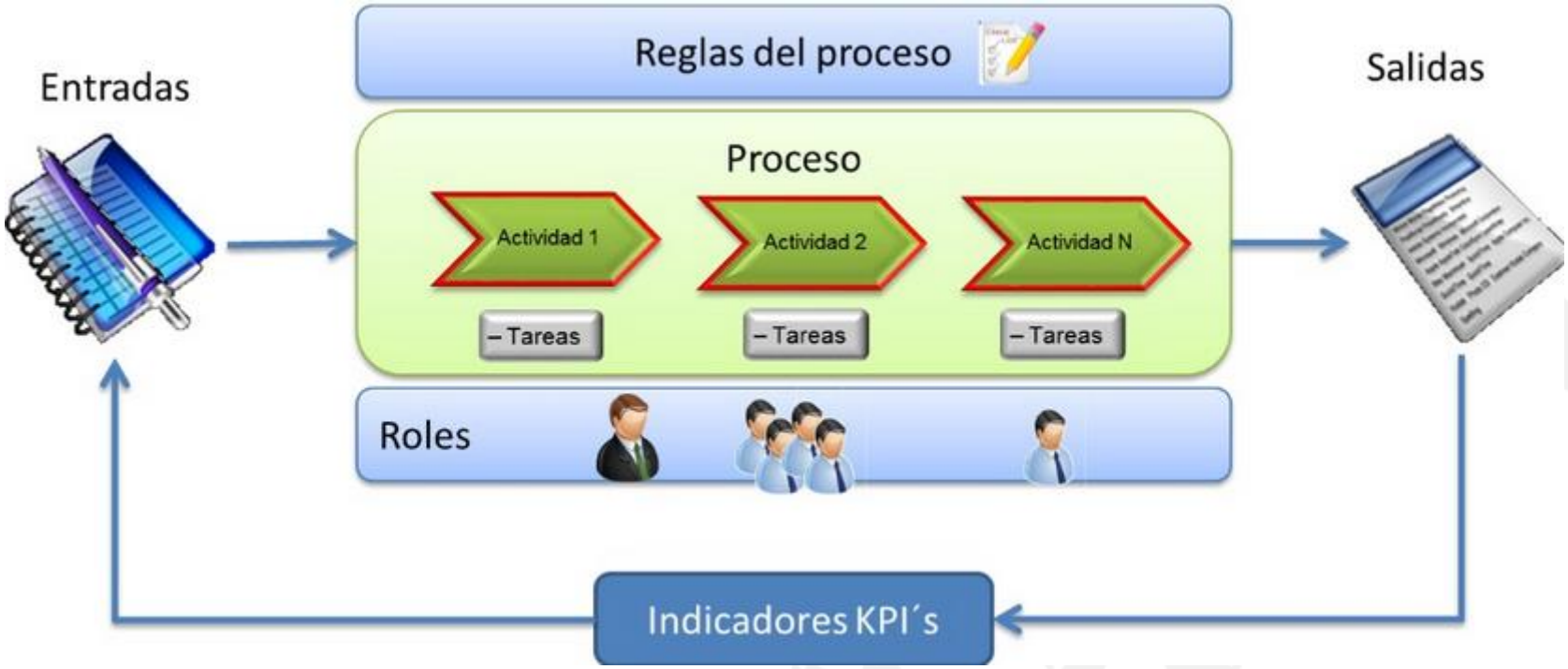
UNIVERSIDAD D SEVILLA

Auditoría de Sistemas Informáticos y Análisis de Vulnerabilidades Web

Dr. Rafael Martínez Gasca
Grupo de Investigación IDEA, LSI.
Universidad de Sevilla
CISO en INSEGUS

- Fundamentos empresariales
- Proceso de auditoría de seguridad de la información
  - Establecer el alcance y objetivos de la auditoría de seguridad
  - Seleccionar las herramientas para la auditoría

¡¡Auditoría es un proceso!!



