INFO 2017 Tercer Congreso Internacional de Ingeniería Informática
RETOS Y PERSPECTIVAS DEL MUNDO DIGITAL

100 años PUCP

Taller:
Seguridad Digital (Normas Peruanas)

Mas allá de la Seguridad Digital….
SEGURIDAD DE LA INFORMACIÓN

Carlos Trigo Pérez

Sesión 1

Carlos Trigo

Académico

Ing. Industrial

Maestría en Ingeniería de Sistemas

Certificado PMP

Profesor UNI y Postgrado UPC

Competencias, Habilidades, experiencia

- **Ex-Gerente de TI en Royal & SunAlliance, Seg. Fénix, Seg. La Nacional, Financiera Sudamericana, SBS**
- **Cursos continuos de Especialización en Gerencia de Proyectos (Horsham-England (EPM), Seguridad de la Información ISO 17799 (27001-2005).**
- **Graduado del Programa "2005 ADOC Program´s Training for Trainers" que sobre Desarrollo Digital, Project Management, Redes y Seguridad de Información**
- **Becado del curso "IT Development Policy", patrocinado por la Agencia de Cooperación Internacional de Corea (KOICA)**
- **METRICAS: 18 Proyectos aplicando enfoque PMI (4 sobre seguridad de la información y uno de despliegue de la ISMS; Ex Gerente del Proyecto de la Plataforma de Interoperabilidad del estado (PIDE) ONGEI _ PCM**

Objetivo del Curso - Taller

Seguridad digital (ciberseguridad, seguridad informática, seguridad de cómputo)

Seguridad de la Información

Agenda

- Aclarando diferencias: seguridad digital vs. Seguridad de la Información
- Necesidades de Seguridad de Información
- La información y el sistema de Gestión de Seguridad de la Información
- Taller 1

Seguridad digital es igual a Seguridad de la información?

- En la actualidad, un término ampliamente utilizado como seguridad digital es **"ciberseguridad"** (ciberespacio, ciberamenazas, cibercriminales, etc u otros conceptos compuestos)
- Aunque se tiene una percepción general sobre lo que representa, en ocasiones puede utilizarse como **sinónimo** de *seguridad de la información*, pero esta idea **no es del todo correcta**.

- **"Ciberseguridad":** Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".
- La norma ISO 27001 define: **activo de información** "como los conocimientos o datos que tienen valor para una organización"; **sistemas de información** "aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma".
- Por lo tanto, la ciberseguridad tiene como foco la protección de la **información digital** que "vive" en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información: "*distintas formas y diferentes estados de los datos*"

- **Distintas formas: formato digital** (a través de archivos en medios electrónicos u ópticos), **en forma física** (ya sea escrita o impresa en papel), así como **de manera no representada** (ideas o el conocimiento de las personas).
- **Diferentes estados de los datos:** la información puede ser **almacenada, procesada o transmitida de diferentes maneras:** en formato electrónico, de manera verbal o a través de mensajes escritos o impresos
- Por lo tanto, **sin importar su forma o estado**, la información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad, y éste es precisamente el ámbito de la **seguridad de la información**.

- **Otras definiciones: seguridad en cómputo** "protección de sistemas y equipos que permiten procesar información"; **seguridad informática** "métodos, procesos o técnicas para el tratamiento automático de la información en formato digital, la que incluye la protección de las redes e infraestructura tecnológica."
- Cuando se busca **proteger** el *hardware*, redes, *software*, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la **seguridad informática o ciberseguridad**. Cuando se incluyen actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o **concientización** nos referimos a **seguridad de la información**.

Necesidades de Seguridad de Información

Cybercultura

La ***WEB*** tiene 32aa/4mm [15.03.1985] de historia. ***FACEBOOK***: 13aa/6mm [4.02.2004]. ***TWITTER***: 11aa/01mm/ [15.07.2006]

Cuando se diseñó internet se buscó conectar computadoras. Hoy se busca que todo sea/tenga una computadora conectada.

Todo ser humano está rodeado de entre 1.000 y 5.000 objetos. En todo el mundo hay más antenas que humanos. Hay más sensores que humanos.

Hace sólo unos años apenas 1 o 2 objetos de todos esos se conectaba. El 2020 por cada persona habrá más de 6.6 objetos conectados a la red. Objetos sin software, en extinción.

