Seguridad de los Sistemas Informáticos

Tema 2. Políticas de seguridad

Escuela de Ingeniería Informática
Universidad de Oviedo

Gestión de la seguridad de la información

- La gestión de la seguridad de la información debe realizarse mediante un proceso **sistemático**, **documentado**, **conocido** y **asumido** por toda la organización.
- Este proceso se denomina **Sistema de Gestión de la Seguridad de la Información** (SGSI / ISMS). Su propósito es:

  *"Garantizar que los **riesgos** de la seguridad de la información sean **conocidos, asumidos, gestionados y minimizados** por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los **cambios que se produzcan** en los riesgos, el entorno y las tecnologías".*

- El propósito de un Sistema de Gestión de Seguridad de la Información NO es garantizar la seguridad absoluta, ya que ésta nunca podrá serlo, si no asegurar que la información de la organización está protegida frente a la pérdida de Confidencialidad, Integridad y Disponibilidad.

Elementos de un SGSI

- Comprende la **política**, la **estructura organizativa**, los **procedimientos**, los **procesos** y los **recursos** necesarios para implantar la gestión de la seguridad de la información.
- Un SGSI implica que la organización en la que se ha implantado ha:
  - **Estudiado** los riesgos a los que está sometida toda su información.
  - **Evaluado** qué nivel de riesgo asume.
  - **Implantado controles** (no sólo tecnológicos, sino también organizativos) para aquellos riesgos que superan dicho nivel.
  - **Documentado** las políticas y procedimientos relacionados.
  - Entrado en un proceso continuo de **revisión y mejora** de todo el sistema.

Ventajas de la implantación de un SGSI

1. **Reducción de riesgos** debido al establecimiento y seguimiento de los controles establecidos sobre ellos. Con ello se logran reducir las amenazas hasta alcanzar un nivel asumible por la organización → si se produce una incidencia los daños se minimizan.
2. **Ahorro de costes** derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.
3. La seguridad en la organización pasa a tener un **ciclo de vida metódico** y controlado en el que participa toda la organización.
4. La organización se asegura del cumplimiento del **marco legal** que la protege respecto a ciertos aspectos que no se hubiesen considerado previamente.

   https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/medidas_seguridad/index-ides-idphp.php

   http://administracionelectronica.gob.es/ctt/ens

5. Contribuye a mejorar la competitividad en el mercado. Actualmente, las administraciones públicas están empezando a exigir certificados relacionados con la seguridad a las empresas que quieran acceder a concursos públicos de productos o servicios relacionados con sistemas de información.

Legislación española relativa a la Seguridad

- Tanto en Europa como en España, los principales delitos informáticos que se contemplan en la legislación se engloban en cuatro grupos:
  - Delitos contra la **intimidad**, en los que se produce un tratamiento ilegal de los datos de carácter personal.
  - Delitos relativos a la difusión de **contenidos ilegales** en la red.
  - Delitos **económicos**, relacionados con el acceso (no) autorizado a sistemas informáticos para llevar a cabo fraude, sabotaje o falsificación.
  - Delitos contra la **propiedad intelectual**, vinculados con la protección de programas de ordenador, bases de datos y derechos de autor.
- Cumplir con la legislación vigente en España es uno de los requisitos que se deben satisfacer para implantar y certificar un SGSI.
- Algunas leyes españolas: Ley Orgánica 15/99 de protección de Datos de Carácter Personal (LOPD), Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio electrónico (LSSI), Ley 32/2003 General de Telecomunicaciones, Ley 59/2003 de Firma Electrónica, Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios públicos,…

