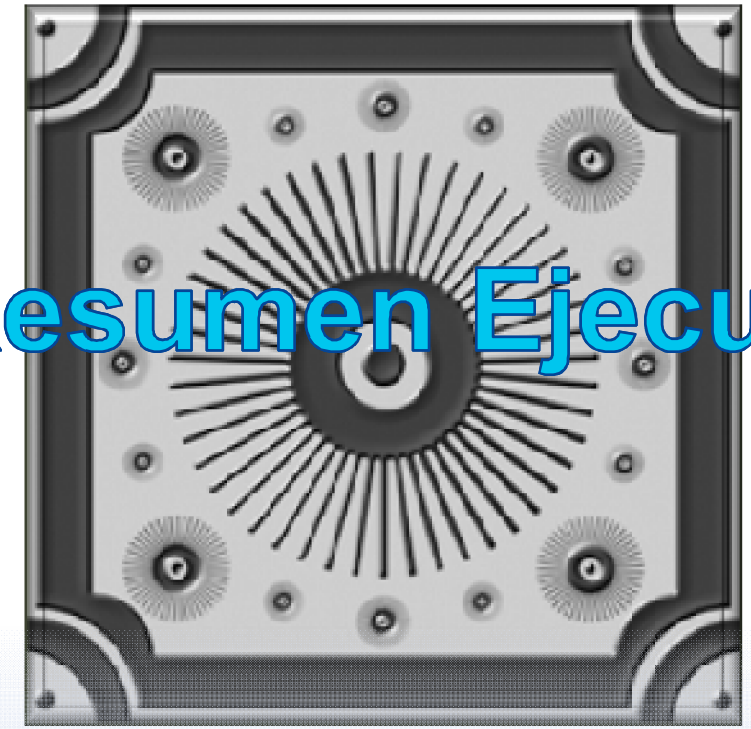
Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Elaboración Plan de Implementación de la ISO 27001-SOC



Resumen Ejecutivo

(*)-Caja fuerte de pared con muchas ruedas de bloqueo para mayor seguridad (licencia Creative Commons-openclipart)

ÍNDICE

Objetivo del Proyecto

El desarrollo del presente TFM tiene como objetivo la realización de un proyecto que lleve a cabo la realización de un **Plan Director de Seguridad de la Información** (PDSI) tomando como referencia un modelo de empresa real.

Aspectos Principales

- **El Conocimiento de las estrategias y objetivos de la Organización.**
- **El Conocimiento de la situación actual de la organización Seguridad de la Información.**
- **La Elaboración de las propuestas de los Proyectos a acometer y su planificación.**
- **La evaluación del estado actual estableciendo el nivel de madurez de cumplimiento de la Seguridad de la Información**