Hay 25 mil millones de dispositivos conectados a la red. En el 2020 habrá 50 mil millones.

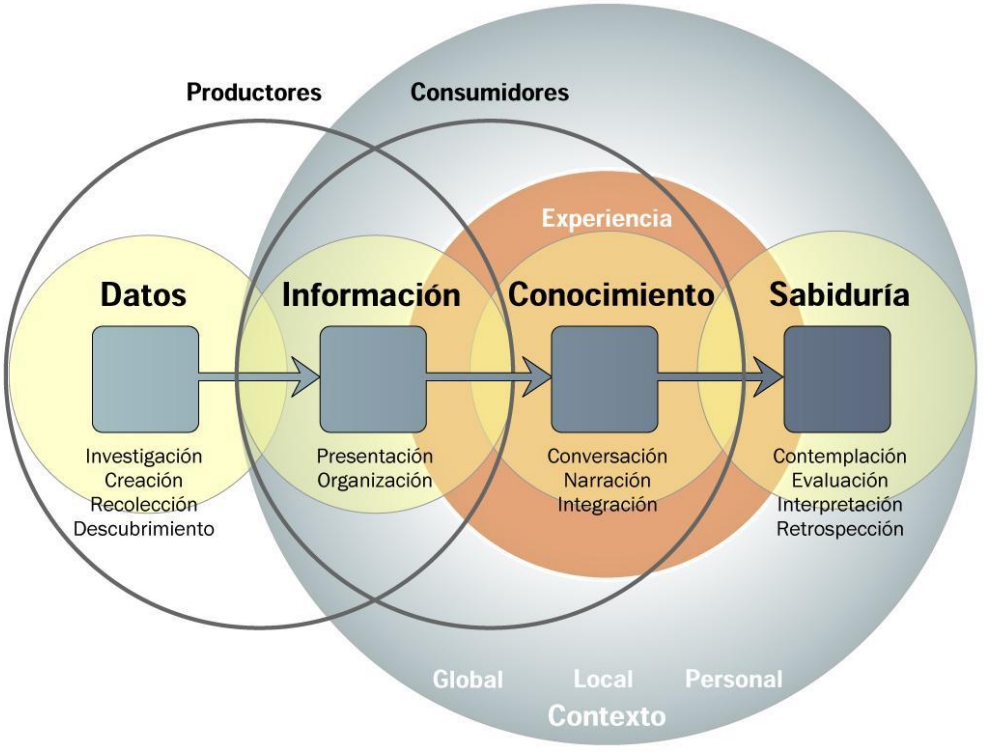
……. pero esto añade complejidad

y lo que viene …… Expande las necesidades de seguridad

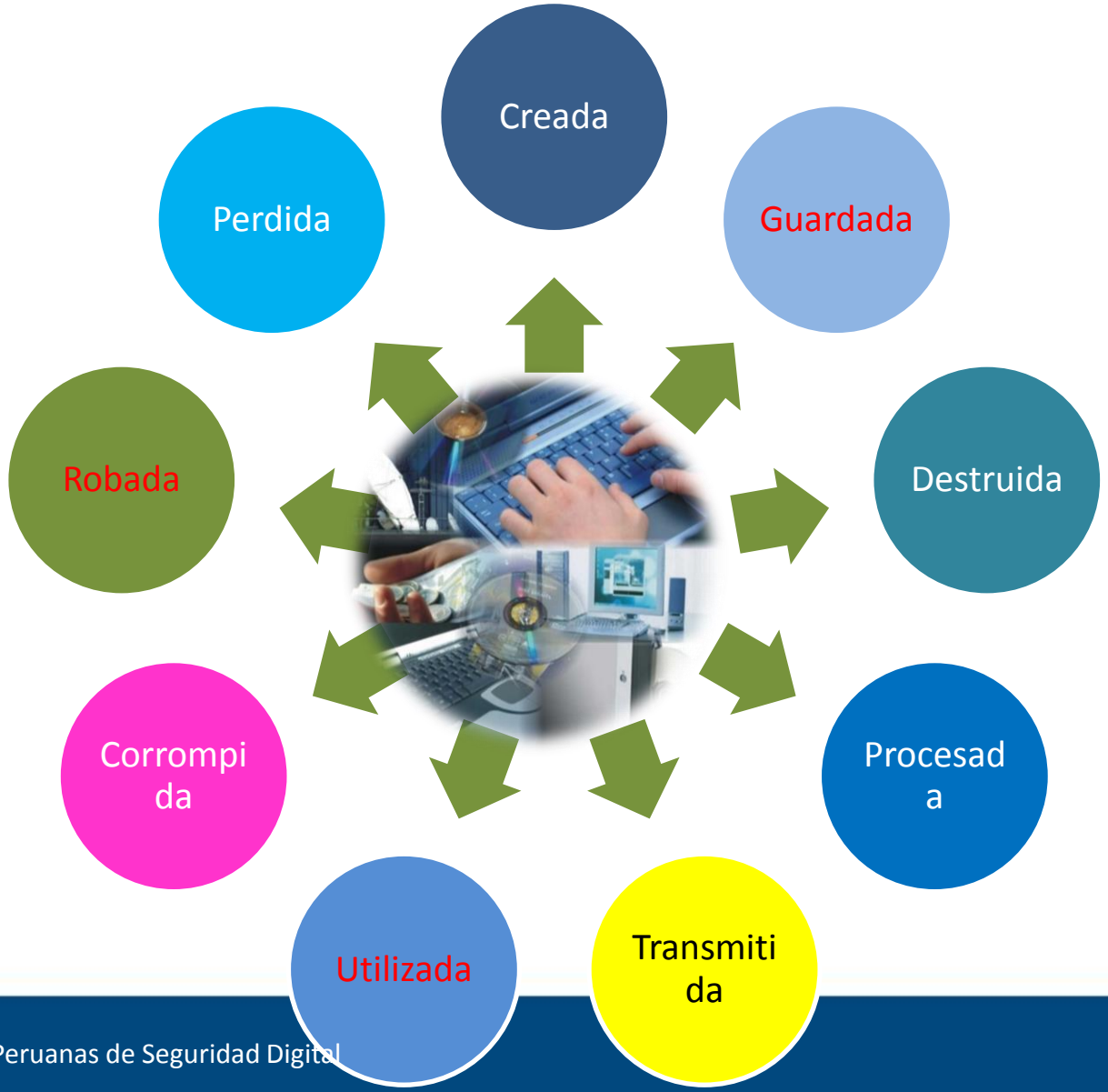
La información y el Sistema de Gestión de Seguridad de la Información

Información

