Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Introducción a la seguridad

Presentación

Daniel F. García

Definición de seguridad

Conjunto de medidas que impiden realizar operaciones no autorizadas en un sistema para:

- Acceder a la información contenida en el sistema
- Reducir el rendimiento del sistema
- Impedir el acceso a usuarios autorizados al sistema

Otros aspectos a considerar en la seguridad:

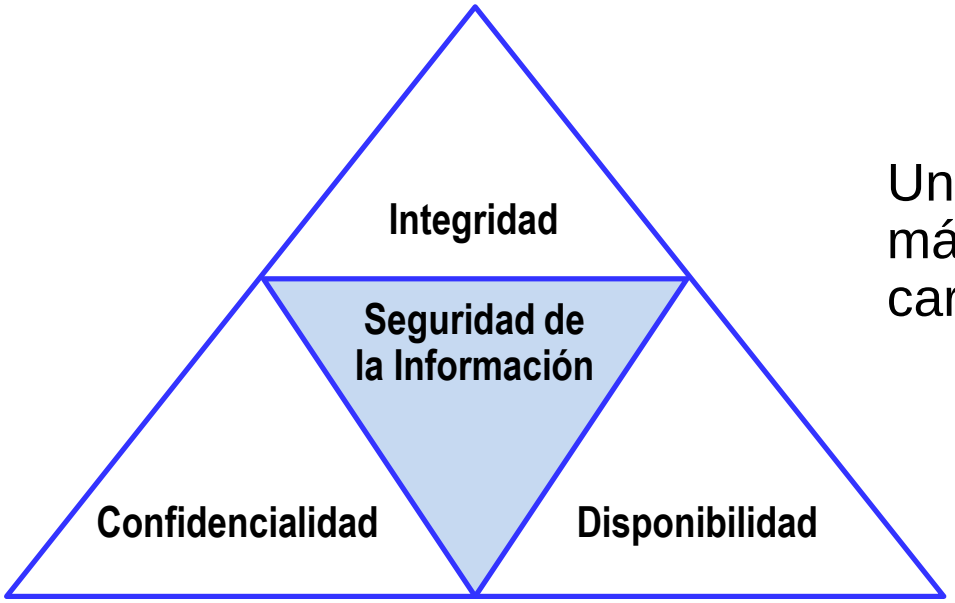
1. Cumplimiento de la legislación aplicable a un { Tipo de empresas / Sector empresarial }
2. Control de acceso a un sistema (Servicios e Información)
3. Control de ficheros protegidos por la ley { Contenidos digitales con derechos de autor / Ficheros con datos de carácter personal }
4. Identificación de los autores de información o de mensajes
5. Registro de la utilización de los servicios e información de un sistema

Definición de seguridad (ISO/IEC 27001)

Seguridad de la Información = Preservación de la { Confidencialidad, Integridad, Disponibilidad } información

Estas características se conocen en inglés como ***CIA***:

Confidentiality, Integrity, Availability



Una organización puede dar más importancia a una de las características

CONFIDENCIALIDAD

La confidencialidad se refiere a la ocultación (*concealment*) de la información y otros recursos

La necesidad de ocultar la información surge del uso de computadores en { Gobierno / Industria

- Las organizaciones gubernamentales (civiles y militares) restringen el acceso a la información implementando controles para hacer cumplir el principio "***Need to Know***"

  "***Need to Know***": Cada persona solo accede a la información que necesita para realizar su tarea

- Las corporaciones industriales tratan de mantener en secreto sus diseños para evitar que los conozcan sus competidores

La confidencialidad también se aplica a la mera existencia de unos datos, que a veces, es más reveladora que los propios datos

Ej: Saber como una agencia gubernamental acosó a ciudadanos tiene menos importancia que saber que tal acoso ha ocurrido

Para proporcionar confidencialidad hay que utilizar mecanismos de control de acceso:

- Contraseñas en los equipos que contienen información
- Cifrado de la información, etc., …