ISO /IEC 27000

- Además de leyes, existe un conjunto de normas internacionales elaboradas por ISO (Organización Internacional de Normalización) / IEC (Comisión Electrotécnica Internacional)
- Con el fin de proporcionar un **marco de Gestión de la Seguridad de la Información** aplicable en cualquier tipo de organización, se ha creado un conjunto de normas bajo el nombre **ISO/IEC 27000**.
- Son numerosas las normas recogidas bajo este epígrafe, siendo algunas de las más importantes:
  - ISO/IEC 27001: contiene los requisitos para establecer, implementar, operar, supervisar, mantener y mejorar un SGSI. Recoge los componentes del sistema, los documentos mínimos que forman parte de él, los registros, los controles a implementar y las medidas de seguridad adaptadas a las necesidades de cada organización. Esta norma es la única de la familia 27000 que es **certificable**.
  - ISO/IEC 27002: es una guía de buenas prácticas o recomendaciones sobre las medidas a tomar para asegurar los sistemas de información de una organización. Describe 14 dominios o áreas de actuación, 35 objetivos de control o aspectos a asegurar dentro de cada área y 114 controles o mecanismos para asegurar los objetivos.

http://www.iso27000.es/download/ControlesISO27002-2013.pdf

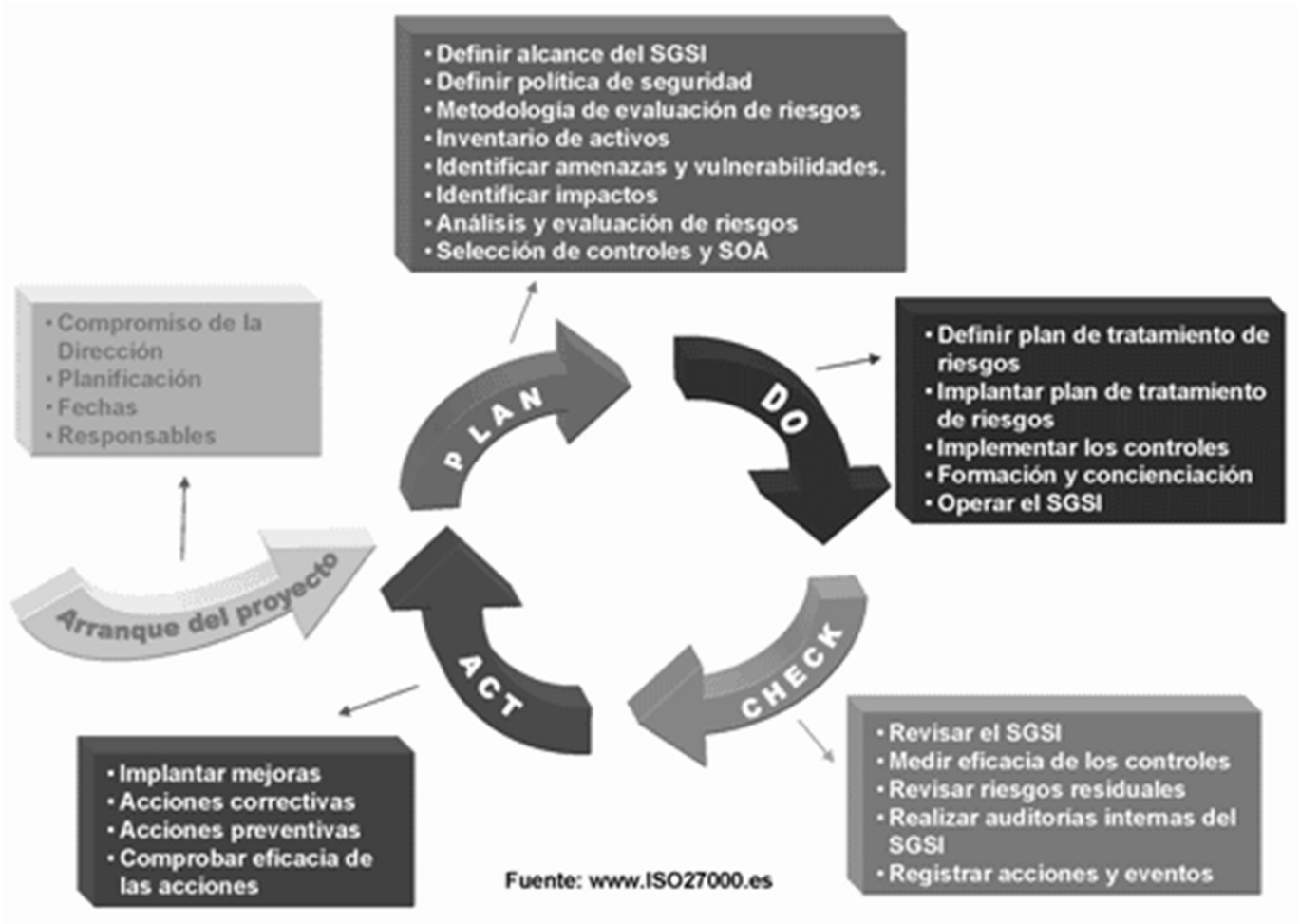
Certificación ISO 27001

- Tras la implantación de la norma ISO 27001, la organización puede certificarse en dicha norma. En España es AENOR (Asociación Española de Normalización y Certificación) la principal agencia certificadora.

  http://www.aenor.es/aenor/inicio/home/home.asp

- Y parece que nos lo estamos tomando en serio…

Etapas en la implantación de un SGSI. Ciclo de Deming



- **Plan** (Planificar) Establecer el SGSI
- **Do** (Hacer) Implementar y utilizar el SGSI
- **Check** (Verificar) Monitorizar y revisar el SGSI
- **ACT** (Actuar) Mantener y mejorar el SGSI

http://www.iso27000.es/sgsi_implantar.html

1 Definir el alcance del SGSI

- El diseño de un SGSI depende de los objetivos, necesidades y estructura de la organización.
- Estos elementos son los que van a definir las áreas de la misma que van a verse involucradas; puede que la implantación del SGSI sólo sea necesaria en un departamento, una sede en concreto o área de negocio de la organización.