- La información, junto a los procesos y sistemas que hacen uso de ella, es un activo vital para el éxito y la continuidad en el mercado de cualquier organización, y debe ser protegida adecuadament

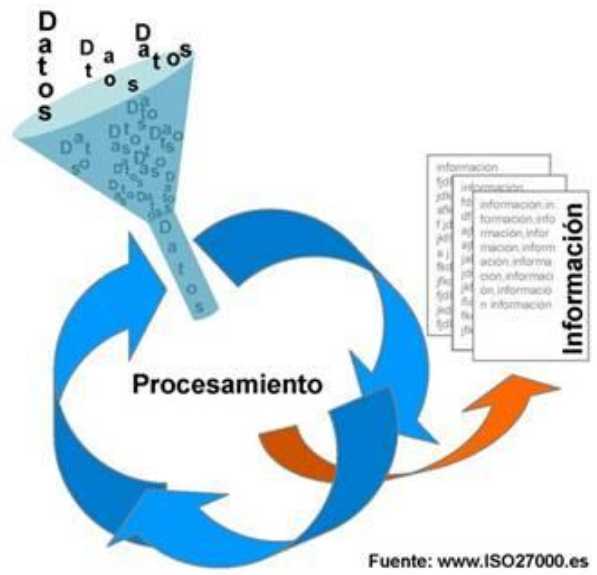


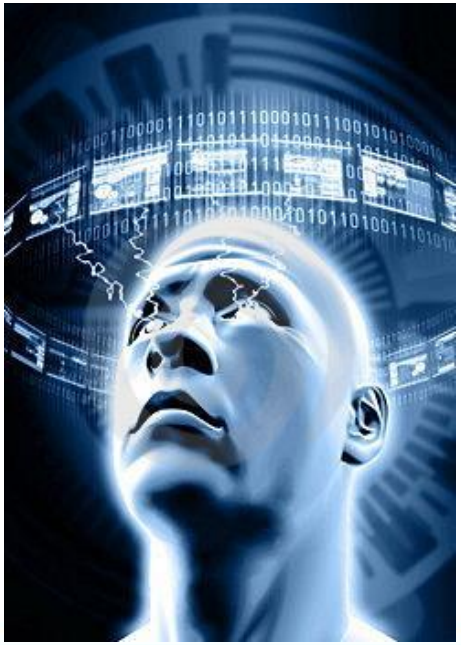
La información, puede ser…



Entonces, ¿cómo la definimos?

