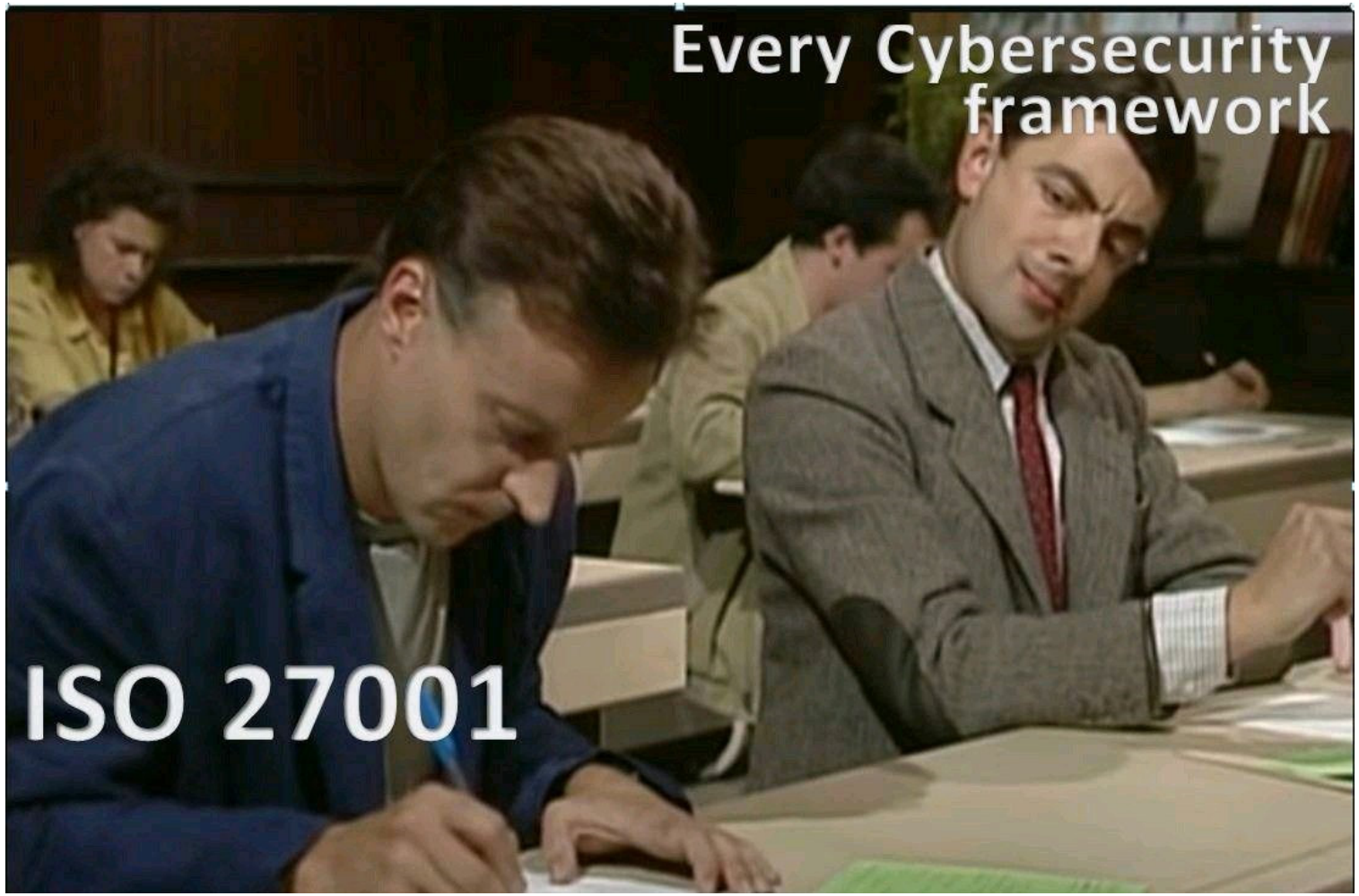
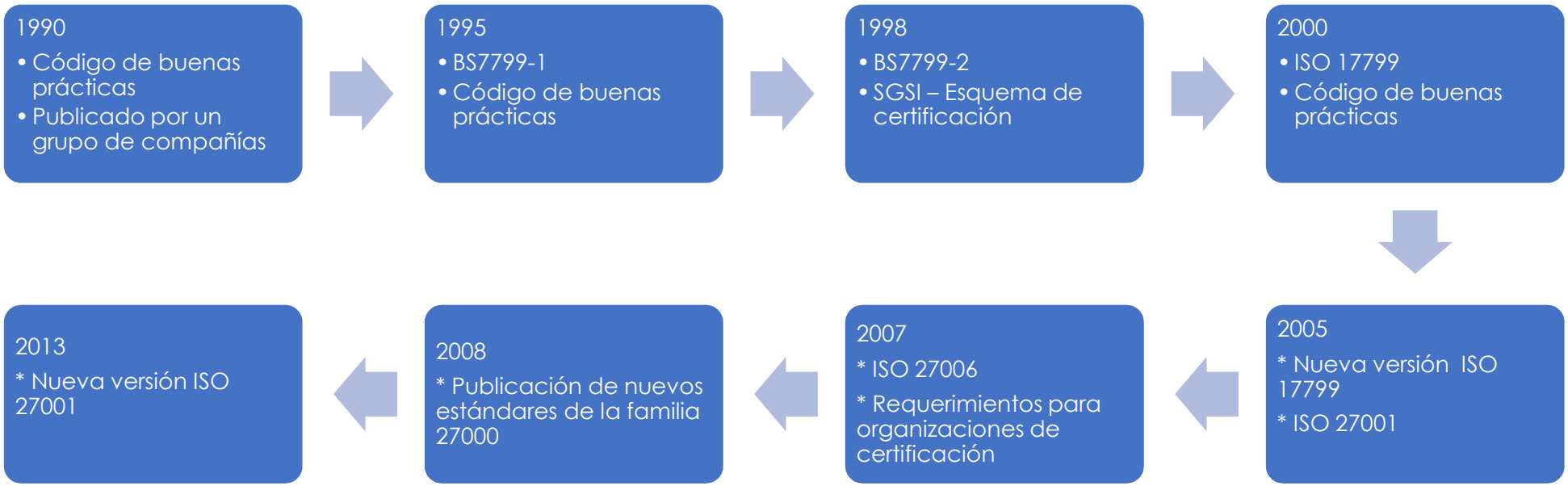
Sistema de Gestión de Seguridad de la Información (SGSI)