- El tiempo de implantación de un SGSI varía en función del tamaño de la organización, el estado inicial de la seguridad de la información y de los recursos destinados a ellos, pero puede estimarse su duración entre 6 meses y un año.

Definir el alcance del SGSI - Ejemplo

Empresa de impresión 3D de piezas para maquinaria industrial.

- 800 empleados entre operarios, personal de administración…
- Departamentos
  - Nóminas: 4 personas
  - Recursos humanos: 3 personas
  - Sistemas: 5 personas
  - Diseño industrial: 8 personas
  - Producción: resto del personal

Se decide implantar un SGSI.
Alcance: ¿Todos los departamentos? → Aquellos que manejan información sensible en la empresa: Nóminas, RRHH, Sistemas y Diseño. Total: 20 empleados + dirección de la empresa.

2 Definir la política de seguridad

- Son las **directrices y objetivos generales** de una organización relativos a la seguridad, expresados formalmente por la dirección general.
- Una política de seguridad expresa en su contenido la intención y los objetivos de seguridad de una organización. Las políticas de seguridad de una organización son con frecuencia muy complejas y con muchas personas afectadas en su desarrollo y mantenimiento.
- La política de seguridad forma parte de la política general y debe ser aprobada por la alta dirección.
- Incluye:
  - Objetivos y alcance general de seguridad.
  - Apoyo expreso de la dirección.
  - Explicación de los valores de seguridad de la organización.
  - Definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información.
  - Referencias a documentos que puedan respaldar la política.

2 Definir la política de seguridad- Ejemplo

Objetivo:
Definir las pautas de propósito general para asegurar una adecuada protección de la información del DAPRE.
Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Aplicabilidad:
Estas son políticas que aplican a la Alta Dirección, Ministros Consejeros, Consejeros Presidenciales, Directores, Secretarios, Jefes de Oficina, Jefes de Área, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales del DAPRE.