Conjunto de datos organizados **en poder** de una entidad que posean ***VALOR PARA LA MISMA***, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración.





Primero, … clasificarla

Activos de información	Activos físicos	Activos de servicios TI	Activos humanos
• Datos digitales: bases de datos, copias de seguridad, claves • Activos tangibles: correo, fax, llaves, libros, … • Activos intangibles: patentes, conocimiento, relaciones, … • Software • Sistemas operativos	• Infraestructura TI: edificios, oficinas, armarios • Hardware TI estaciones de trabajo, portátiles, … • Controles de entorno TI: aire acondicionado, alarmas	• Servicios de autenticación, servicios de red,	• Empleados • Externos

Luego, ¿implementar controles?

Nos acechan amenazas…

Red

Topología seleccionada, Sistema operativo, Incumplimiento de las normas

Hardware

Errores de fabricación, mal diseño, Suministro de energía, Desgaste, Descuido y mal uso

Software

Software de desarrollo, Software de aplicación, Código malicioso, Virus, Troyanos, Gusanos, Errores de programación y diseño

Desastre natural

Incendios, Inundaciones

Humanas

Curiosos, Intrusos remunerados, Usuarios, Terroristas, Fuga de datos, Sabotaje, Fraude, Ingeniería social

¿Y qué hacemos habitualmente?

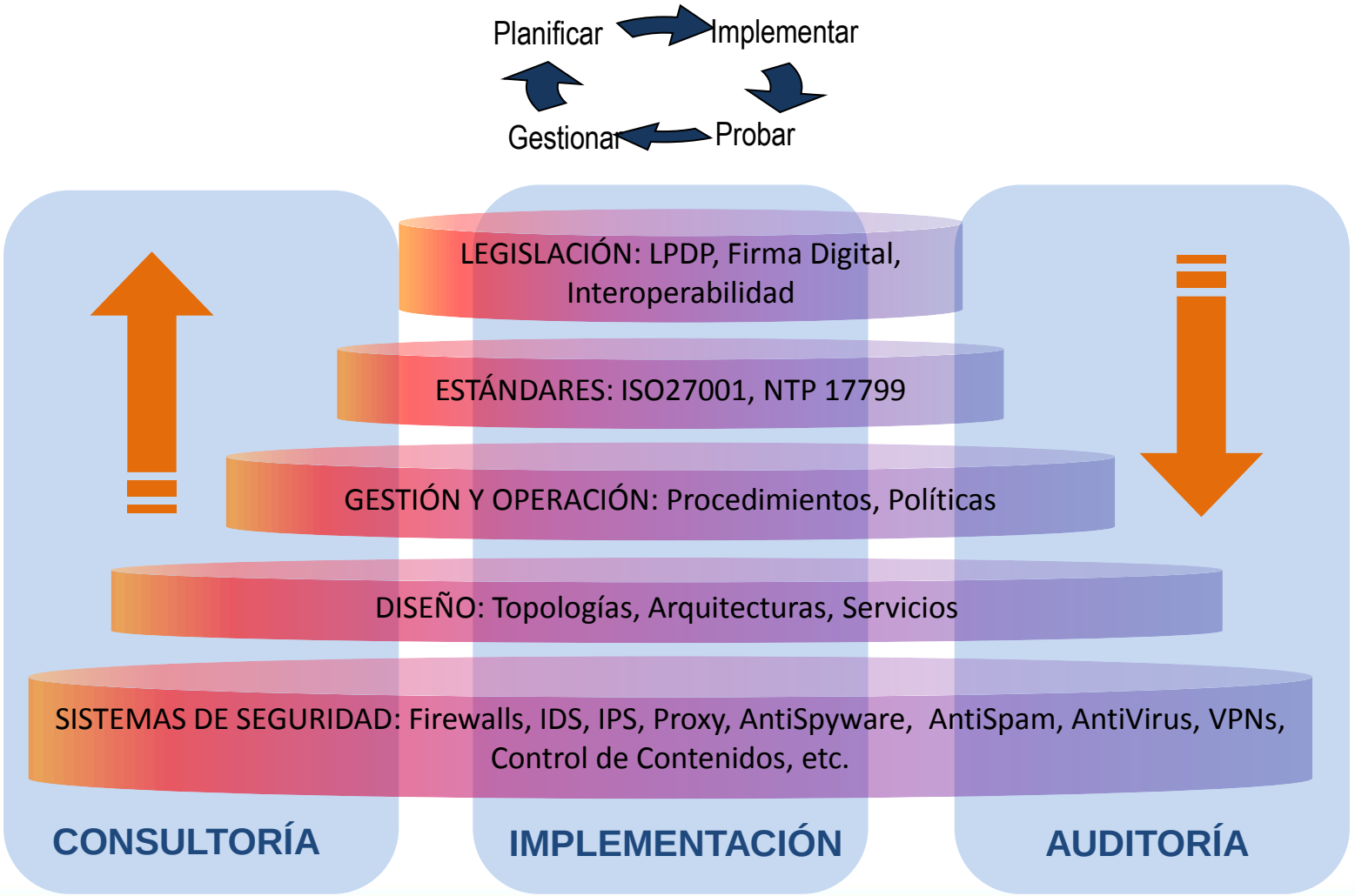
¡A quién va a interesarle mi información!