15 de noviembre del 2021

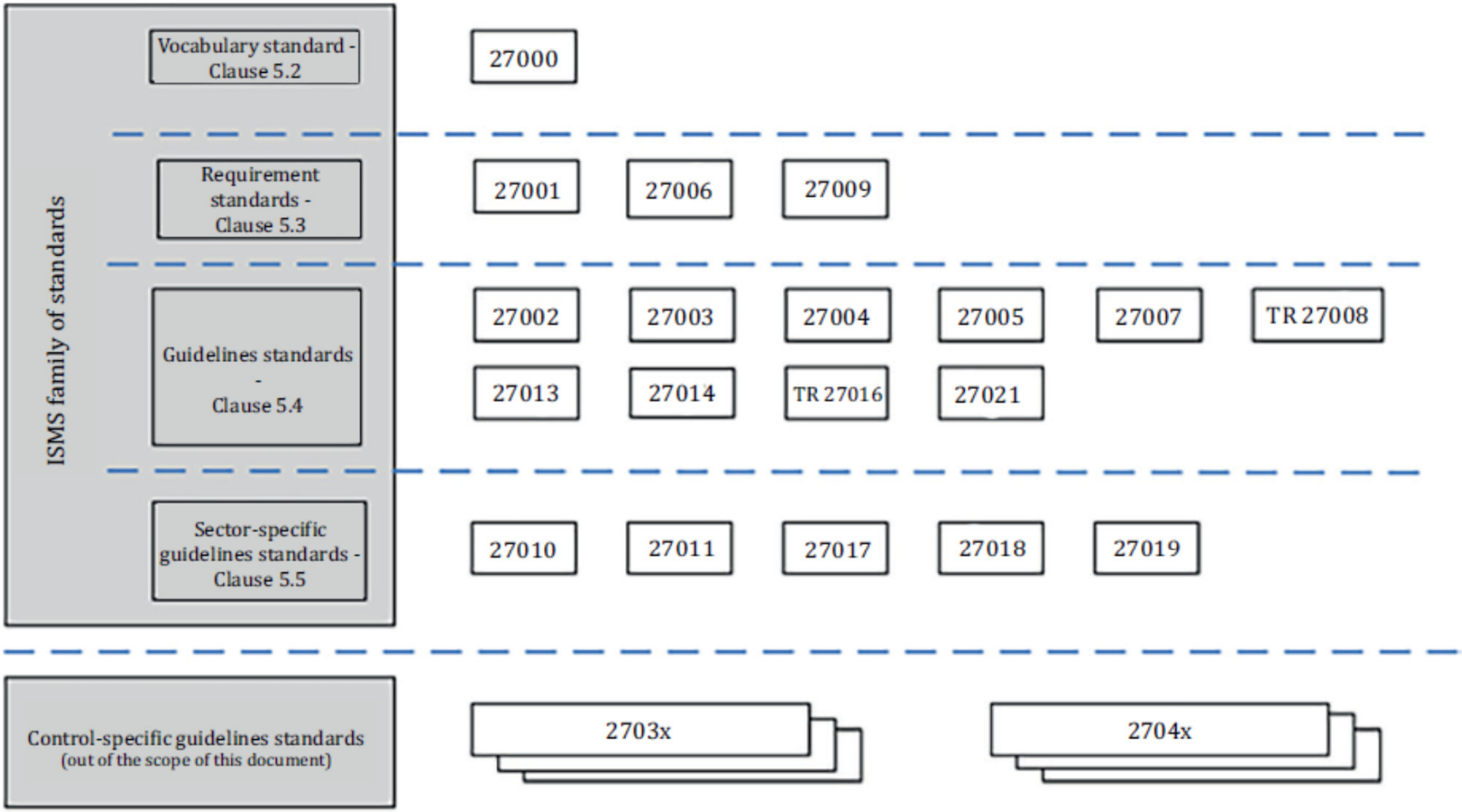
Introducción



HISTORIA


1990
• Código de buenas prácticas
• Publicado por un grupo de compañías
1995
• BS7799-1
• Código de buenas prácticas
1998
• BS7799-2
• SGSI – Esquema de certificación
2000
• ISO 17799
• Código de buenas prácticas
2005
* Nueva versión ISO 17799
* ISO 27001
2007
* ISO 27006
* Requerimientos para organizaciones de certificación
2008
* Publicación de nuevos estándares de la familia 27000
2013
* Nueva versión ISO 27001