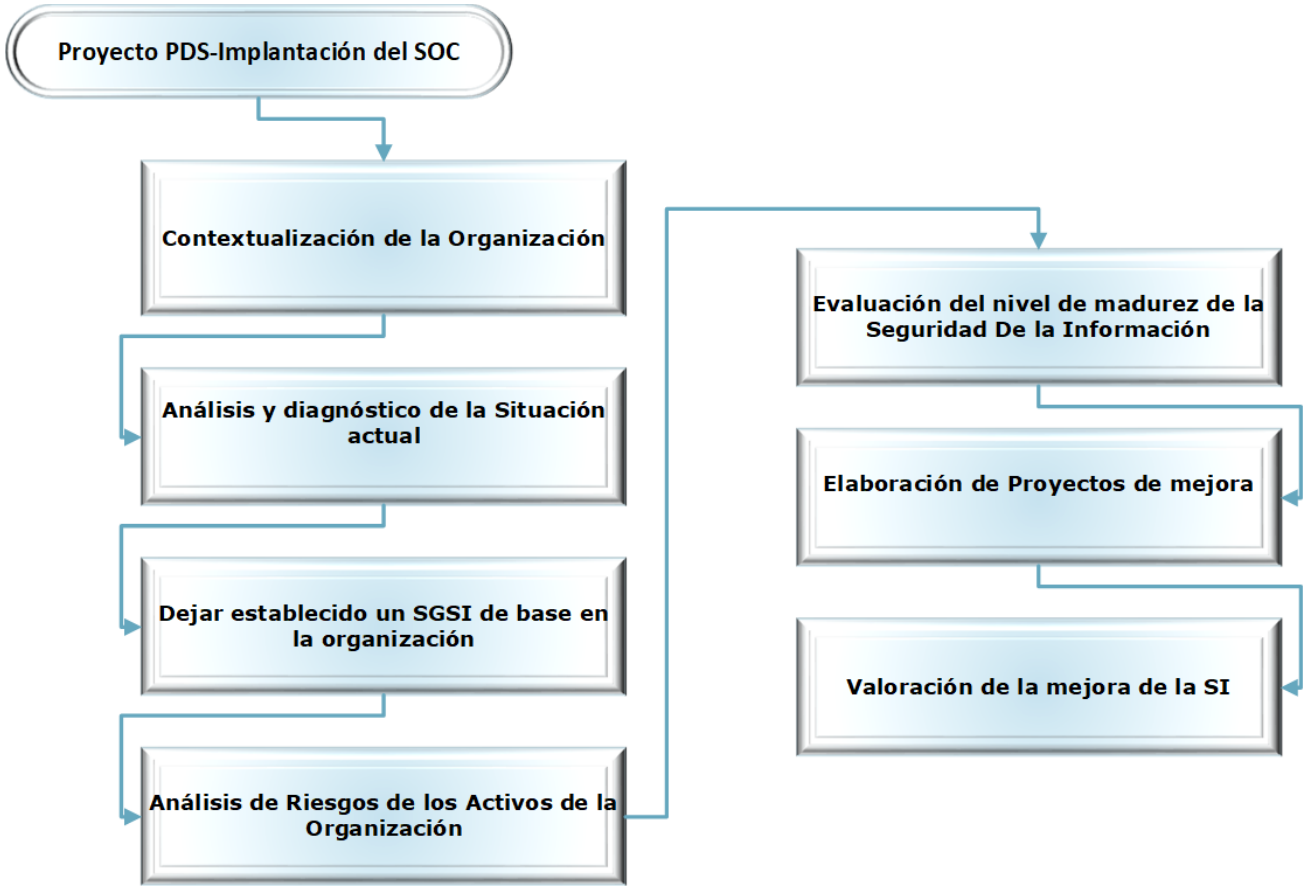
Metodología

La UNE-ISO/IEC 27001-Sistemas de Gestión de Seguridad de la Información-Requisitos (UNE-ISO/IEC 27001-Tecnología de la información-Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información (SGSI)-Requisitos)

