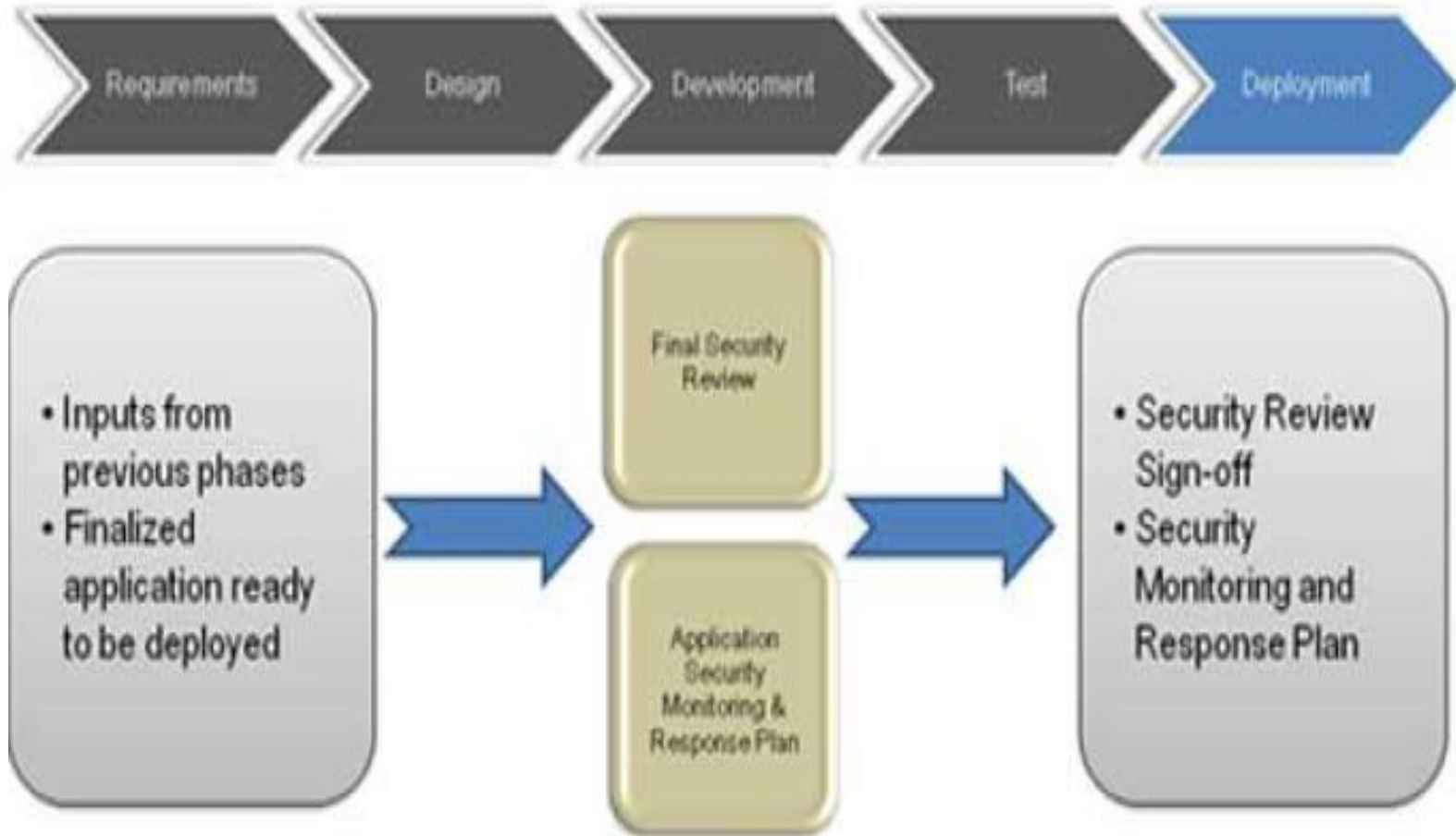
# Seguridad en el SDLC



# Seguridad en el SDLC



# Seguridad en el SDLC



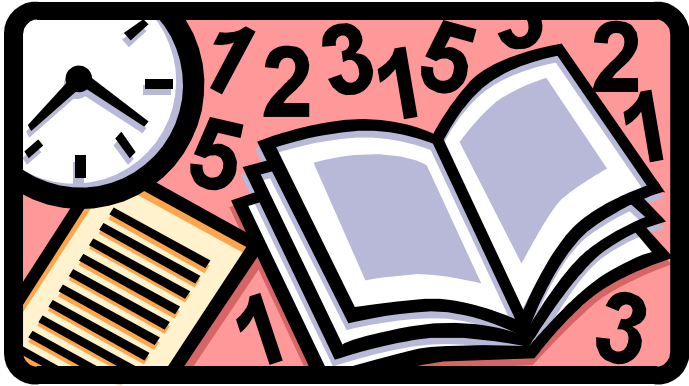


# Buenas prácticas

1. Apply Defense in Depth
2. Use a positive security model (Whitelisting)
3. Fail securely (buffer overflow fue el 90 % de los ataques a Windows en el 2009 (SANS))
4. Run with least privilege
5. Avoid security by obscurity
6. Detect intrusions
7. Don't trust infrastructure
8. Don't trust services
9. Establish secure defaults

# Salvas

- Qué datos se salvarán?.
- Qué tiempo se dispone para realizar el backup (Backup Window)?.
- Cuánto tiempo debe estar esta información guardada y disponible (Restore Horizon)?.
- Con qué frecuencia y rapidez se accede a esta salva?.



# Análisis de logs

Permite detectar brechas,  
seguir pistas...:

- Ataques que usan contraseñas aleatorias.
- Conexiones con contraseñas robadas.
- Uso incorrecto de privilegios de administración.
- Actividad de virus.
- Acceso indebido a datos sensibles.
- Acceso indebido a la impresora, proyector,...

# Protección Física

Todas las medidas de seguridad aplicadas, empleando medios de software o hardware, pierden su efectividad si no se cuida la seguridad física.

Se trata de proteger todos los medios informáticos a través de alarmas, guardias, rejas, llavines...



# Contraseñas de una sola vez

Las contraseñas que puedan ser capturadas no son reusables por los atacantes para ganar acceso a los sistemas.

Esta tecnología garantiza que las contraseñas empleadas por los usuarios sean válidas en un cortísimo período de tiempo y que no se repitan jamás.

# Herramientas de monitoreo

- Los monitores de red recogen información del uso del sistema y los servicios que brinda: Nmap
- Es posible configurar la notificación de la detección de eventos anómalos que pueden resultar sospechosos, de manera automática.
- Existe una buena variedad de programas de identificación de vulnerabilidades.
- Antivirus.




# Nessus Report

## Summary

Number of hosts tested : 5

Found 17 security holes





Found 93 security warnings


-  bonsai.fr.nessus.org
-  prof.fr.nessus.org
-  dormeur.fr.nessus.org
-  gateway.fr.nessus.org
-  grincheux.fr.nessus.org

Solution : install all the latest Microsoft Security Patches

Risk factor : Serious

CVE : CVE-1999-0278

-  poppassd (106/tcp)
-  pop-3 (110/tcp)
-  unknown (135/tcp)
-  netbios-ssn (139/tcp)

 Security warnings

The remote registry can be accessed remotely using the login / password combination used for the SMB tests.

Having the registry accessible to the world is not a good thing as it gives extra knowledge to a hacker.

Solution : filter incoming traffic to this port or set tight login restrictions.

Risk factor : Low

The domain SID can be obtained remotely. Its value is :

INTRANET : 5-21-20333150-368275040-1648912389

Save as...