Calidad

Proceso de auditoría de Seguridad de la Información.
Calidad del Proceso

- ISO/IEC 9001:2015 Clausula 4.4) **Describir los procesos de negocio que operan y con se relacionan con otros procesos necesarios** para el Sistema de gestion de la calidad. Incluirán:
  i. ¿ **Qué (S) proveedores** tendrá para tu proceso?
  ii. ¿ **Qué (I) Inputs son necesarios** para tu proceso de auditoría? (materiales, información, roles)
  iii. ¿ **Qué (P) tareas del proceso** transforman las entradas en salidas?
  iv. ¿ **Qué (O) Outputs** resultan de tu proceso de auditoría?
  v. ¿ **Qué (C) Clientes** reciben las salidas del proceso de auditoría?

Plan Director de la Seguridad de la Información

Política de Seguridad

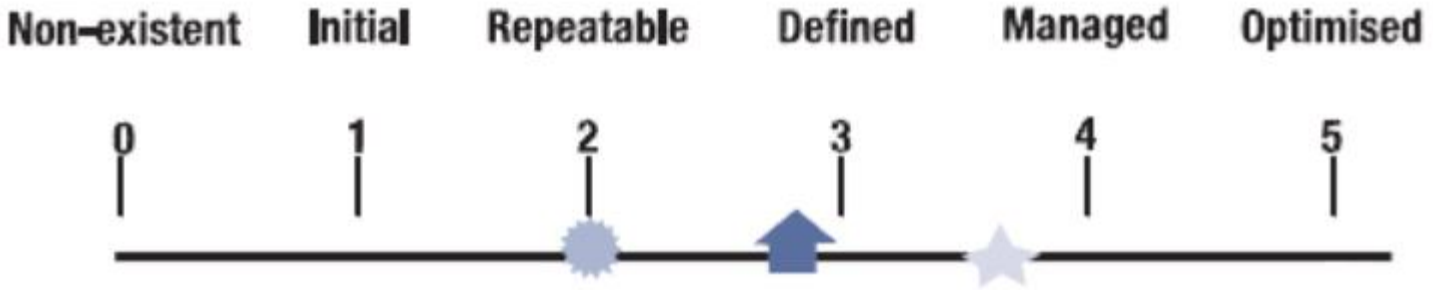
Proceso Global de Seguridad

ISO/IEC 21827:2008 Information Technology – Systems Security Engineering – Capability Maturity Model). SSE-CMM

Funcional: ISO/IEC 27001:2013

- **Plan Director de Seguridad de la Información (PDSI):**
  - **Definición y priorización de un conjunto de proyectos en materia de seguridad de la información** con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, **a partir de un análisis de la situación inicial.**
  - **Debe estar alineado con los objetivos estratégicos de la empresa.**
  - **Debe incluir las buenas prácticas y políticas en seguridad de la información.**

- **Grado de Madurez en seguridad de la información para un cuadro de mando (dashboard)** para la empresa