Directrices:

- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo de control interno.
- Todo aplicativo informático o software debe ser comprado o aprobado por el Área de Información y Sistemas en concordancia con la política de adquisición de bienes de la entidad de acuerdo con lo definido en el proceso **C-BS-07 Adquisición de Bienes y Servicios**.
- El DAPRE debe contar con un *firewall* o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en *outsourcing* o de terceros.
- La conexión remota a la red de área local del DAPRE debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice el Área de Información y Sistemas.
- Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del DAPRE.

http://wp.presidencia.gov.co/sitios/dapre/sigepre/manuales/M-TI-01%20Manual%20general%20Sistema%20de%20Seguridad%20de%20la%20Informacion.pdf

PLAN

3 Definir activos

- **Activos**:
  - Recursos del sistema necesarios para que la organización funcione y susceptibles de ser protegidos.
  - Información, edificios, sistemas informáticos, aplicaciones, bases de datos, usuarios, personal, redes de comunicaciones, soportes de información…
- Inventario de activos
  - Descripción, localización y propietario.
- Análisis de dependencias entre los activos.
- Valoración de los activos en función de la relevancia para la organización y el impacto que pueda causar una incidencia sobre el mismo.

PLAN

3

Definir activos- Ejemplo

4 Análisis de riesgos

- Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Existen muchas metodologías de evaluación de riesgos aceptadas; un ejemplo es MAGERIT para la administración pública española. ISO 27001 no impone ninguna
- Cálculo de los niveles de **riesgo de los activos** identificados en el paso anterior:
  - Identificar las **amenazas** a los activos dentro del SGSI.
  - Identificar las **vulnerabilidades** que podrían ser explotadas por las amenazas.
  - Identificar y valorar los impactos (coste) que pueden tener en los activos los fallos de seguridad.
  - Valorar la probabilidad realista de ocurrencia de fallos de seguridad a la luz de las amenazas, las vulnerabilidades y los impactos asociados.
  - Estimar los niveles de riesgo con un método objetivo.
  - Determinar si los riesgos son aceptables o requieren de un tratamiento.

AMENAZA	VULNERABILIDAD
Ataque por un pirata informático	Problema de configuración. Permite realizar conexiones a puertos sensibles dándole la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.
Ataque por un pirata informático	Cross Site Scripting (XSS). El sistema de validación de HTML permite ejecutar scripts maliciosos
Ataque por un pirata informático	Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP
Calentamiento del equipo	Falta de monitores de las condiciones ambientales.
Divulgación de información sobre el activo	Instalación predeterminada de TOMCAT
Incendio.	Ausencia de extintores en el cuarto.

Activo	Amenaza	Vulnerabilidad	Impacto			Probabilidad	Riesgo	Clasificacion del riesgo
			Confidencialidad	Integridad	Disponibilidad			
Laptop	Robo	Portabilidad	2	3	1	1	3	
Servidor Archivos	Virus	Antivirus no actualizado	3	3	3	1	4	
Contrato Clientes	Robo	No hay caja fuerte	4	4	1	2	5	
Datos de los clientes	Divulgar	Acceso no controlado	5	4	3	2	6	

5 Gestión de riesgos

- Identificar y evaluar alternativas para tratar los riesgos.
- El objetivo puede ser:
  - Eliminarlo (Ej. dar de baja un servidor)
  - Mitigarlo (aplicar un control).
  - Transferirlo a un tercero (subcontratar el servicio)
  - Asumirlo.
- Finalmente se analiza el riesgo residual:
  - Nivel de riesgo existente después de la implantación de salvaguardas.

6 Definir los controles y procedimientos

- Un control es el conjunto de medidas, acciones y/o documentos que permiten **cubrir y auditar** cierto riesgo.
- Un procedimiento es el conjunto de instrucciones necesarias para llevar a cabo una tarea o proceso asociado a la implementación de los controles de seguridad y las tareas de administración del SGSI. Debe reflejar fielmente los pasos a seguir para la realización de las tareas, y debe ser conciso y claro para que no se cometan errores.
- Recordemos que ISO 27002 recoge los 133 controles aplicables como mínimo. Ej:
  - Control de acceso (*Area de actuación*)
    - Gestión de acceso de usuario (*Obj. de control*)
      - Gestión de contraseñas de usuario (*Control)*
        - Se formarán mediante combinación de dígitos, letras y caracteres especiales
        - Se alternarán aleatoriamente letras mayúsculas y minúsculas
        - Se cambiarán periódicamente sin regla secuencial de cambio
        - No reutilizarán contraseñas

- Los objetivos de control, los controles seleccionados del estándar, las razones por las cuales han sido seleccionados y las medidas de seguridad adoptadas se recogerán en un documento denominado **SOA** (Declaración de Aplicabilidad / Statement of Applicability).