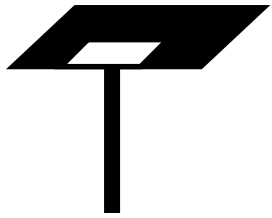
Save as HTML with Pies :

Close

# Gestión de seguridad

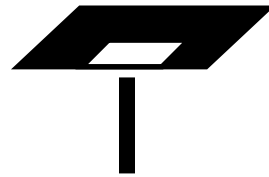


# Áreas Funcionales de la Gestión de Red



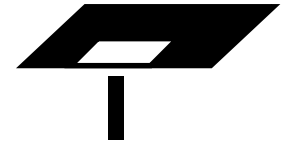
## Gestión de Configuración

Monitoreo y control de inventario (hard y soft), localización de equipos y servicios, distribución de software.



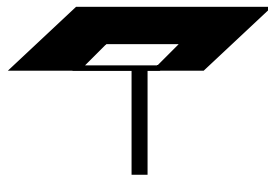
## Gestión de Prestaciones

Supervisión de Estado.  
Alarmas y Eventos.  
Estadísticas, Utilización.  
Errores



## Gestión de Fallos

Rapidez en el diagnóstico, localización y reparación.

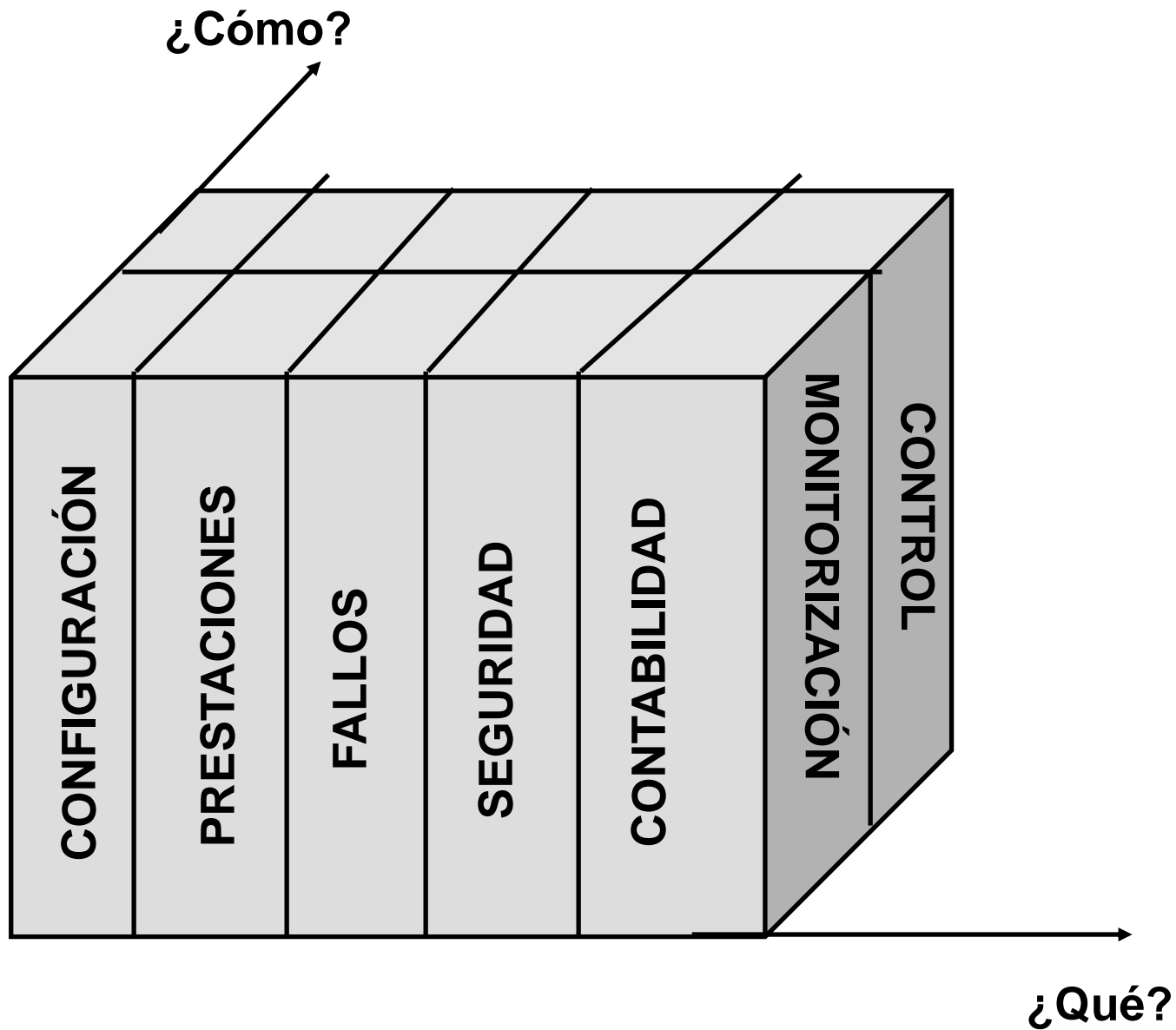


## Gestión de Seguridad

Autenticación de Usuarios  
y Control de Acceso a Recursos

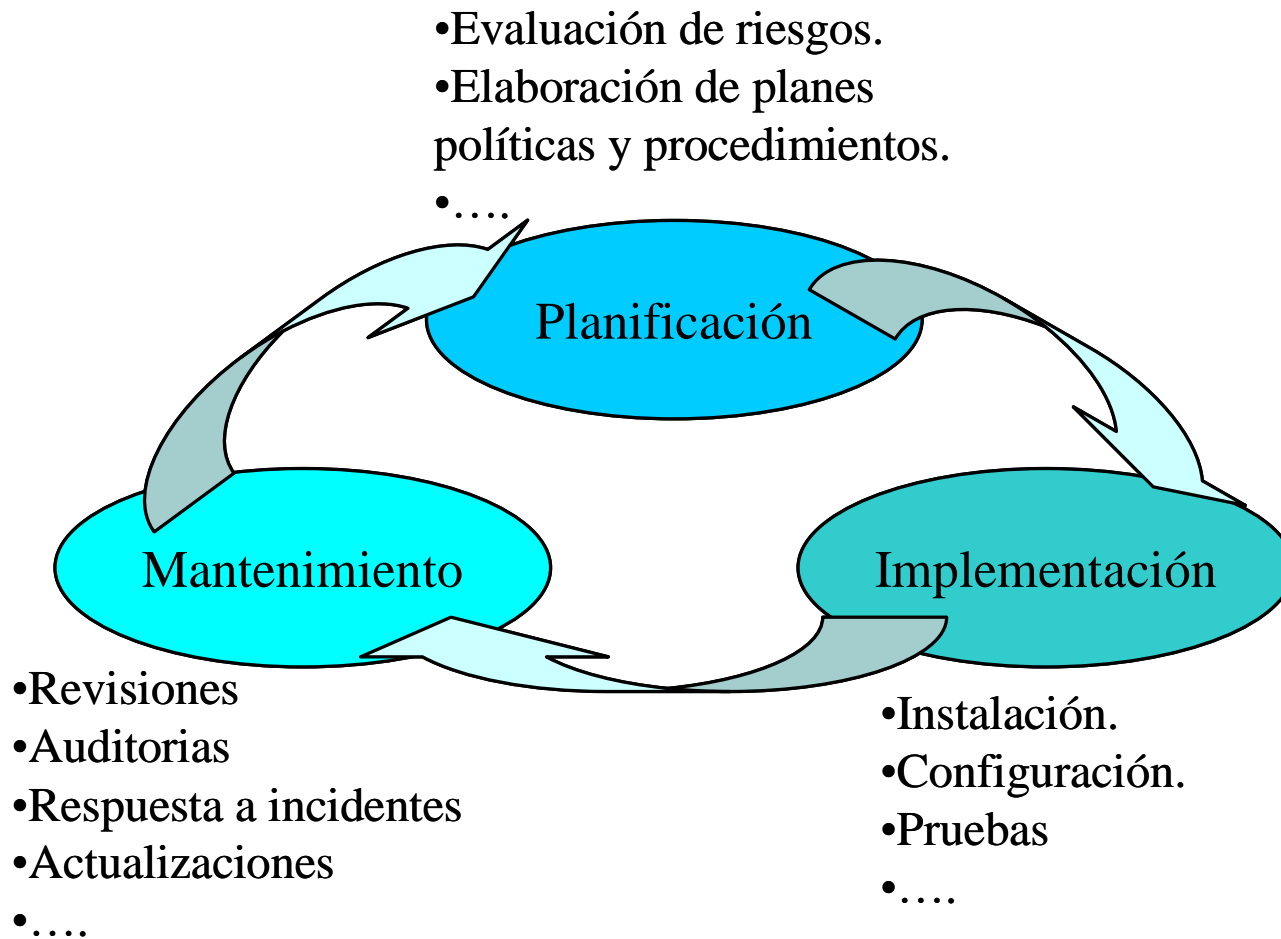


Gestión de Contabilidad Utilización de la Red y sus servicios por parte de los usuarios