Ya sería mala suerte que tuviese una Inspección

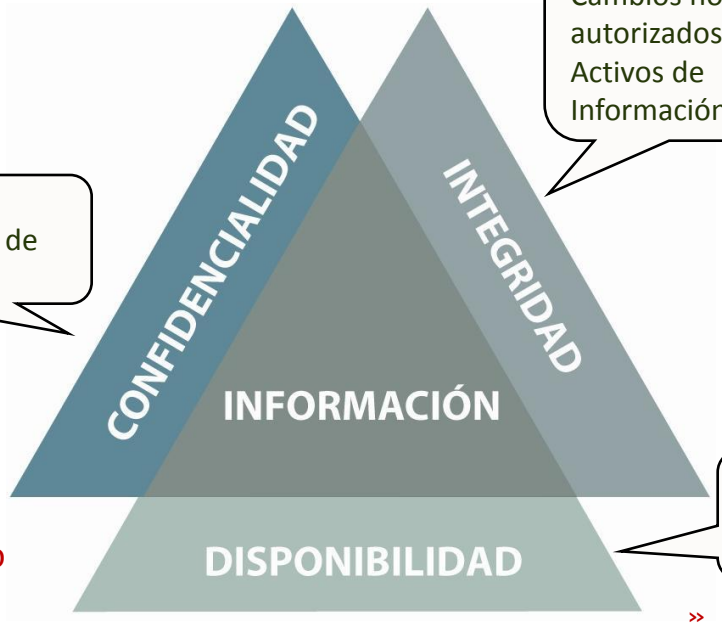
Tengo un Firewall, así que estoy protegido

¡Lo que me interesa es que FUNCIONE YA!, después ya veremos la seguridad…

Visión de la seguridad



Asegurando la información



Prevenir
Cambios no autorizados en Activos de Información.

- Validez y Precisión de información y sistemas.
- SINO: Información manipulada, incompleta, corrupta y por lo tanto mal desempeño de funciones.

Prevenir
Divulgación no autorizada de Activos de Información.

- Secreto impuesto de acuerdo con políticas de seguridad.
- SINO: Fugas y filtraciones de información; accesos no autorizados; pérdida de confianza de los demás (incumplimiento de leyes y compromisos).

Prevenir
Destrucción no autorizada de Activos de Información.

- Acceso en tiempo correcto y confiable a datos y recursos.
- SINO: Interrupción de Servicios o Baja Productividad.