7 Plan general de seguridad

- Todas las actividades desarrolladas hasta este momento generan un documento final que plasma las acciones que van a llevarse a cabo para implantar los controles de seguridad que se han escogido para el SGSI.
- El plan recogerá las acciones a corto, medio y largo plazo e incluirá:
  - los objetivos de seguridad,
  - las responsabilidades,
  - los presupuestos,
  - estimaciones de recursos humanos y materiales y
  - el calendario de las acciones.

8 Implantar el plan de tto. de riesgos

- Implantar controles y procedimientos que permitan una rápida detección y respuesta a los incidentes de seguridad.
- Asignación de recursos, responsabilidades y prioridades.

9 Formación y concienciación

- Procurar programas de formación y concienciación en relación a la seguridad de la información al personal de la organización.
- Para que la implantación de un SGSI se pueda llevar a cabo con éxito es fundamental que el personal esté concienciado de la importancia de la seguridad de la información para su trabajo y para la organización.
- También debe estar formado para llevar a cabo sus tareas y responsabilidades adecuadamente.
- Debe prepararse un plan de formación que cubra los aspectos más importantes del SGSI, en particular los controles implantados.
- Formación: a todo el personal involucrado directamente en el SGSI
- Concienciación: al resto del personal

10 Medir la eficacia de los controles

- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Ejemplos:
  - Control de acceso a la red:
    - Estadísticas de cortafuegos: intentos de acceso a páginas web prohibidas.
  - Controles criptográficos:
    - Porcentaje de sistemas que contienen datos valiosos o sensibles para los cuales se han implantado totalmente controles criptográficos apropiados.

