



Gestión de la seguridad

Gestión de Redes

Última “pata” de FCAPS

2

- Recordemos FCAPS (ITU M.3400):
 - ▣ F – Detección y corrección de errores (*faults*)
 - ▣ C – Configuración y operación
 - ▣ A – Contabilidad (*accounting*) y Facturación
 - ▣ P – Optimización y evaluación del rendimiento (*performance*)
 - ▣ S – Valoración y protección de seguridad
- Hoy veremos el último aspecto: Seguridad
- Nos centraremos en el punto de vista de la gestión de red
 - ▣ La parte más “tecnológica” se ve en otras asignaturas
 - ▣ Ligero solapamiento (porque son optativas)

La ilusión de la red segura

3

- La actitud tradicional es considerar la seguridad como un *objetivo*
 - ▣ El administrador quiere una red segura
 - ▣ El vendedor ofrece soluciones para hacer la red segura
- ¿Qué es una red segura?
 - ▣ “Una red de la que no me tengo que preocupar”
 - ▣ “Una red que nadie puede utilizar de forma indebida”
 - ▣ “Una red en la que nada puede salir mal”
 - ▣ ...
- Evidentemente, esto es imposible
 - ▣ Las redes seguras no existen

Terminología de Seguridad

4

- **Identidad:** un valor asociado a una determinada entidad (individuo, aplicación, elemento de red) que lo distingue de forma única
- **Autenticación:** el proceso de verificación de la identidad de una entidad
- **Autorización:** verificación de que una solicitud (e.g. un acceso a un recurso) está dentro de los *privilegios* de la entidad solicitante.
- **Integridad:** Comprobación de que un recurso o activo de información no ha sido alterado.
- **Confidencialidad:** garantía de que determinada información sólo es accesible por el destinatario legítimo de la misma.
- **Privacidad:** control sobre la compartición de información personal.
- **Cifrado:** operación sobre un conjunto de datos llamado *texto en claro* (típicamente, un mensaje) que hace que sólo el usuario legítimo de los datos (típicamente, el destinatario del mensaje) pueda recuperarlos a partir del resultado de la operación (*texto cifrado*)

Tecnologías empleadas para la Seguridad

5

- Veremos brevemente cuatro categorías
 1. Tecnologías de cifrado
 2. Tecnologías de control perimetral
 3. Tecnologías de control de contenidos
 4. Híbridas: Data Loss Prevention (DLPs)
 5. Tecnologías de atracción de atacantes
- No las veremos en detalle; sólo los aspectos que afectan a la gestión

1. Tecnologías de Cifrado

6

- Son la base de los mecanismos de autenticación, confidencialidad e integridad
- Cifrado de clave secreta compartida
 - ▣ Todos los participantes comparten la misma clave
 - ▣ ¿Quién puede conocer la clave secreta?
 - ▣ ¿Cómo se hace llegar la clave secreta desde un origen a un destino?
- Cifrado de clave pública
 - ▣ Cada participante tiene un par de claves
 - Privada: sólo la conoce él
 - Pública: la puede conocer todo el mundo
- Claves de sesión
 - ▣ Sólo válidas en el contexto de una misma comunicación
 - ▣ Generadas automáticamente (no tenemos que preocuparnos de ellas)

2. Tecnologías de Control Perimetral

7

- **Perímetro de la red**
 - ▣ Los elementos de red que pueden recibir paquetes de redes externas
 - ▣ Diferentes mecanismos para asegurar el perímetro de una red
- **Cortafuegos (*firewalls*)**
 - ▣ Implementan políticas de filtrado de paquetes (entrantes o salientes)
 - ▣ Algunos permiten reglas basadas en estado (*stateful firewalls*)
 - ▣ Pueden establecer redes perimetrales (DMZs) concéntricas
- **Sistemas de detección de Intrusiones (IDS)**
 - ▣ Monitores que detectan el incumplimiento de políticas de seguridad
 - ▣ O simplemente anomalías
- **Redes privadas virtuales (VPNs)**
 - ▣ Solución criptográfica para “saltarse” restricciones perimetrales
 - ▣ Puede ser muy útil y/o muy peligrosa

3. Tecnologías de Control de Contenidos

8

- Trabajan a nivel de flujo de datos de aplicación
 - ▣ Aplicación por excelencia para monitorizar: email
- Filtros *anti-spam*
 - ▣ Etiquetan los mensajes como legítimos o *spam*
 - Técnicas de inteligencia artificial (hablaremos de ellas)
 - ▣ El *spam* puede ser descartado o puesto en cuarentena
- Antivirus
 - ▣ Pueden implementarse en diferentes ámbitos (email, web, disco duro...)
 - ▣ Identifican *malware* conocido (no sólo virus)
- Identificador de patrones
 - ▣ Generalización de los casos anteriores
 - ▣ Busca patrones arbitrarios en el contenido
- Problemas de eficiencia y capacidad de almacenamiento