Familia de Normas



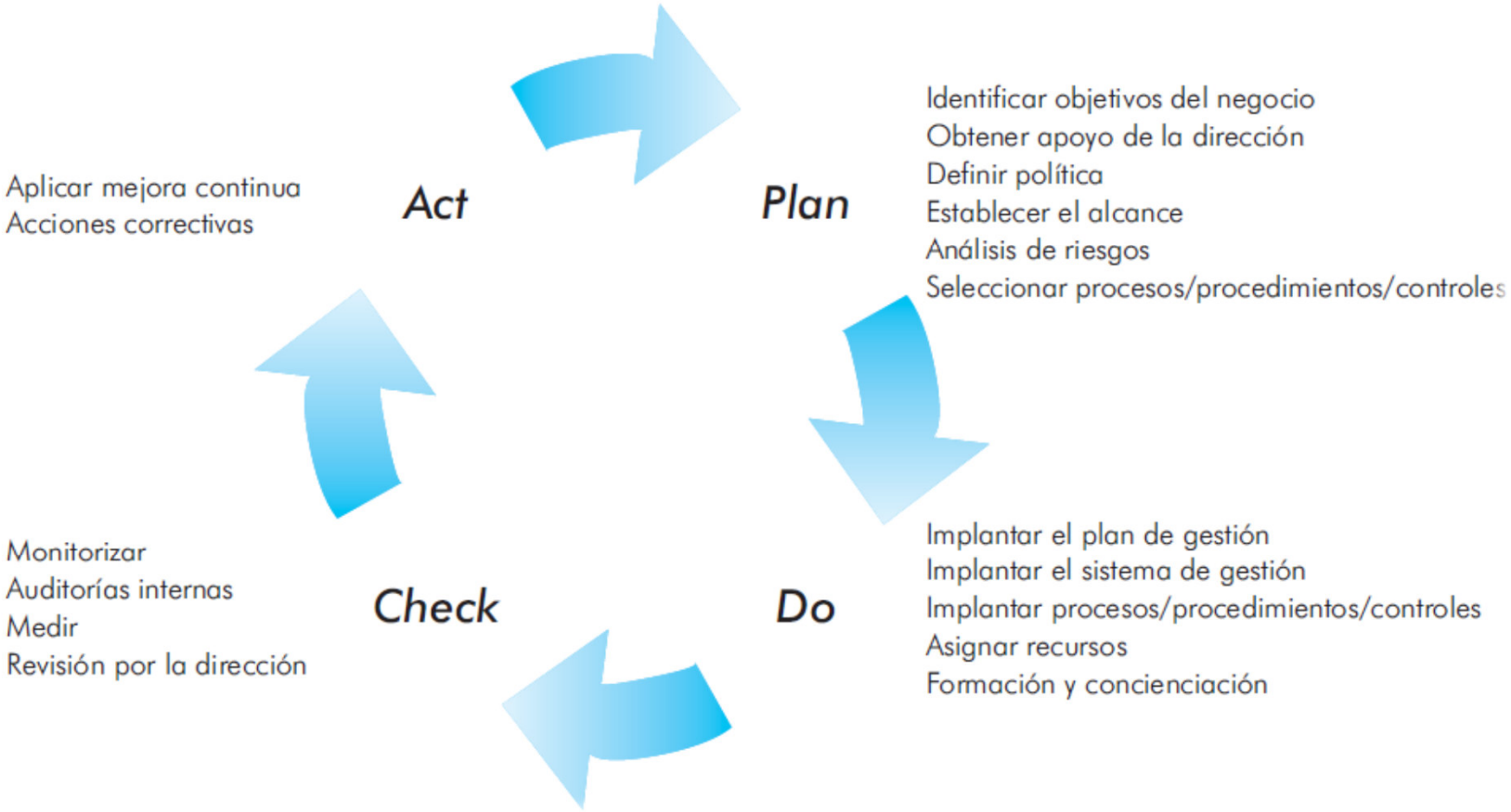
Estructura

- **4. Contexto de la organización**
  - 4.1 Comprensión de la organización y su contexto
  - 4.2 Comprensión de las necesidades y expectativas de las partes interesadas
  - 4.3 Determinación del alcance del SSI
  - 4.4. Sistema de gestión de seguridad de la información.
- **5. Liderazgo**
  - 5.1. Liderazgo y compromiso.
  - 5.2. Política
  - 5.3. Roles, responsabilidades y autoridades en la organización
- **6. Planificación**
  - 6.1. Acciones para enfrentar riesgos y oportunidades.
    - 6.1.1. Generalidades
    - 6.1.2. Evaluación de los riesgos de SI
    - 6.1.3. Tratamiento de los riesgos de SI
  - 6.2. Objetivos de SI y la planificación para alcanzarlos.
- **7. Apoyo**
  - 7.1. Recursos.
  - 7.2. Competencia
  - 7.3. Concienciación
  - 7.4. Comunicación.
  - 7.5. Documentación de la información
    - 7.5.1. Generalidades
    - 7.5.2. Creación y actualización
    - 7.5.3. Control de la información documentada
- **8. Operación**
  - 8.1. Planificación y control operacional
  - 8.2. Evaluación de los riesgos de SI
  - 8.3. Tratamiento de los riesgos de SI
- **9. Evaluación del desempeño**
  - 9.1. Seguimiento, medición, análisis y evaluación.
  - 9.2. Auditoria interna
  - 9.3. Revisión por parte de la dirección.
- **10. Mejora.**
  - 10.1 No conformidad y acción correctiva
  - 10.2 Mejora continua