CHECK

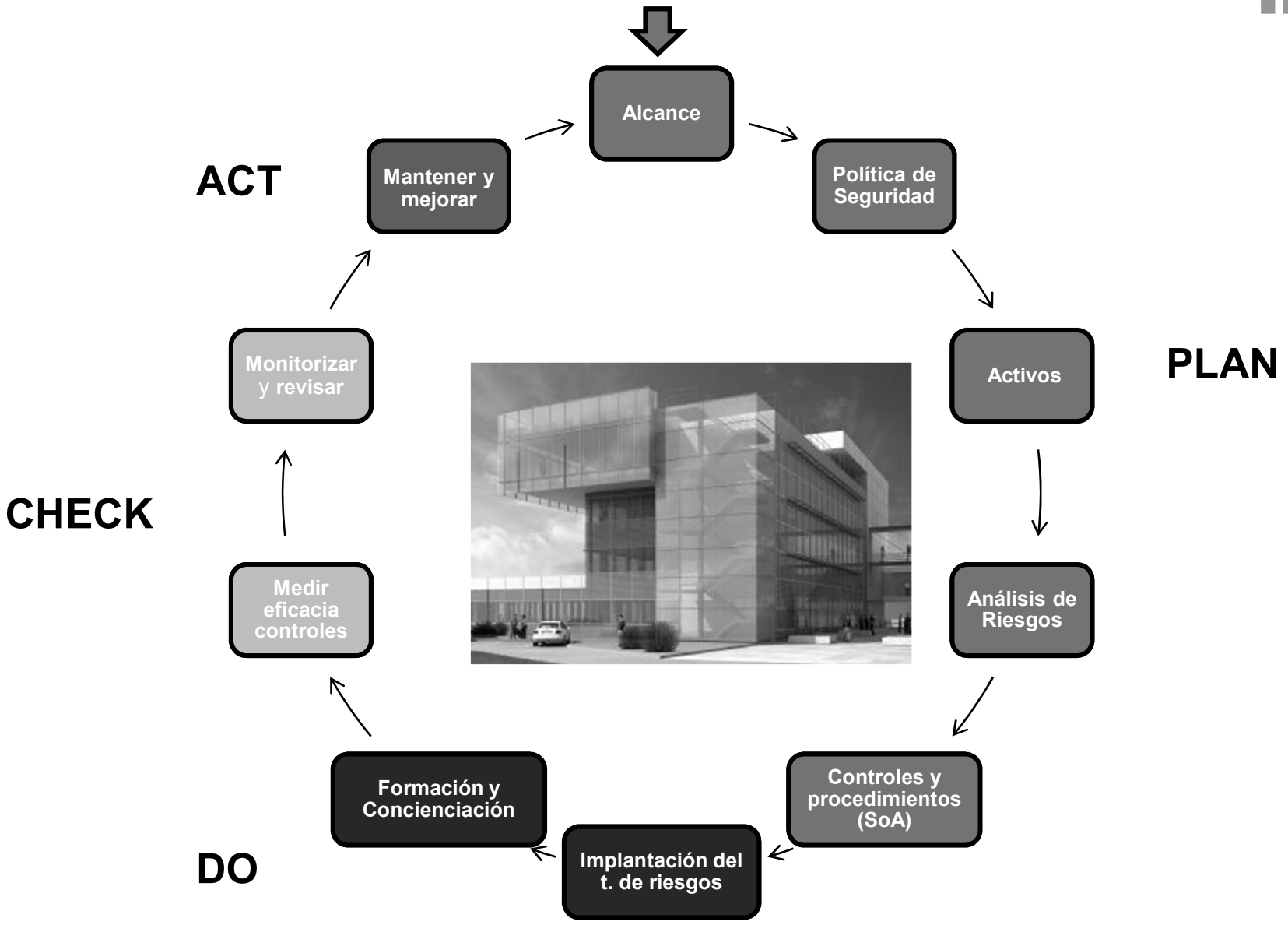
11 Monitorizar y revisar

- Ejecutar procedimientos de monitorización y revisión:
  - Revisar regularmente la **efectividad** del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
  - Revisar regularmente en intervalos planificados las evaluaciones de **riesgo**, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios.
  - Realizar periódicamente **auditorías internas** del SGSI en intervalos planificados.
  - Revisar el SGSI por parte de la dirección periódicamente para garantizar que el **alcance definido** sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

12 Mantener y mejorar el SGSI

- La organización deberá regularmente:
  - Implantar en el SGSI las mejoras identificadas.
  - Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 (mejora continua) considerando todo lo aprendido de la propia experiencia y de otras organizaciones.
  - Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
  - Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

Esquema – Resumen implantación SGSI



Diagnóstico de la Seguridad

- Para poder abordar alguna de las fases propuestas en ISO 27001 se realizará un **exhaustivo test de seguridad** de cada sección con presencia de seguridad. Con esto se podrán determinar las vulnerabilidades de los activos de la organización.
- La metodología de auditoría de seguridad OSSTMM (Open Source Security Testing Methodology Manual) es uno de los estándares profesionales mas completos y comúnmente utilizados a la hora de revisar la Seguridad de los Sistemas.
- Se trata de proporcionar un método estandarizado para realizar un **exhaustivo test de seguridad** de cada sección con presencia de seguridad (seguridad física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la información, seguridad de las tecnologías de Internet y seguridad de procesos) de una organización.
- Este manual también contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001 – 27002 e ITIL entre otras, lo que la hace uno de los manuales mas completos en cuanto a la aplicación de pruebas a la seguridad de la información en las instituciones.

Secciones OSSTMM

- Para estructurar su contenido, la metodología se subdivide en secciones, correspondientes a los aspectos más importantes de los sistemas de información:
  - Seguridad de la Información
  - Seguridad de los Procesos
  - Seguridad en las Tecnologías de Internet
  - Seguridad en las Comunicaciones
  - Seguridad Inalámbrica
  - Seguridad Física

- (enlace a la documentación de OSSTMM)

https://drive.google.com/file/d/0B-Yy4W4DWoh9bXRycmhNYWpOMU0/edit
http://www.isecom.org/mirror/OSSTMM.3.pdf
http://www.isecom.org/research/osstmm.html (versión 3 y borrador de la 4)

Módulos OSSTM

- Cada una de estas secciones está formada por módulos. Ej.:

Seguridad en las Tecnologías de Internet

- …
- Revisión del sistema de detección de intrusiones
- Sondeo de red
- Identificación de servicios y sistemas
- Testeo de aplicaciones de internet
- Descifrado de contraseñas
- Testeo de denegación de servicio
- …

- Cada módulo se describe, se proponen una serie de acciones y se enumeran los resultados esperados.