Seguridad de la información

- En la ***GESTIÓN EFECTIVA DE LA SEGURIDAD*** debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores.
- El ***MODELO DE GESTIÓN DE LA SEGURIDAD*** debe contemplar procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

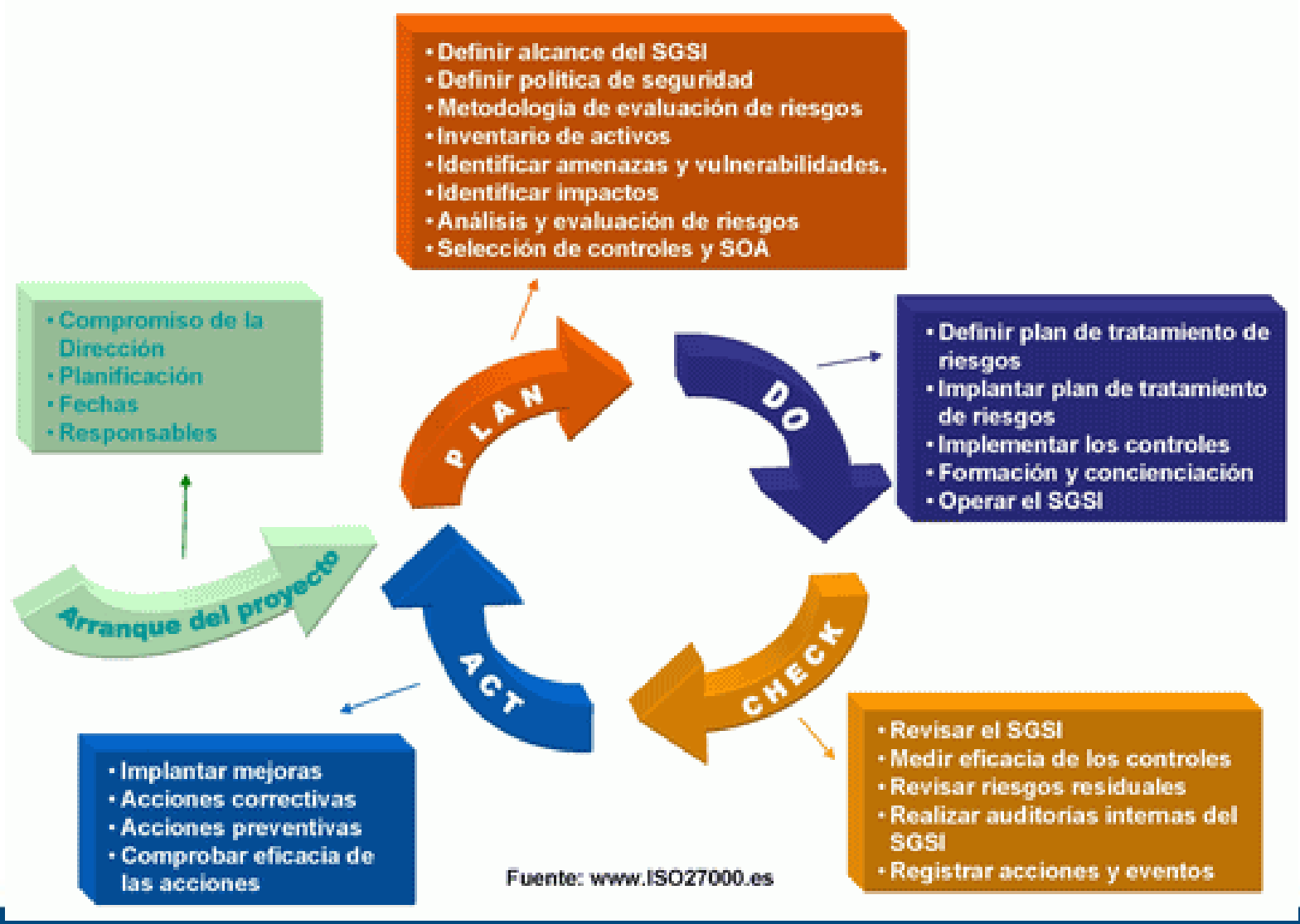
Sistema de Gestión de la Seguridad de la Información

- Es la ***HERRAMIENTA*** empleada por una organización para dotarse en cada momento de las *medidas* de seguridad *oportunas*, que proporcionen los niveles de *protección* de la información que en cada momento sean *necesarias*, de la forma más *eficiente*, en un entorno de *mejora continua*.