**Dimensiones presentes en la Gestión de Redes**

# Gestión de Seguridad

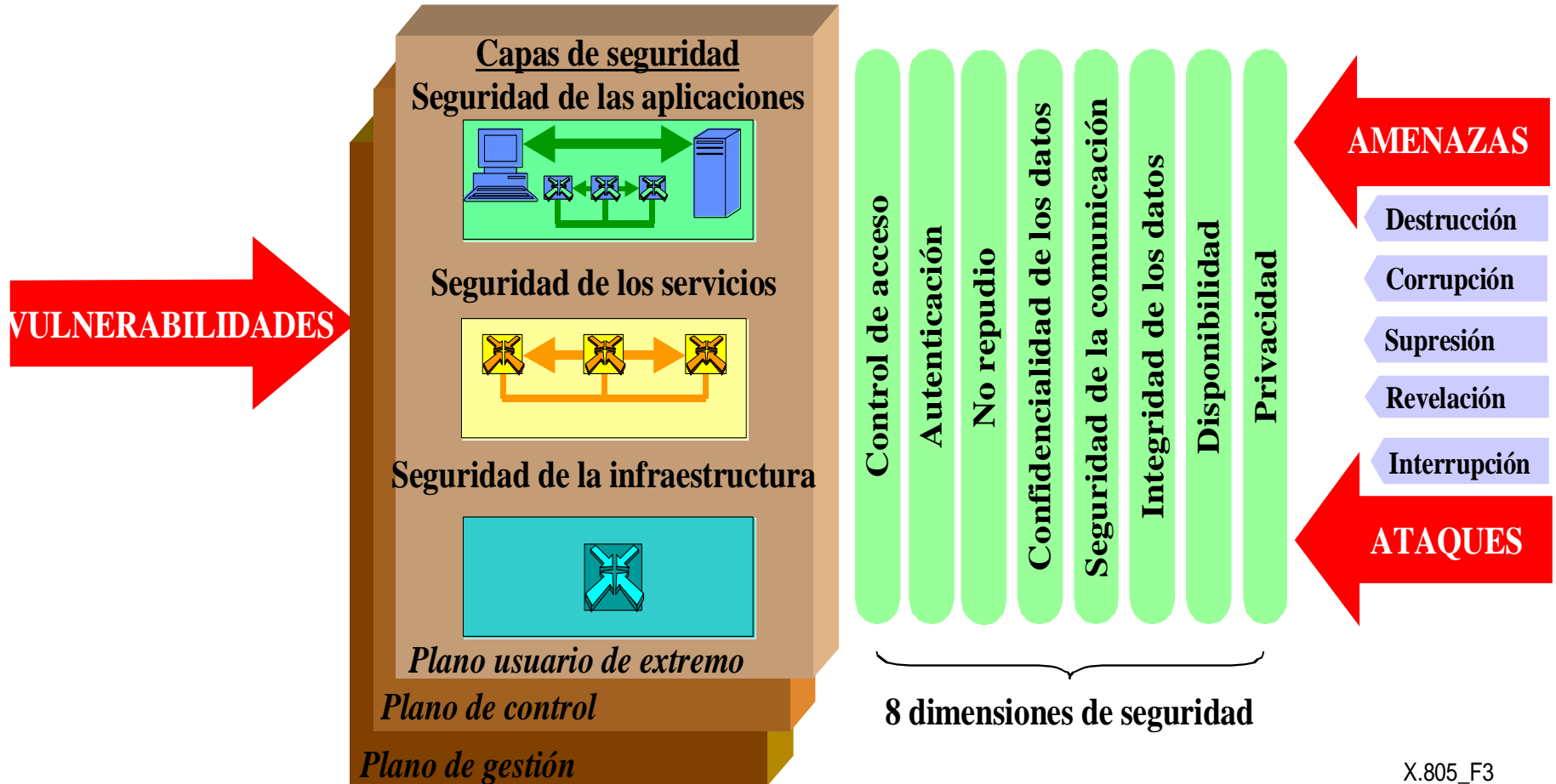


# Estándares para la Gestión de Seguridad

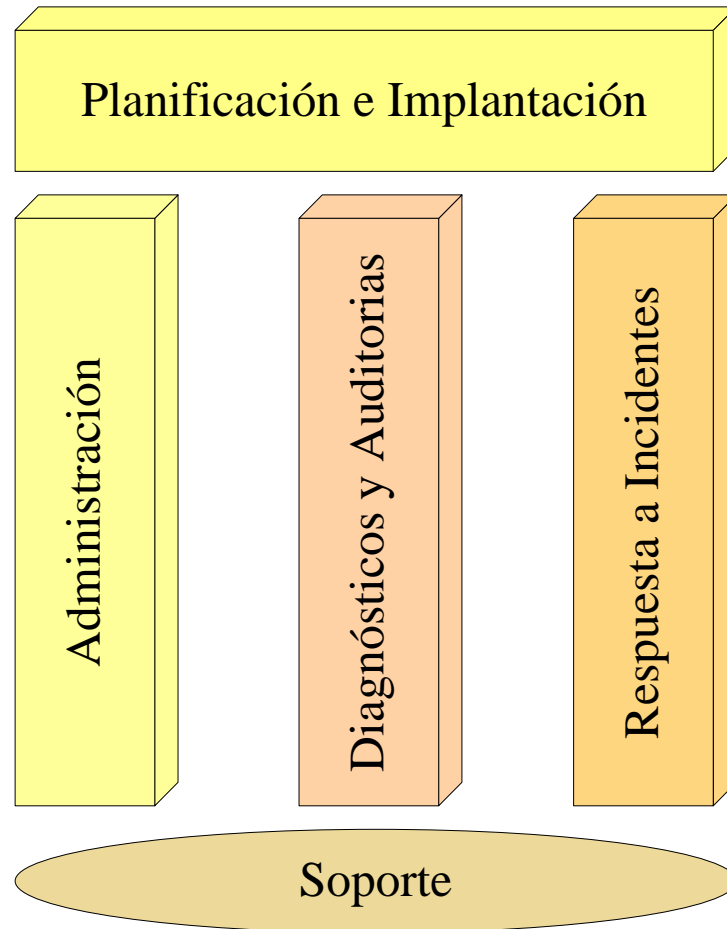
# Normas de seguridad

- Estándares más representativos: ISO/IEC 17799:2005, ISO/IEC 27000, X.800, M.3400 y X.805.
- Debe prestarse atención a las propuestas de otras organizaciones como ETSI, 3GPP y NIST.