Ejemplo de aplicación (I)

Ejemplo de aplicación: **Descifrado de contraseñas.**

- **Descripción**:

  Descifrar las contraseñas es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas automatizados, que dejan al descubierto la aplicación de algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas débiles debido a factores humanos.

- **Resultados esperados**:
  - Ficheros de contraseñas descifrados y no descifrados
  - Lista de cuentas con usuarios o contraseñas del sistema
  - Lista de sistemas vulnerables a ataques de descifrado de contraseñas
  - Lista de archivos o documentos vulnerables a ataques de descifrado de contraseñas
  - Lista de sistemas con usuario o cuenta de sistema que usan las mismas contraseñas

Ejemplo de aplicación (II)

- **Acciones de verificación:**

1. Obtener el fichero de contraseñas del sistema.
2. Iniciar un ataque automatizado de diccionario al fichero de contraseñas.
3. Iniciar un ataque de fuerza bruta al fichero de contraseñas.
4. Usar las contraseñas obtenidas o sus variaciones para acceder a sistemas o aplicaciones adicionales.
5. Arrancar programas automatizados de descifrado en ficheros cifrados que se hayan localizado (como documentos PDF o Word) como intento de recopilar más datos.
6. Verificar la fecha de establecimiento de las contraseñas.

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Algunas herramientas identificación de vulnerabilidades

- Wireshark: es un analizador de protocolos de red, que permite capturar cualquier paquete que circule por la red. Con este programa se puede verificar si por medio de la red se capturan datos sin cifrar, es decir que existe la posibilidad de que determinada aplicación envíe información confidencial que puede ser fácilmente interceptada por cualquier persona dentro de la red.
- Ettercap: es una herramienta para realizar ataques de "man in the middle" sobre las redes LAN, en especial en las basadas en switches. Entre sus características se encuentra las de sniffer, ARP Spoofing y otras para el análisis de redes y equipos.
- Kali Linux: evolución de BackTrack, es una de las herramientas más completas para las auditorias de seguridad. Incluye más de 600 herramientas para realizar evaluaciones de la seguridad informática, desde sniffers, exploits, auditoria wireless, análisis forense y otras.
- Metasploit Framework: es una herramienta para escribir, probar y usar código exploit, que son utilizados para aprovechar las vulnerabilidades de los equipos de red. Esta herramienta es una sólida plataforma para las pruebas de penetración e investigación de vulnerabilidades.
- Nmap: Su objetivo es determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando. También permite evaluar el funcionamiento del firewall.
- Nessus: es una herramienta que se utiliza para escanear uno o varios equipos de la red con el fin de encontrar sus vulnerabilidades. Con esta herramienta se puede identificar si el equipo tiene algún problema de seguridad que puede ser aprovechado por alguien para comprometer el equipo. Puede indicar si al equipo le falta algún parche o está desactualizado. Detecta puertos abiertos y lanza exploits para atacarlos.
- NetStumbler: es una herramienta en Windows que permite detectar redes inalámbricas usando 802.11a, 802.11b y 802.11g, y permite identificar la presencia de redes inalámbricas inseguras, conocer la cobertura de las redes, detectar interferencias de otras redes, detectar puntos de acceso no autorizados y otros usos más.
- Yersinia: Herramienta de red diseñada para aprovechar debilidades en diferentes protocolos de la capa de enlace, como STP, DTP, CDP, IEEE 802.1Q, IEEE 802.1X, VTP y otros. Permite realizar ataques de negación de servicio a dichos protocolos, ganar privilegios dentro de las redes segmentadas en VLAN's y así capturar todo el tráfico de otras VLAN's.
- …..