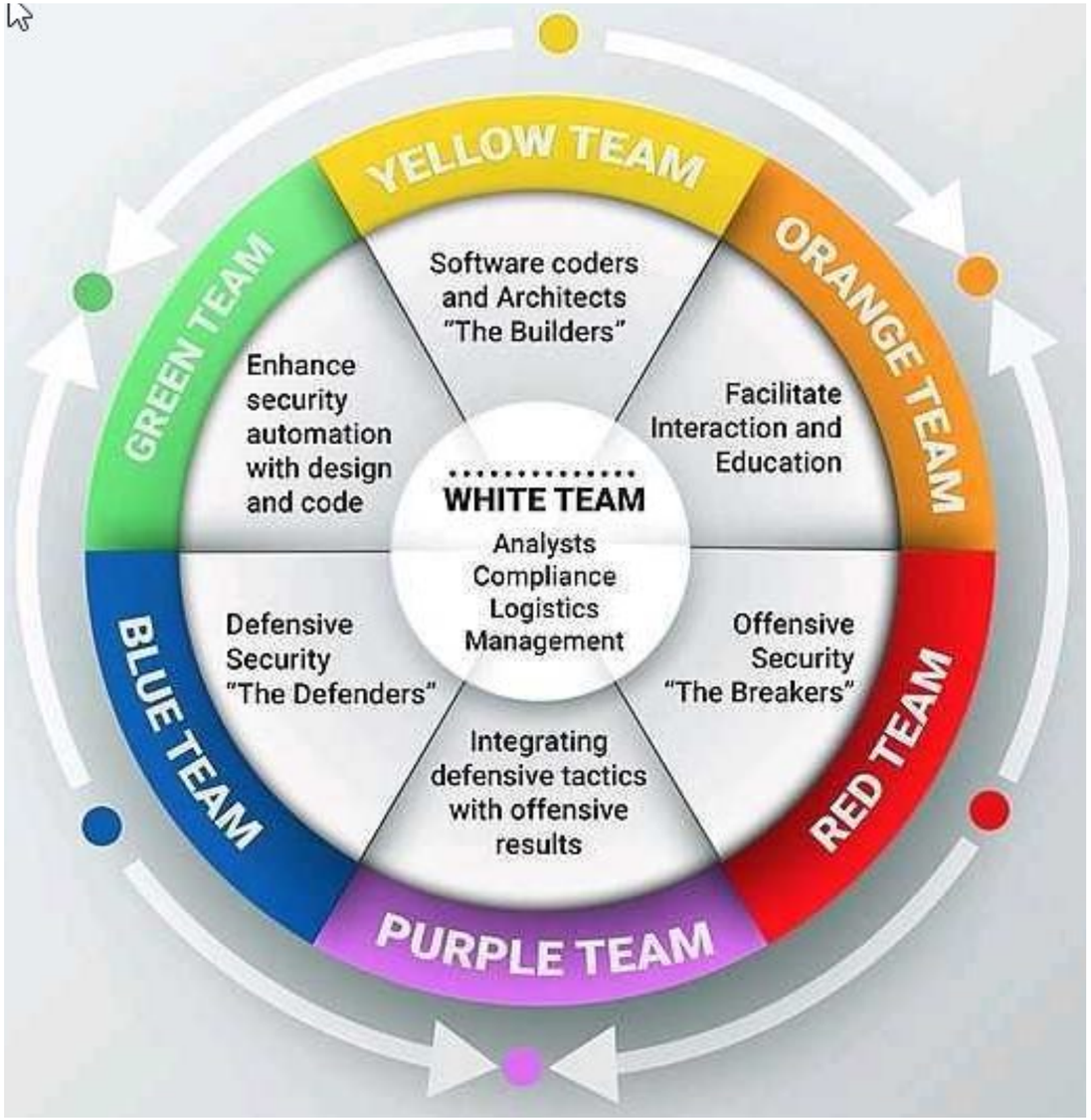
THE BRIDGE

CYBER SECURITY

Fundamentos de un SGSI

I

Equipos en Ciberseguridad

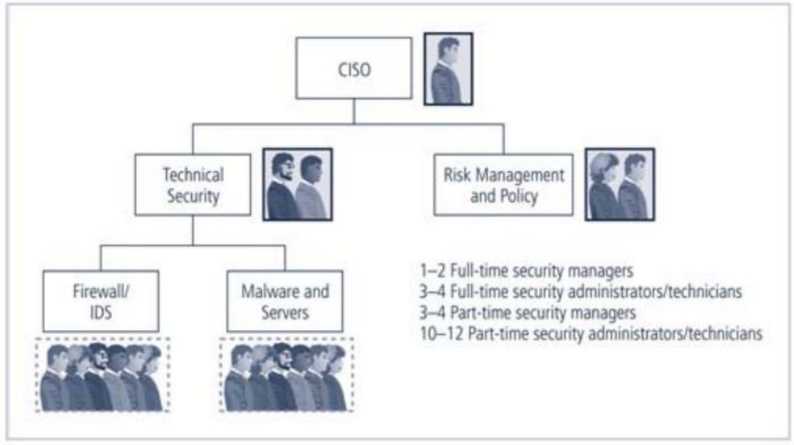


https://www.veritas.com/es/es/blogs/cyber-security-as-a-team-sport

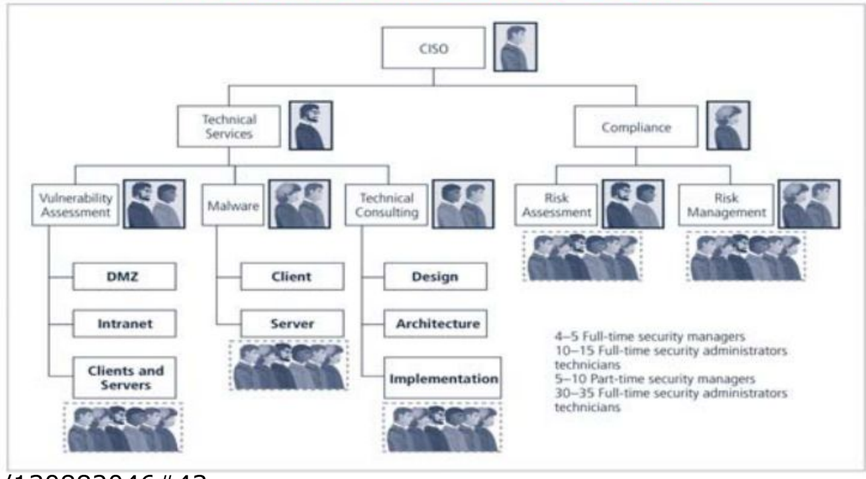
Ejemplos de Organigrama área de Ciberseguridad

https://www.linkedin.com/posts/hermes-jos%C3%A9-berbesi-bustamante-7344b186_gesti%C3%B3n-de-la-ciberseguridad-perfiles-de-activity-7217604480433876992-fYpc/?originalSubdomain=es

Típico Organigrama del Staff en Seguridad de la Información en las Grandes Organizaciones



Típica Estructura de Organización en Seguridad de la Información en una Muy Grande



https://es.slideshare.net/slideshow/4482-l3/130882046#43

Algunos Términos Básicos

- **Activo**: cualquier elemento que tiene valor para la organización, ya sea tecnológico, persona, información, documentos en papel, entre otros.
- **Confidencialidad**: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Integridad**: propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Disponibilidad**: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

https://www.pmg-ssi.com/2021/02/las-buenas-practicas-de-la-seguridad-de-la-informacion/

Algunos Términos Básicos

- **Amenaza**: Corresponde a toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad del sistema de gestión de seguridad de la información.
  - Algunos ejemplos son:
    - Fraude asistido por computadora
    - Espionaje, sabotaje y vandalismo
    - Fenómenos naturales
    - Desconocimiento o mal uso de la información por parte del recurso humano

- **Vulnerabilidad**: Es una debilidad o fallo en el sistema de gestión de seguridad de la información que pone en riesgo la seguridad de la información.
  - por ejemplo, pueden presentarse:
    - Fallos en los diseños.
    - Errores de configuración.
    - No generar backup de información.
    - Carencias de procedimiento y controles.