# X.805



# Sistema de Gestión de Seguridad para redes de Telecomunicaciones (SGS-T)

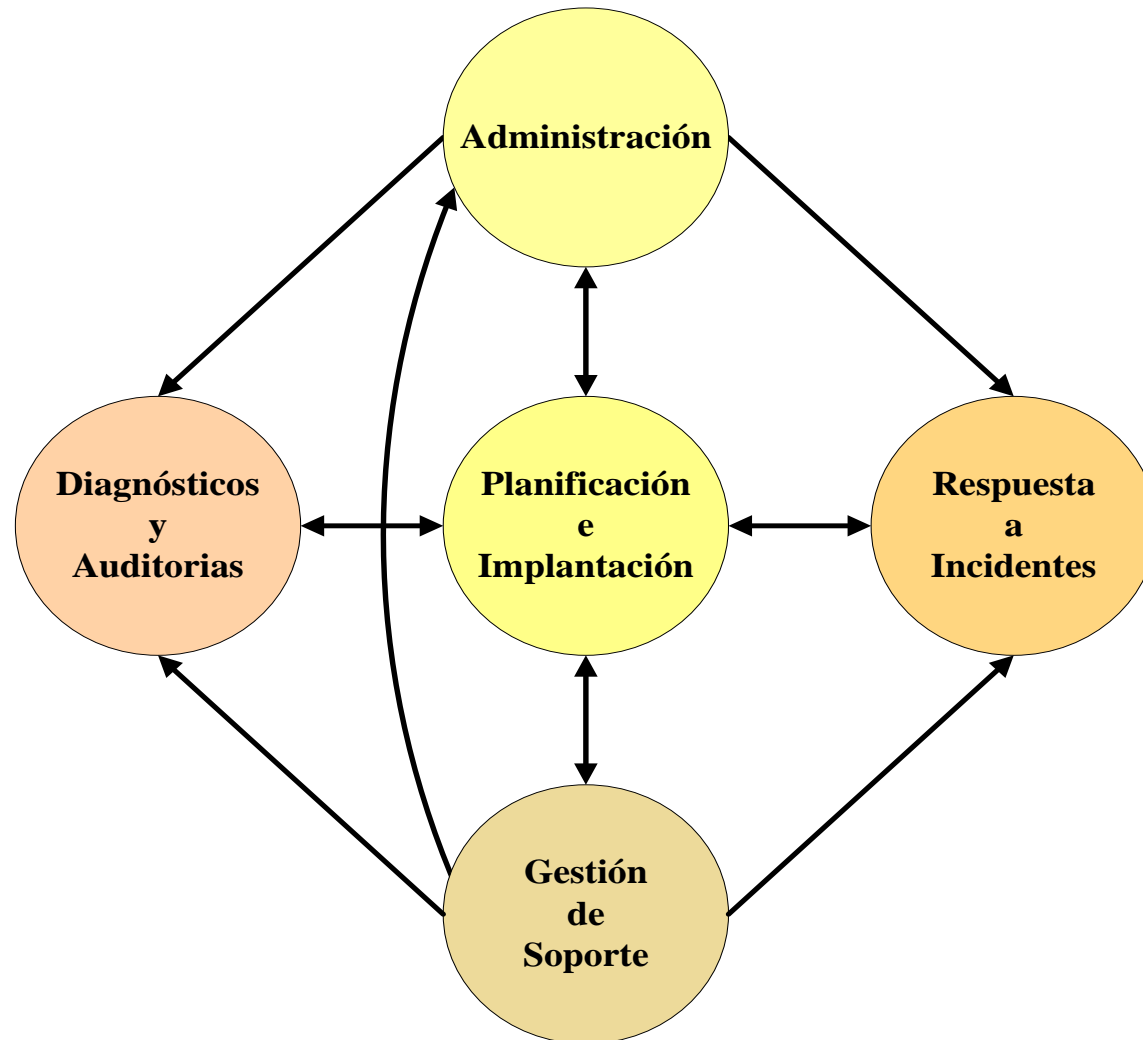


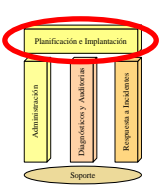
# Características del SGS-T

- Permite el trabajo de seguridad en las áreas de prevención, detección y recuperación de incidentes.
- Sus tareas están relacionadas con las del resto de los sistemas que se ocupan de las otras áreas funcionales de gestión de la red de telecomunicaciones (FCAP).
- Organiza las tareas de gestión de seguridad en cinco grupos, interrelacionados entre sí.
- Permite abordar la gestión de seguridad como un proceso continuo de Planificación, Implantación y Mantenimiento.
- La ejecución de los grupos de tareas se puede basar en el empleo de la Arquitectura de Seguridad propuesta.