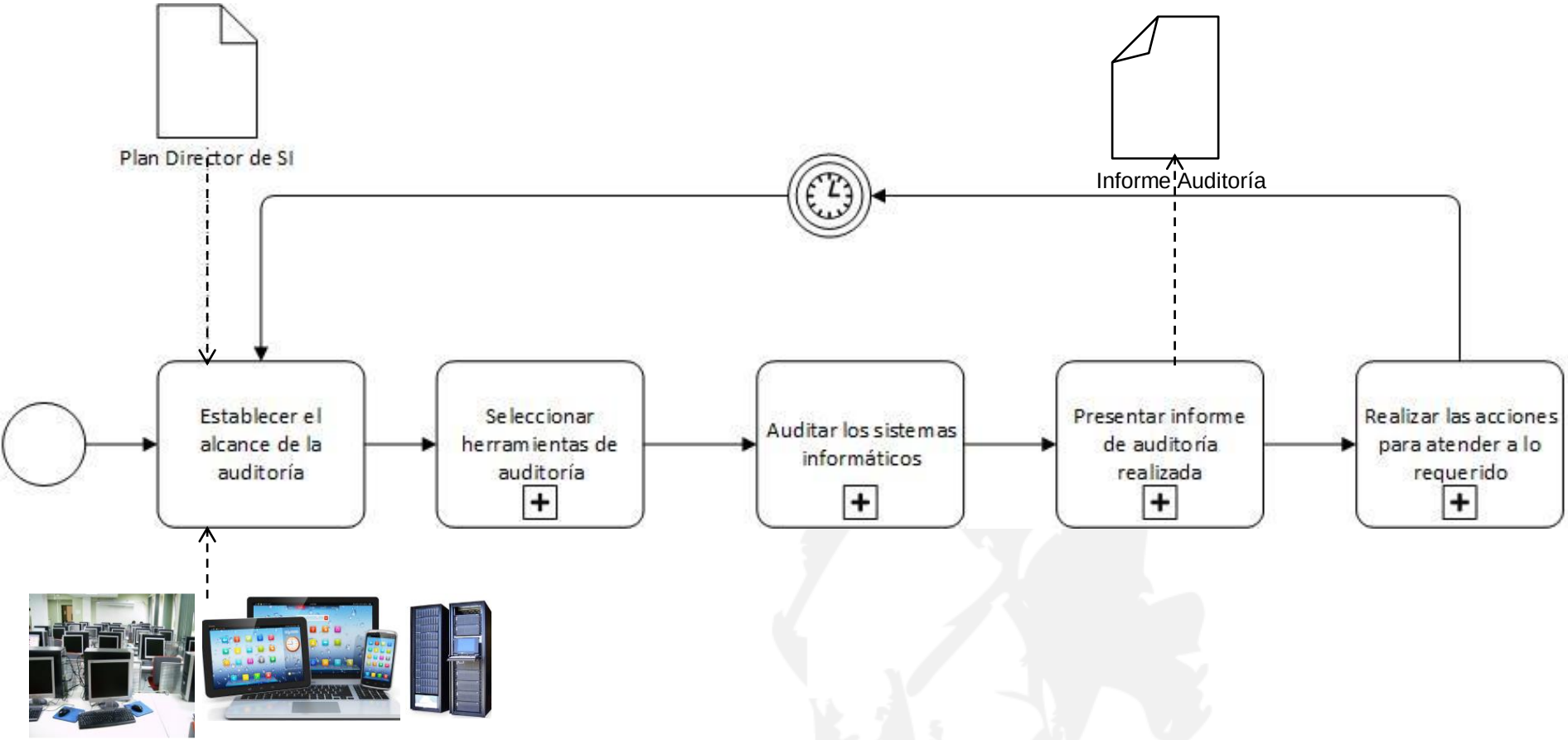


- ○ Estado actual
- ↑ Estado del sector
- ❖ Estado objetivo

0. No se aplica gestión de procesos
1. Los procesos son ad hoc y desorganizados
2. Los procesos siguen patrones regulares
3. Los procesos son documentados y comunicados
4. Los procesos son monitorizados y medidos
5. Buenas prácticas se supervisan y automatizan

- Fundamentos empresariales
- Proceso de auditoría de seguridad de la información
  - Establecer el alcance y objetivos de la auditoría de seguridad
  - Seleccionar las herramientas para la auditoría
    - Lynis
    - Conan Mobile
    - Web Application Scanner y Entornos Web Vulnerables
    - Entornos Vulnerables

Proceso de auditoría de Seguridad de la Información.
Modelo del Proceso



- **Muy importante**
  - Que la auditoría sea **precisa, objetiva, clara, concisa, constructiva y oportuna.**
  - Que se **cumplan los objetivos de la auditoría** para los sistemas informáticos incluidos en el alcance.
  - Que la auditoría sea **debidamente documentada incluyendo las propuestas de mejora y que se conserve la evidencia apropiada de la revisión.**
  - Que los auditores cumplan con **las normas profesionales de buenas prácticas.**
  - **Una vez realizada la auditoría es NECESARIO DISPONER DE UN BUEN PLAN DE ACCIONES DE HARDENING DE LOS SISTEMAS INFORMÁTICOS (INCLUIDA APLICACIONES)**

Proceso de auditoría de Seguridad de la Información.
Comparación del proceso con otros