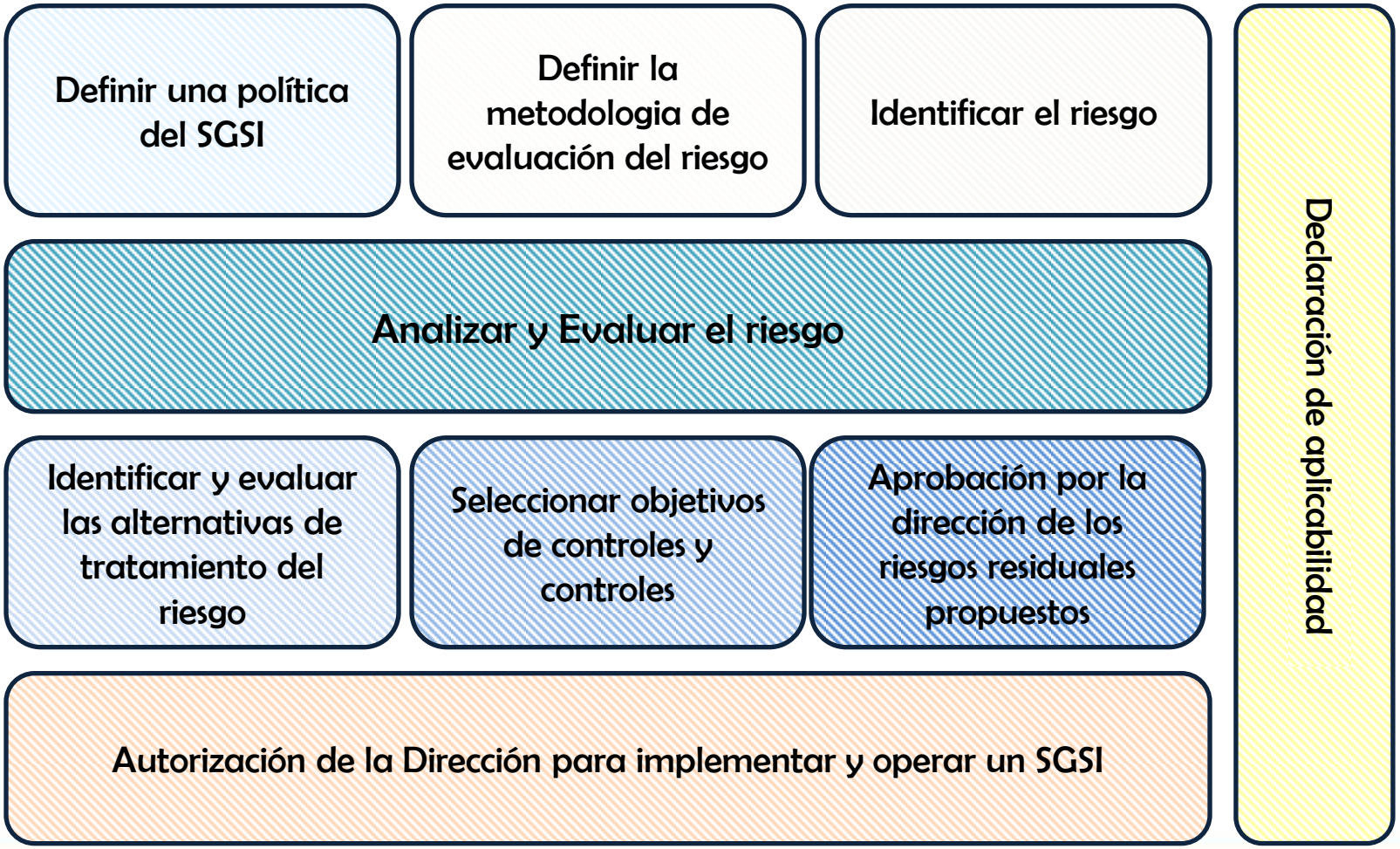
Sistema de Gestión de la Seguridad de la Información - SGSI

- Proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial.
- Ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.
- Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Fases del SGSI



Establecer el SGSI



Taller #1: Información sensible

- *Instrucciones*:
  1) Forme grupos de hasta 5 miembros,
  2) Identifique algún ***elemento de información*** dentro de la universidad que ustedes consideren que resultaría importante preservar.
  3) Discuta y formule una propuesta innovadora que permita resguardo del elemento de información, sus beneficios, y los beneficiarios.
- *Tiempo*: 35 minutos.

FIN

Carlos Trigo Pérez
trigoperezc@gmail.com