INTEGRIDAD

La integridad se refiere a ausencia de alteraciones no autorizadas de la información

En general la integridad considera la (*trustworthiness*) de una información por no haber sido modificada de forma no autorizada

(***trustworthiness***)
Confiabilidad
Fiabilidad
Veracidad
Carácter fidedigno

Hay autores que consideran **2 aspectos** en la integridad:
- Integridad de los **datos** (el contenido de la información)
- Integridad del **origen** (la fuente de la información)

La fuente de la información influye en su credibilidad y en la confianza que la gente le otorga

Para asegurar la integridad hay que utilizar mecanismos de { Prevención / Detección

Los mecanismos de **prevención** tratan de mantener la integridad bloqueando cualquier intento de

(1) Modificar los datos no autorizado
(2) Modificar los datos una forma no autorizada

Los mecanismos de **detección** simplemente indican que la integridad de unos datos ya no es creíble

- Pueden analizar eventos del sistema y/o de los usuarios para detectar problemas
- Pueden analizar los propios datos para comprobar si se verifican ciertas condiciones

DISPONIBILIDAD

La disponibilidad se refiere a la probabilidad de que la información (o un recurso) sea utilizable cuando se desee usarla

Aspecto de la disponibilidad que es relevante para la seguridad:

Alguien puede deliberadamente realizar acciones para **denegar el acceso** a la información o los servicios que proporciona un sistema informático, haciéndolo indisponible para sus usuarios

El diseño de un sistema informático se suele basar en un modelo o patrón de utilización esperado durante su funcionamiento y si funciona dentro de las condiciones del diseño estará disponible

Pero si se alteran las condiciones de funcionamiento (ej: trafico de peticiones masivo) el diseño ya no es valido y el sistema puede fallar quedando indisponible

La acción más común para hacer que un sistema esté indisponible es:

Un Ataque de Denegación de Servicio (*Denial of Service Attack, DoS*)

Consiste en saturar la capacidad computacional de un sistema informático enviándole una cantidad de peticiones basura por segundo enorme

Para asegurar la disponibilidad hay que utilizar mecanismos que detecten los ataques

Es difícil porque hay que distinguir los eventos atípicos y los picos de la carga de trabajo de los ataques deliberados

Amenazas a la seguridad

Una amenaza (*threat*) es una causa potencial de una brecha de seguridad

No se necesita que ocurra realmente la brecha para que haya o exista una amenaza

Como la brecha puede ocurrir …

Hay que proteger a un sistema informático contra (poner los medios para evitar) las acciones que hacen que se produzca la brecha

Esas acciones se denominan ataques (*attacks*)
Los que ejecutan las acciones se denominan atacantes (*attackers*)

Ejemplos de amenazas:

Revelación (*disclosure*) o acceso no autorizado a la información
Ejemplo: el fisgoneo (*snooping*) en una red

Engaño (*deception*) al aceptar y usar datos falsos consecuencia de alteraciones no autorizadas
Ejemplo: el ataque "man-in-the-middle" que captura, modifica y reenvía mensajes

Perturbación o interrupción (*disruption, interruption*) del funcionamiento correcto de un sistema
Ejemplo: el ataque "*denial of service*" que agota la capacidad de un sistema

Usurpación (*usurpation*) o control no autorizado de un sistema informático
Ejemplo: el ataque de un hacker que toma el control de un servidor

Objetivos de seguridad

Los principales objetivos de seguridad son:

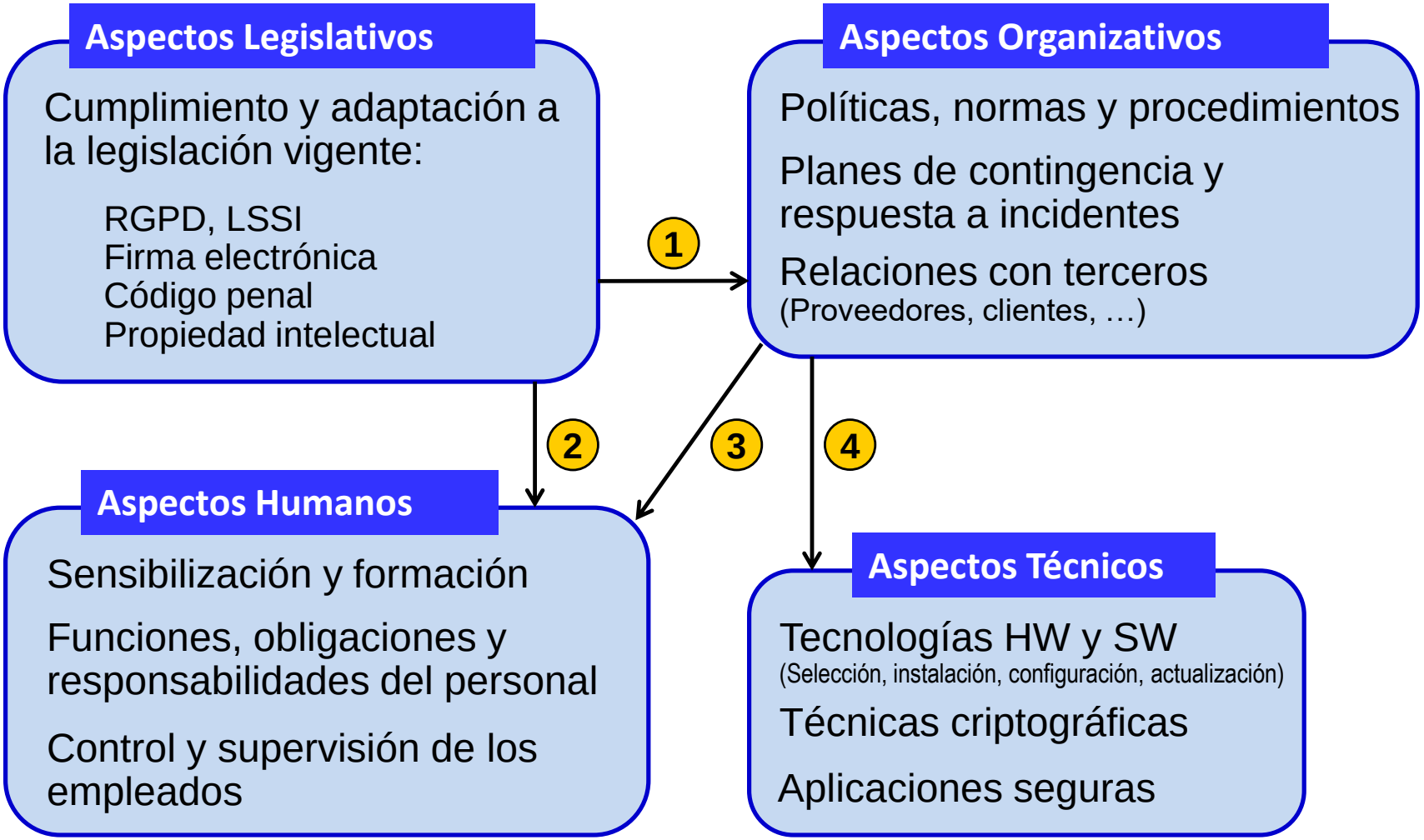
1. Detectar los posibles problemas y amenazas a la seguridad
2. Gestionar y minimizar los riesgos de seguridad
3. Garantizar la correcta utilización de los recursos y aplicaciones de un sistema
4. En caso de un incidente de seguridad → { Limitar las pérdidas / Recuperarse adecuadamente
5. Cumplir la legislación y los requisitos contractuales de seguridad

Para cumplir sus objetivos de seguridad
una organización debe implantar y utilizar un:

SGSI → Sistema de Gestión de la Seguridad de la Información

ISMS → Information Security Management System

Sistema de Gestión de la Seguridad de la Información



Servicios proporcionados por un SGSI (1)