4. Tecnologías Híbridas

9

- Combinan varias de las tecnologías anteriores
 - ▣ Ejemplo paradigmático: DLP
- Data Leak/Loss Prevention (DLP)
 - ▣ Pretende evitar la fuga de datos sensibles
 - A través del perímetro de la red
 - Desde los propios ordenadores
 - ▣ Incorpora diversos elementos vistos anteriormente
 - Identificadores de patrones → ¿qué es sensible?
 - Control perimetral → ¿de dónde no debe salir la información?
 - Detección de intrusiones → ¿quién intenta acceder a la información?
 - ▣ Así como técnicas adicionales
 - Restricciones de sistema operativo (bloqueo de impresión, etc)

5. Tecnologías de atracción de atacantes

10

- Permiten llamar la atención del atacante y observar su comportamiento
 - ▣ HoneyNet
 - ▣ HoneyPot
 - ▣ Padded cell
- Llevan herramientas como IDS para analizar el comportamiento

- Los activos de una organización pueden sufrir ataques (amenaza/riesgo):
 - ▣ Intencionados: contra la disponibilidad, integridad y confidencialidad.
 - ▣ Desastres naturales o no intencionados que amenazan la disponibilidad.



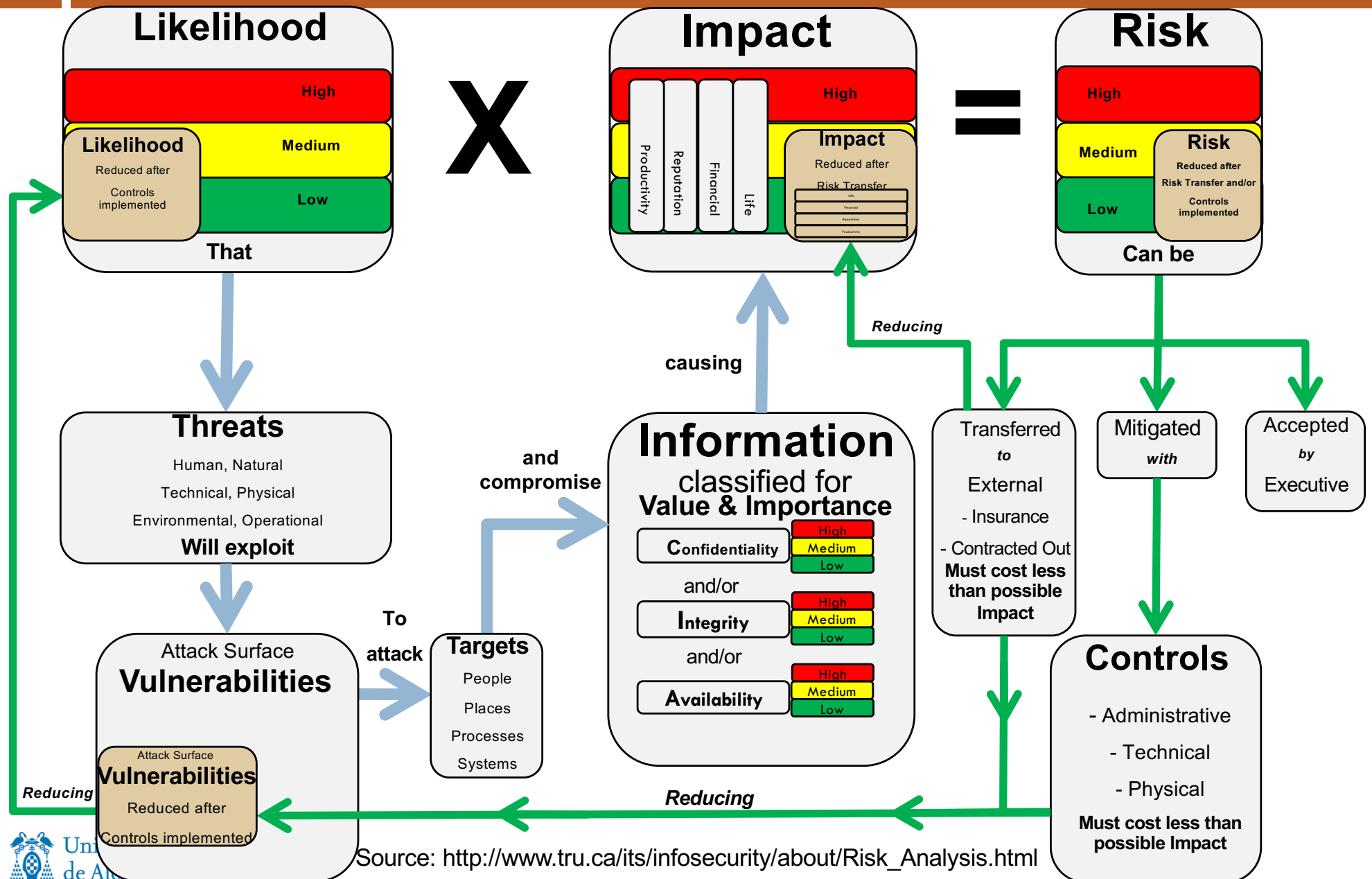
- Objetivo: mantener la información razonablemente salvaguardada de estos ataques
- Aplicar un Sistema de Gestión de Seguridad de la Información (SGSI)