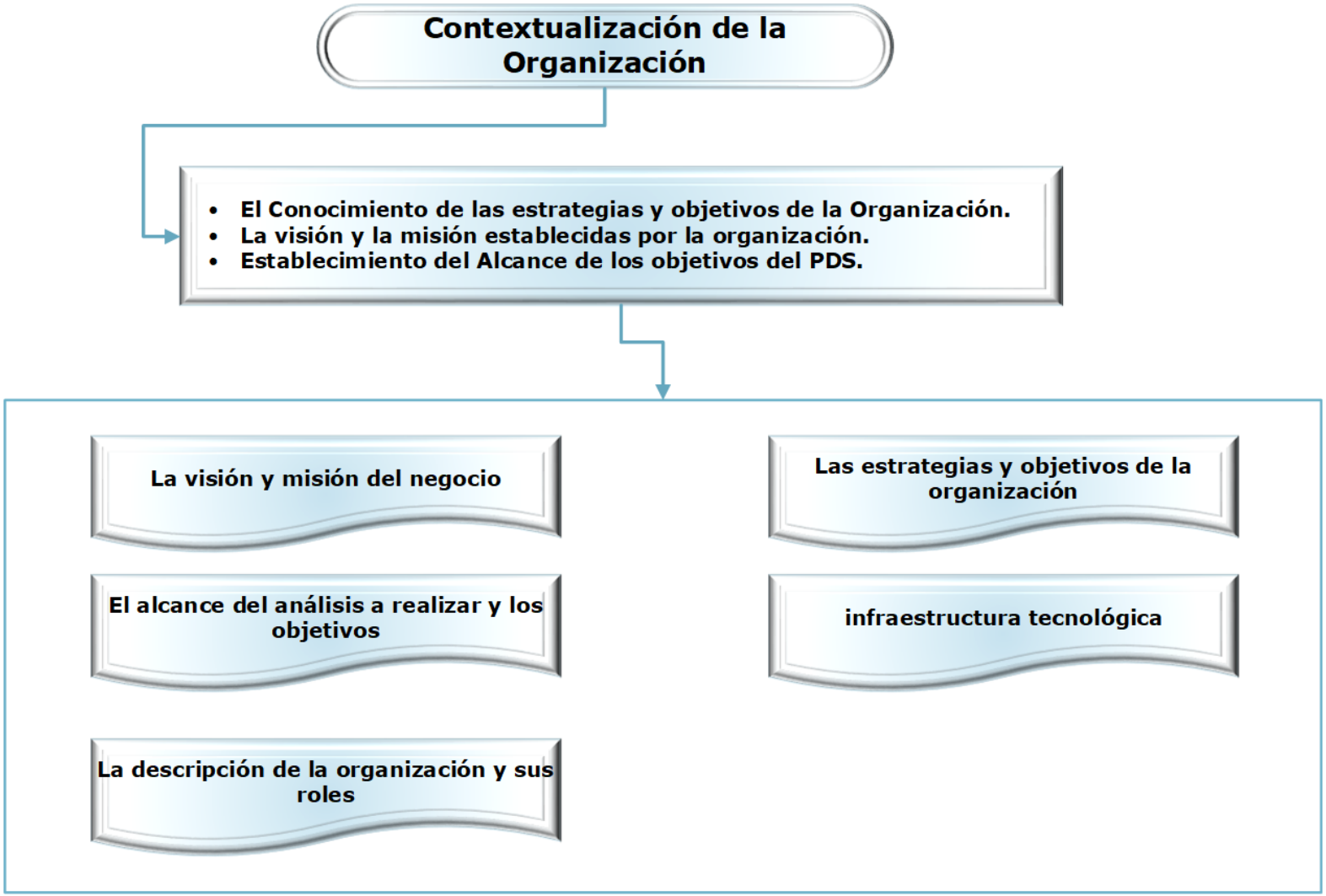
La UNE-ISO/IEC 27002-Código de prácticas para os controles de Seguridad de la información (UNE-ISO/IEC 27002-Tecnología de la información-Técnicas de seguridad– Código de prácticas para los controles de seguridad de la información).