Confidencialidad

Garantiza que una información (mensaje, archivo) solo puede ser leída por su legítimo propietario o destinatario

Autenticación

Garantiza al destinatario de una información (mensaje, archivo) que el remitente es realmente el que figura en la información recibida

Integridad

Garantiza al destinatario o usuario de una información (mensaje, archivo) que la información no ha sido alterada

Disponibilidad

Garantiza que un sistema continua disponible para sus legítimos usuarios frente a ataques e incidentes de seguridad

Servicios proporcionados por un SGSI (2)

NO repudio

No repudio **de origen**: Permite demostrar la autoría y el envío de un determinado mensaje.

No repudio **de destino**: Permite demostrar la recepción de un determinado mensaje.

Es importante como soporte jurídico de las transacciones comerciales electrónicas

Autorización

Controla el acceso de los usuarios a los recursos y servicios del sistema
(Después de que el usuario a sido autenticado en el sistema)

Generalmente se usan Listas de Control de Acceso
(Después de que el usuario a sido autenticado en el sistema)

Servicios proporcionados por un SGSI (3)

Auditoria o Trazabilidad

Monitoriza y registra el uso de los recursos del sistema por los usuarios (previamente autenticados y autorizados) para detectar comportamientos anómalos

Monitoriza el rendimiento del sistema, para detectar anomalías (Transacciones realizadas, Tráfico en la red, Volumen de información almacenada, …)

Reclamación de propiedad

Permite probar que un documento o contenido digital protegido por derechos de autor pertenece a un usuario o una organización (que ostenta la titularidad de los derechos)

Reclamación de origen

Permite probar quién ha sido el creador de un mensaje o documento

Servicios proporcionados por un SGSI (4)

Anonimato

Garantiza el anonimato de los usuarios que acceden a recursos y servicios garantizando la privacidad de los usuarios
Entra en conflicto con otros servicios → Autenticación, Acceso, Auditoria

Protección contra réplicas

Impide ataques basados en la replicación de operaciones
Un usuario intercepta mensajes y los reenvía para engañar al sistema
(Por ejemplo para realizar varias veces una misma transacción bancaria)

Se pueden usar números de secuencia y/o sellos temporales con los mensajes y documentos para detectar y eliminar repeticiones

Servicios proporcionados por un SGSI (5)

Confirmación de operaciones

Confirma la realización de una operación (transacción) reflejando los intervinientes

Certificación de fecha y hora

Certifica el instante en el que se ha enviado un mensaje o realizado una operación
Añade un sello temporal al mensaje o documento en formato UTC

Certificación mediante terceros de confianza

Cuando dos entidades realizan transacciones electrónicas, pueden usar una tercera entidad de confianza que certifica:

- La identidad de las entidades intervinientes en una transacción
- La realización de la transacción
- El contenido de la transacción …