□ OBJETIVO de un SGSI:

Garantizar que los riesgos de la seguridad de la información son 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

- **Riesgo:** impacto potencial asociado a un aspecto específico de un sistema
 - ▣ En función del valor los activos que se ven afectados
 - ▣ En función de la probabilidad de que los eventos adversos tengan lugar
- **Control:** mecanismo desplegado con objeto de mitigar un riesgo o conjunto de riesgos
 - ▣ Compromiso seguridad/usabilidad
- **Análisis de riesgos**
 - ▣ Valoración de los riesgos a los que se exponen los activos de una organización y de los controles necesarios para mitigarlos
 - ▣ Rentabilidad de los controles: relación entre la reducción del riesgo y el coste de implementación de los controles

Risk Analysis overview



Source: http://www.tru.ca/its/infosecurity/about/Risk_Analysis.html

Aplicación del Análisis de riesgos

15

Identificar activos

Identificar amenazas del activo y las dimensiones a las que afectan (confidencialidad, disponibilidad, integridad)

Asignar la probabilidad se materialice la amenaza

Asignar el impacto de una amenaza

Calcular el riesgo: probabilidad x impacto

Identificar control: afecta a una reducción de la probabilidad o del impacto, ¿en qué medida?

Calcular el riesgo residual al aplicar el control

- Documento de lo que se considera seguro para una organización
 - ▣ En cuanto a operación de red
 - e.g. Todos los datos financieros que entran o salen de la red deben ir cifrados
 - ▣ En cuanto a requisitos de acceso a recursos
 - e.g. Sólo el jefe de seguridad puede tener acceso al almacén de certificados
 - ▣ En cuanto a respuesta a incidentes
 - e.g. Todo incidente de seguridad debe ser comunicado al jefe de seguridad
 - ▣ En cuanto a trazabilidad de eventos
 - e.g. Debe guardarse un registro de todas las incidencias.
- ¿Mejor que sea más general o específica?

□ *Acceptable Use Policy (AUP)*

▣ Define reglas en cuanto al uso de la red

- Actividades permitidas y no permitidas
- Generalmente destinadas a restringir a los usuarios.
 - e.g. No está permitido utilizar herramientas de compartición de archivos peer-to-peer

▣ Puede estar motivada por diferentes criterios

■ Aspectos legales

- e.g. La descarga de archivos con copyright desde la red de la universidad podría ser imputable a la universidad

■ Aspectos económicos

- e.g. No se puede emplear la red de la universidad para fines comerciales

■ Aspectos de seguridad

- e.g. No se pueden encaminar paquetes que provengan de fuera de la red (e.g. via interfaces 4G)

- Necesidad de normalizar los procesos de gestión de la seguridad de la información
- <http://27000.org/>
- Algunas de las normas referente:
 - ▣ ISO 27001:2005: auditoria y certificación de un SGSI (origen de BS7799-2)
 - ▣ ISO 27002:2013: buenas prácticas de seguridad - controles (origen de BS7799-1)
 - ▣ ISO 27003: guía de implementación de un SGSI
 - ▣ ISO 27004: medidas y métricas de sistemas de gestión de la seguridad, alineado con los controles de 27002
 - ▣ ISO 27005: metodología de análisis de riesgos de la seguridad de la información
 - ▣ ISO 27006: guía de la acreditación de un organización para obtener un certificado de SGSI