- **Riesgo**: Es la posibilidad de que una amenaza explote una vulnerabilidad en un activo de información, causando un impacto negativo en la organización.
  - El riesgo se evalúa considerando tanto la probabilidad de que ocurra el evento como la gravedad de sus consecuencias
  - **Ejemplo:**
    - Phishing
    - Ramsonware
    - Etc.

https://www.pmg-ssi.com/2021/02/las-buenas-practicas-de-la-seguridad-de-la-informacion/

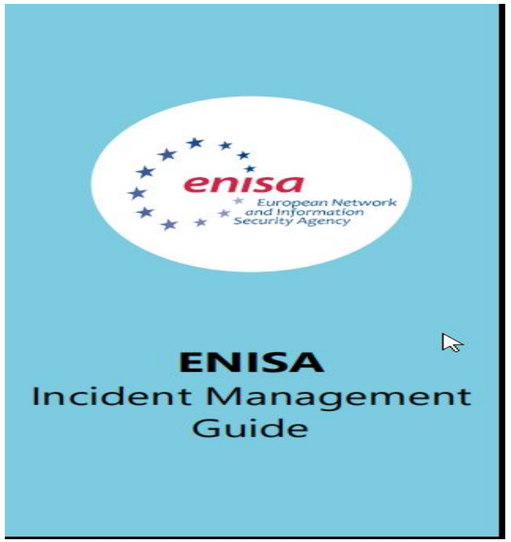
Gobierno, Riesgo y Cumplimiento (GRC).

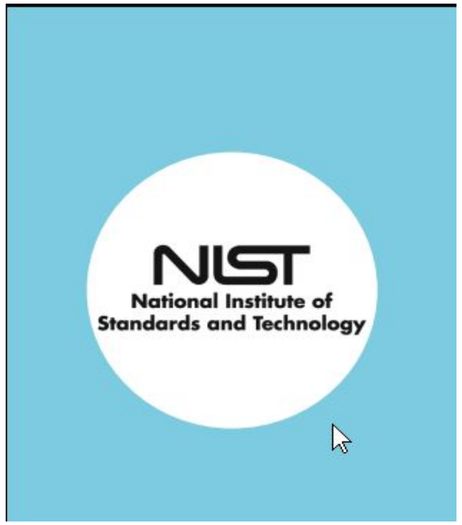
- **Gobierno, Riesgo y Cumplimiento (GRC)** aglutinan los principales imperativos del mundo de la ciberseguridad hoy en día.
- Contar con una estructura de estas características significa tener una visión holística de la superficie de exposición y mejorar las auditorías internas y las relaciones con la legislación.
- Además, otorga un enfoque estructurado que alinea el departamento de TI con los objetivos de negocio.

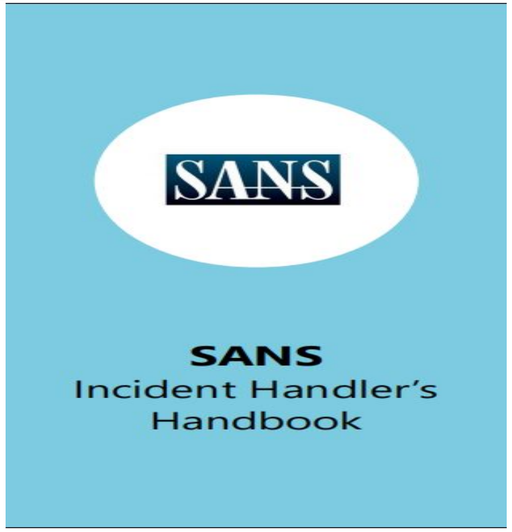
http://cef-ugr.org/wp-content/uploads/2017/03/19-20-David-Garcia-Vega.pdf