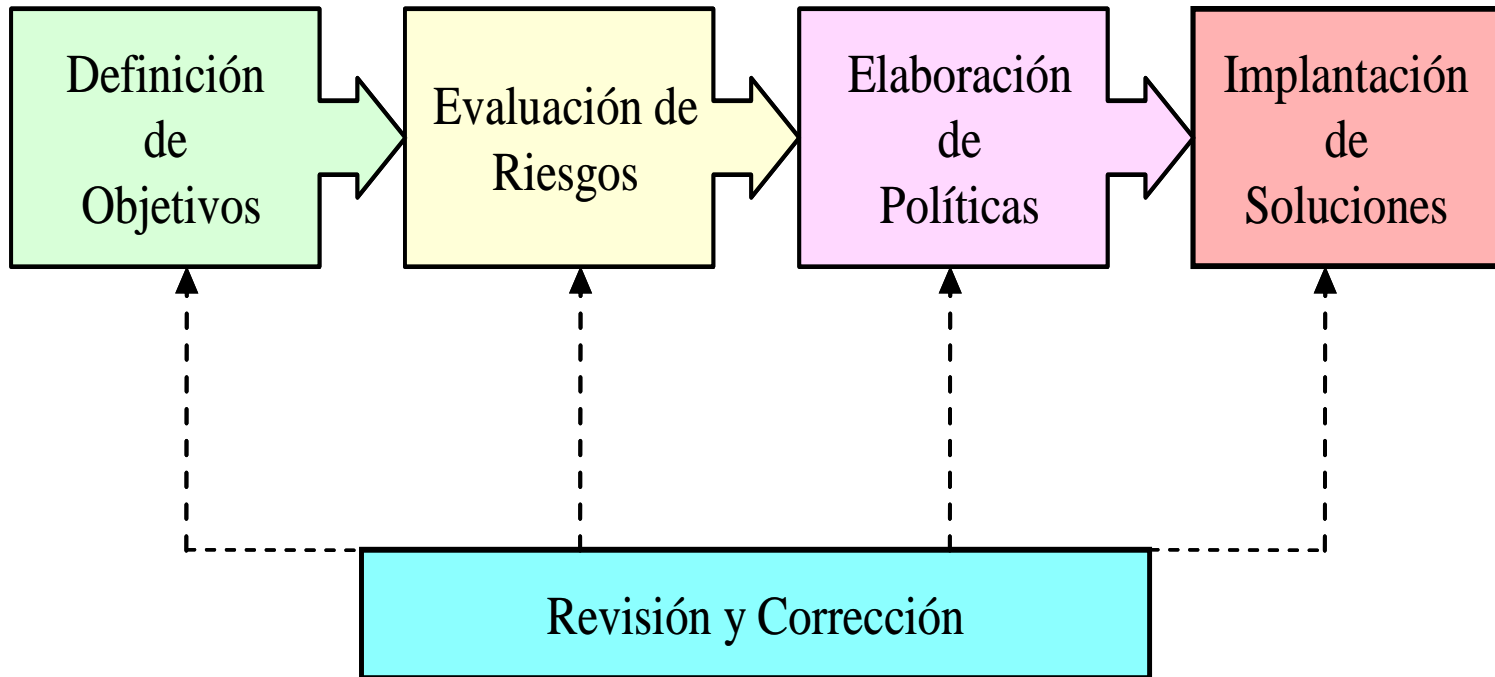


# Relaciones entre los grupos de tareas del SGS-T



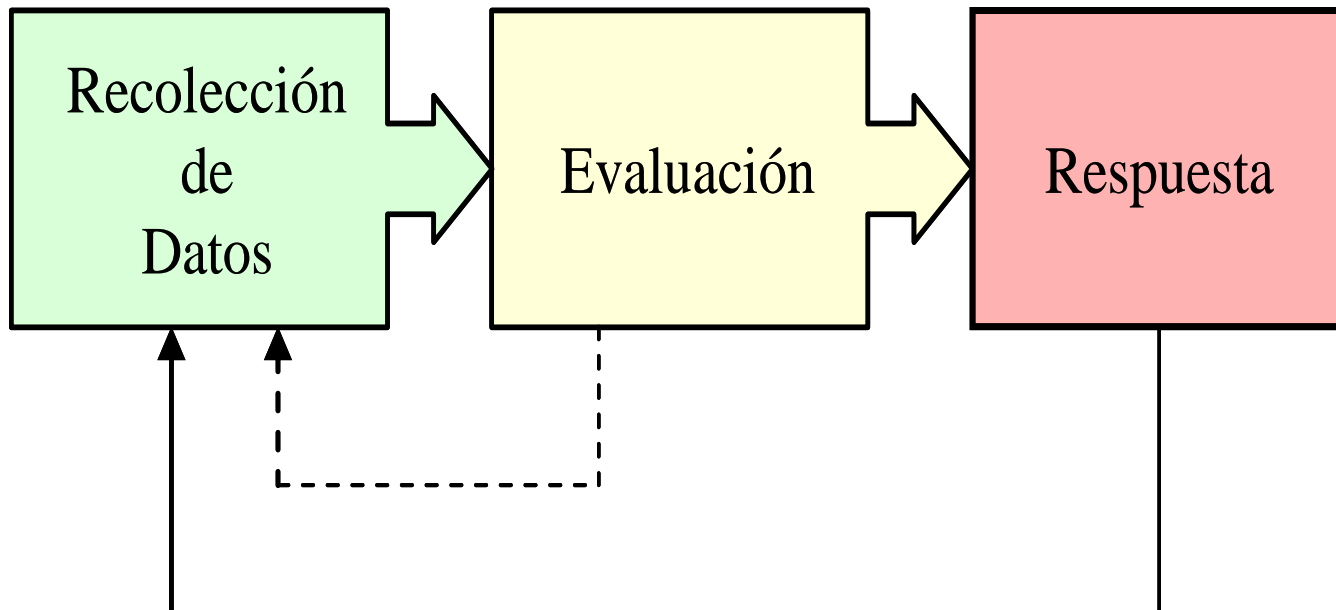


# Planificación e Implantación



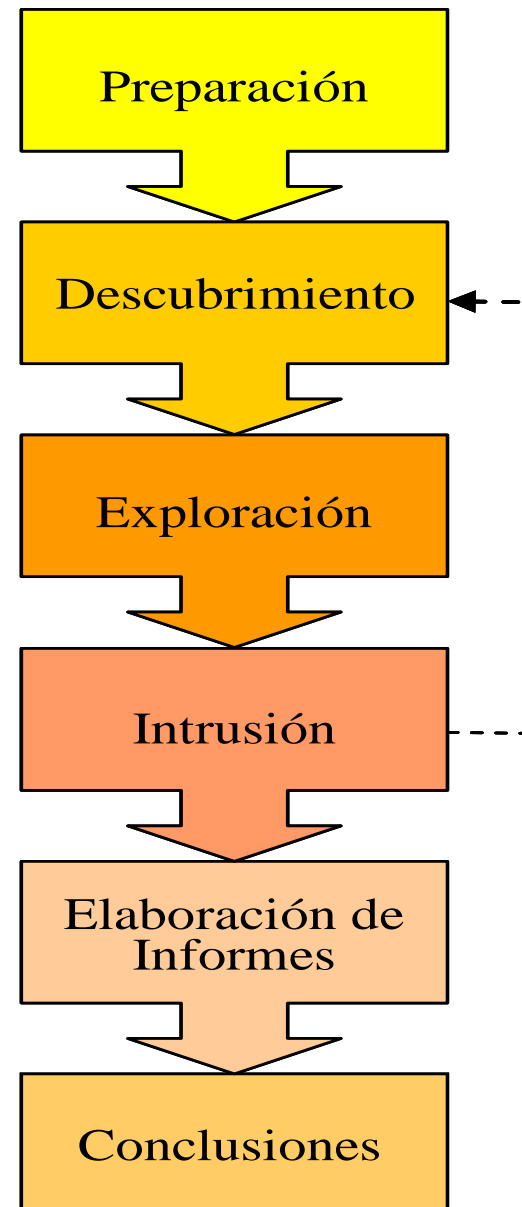


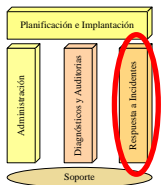
# Administración



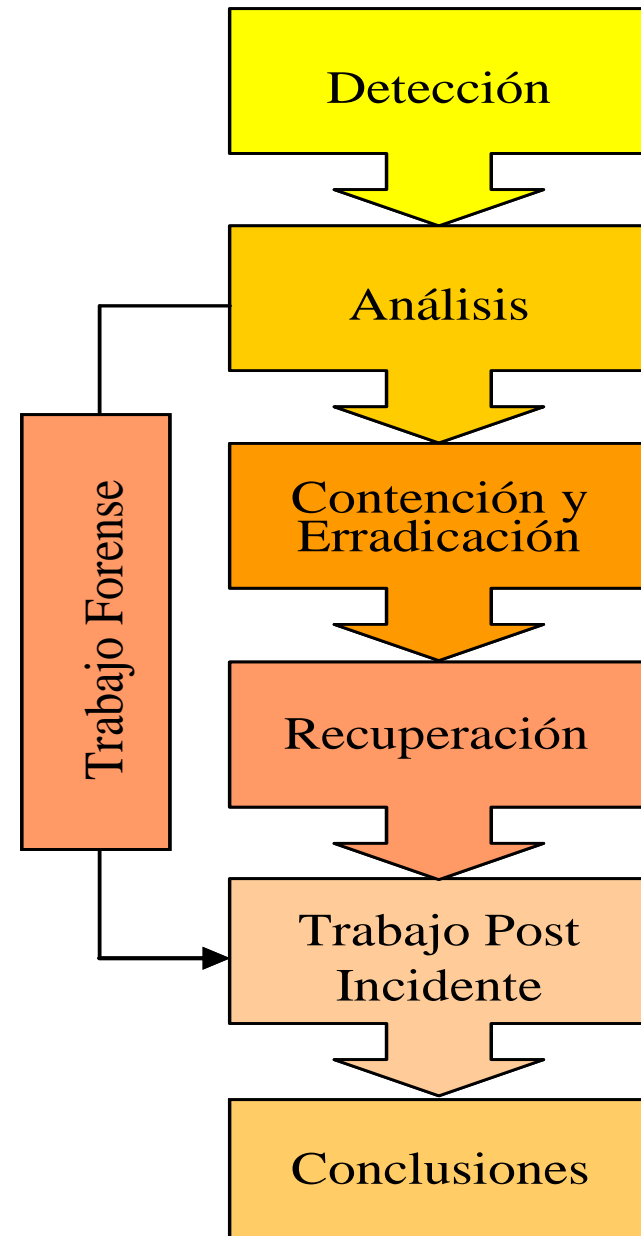


# Diagnósticos de Seguridad





# Respuesta a Incidentes



# Planificación e Implantación

- Abarca tareas como la precisión de objetivos a lograr, la selección de las herramientas necesarias, su instalación y la elaboración de los procedimientos de su explotación, la seguridad física, el cálculo de costos, la organización de los recursos humanos y otros.

# Planificación e Implantación

- Aborda la Planificación e Implantación de las infraestructuras, políticas y procedimientos de todos los grupos de tareas del SGS-T.
- Estas tareas pueden ser ejecutadas de forma simultánea o en diferentes momentos, y por diferentes grupos de especialistas.