- Las buenas prácticas de seguridad se enuncian en forma de controles.
- Cada control define:
 - ▣ Recomendación práctica para reducir un riesgo de seguridad concreto
 - ▣ Guías de implementación: qué hacer y cómo hacerlo
- Las recomendaciones son de alto nivel
- Los **controles** se agrupan en **objetivos**
- A su vez los **objetivos** se agrupan en **dominios**
- Hay:
 - ▣ **11 dominios**
 - ▣ **39 objetivos**
 - ▣ **133 controles** (recomendación, Guía práctica)

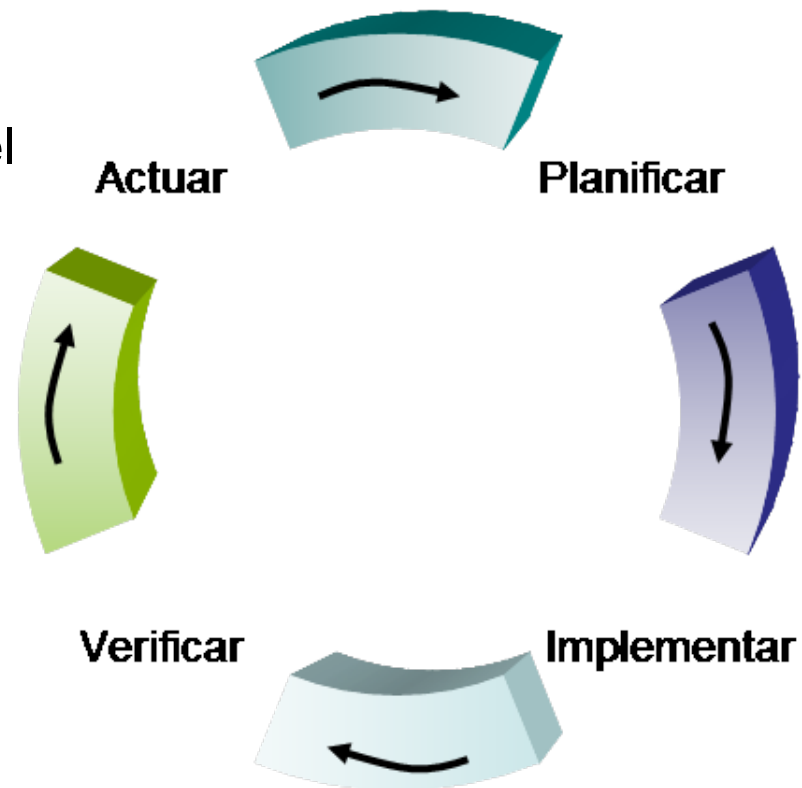


- **Dominio:** Organización de información de seguridad
- **Objetivo:** Gestionar la seguridad de la información en la organización
- **Control:** Las actividades de seguridad de la información se deberían coordinar por representantes de diferentes partes de la organización con diferentes roles y funciones
- Guías de cómo llevar a cabo este control:
 - ▣ Garantizar que las actividades se realizan de acuerdo a las **políticas de seguridad**
 - ▣ Identificar cómo tratar **no cumplimientos**
 - ▣

ISO 27001. Desarrollo de un SGSI en una empresa

22

- Para establecer y gestionar un SGSI se usa el modelo de ciclo continuo PDCA
 - ▣ **Planificar** (Plan): establecer el SGSI
 - ▣ **Hacer** (Do): implementar y utilizar el SGSI
 - ▣ **Verificar** (Check): monitorizar y revisar el SGSI
 - ▣ **Actuar** (Act): mantener y mejorar el SGSI



- Definir el Alcance del SGSI.
- Definir una Política de seguridad.
- Definir un Método de evaluación de riesgos.
- Identificar los riesgos.
- Evaluar los riesgos.
- Identificar y evaluar las opciones de tratamiento de riesgos.
- Seleccionar los objetivos de control y los controles.
- Definir una Declaración de aplicabilidad. Lista de controles y exclusiones.
- Aprobación por la parte de la dirección: riesgos residuales e implantación.