Metodologías

- **TODAS TIENEN EL MISMO OBJETIVO: IMPLANTACIÓN, MANTENIMIENTO Y EVOLUCIÓN DE UN SGSI**

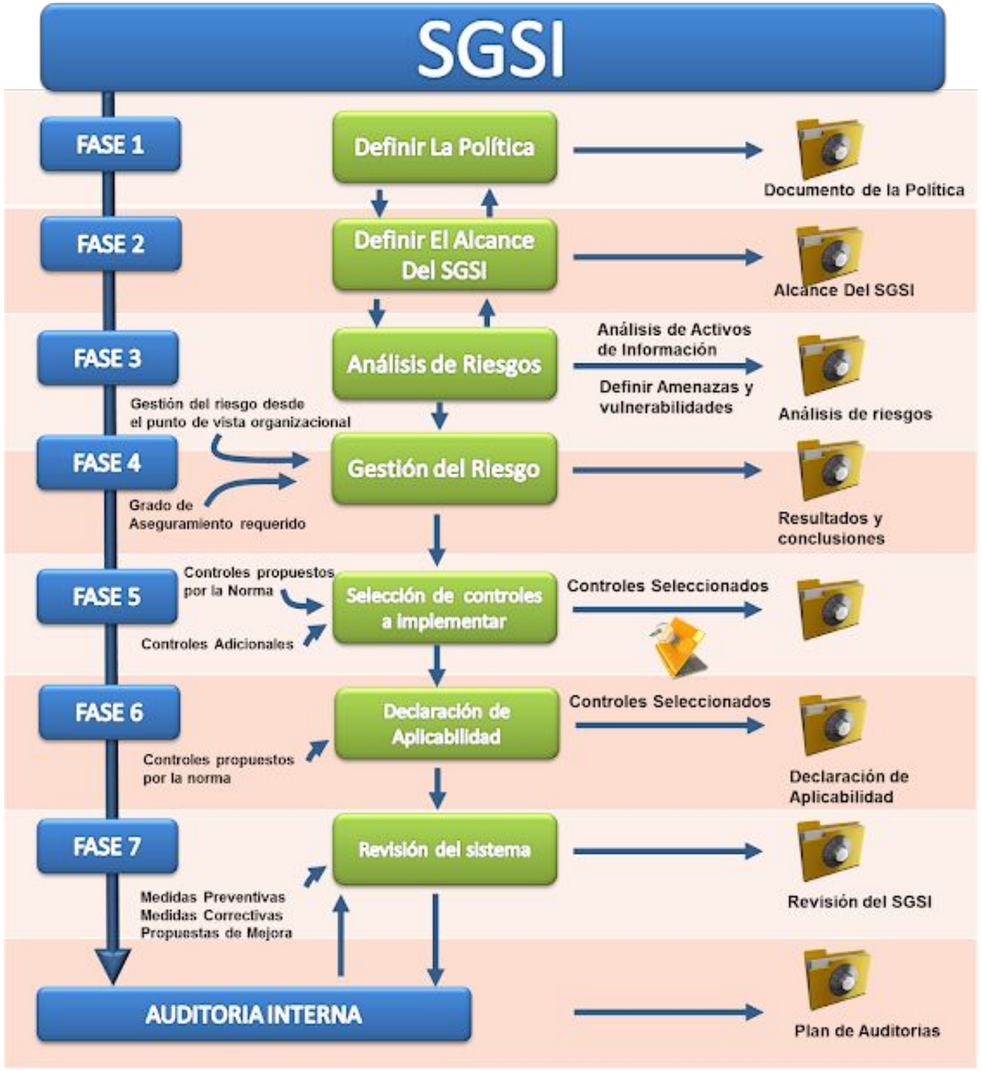






SGSI

- **SGSI** son las siglas de **Sistema de Gestión de Seguridad de la Información**.
- Es un conjunto de políticas y procedimientos para gestionar sistemáticamente los datos confidenciales de una organización.
- El objetivo de un **SGSI** es minimizar el riesgo y garantizar la continuidad del negocio limitando proactivamente el impacto de una brecha de seguridad. Básicamente, busca lograr un sistema de prácticas por parte de todo el personal de la empresa para que esta no pierda información.
- Un **SGSI** desde la visión del estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (p.ej. en empresas públicas, organizaciones sin ánimo de lucro, ...)



https://siforense.blogspot.com/2016/05/sistema-de-gestion-de-la-seguridad-de.html

Diferencia entre el SI y el SGSI

SISTEMA DE INFORMACIÓN

Es un conjunto de elementos, habitualmente tecnológicos pero pueden incluir personas, que interactúan para soportar los servicios, tratando la información que éstos requieren.

SISTEMA DE GESTIÓN

Es el conjunto de instrumentos organizativos (Políticas, normas internas, procedimientos) interrelacionados y orientados a mejorar la eficacia y la eficiencia de lo gestionado (por ejemplo, la seguridad de un Sistema de Información).