# Planificación

- Permiten definir cuáles serán y cómo se ejecutarán las tareas para mantener un nivel determinado de seguridad.
- En la Planificación de Seguridad se debe considerar la prevención, la detección y la recuperación de incidentes. Es importante insistir en la prevención, con el objetivo de minimizar las posibilidades de que la red protegida sea atacada con éxito y, por otro lado, evitar que se convierta en el origen de los ataques a otras redes.



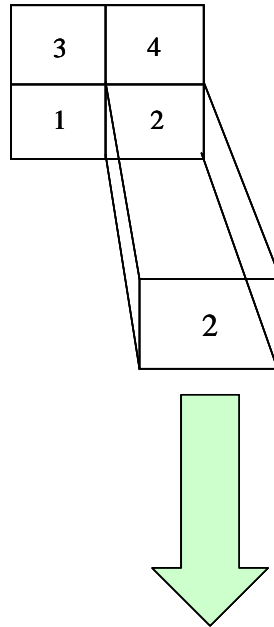
# Planificación

Durante esta labor se realiza una identificación de las necesidades o requerimientos de seguridad a través de las vías siguientes:

- Evaluación de riesgos de la red y sus servicios.
- Revisión de cláusulas de contratos, regulaciones legales u oficiales, relacionadas con contrapartes, proveedores y otros.
- Revisión a principios, objetivos y requerimientos del negocio, definidos por la organización en cuestión con el objetivo de regular la operación del sistema o red de telecomunicaciones.

# Elaboración de Políticas

**Estructura Modular de la Red**



Autenticación
Control de Acceso
No Repudio
Confidencialidad
Integridad
Disponibilidad

**Plantilla de Dimensiones de Seguridad**

P r e v e n c i ó n	D e t e c c i ó n	R e c u p e r a c i ó n
--	---	--

**Plantilla PDR**

Módulo 2			
Dimensiones de Seguridad	Medidas de seguridad		
	Prevención	Detección	Recuperación
Autenticación			
Control de Acceso			
No repudio			
Confidencialidad			
Integridad			
Disponibilidad			

**Tabla de Medidas de Seguridad**

# Implantación

- Considera una serie de tareas a ejecutar posterior a la definición del Plan de Seguridad.
- No tiene que ser realizada por los mismos especialistas que escriben el plan, pero sí debe contar con su asistencia.
- Incluye, entre muchas otras tareas, la puesta en práctica de políticas y procedimientos, la instalación y configuración de cortafuegos, antivirus y su infraestructura de actualización, PKI, IDS/IPS, infraestructura de actualización de software (parches), y sistemas para la gestión y capacitación de usuarios.

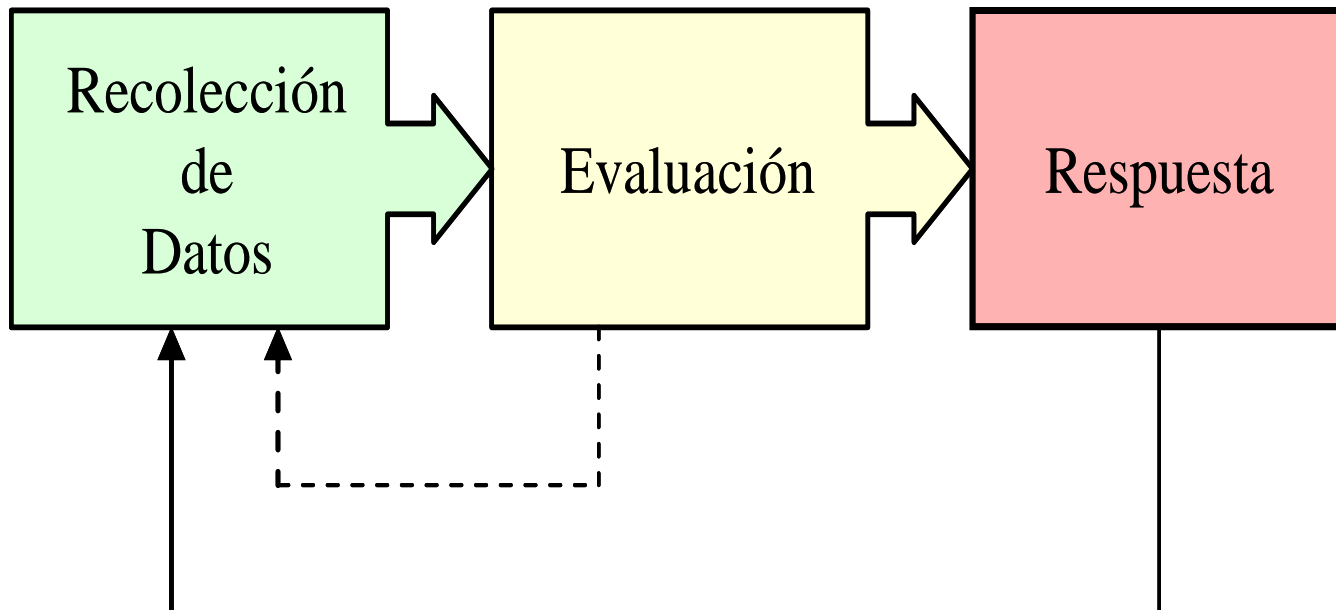
# Administración

La Administración del SGS-T, en forma resumida, tiene los siguientes objetivos:

- Detectar errores en la implantación de la seguridad.
- Determinar los niveles de efectividad de las soluciones de seguridad propuestas.
- Detectar intentos de intrusión.
- Detectar nuevas brechas o amenazas de seguridad.
- Corregir en lo posible, con respuestas inmediatas o a través de la activación de las tareas de los otros grupos, los problemas encontrados.



# Administración



# Administración

## Tareas importantes

Administración de la infraestructura de detección de incidentes:

- Chequeo de la integridad de las bases de información (bases de datos, salvas, configuración de equipos y servicios, entre otros).
- Análisis de *logs* de dispositivos y servicios.
- Atención a alertas de seguridad que pueden ser lanzadas por la infraestructura de detección de incidentes.

# Administración

## Tareas importantes

- Análisis del tráfico que circula por las diferentes zonas de la red.
- Administración de las soluciones de seguridad implantadas (software y hardware): cortafuegos, VPN, PKI, sistemas de actualizaciones de software, soluciones antivirus, sistemas de respaldos de información, entre otros.
- Chequeo periódico de vulnerabilidades (gestión de vulnerabilidades).
- Chequeo de actualizaciones o parches para todos los sistemas (gestión de parches). Esto incluye pruebas de cuarentena para no afectar el funcionamiento de elementos vitales en la red de telecomunicaciones, como los *softswitchs* por ejemplo.

# Administración

## Tareas importantes

- Atención a los reportes de sistemas que puedan estar relacionados con problemas de seguridad (TTS, sistemas de facturación y otros).
- Revisión de la implantación de las políticas de cuentas de usuarios, manejo de privilegios, altas y bajas, entre otras.
- Corrección de los problemas encontrados. Si no se puede ofrecer la solución adecuada o esta conlleva una labor muy compleja, se hace necesaria la intervención de especialistas del resto de los grupos de tareas.



# Diagnósticos de seguridad (PT)



# Penetration Test

## Concepto

Es un conjunto de métodos y técnicas de intrusión aplicadas sobre un sistema en un tiempo determinado, con el objetivo de conocer el nivel de seguridad informática real del mismo, detectando y explotando vulnerabilidades.

# Penetration Test



- También conocido como “ethical hacking”.
- Conjunto de métodos y técnicas para realizar un análisis integral de las debilidades de los sistemas informáticos.
- Proceso activo de evaluación de las medidas de seguridad adoptadas por una entidad.
- Reproduce intentos de acceso de un intruso a cualquier entorno informático desde los diferentes puntos de entrada que existan, tanto internos como remotos.

# Evolución del PT

70's

{ Evaluación de Seguridad al sistema MULTICS, Fuerza Central de Servicios de Datos de la Fuerza Aérea EUA

1993

{ Farmer and Venena, SATAN

Actualidad

{ Desarrollo de Herramientas y Metodologías .  
Uso habitual en los estudios de seguridad.