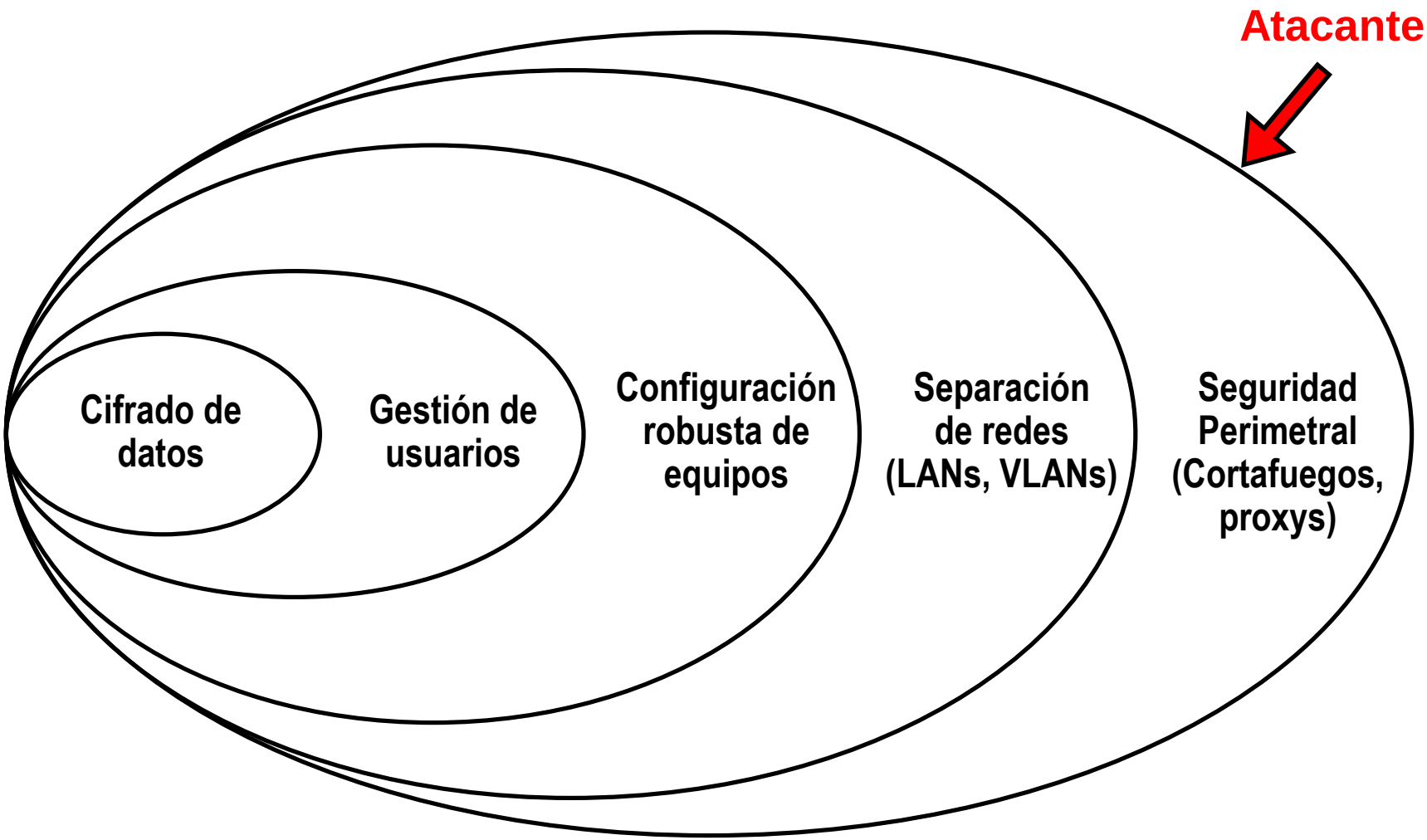
Técnicas y mecanismos de seguridad

Para que un SGSI proporcione los servicios de seguridad
Tiene que utilizar técnicas y mecanismos de seguridad:

- Copias de seguridad y Centros de respaldo
- Protocolos criptográficos
  - Cifrado de información y mensajes
  - Utilización de firmas electrónicas
- Identificación de usuarios y Control del acceso a recursos
- Huella digital de mensajes y Sellado temporal de mensajes
- Antivirus y Sistemas de detección de intrusiones
- Análisis y filtrado de tráfico (cortafuegos) y Servidores proxy