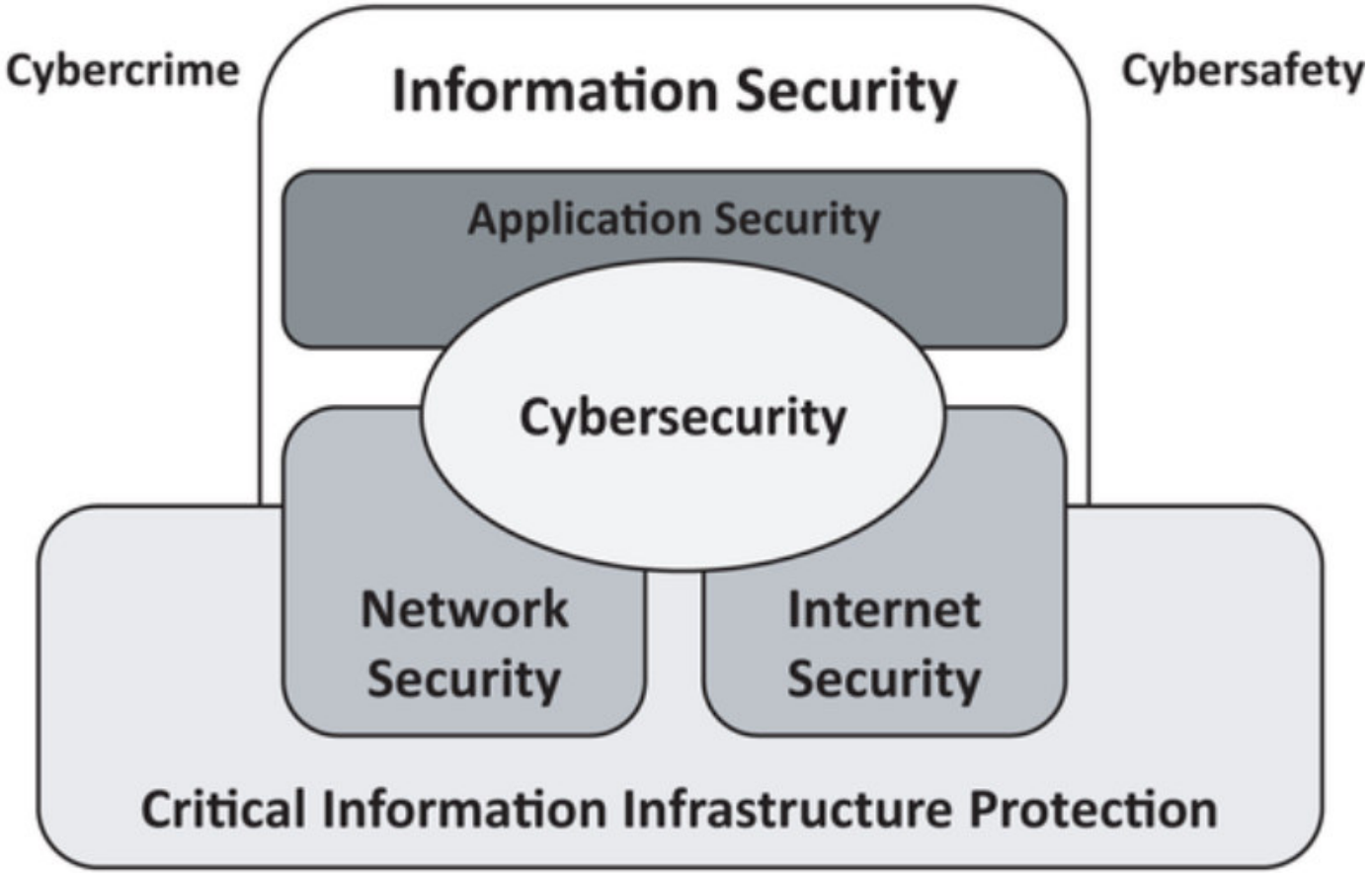
Controles

Controles de ISO 27001	• Política • Gestión de riesgos • Liderazgo • Información documentada • Indicadores
Controles del Anexo A de ISO 27001	• 114 controles
Controles específicos	• Base de datos • Cloud • Aplicaciones propietarias