# Actualmente

- Nivel de madurez elevado en el mercado.
- Diferentes fines: conocimiento, validación de proyectos, un “seguro” de trabajo.
- Evaluación de aplicaciones web.
- Aumento constante de la complejidad de ejecución.
- Proposición de medidas correctivas.

# ¿Para qué?

- Conocer la situación real de los sistemas y mejorarlos.
- Demostrar a la administración los riesgos existentes.
- Justificar la obtención de más recursos económicos.
- Verificar que los mecanismos de seguridad se encuentren funcionando correctamente.

# Objetivos

Se plantea como el principal objetivo determinar las debilidades de seguridad de la infraestructura y servicios de red de una organización.



# Objetivos

## Objetivos secundarios:

- probar la capacidad de identificación y respuesta a incidentes
- probar el conocimiento y conciencia de los usuarios desde el punto de vista de la seguridad
- comprobar el cumplimiento de las políticas de seguridad



# Etapas básicas de un PT

- Definición del alcance.
- Definición de la metodología a utilizar.
- Aplicación de la metodología.
- Evaluación de los resultados obtenidos.
- Corrección de los problemas detectados.

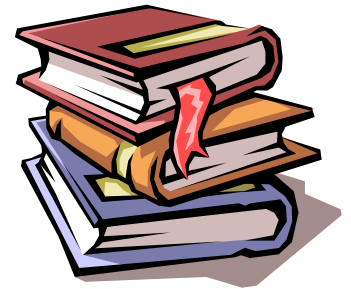
# Alcance y duración



- Factores muy relacionados.
- Se definen a partir de las necesidades del cliente.
- Se establece qué pruebas se van a realizar y en qué partes del sistema, qué técnicas se pueden emplear y cuánto tiempo va a durar el proceso.
- Un test puede tomar varios días y hasta semanas.

# ¿Qué conocimientos se necesita?

- Diseño e infraestructura de red
- Arquitectura de Comunicaciones TCP/IP
- Servicios de Internet
- Sistemas Operativos
- Seguridad Informática



# Tipos de diagnósticos

- Internos.

*En la actualidad se estima que un 70% de los ataques o intrusiones, se produce desde el interior de las Organizaciones.*

*(Network Associates)*

- Externos.

# Test Externo

- Los PT externos apuntan a analizar el nivel de seguridad real de una organización desde el exterior.
- Solo se dispone de la información pública del cliente, las direcciones IP y los nombres de dominios visibles.
- El principal objetivo es acceder en forma remota a la organización y posicionarse como administrador del sistema.

# Test Externo

## Algunas de las actividades principales:

- Barrido de líneas telefónicas.
- Situación de la seguridad de la Central Telefónica.
- Análisis del sistema de acceso remoto.
- Situación de la seguridad en la conexión a Internet.
- Seguridad en la conexión con otras redes.

# Diagnóstico Externo

- Reconocimiento

Se obtendrán los antecedentes necesarios para verificar la correcta configuración de los servicios externos de la red, servidores y vulnerabilidad a ataques conocidos.

- Ataque Controlado

Ejecución de un conjunto de procesos y pruebas de penetración, siguiendo una metodología y procedimientos propietarios.

# Diagnóstico Externo

- Análisis de Vulnerabilidades

Estudio detallado de cada una de las vulnerabilidades detectadas en las etapas anteriores.

- Informes

Resumen ejecutivo y un documento detallado, indicando cada una de las debilidades encontradas, concluyendo sobre la problemática que conlleva la no solución de éstas y las recomendaciones para cerrar estas brechas.



# Test Internos

- Se focalizan en analizar el nivel de seguridad de una organización a nivel interno.
- Incluyen análisis de la infraestructura de la red, estaciones de trabajo, servidores, aplicaciones y otros.
- Generalmente, se hacen pruebas con privilegios normales. Simulando ser un empleado descontento o un visitante autorizado.

# Diagnóstico Interno

- Trata de demostrar hasta donde puede llegar un usuario que posea los privilegios de un usuario común dentro de la organización.
- Se requiere que la organización provea una computadora típica, un nombre de usuario y una clave de acceso de un usuario común.

# Penetration Test Interno

## Algunas de las actividades principales:

- Pruebas del nivel de seguridad en los dispositivos de red.
- Pruebas de seguridad de los principales servidores.
- Prueba de seguridad de las estaciones de trabajo.
- Prueba a la seguridad de las aplicaciones.

# Diagnóstico Interno

- Levantamiento inicial de Infraestructura

Se persigue obtener el diagrama de la Red, identificación de las máquinas críticas, las distintas direcciones IP internas y los servicios mínimos empleados para la normal operación de la entidad.

- Análisis de Máquinas Críticas

Mediante softwares especializados, se revisa la configuración y vulnerabilidades de los servidores y computadoras identificadas como sensibles.

# Diagnóstico Interno

- Análisis de la Red

Se persigue analizar los distintos protocolos que existen en la Red, compararlos con los identificados en la etapa de levantamiento. Adicionalmente se revisarán falencias de comunicación de datos críticos o confidenciales.

- Informes

Resumen ejecutivo y un documento detallado, indicando cada una de las debilidades encontradas, concluyendo sobre la problemática que conlleva la no solución de éstas y las recomendaciones para cerrar estas brechas.

# Actividades típicas de un test

- Examen de la red.
- Exploración de puertos.
- Reconocimiento de sistemas.
- Sondeo de servicios.
- Búsqueda de *exploits*.
- Verificación manual y automática de las vulnerabilidades.
- Pruebas limitadas a aplicaciones.
- Pruebas de ACL y cortafuegos.
- Test de IDS.





# Cajas negras y blancas

- Negra: sin conocimientos ni facilidades de la infraestructura que se comprueba.
- Blanca: con conocimientos y facilidades en la red comprobada.

¿Cuál es la forma más apropiada?.

# Principios

- El analista inicialmente debe probar sin privilegios en un ambiente de caja negra y luego probar de nuevo con privilegios en el mismo ambiente.
- Los analistas deben conocer sus herramientas, de dónde vienen, cómo trabajan, y haberlas probado en un área restringida.
- La aplicación de pruebas para DoS, puede realizarse únicamente con permiso explícito.



# Principios

- Las vulnerabilidades de alto riesgo deben ser reportadas al cliente con una solución práctica tan pronto sean encontradas.
- Prohibidas las pruebas de DDoS por Internet.





# Principios

- Los informes deben incluir soluciones prácticas orientadas a resolver los problemas descubiertos.
- Deben incluir todos los hallazgos desconocidos y deben ser identificados como tales.
- Deben especificar claramente todas las barreras de seguridad encontradas, no sólo las fallidas.



# Políticas de ejecución

- Deben realizarse PT internos y externos.
- La frecuencia depende de las características de la organización.
- Los auditores pueden ser externos o internos a la organización.
- La corrección puede realizarse por el mismo equipo auditor o por otro equipo, ya sea externo o interno.

# Aspectos legales y éticos

- Se hace necesario que la organización firme dos cartas a la empresa que realiza el PT.
- Se trata de un convenio de confidencialidad y una carta de autorización.





# Metodologías

- ✓ Aplicación de Test de Penetración a Organizaciones, del Instituto SANS.
- ✓ Guía de Pruebas de Seguridad en RED, del NIST.
- ✓ Metodología OSSTMM, de ISECOM.

# Metodología

## Fases

Open Source Security Testing Guide:  
([www.osstmm.org](http://www.osstmm.org))

- Fase de Descubrimiento.
- Fase de Exploración.
- Fase de Evaluación.
- Fase de Intrusión.