Para que sirve un SGSI

- Es fundamental para proteger la información de la organización.
- un SGSI es una herramienta integral que ayuda a las organizaciones a proteger su información, cumplir con las normativas y mejorar continuamente sus prácticas de seguridad
- Ayuda a establecer el marco documental en donde están las políticas y procedimientos con 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.
- Garantiza que la información sea accesible solo para quienes están autorizados (confidencialidad), que los datos sean precisos y completos (integridad), y que estén disponibles cuando se necesiten (disponibilidad.
- Al gestionar los riesgos de manera eficiente, se pueden reducir los costes asociados con incidentes de seguridad y optimizar el uso de recursos.
- Incrementa la confianza de clientes y socios al demostrar un compromiso con la seguridad de la información, mejorando la reputación de la organización.

https://siforense.blogspot.com/2016/05/sistema-de-gestion-de-la-seguridad-de.html

Beneficios de tener un SGSI

Un SGSI tiene los siguientes **beneficios**:

Cara al exterior de la empresa:

- **Mejorar la confianza** con clientes, proveedores y partners.
- Asegurar la **conformidad** con la legislación y los contratos firmados.

Cara al interior de la empresa:

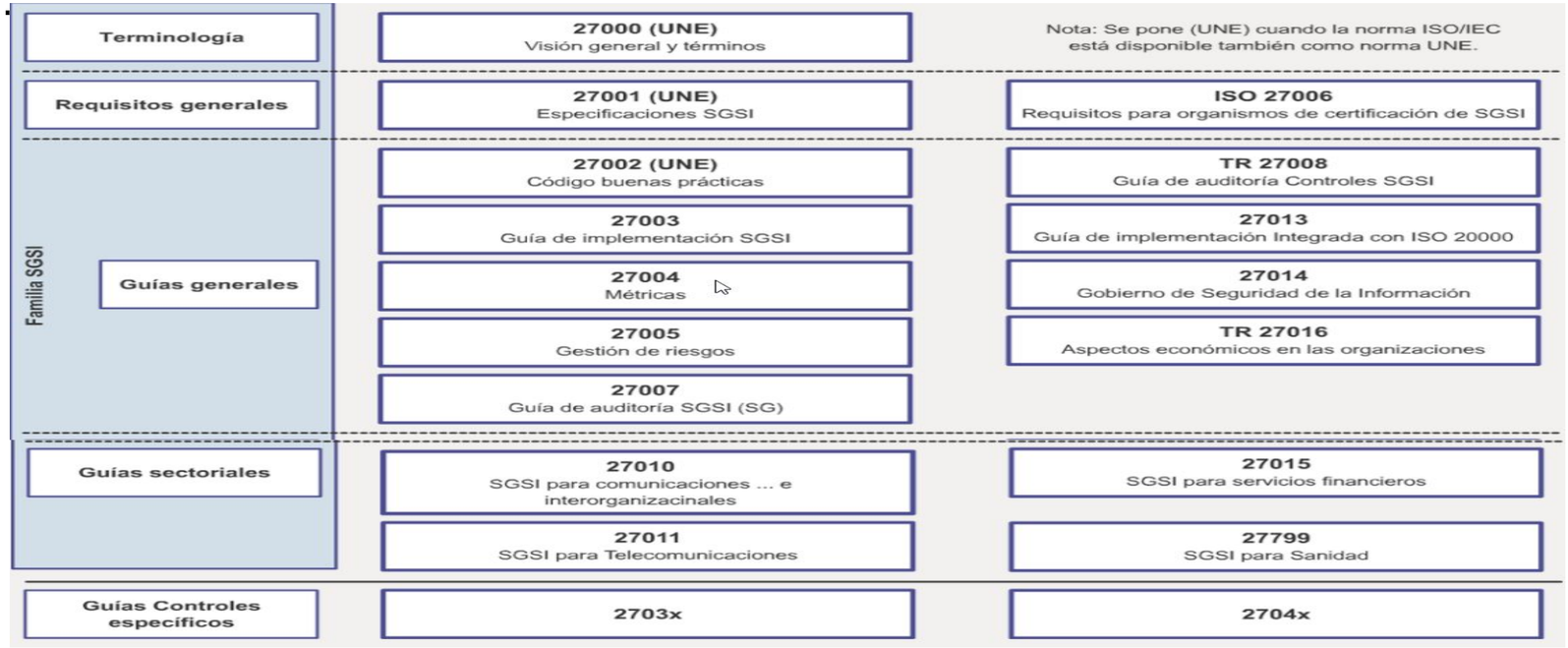
- **Garantía interna** de una adecuación independiente de la seguridad a sus objetivos.
- **Mejorar el R.O.I.** (Return Of Investments - Retorno de la Inversión) de la tecnologías y de la seguridad.
- **Reducir el impacto** de los incidentes.
- **Consistencia** de las acciones de seguridad.
- **Alineamiento con estándares** de T.I (Tecnologías de la Información).