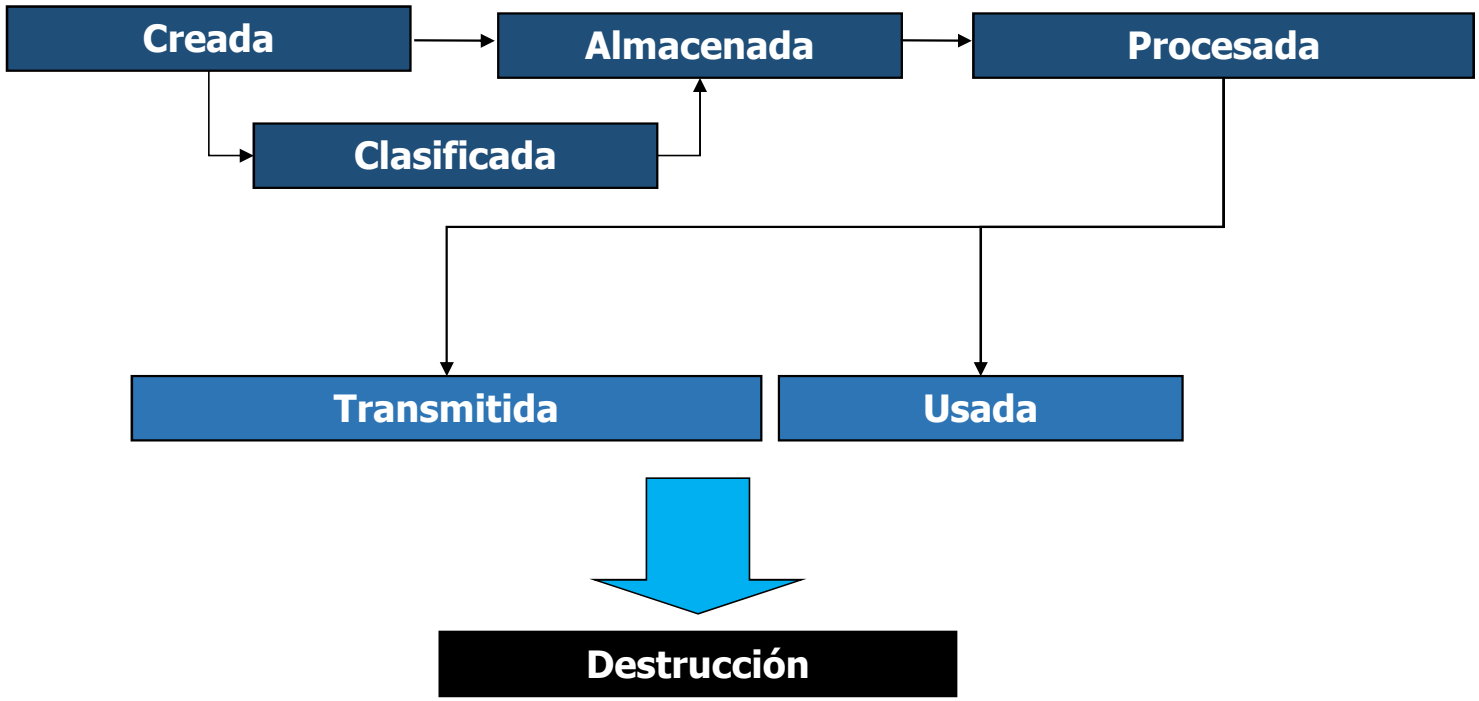
Mejora


Act
Aplicar mejora continua
Acciones correctivas
Plan
Identificar objetivos del negocio
Obtener apoyo de la dirección
Definir política
Establecer el alcance
Análisis de riesgos
Seleccionar procesos/procedimientos/controles
Do
Implantar el plan de gestión
Implantar el sistema de gestión
Implantar procesos/procedimientos/controles
Asignar recursos
Formación y concienciación
Check
Monitorizar
Auditorías internas
Medir
Revisión por la dirección

Conceptos similares



Ciclo de vida de la información



Alcance

La seguridad de la información es holística, cubre a cualquier tipo de información, independiente del medio en el que se encuentre:

- Papel
- Discos
- Verbal
- Video
- Audio
- Dispositivos ópticos
- Correo electrónico
- Conversaciones
- Información de la empresa en Internet

Criterios de seguridad de la información

C 

- **CONFIDENCIALIDAD:** La información **sólo debe ser conocida por el personal autorizado** que la requiera para el desarrollo de sus funciones.

I 

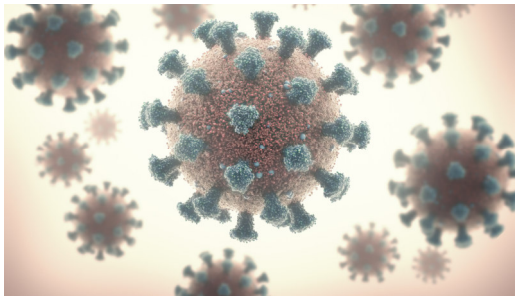
- **INTEGRIDAD:** la información **no debe ser alterada ni eliminada**, se debe garantizar su precisión, completitud, suficiencia y validez.