Objetivo del Proyecto

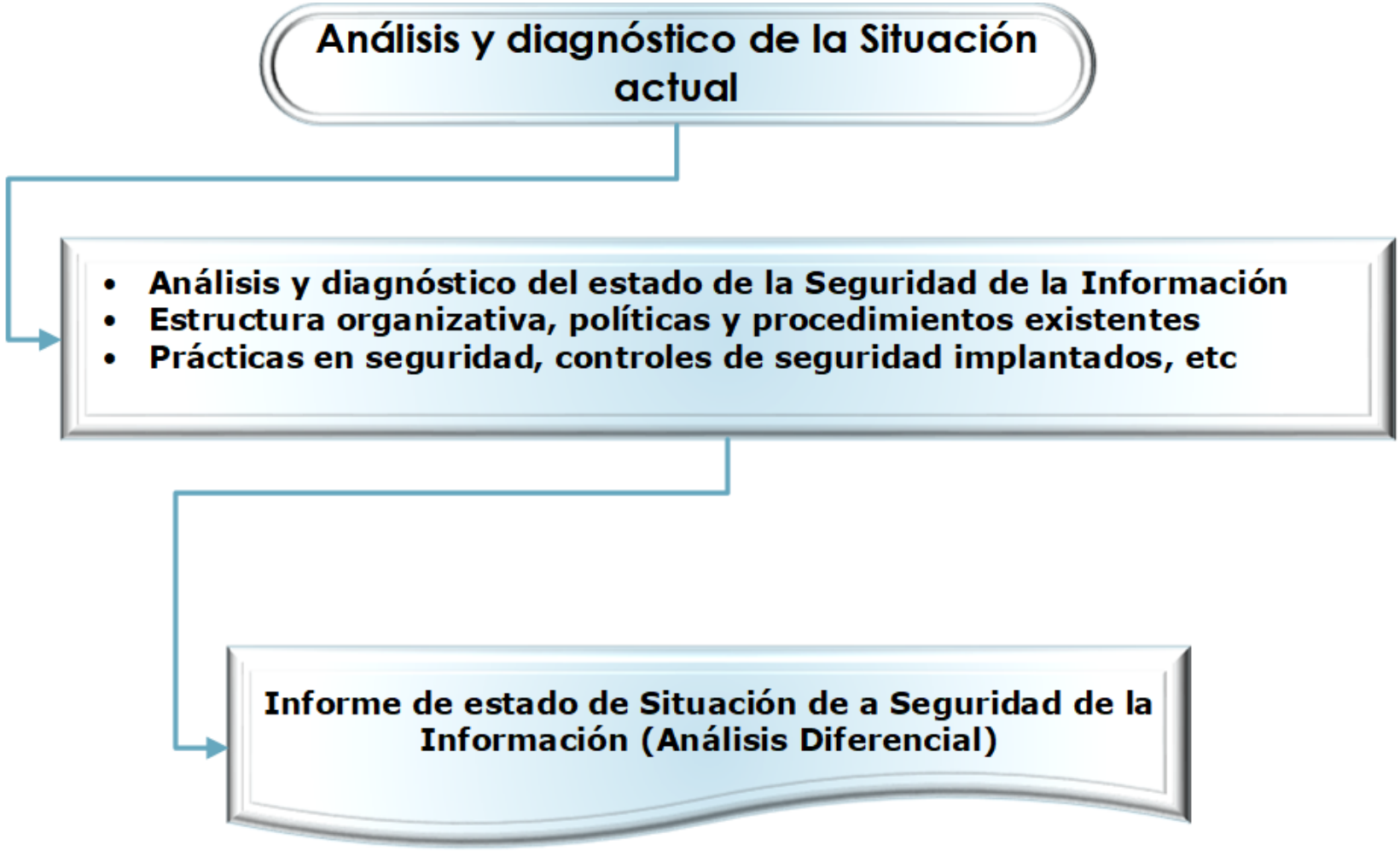
El proyecto que se ha abordado se estructura en las siguientes fases:



Contextualización de la organización

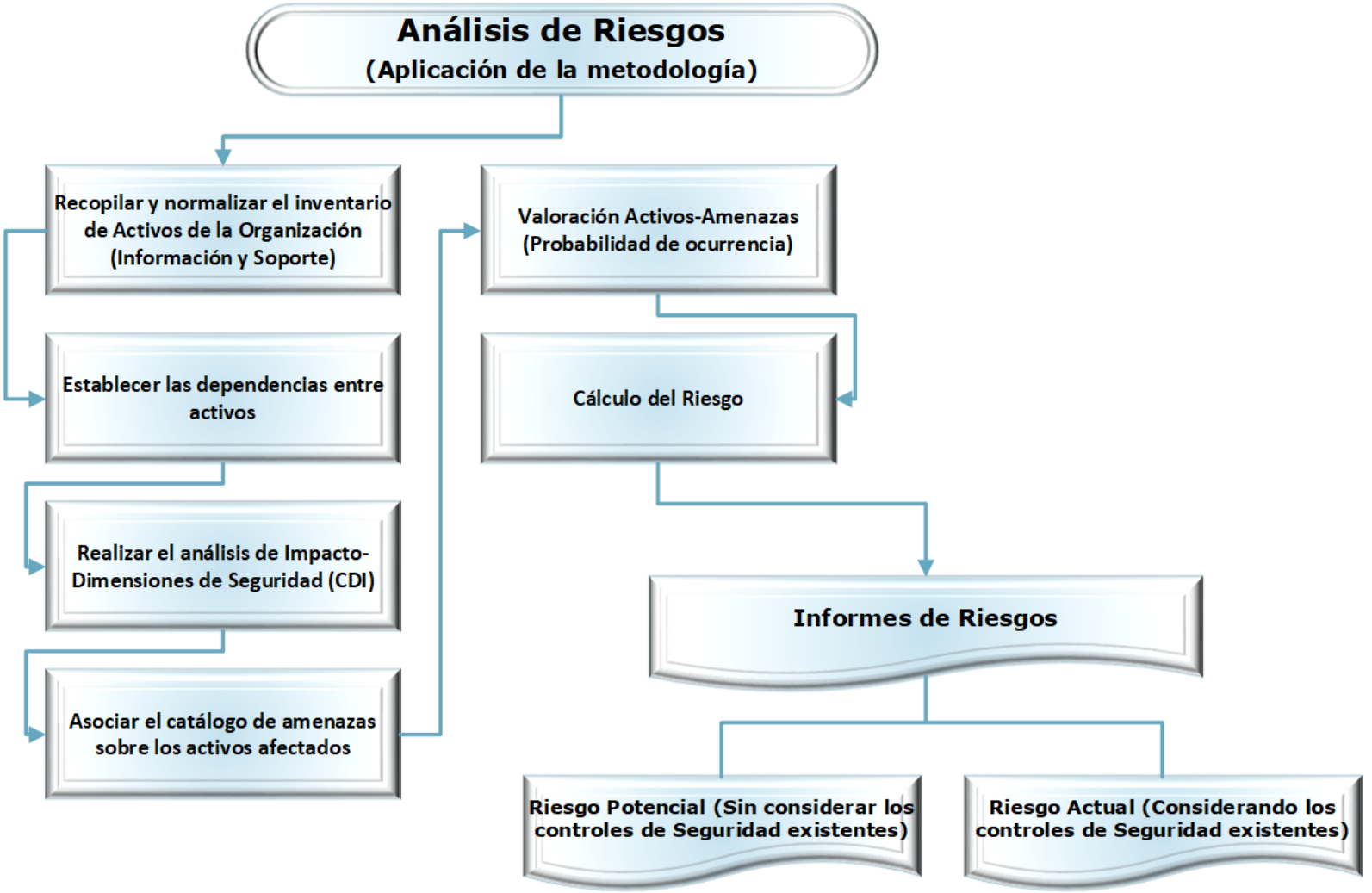


Análisis y diagnóstico de la Situación actual



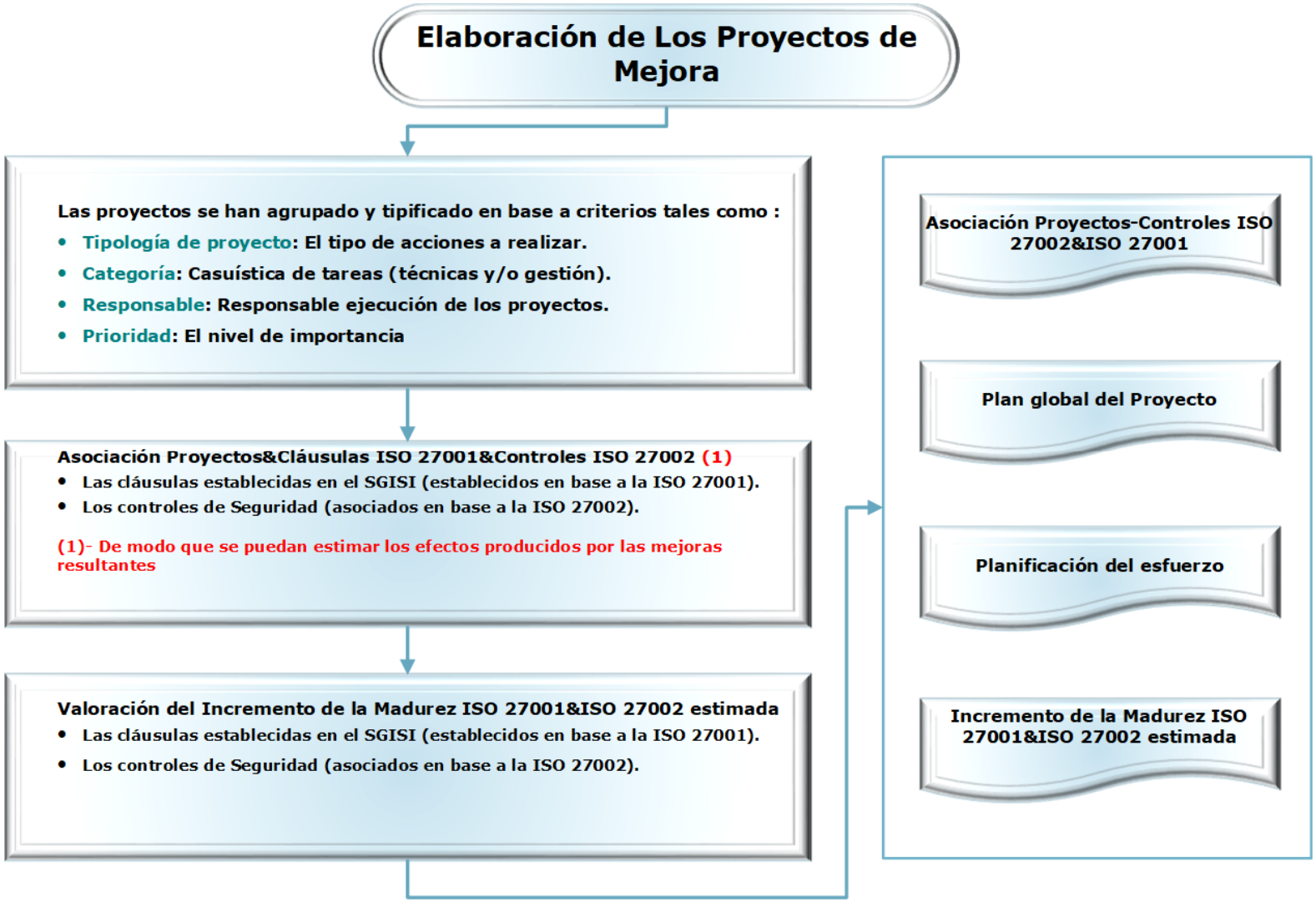
Establecimiento de SGSI

Análisis de Riesgos

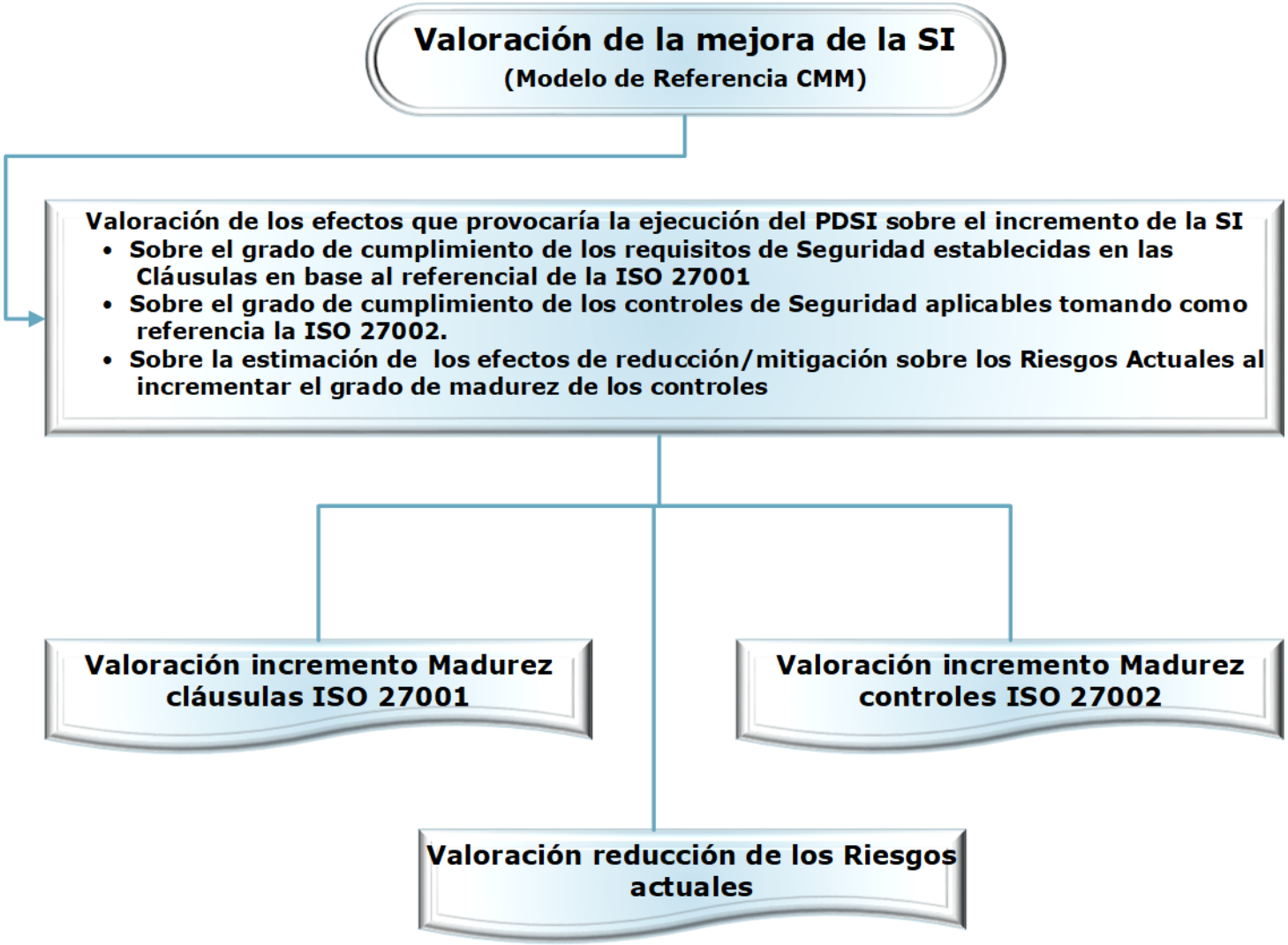


Evaluación del nivel de madurez en SI

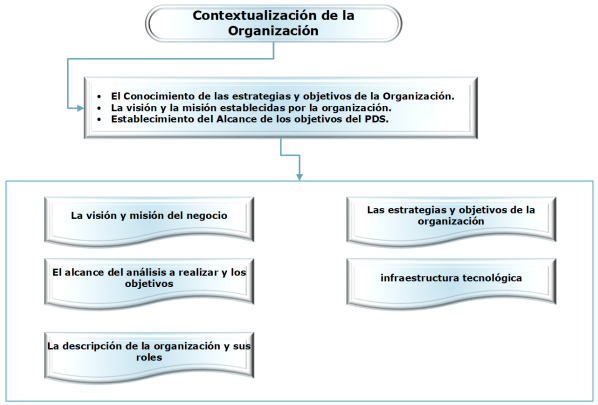
Elaboración de los Proyectos de Mejora



Valoración de la mejora de la SI



Conclusiones



Contexto

- **Tener la oportunidad de establecer un modelo de organización de empresa, que creo en base a mi experiencia, que se da en la práctica; en dónde se destaca que las organizaciones están dotadas de empleados con buenas