Vulnerability Assessment	Penetration Testing, Pentest o Hacking Ético	Auditoría de Seguridad IT
Identificación de fallos de seguridad	**Identificación de fallos de seguridad**	**Identificación del cumplimiento o conformidad**
Foco: debilidades conocidas. Puede ser automatizado, No requiere ser un experto necesariamente.	**Foco: debilidades conocidas y no conocidas Requiere tester muy preparados y expertos. Conlleva una tremenda carga legal en ciertos países/organizaciones.**	**Foco: en políticas de seguridad y procedimientos** **Usado para proporcionar pruebas en la industria de cumplimiento de las regulaciones y buenas prácticas (COBIT, ISO 27001, ENS).**
Enumeración y evaluación de las vulnerabilidades	**Explotación de las vulnerabilidades para mostrar los fallos.**	**Enumeración de No conformidades**
Ejecutado al inicio de un plan de seguridad para adoptar medidas correctivas	**Efectuado al final del plan de SI para verificar la seguridad alcanzada.**	**Ejecutado en los plazos que indiquen las regulaciones legales o normas industriales**
Metodologías para realizar análisis de riesgos ISO/IEC 27005:2018, (Information technology — Security techniques — Information security risk management), DAST	Metodologías para realizar un test de penetración de seguridad, más conocida la **OSSTMM** 3:2010 (**Open Source Security Testing Methodology Manual) del ISECOM,**	**Metodologías de auditorías de Seguridad IT ISO 27007:2017 (Security techniques Guidelines for information security management systems auditing)**

Proceso de auditoría de Seguridad de la Información.
Establecer el alcance y objetivos de la auditoría

- Establecer el alcance de la auditoría
  - **Dispositivos de sobremesa de la empresa**
  - **Dispositivos móviles (Smartphones y Tablet),**
  - **Servidores Web y aplicaciones Web empresariales**, es necesario **la autorización de la empresa** para llevar a cabo las auditorías a dichos sistemas.

- Fundamentos empresariales
- Proceso de auditoría de seguridad de la información
  - Establecer el alcance de auditoría
  - Seleccionar las herramientas para la auditoría
    - Lynis
    - Conan Mobile
    - Web Application Scanners y Entornos Web Vulnerables

Seleccionar las herramientas para la auditoría.
Lynis

- **Objetivos**:
  - **Hardening de sistemas,**
  - **Testing de cumplimiento (ejemplos. PCI, HIPAA, SOX),**
  - **Auditoría de seguridad,**
  - **Pentesting y Detección de Vulnerabilidades**.
- **Contextos:** Sistemas Operativos basados en Linux, macOS, o
- **Proyecto** open source con licencia GPL desde 2007.
- **Beneficiaros:** Desarrolladores, administradores de sistemas, auditores TI y Pentesters.

- **Proceso de Escaneado Lynis:**
  - Inicialización
  - Ejecutar comprobaciones básicas, tales como la propiedad de los ficheros
  - Identificar el sistema operativo y las herramientas disponibles
  - Buscar los componentes software disponibles
  - Comprobar la última versión de Lynis
  - Ejecutar los plugins habilitados
  - Ejecutar de los test de seguridad por categorías
  - Llevar a cabo la ejecución de tus test personales. (Plugin opcional)
  - Informar del estado de seguridad tras el escaneo

Seleccionar las herramientas para la auditoría.
Lynis

```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts...                [ OK ]
  - Checking UIDs...                                [ OK ]
  - Checking chkgrp tool...                         [ FOUND ]
  - Consistency check /etc/group file...            [ OK ]
  - Test group files (grpck)...                     [ OK ]
  - Checking login shells...                        [ WARNING ]
  - Checking non unique group ID's...               [ OK ]
  - Checking non unique group names...              [ OK ]
  - Checking LDAP authentication support            [ NOT ENABLED ]
  - Check /etc/sudoers file                         [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] Shells
------------------------------------
  - Checking console TTYs...                        [ WARNING ]
  - Checking shells from /etc/shells...
    Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] File systems
------------------------------------
  - [FreeBSD] Querying UFS mount points (fstab)...  [ OK ]
  - Query swap partitions (fstab)...                [ OK ]
  - Testing swap partitions...                      [ OK ]
  - Checking for old files in /tmp...               [ WARNING ]
  - Checking /tmp sticky bit...                     [ OK ]
```