D 

- **DISPONIBILIDAD:** La información **debe ser accesible de manera oportuna**, según sus niveles de responsabilidad y autorización.

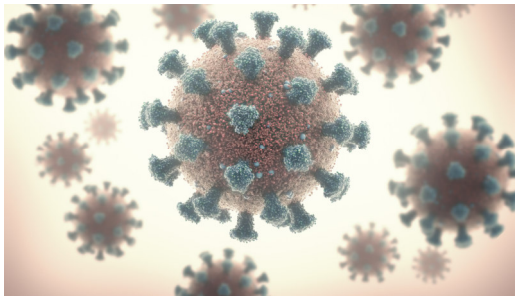
Amenazas

- **Causa** potencial de un incidente no deseado, que puede provocar daños a un sistema u organización.



Amenazas

- **Causa** potencial de un incidente no deseado, que puede provocar daños a un sistema u organización.



Vulnerabilidad

Debilidad de un activo o control que puede ser explotado por una o más amenazas.

Sistema de Gestión de Seguridad de la Información - SGSI

Sistema de Gestión, es aquel que utiliza un marco de recursos para alcanzar los objetivos de una organización. El sistema de gestión incluye estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos. (Definición tomada de ISO/IEC 27000:2018 – Traducción propia).

Sistema de Gestión de Seguridad de la Información - SGSI

SGSI: consiste en políticas, procedimientos, directrices, recursos y actividades asociados, los cuales son administrados por una organización, con el objetivo de proteger sus activos de información.

Fuente: ISO/IEC 27000:2018

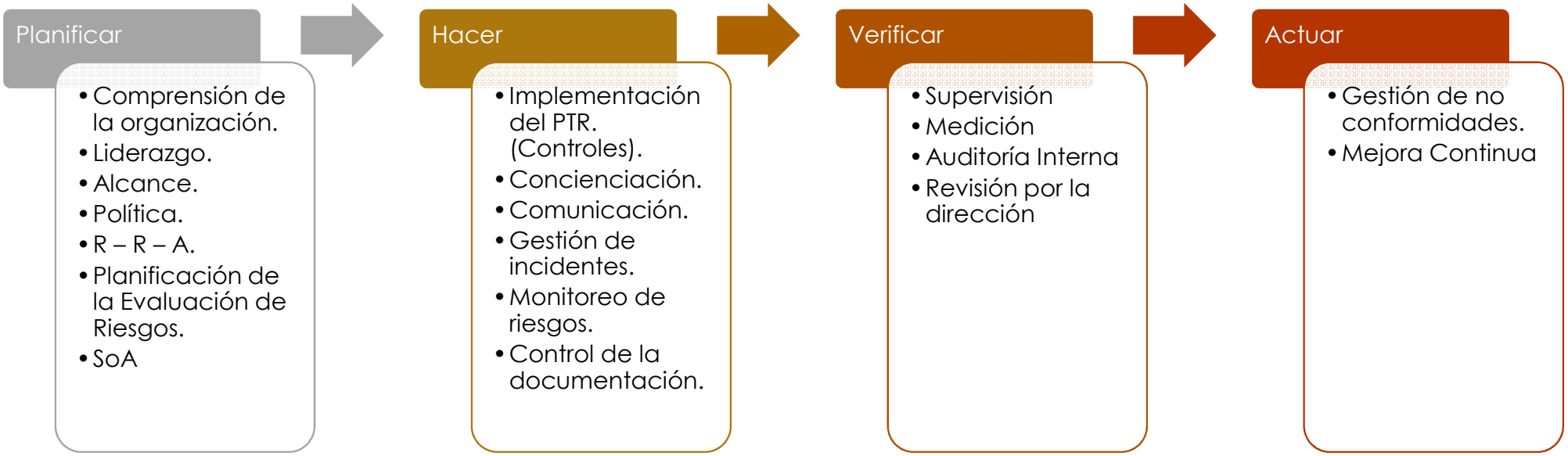
Principios del SGSI

1. Conciencia sobre la necesidad de seguridad de la información.
2. Asignación de responsabilidades.
3. Incorporar el compromiso de la alta dirección y partes interesadas.
4. Mejorar los valores sociales.
5. Evaluaciones de riesgos que determinan controles apropiados para alcanzar niveles aceptables de riesgo.
6. Seguridad incorporada como un elemento esencial de las redes y sistemas de información.
7. Prevención activa y detección de incidentes.
8. Garantizar un enfoque integral.
9. Reevaluación continua y actualización según corresponda.