¿Que es la Norma ISO 27000?

- La serie **ISO 27000** es un conjunto de estándares internacionales desarrollados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

- Aquí tienes una breve descripción de algunos de los estándares más importantes dentro de esta serie:

  - **ISO 27001**: Especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Es la norma más importante y certificable.
  - **ISO 27002**: Proporciona un conjunto de buenas prácticas para la implementación del SGSI, con 93 controles estructurados en 4 dominios.
  - **ISO 27003**: Guía para la implementación correcta de un SGSI.
  - **ISO 27004**: Pautas para definir y establecer métricas para evaluar el rendimiento del SGSI.
  - **ISO 27005**: Gestión de riesgos vinculados a los sistemas de gestión de la información.
  - **ISO 27006**: Requisitos para organizaciones que quieran certificar a otras en ISO/IEC 27001.
  - **ISO 27007**: Procedimientos para auditorías internas y externas.
  - **ISO 27008**: Evaluación de controles del SGSI.



Que incluye un SGSI

- En el ámbito de la gestión de la calidad según **ISO 9001**, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles.

- Si trasladamos a la normativa **ISO 27001**, seria así:

  - **Manual de seguridad**: Documentación que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del **SGSI**.

  - **Procedimientos**: Documentación que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

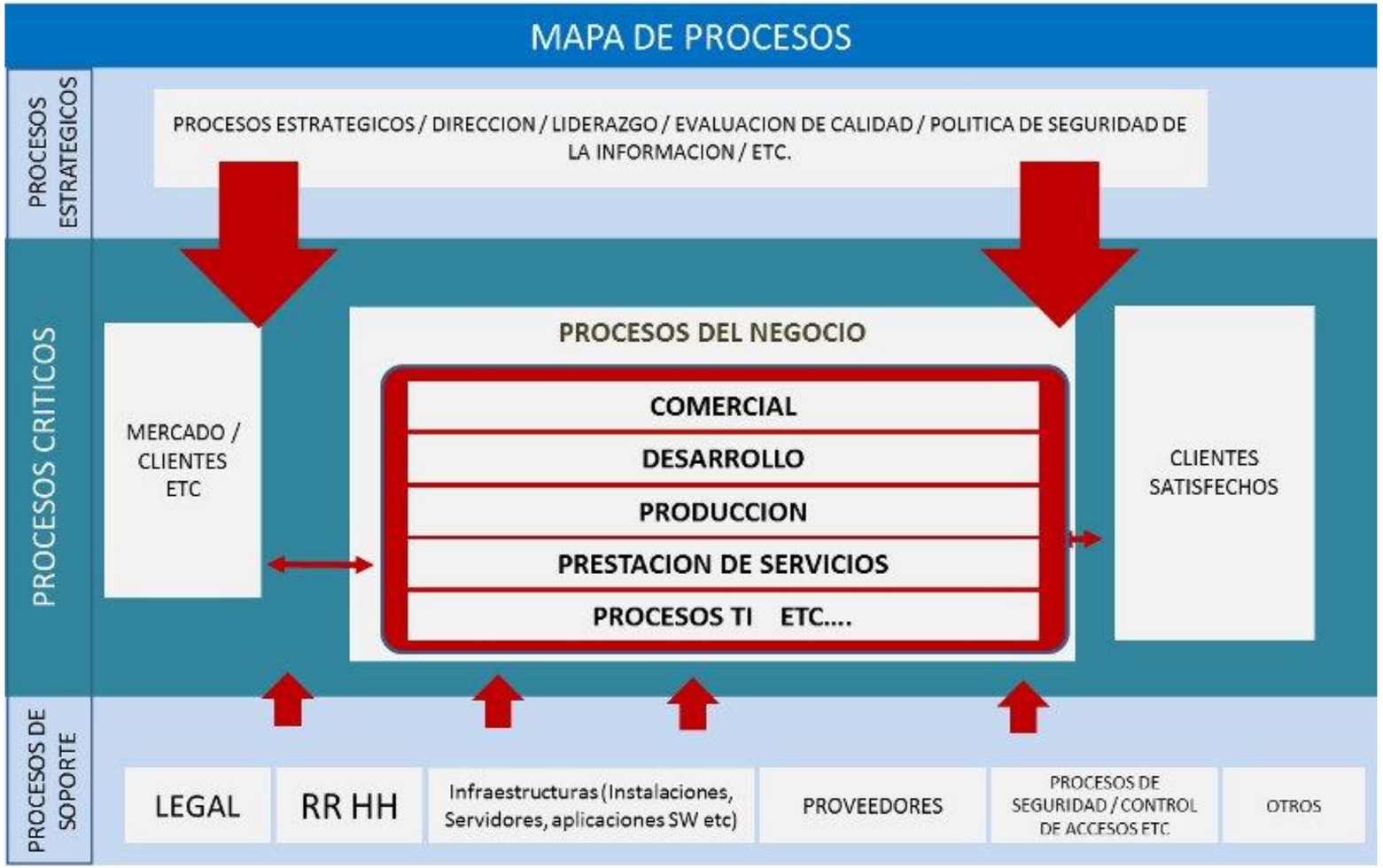
  - **Instrucciones, checklists y formularios**: Documentación que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