- Fundamentos empresariales
- Proceso de auditoría de seguridad de la información
  - Establecer el alcance y objetivos de la auditoría de seguridad
  - Seleccionar las herramientas para la auditoría
    - Lynis
    - Conan Mobile
    - Web Application Scanners y Entornos Web Vulnerables

Seleccionar las herramientas para la auditoría.
Conan Mobile

- **Análisis de seguridad de dispositivos Android**
  - la configuración de seguridad,
  - las aplicaciones instaladas,
  - los permisos que usan estas aplicaciones,
  - las conexiones a Internet que realizan y
  - Mostrar eventos relevantes de seguridad (envío de SMS Premium o llamadas a números de tarificación especial, conexión a redes Wi-Fi inseguras, etc).
  - Necesita conexión a Internet

- Proceso de auditoría de seguridad de la información
- Establecer el alcance de auditoría
- Seleccionar las herramientas para la auditoría
  - Lynis
  - Conan Mobile
  - Web Application Scanners y Entornos Web Vulnerables

Seleccionar las herramientas de Auditoría.
Web Application Scanners

- Herramientas de **Dynamic Application Security Testing (DAST)**,
  - **Nikto**
  - **W3af**
  - **WebScarab NG**
  - **ZAP**
  - **Paros Proxy**
  - **Sqlmap**
  - **Wikto**
  - **Websecurity**
  - **WAPITI**
  - **IBMAppscan**
  - **Netsparker**
  - **NTOSpider**
  - **HPWebInspect**
  - **Acunetix**
  - **Bursuite**
  - **SyHunt**
  - **N-Stalker**

Seleccionar las herramientas de auditoría.
Web Application Scanners

Problemas con servidores que responden con error en conexiones https???

Seleccionar las herramientas de Auditoría.
Web Application Scanners

Wapiti

```
andres@PCMaxwell:~/Descargas/wapiti-2.3.0$ sudo wapiti http://localhost:5080/soporte
[sudo] password for andres:
Wapiti-2.3.0 (wapiti.sourceforge.net)

 Note
========
Este escaneo se ha guardado en el archivo /home/andres/.wapiti/scans/localhost:5080.xml
Puedes usarlo para realizar ataques sin escanear de nuevo el website mediante el parámetro "-k"
[*] Cargando modulos:
        mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_permanentxss, mo
d_nikto

[+] Lanzando módulo exec

[+] Lanzando módulo file

[+] Lanzando módulo sql

[+] Lanzando módulo xss
Vulnerabilidad XSS en http://localhost:5080/soporte/swf mediante inyección en el parámetro swf
  URL maliciosa: http://localhost:5080/soporte/swf?swf=String.fromCharCode%280%2Cw8r5hdvcyx%2C1%29

[+] Lanzando módulo blindsql

[+] Lanzando módulo permanentxss

Informe
------
Se ha generado un informe en el fichero /home/andres/.wapiti/generated_report
Abrir /home/andres/.wapiti/generated_report/index.html con el navegador para ver el informe
```

- **Entornos para aprendizaje**
  - **OWASP Mutillidae II**
  - **Web Goat OWASP**
  - **Damn Vulnerable Web Application**
- **Web Application Scanners**: Encuentran automáticamente vulnerabilidades en aplicaciones Web con 3 componentes:
  - Crawler
  - Inyector de Fallos
  - Analizador
- Ventajas: rapidez y automatización
- Inconvenientes: falsos positivos, falsos negativos

- **WebGoat 8.0** de OWASP
  - Entorno de prueba para numerosas vulnerabilidades tales como **fallos de Inyección**, **Cross-Site Scripting (XSS)**, **Denial of Service**, **Control de acceso**, **Seguridad de Hilos**, **Manipulación de campos ocultos**, …

- **Foro personal** donde los usuarios pueden escribir, leer y responder a los mensajes

¿Cuestiones?