Principio de defensa en profundidad

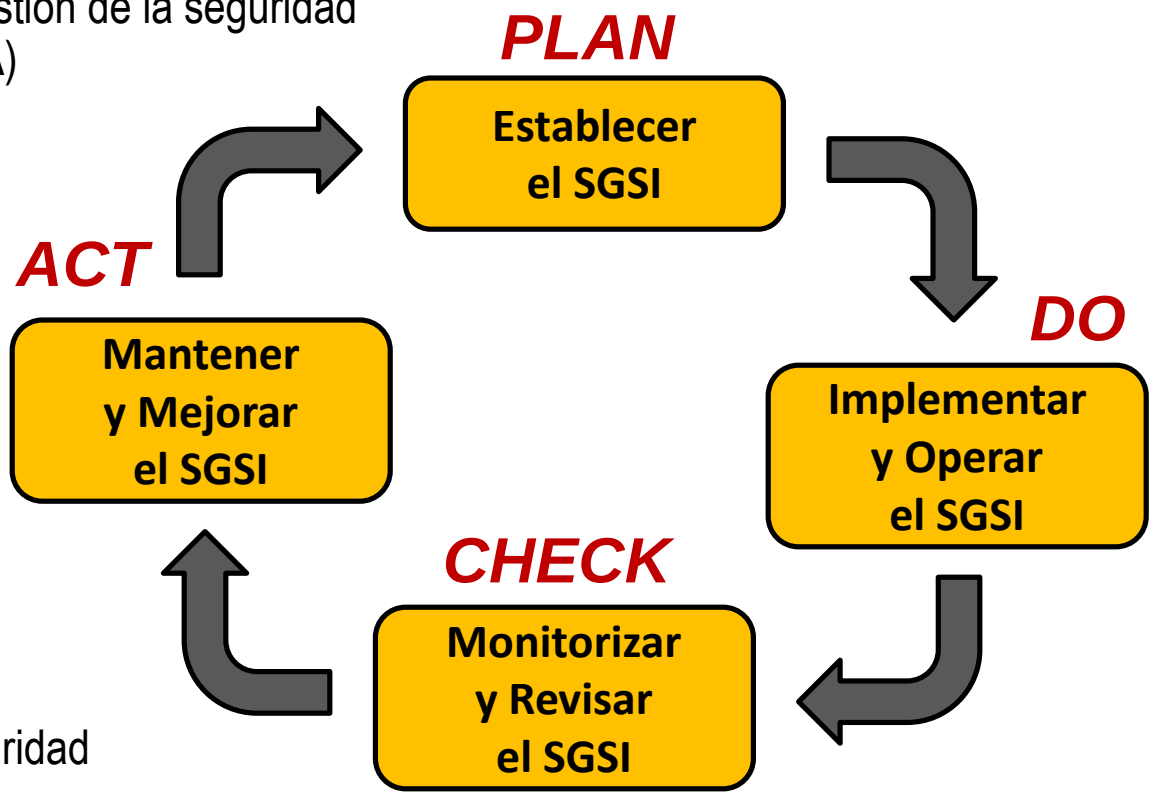
Diseñar e implantar varios niveles de defensa dentro del sistema informático



Implantación de un SGSI

Aspectos a considerar en la implantación de un SGSI

1. Formalizar la gestión de la seguridad de la información
2. Analizar y gestionar los riesgos de seguridad
3. Establecer los procesos de gestión de la seguridad (Usando la metodología PDCA)



4. Certificar la gestión de la seguridad

Niveles de madurez en la gestión de la seguridad (1)

1 Implantación de medidas básicas

La organización aplica …

Medidas de sentido común →
- Realización de copias de seguridad
- Control del acceso a los recursos informáticos

2 Adaptación al marco legal y las exigencias de clientes

La organización cumple …

Los requisitos de la legislación vigente (RGPD)

Las exigencias derivadas de la relación con terceros (proveedores, clientes)

Protección de datos de carácter personal

Niveles de madurez en la gestión de la seguridad (2)

3 Gestión integral de la seguridad de la información

La organización gestiona …

La seguridad con un planteamiento global →
- Define políticas de seguridad
- Analiza y gestiona los riesgos de seguridad
- Implanta planes y procedimientos de seguridad
- Define planes de
  - respuesta a incidentes
  - continuidad del negocio

4 Certificación de la gestión de la seguridad de la información

La organización obtiene …

Una certificación de su SGSI ⟺ Obtiene el reconocimiento de las buenas prácticas implementadas

Además puede acreditarlo ante terceros →
- Clientes
- Administraciones públicas
- Otras instituciones