  - **Registros**: Documentación que proporcionan una evidencia objetiva del cumplimiento de los requisitos del **SGSI**; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

https://siforense.blogspot.com/2016/05/sistema-de-gestion-de-la-seguridad-de.html

8 Fases de Implementación del SGSI

- **1.-Establecer el alcance y contexto**
  - El alcance del **SGSI** aclara los límites del **SGSI** en función del contexto y/o importancia.
  - Ubicación de los activos críticos de información de la organización (por ejemplo, unidades, ubicaciones o departamentos)
  - Los riesgos propios o externos asociados (p.ej. leyes y reglamentos, obligaciones contractuales, estrategias y políticas impuestas por organismos centrales).
  - Se debe tener en cuenta los flujos de información que cruza los límites del alcance del negocio.
  - Una estrategia de **alto nivel** impulsada por la organización o una declaración de visión (ya sea hecha o al menos formalmente respaldada por la alta gerencia) es una forma de cristalizar tanto el alcance como el propósito de aplicación del SGSI, y puede ser útil para fines de concientización, así como de promoción.



https://www.normaiso27001.es/objeto-y-campo-de-aplicacion/

8 Fases de Implementación del SGSI

- **2.-Realizar una evaluación de riesgos.**
  - Inventario de todos los Activos de información.
  - Identificar las posibles Amenazas
  - Identificar Vulnerabilidades
  - Identificar aspectos Legales.
  - Análisis de impacto
  - Selección de los controles.
  - Aplicar tratamiento del riesgo.

https://www.normas-iso.com/iso-27001/

8 Fases de Implementación del SGSI

- **3.-Desarrollar una política de seguridad:**

  - Crear políticas y procedimientos que establezcan cómo se manejará la seguridad de la información en la organización.

  - Algunos ejemplos son:
    - Política del Sistema de Gestión de Seguridad de la Información (SGSI).
    - Control de acceso físico.
    - Limpieza del puesto de trabajo.
    - Software no autorizado.
    - Copias de seguridad.
    - Intercambio de información con otras organizacione
    - Uso de los servicios de mensajería.
    - Retención de registros.
    - Uso de los servicios de red.
    - Teletrabajo.
    - Política de cumplimiento de disposiciones legales.
    - Uso de licencias de software.
    - Protección de datos y privacidad.

https://siforense.blogspot.com/2016/05/sistema-de-gestion-de-la-seguridad-de.html


THE
BRIDGE