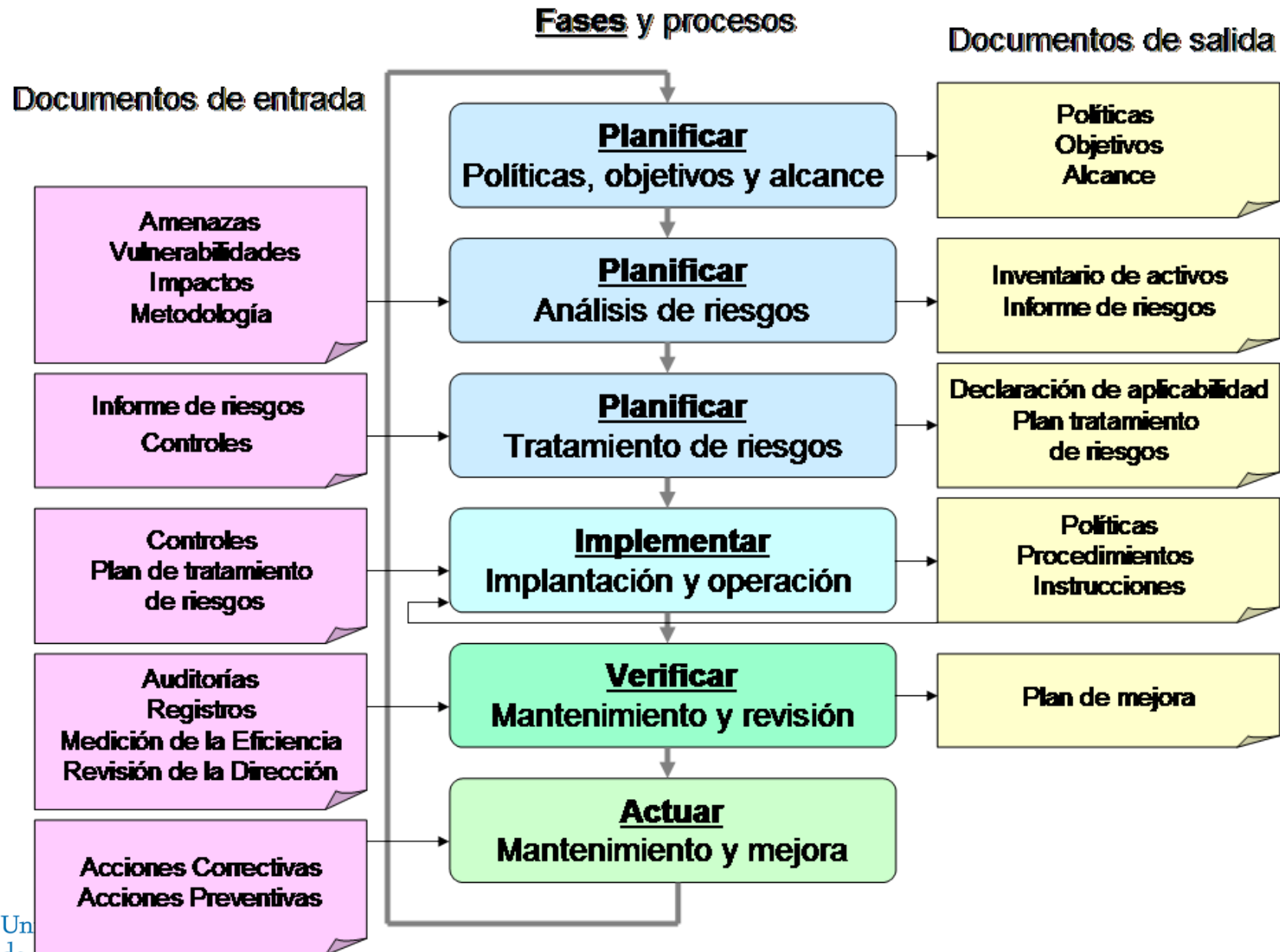
- Definir un plan de tratamiento de riesgos
 - ▣ Riesgos
 - ▣ Responsable
 - ▣ Prioridades.
- Implementar el plan de tratamiento de riesgos
- Implementar controles
- Formación y concienciación
- Gestión de operaciones
- Gestión de recursos asignados al SGSI
- Implantar procedimientos y controles de detección y respuesta de incidencias de seguridad

- ❑ Verificar si el SGSI cumple con los objetivos de forma eficiente.
- ❑ La dirección es responsable de estas revisiones.
- ❑ La verificación se realiza mediante auditorias periódicas.
- ❑ Definir indicadores de eficiencia.
- ❑ Monitorizar y verificar si el SGSI cumple los objetivos y el coste.
- ❑ Se revisa que los controles aplicados son los correctos.
- ❑ La revisión de incidencias ofrece información sobre el estado del SGSI.
- ❑ Se revisa el nivel de riesgo residual (puede variar con el tiempo) y para ver si sigue siendo aceptable.

- El SGSI debe ser revisado de forma periódica.
- Objetivos:
 - ▣ Mejora
 - ▣ Adaptación a cambios en la organización y su entorno
- La necesidad de los cambios se identifica en la fase de verificación.
- Mejoras: definidas en forma de acciones preventivas y correctivas.

Certificación de un SGSI

27



Esquema para obtener la certificación SGSI

28