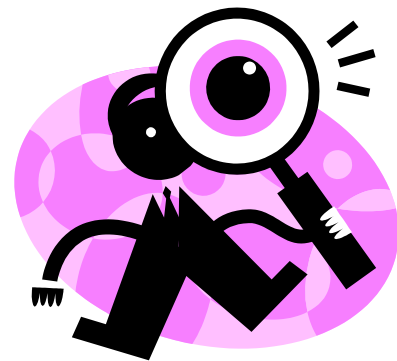


INSTITUTE FOR SECURITY AND OPEN  
METHODOLOGIES

# Descubrimiento

En esta fase, se recolecta la mayor cantidad de evidencia posible sobre la Empresa para la cual se van a realizar las pruebas:

- Rangos de direcciones IP asignados
- Dirección física de la empresa
- Números telefónicos



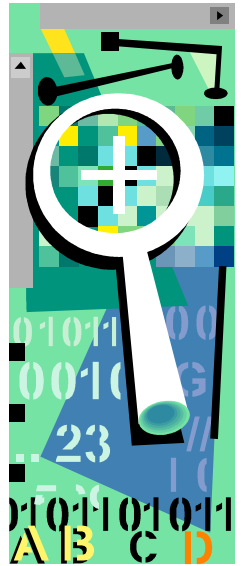
# Descubrimiento

- Nombres de personas y cuentas de correo electrónico
- Fuentes de información
- Análisis de la página WEB
- Existencia de redes inalámbricas
- Servidores
- Máquinas críticas



# Exploración

- En esta etapa se aplican técnicas no intrusivas para identificar todos los blancos potenciales.
- Incluye el análisis de protocolos, reconocimiento de plataforma y barreras de protección.
- Detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones web.



# Exploración

Las tareas que predominan en esta etapa son:

- Detección de módems activos
- Confirmación de rangos de direcciones IP
- Detección de equipos activos e identificación de Sistemas Operativos
- Detección de servicios activos e identificación software y versiones
- Detección de barreras de protección
- Análisis de características de configuración en redes WiFi

# Evaluación

Durante esta etapa se realizan las evaluaciones de seguridad en todos los posibles niveles:

- Ejecución de herramientas de reconocimiento de vulnerabilidades.
- Búsqueda manual de vulnerabilidades.
- Enumeración de usuarios y datos de configuración.
- Evaluación de problemas particulares de la plataforma.

# Intrusión

- Se focaliza en realizar pruebas de los controles de seguridad y, ataques a las vulnerabilidades identificadas por medio de secuencias controladas.



# Intrusión

¿Qué datos tenemos?

- Nombres de usuarios de diversos equipos
- *Exploits* remotos
- Líneas telefónicas que admiten el acceso remoto
- Ubicación y características de nodos inalámbricos
- Mapa de la plataforma
- Aplicaciones web vulnerables
- Recursos compartidos

# Intrusión

¿Y con esto qué podemos hacer?

- Fuerza bruta sobre servicios que autenticuen vía nombre de usuario/contraseña.
- Ejecución de *exploits* remotos.
- Prueba de usuarios y contraseñas por defecto en accesos telefónicos y otros.
- Ataques a la clave de encriptación WEP.
- Explotación de vulnerabilidades en aplicaciones Web.
- Búsqueda de información de acceso en recursos compartidos.
- Ingeniería Social.
- .....

# ¿Qué se busca?

## **INFORMACIÓN DE USUARIO**

- Cuentas compartidas.
- Contraseñas triviales.
- Envejecimiento de las contraseñas.
- Cuentas de administración por defecto.

# ¿Qué se busca?

## INFORMACIÓN NO PROTEGIDA

- Carpetas compartidas indiscriminadamente
- Bajo uso del cifrado
- Versiones antiguas del sistema operativo
- Sistemas sin parches
- Instalaciones por defecto
- Inundación de programas malignos





# ¿Qué se busca?

## **MEDIDAS DE SEGURIDAD**

- Desconocimiento y desinterés de los usuarios
- No empleo de logs
- No empleo de herramientas de administración
- Ausencias de políticas
- Una sola persona con todo el poder



# Resultados

- Salvo algunos casos, las organizaciones esperan que los resultados del PT sean positivos para ellos (que no se encuentren vulnerabilidades o problemas).
- La mayoría de las veces las organizaciones no están preparadas para recibir noticias negativas.

# Herramientas

- Los intrusos cuentan con herramientas efectivas como los *scanners*, *cracking* de contraseñas, software de análisis de vulnerabilidades, los *exploits* y la ingeniería social....
- Un administrador cuenta con todas ellas empleadas para bien.

# Concluyendo...Importante



- Utilizar la tecnología para crear soluciones de seguridad estables.
- Expandir el conocimiento a todos los usuarios potenciales y crear más expertos.
- Aplicar políticas bien definidas acorde con cada lugar.

# Sitios Relacionados

- <http://www.criptored.upm.es>
- <http://www.hispasec.com>
- <http://www.virusprot.com>
- <http://www.cert.org>
- <http://www.linuxsecurity.com>
- <http://www.pgp.com>
- <http://www.infosyssec.net>
- <http://www.hispasec.com/>
- <http://www.incidents.org/>
- <http://www.sans.org/newlook/home.htm>
- <http://www.secnet.com/>
- <http://www.incidents.org/>
- <http://www.sans.org/newlook/home.htm>
- <http://www.securiteam.com/>
- <http://www.gocsi.com/>
- <http://www.insecure.org>
- <http://www.instisec.com/>
- <http://www.securityfocus.com/>
- <http://www.secinf.net/>
- <http://www.psionic.com/abacus/>
- ...

# Materiales empleados

- Ardita, Julio C., “Del Penetration Test a la realidad”. VII Seminario Iberoamericano de Seguridad en Tecnologías de la Información. La Habana, 2004.
- AusCERT, AHTCC, y otros. “2005 Australian Computer Crime and Security Survey”. <http://www.auscert.org.au/>, 2005.
- Comer, D. E., “Internetworking with TCP/IP. Volume I: Principle, Protocols and Architecture”. 4ta Edición. Prentice Hall, 2000.
- CSI, FBI. “2005 CSI/FBI Computer Crime and Security Survey”. <http://www.gocsi.com/>, 2005
- Herzog, Pete. “OSSTMM 2.1, Manual de la Metodología Abierta de Testeo de Seguridad”. ISECOM, 2003.
- Wack, John; Tracy, Miles; Souppaya, Murugiah. “Guideline on Network Security Testing”. Publicación Especial del NIST 800-42 , 2003.

# Materiales empleados

- Fraser, Barbara (Editor). “Site Security Handbook”, RFC 2196. IETF. 1997.
- Grance, Tim; Kent, Karen; Kim, Brian. “Computer Security Incident Handling Guide”. National Institute of Standards and Technology (NIST), 2004. Special Publication 800-61.
- Information Technology Center. “FCC: Computer Incident Response Guide”. Federal Communications Commission, December 2001.
- Killcrece, Georgia (Maintainer). “CERT/CC Overview Incident and Vulnerability Trends: Incident Handling”. CERT/CC, Software Engineering Institute, Carnegie Mellon University. 2002.
- West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; Zajicek, Mark. “Handbook for Computer Security Incident Response Teams (CSIRTs)”. Software Engineering Institute, Carnegie Mellon University. *2nd Edition, April 2003.*

# Materiales empleados

- Anderson, Michael R. .”Electronic Fingerprints, Computer Evidence Comes Of Age”. <http://www.forensics-intl.com/>. 1997.
- Anderson, Michael R..”Defending Against Junk Science Attacks”. <http://www.forensics-intl.com/>. 2003.
- Grance, Tim; Chevalier, Suzanne; Kent, Karen; Dang, Hung. “Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response”. National Institute of Standards and Technology (NIST), 2005. Special Publication 800-86 (Draft).
- NTI Technologies Inc., “Computer Evidence Processing Steps”. <http://www.forensics-intl.com/>. 2004.
- Wright, Timothy E.. “A Method for Forensic Previews”. <http://www.securityfocus.com/>. 2005.