Fuente: ISO/IEC 27000:2018

ISO/IEC 27001

Hoja de ruta para la implementación del SGSI



Información documentada requerida por ISO/IEC 27001

1. Alcance del SGSI (4.3).
2. Política de seguridad de la información (5.2).
3. Proceso de evaluación de riesgos de seguridad de la información (6.1.2).
4. Proceso de tratamiento de riesgos de seguridad de la información (6.1.3).
5. Declaración de aplicabilidad (6.1.3 d)) .
6. Objetivos de seguridad de la información (6.2).
7. Evidencia de competencia (7.2 d)).
8. Información documentada determinada por la organización como necesaria para la eficacia del SGSI (7.5.1. b)).
9. Planificación y control operacional (8.1).
10. Resultados de las evaluaciones de riesgos de seguridad de la información (8.2).
11. Resultados del tratamiento de riesgos de seguridad de la información (8.3).
12. Evidencia de los resultados del seguimiento y la medición (9.1).
13. Evidencia de los programas de auditoría y los resultados de la auditoría (9.2 g)).
14. Evidencia de los resultados de las revisiones por la dirección (9.3).
15. Evidencia de la naturaleza de las no conformidades y cualquier acción posterior tomada (10.1 f)).
16. Evidencia de los resultados de cualquier acción correctiva (10.1 g)).

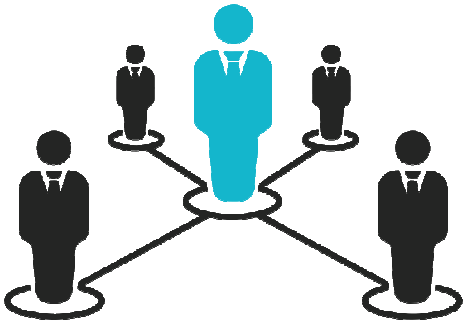
Factores de éxito en "Liderazgo – Planificación"

LIDERAZGO

Máxima autoridad de la organización

PLANIFICACIÓN

Responsable de Seguridad de la Información

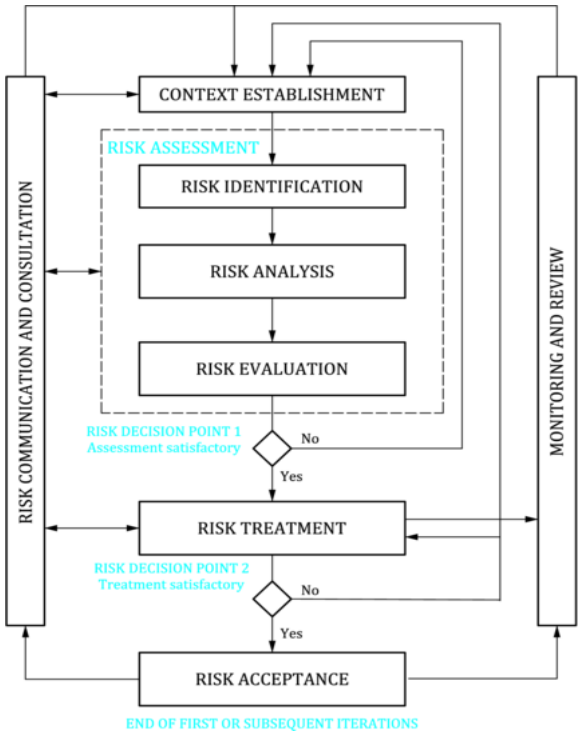


Factores de éxito en “Soporte”

Cultura & Conciencia ción

Factores de éxito en “Operación”

Gestión y monitoreo de riesgos



Factores de éxito en “Evaluación”

Sin seguridad de la información y/o ciberseguridad, **no** existe "Transformación Digital".

GRACIAS POR SU ATENCIÓN

Más información: www.seps.gob.ec
Av. Amazonas N32-87 y La Granja
PBX: (593 2) 394 8840