capacidades; pero no siempre la Dirección tiene la conciencia y pone los medios adecuados para organizar la Seguridad de la Información.**

- **Muchos aspectos de seguridad ya están contemplados, desarrollados y gestionados; pero otros (que incluso pueden ser básicos) no están tratados.**

- **La seguridad de la Información es un ejercicio que hay que realizar de manera global y continuada.**

Conclusiones

Metodología-ISO 27001

- **El uso del referencial de la ISO 27001/ISO 27002 es un valor seguro dado que ya son estándares sobradamente utilizados en el mundo de la Seguridad de la Información.**

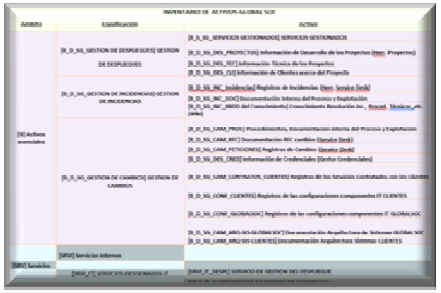
Metodología-ISO 27002

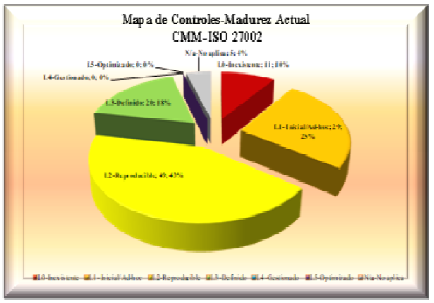
- **El TFM en base al desarrollo de los contenidos y requerimientos ha posibilitado poder desarrollar herramientas para poder afrontar el proceso de organización, análisis, valoración y evaluación de los controles de Seguridad (preferentemente usando herramientas de hojas de cálculo).**

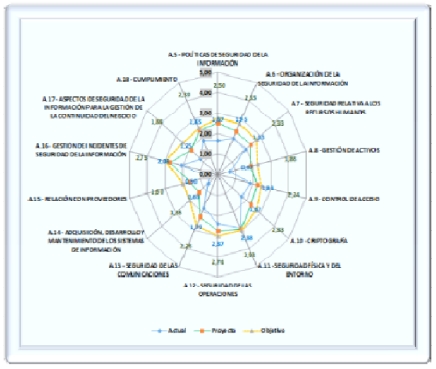
Metodología-Nivel de Madurez CMM

- **Determinar el nivel de madurez de requisitos y controles de Seguridad en base al estándar de CMM.**

Conclusiones







Desarrollo

- **Desde la consideración de la realización del proceso de Análisis de Riesgos, ha posibilitado el desarrollo integrado de herramientas para poder realizar una gestión de todo el proceso**
  - **Registro de inventarios, dependencias entre activos, valoración de impacto.**
  - **Catalogación de amenazas, valoración de amenazas sobre activos.**
  - **Obtención del riesgo Potencial, obtención del riesgo actual (en base a la valoración del grado de madurez actual de los controles).**
- **Ha permitido construir los elementos necesarios para poder realizar una evaluación de la madurez actual y para poder evaluar el incremento de madurez en base a la ejecución del Plan de Proyecto propuesto en el PDS; así como establecer una comparativa entre los dos intervalos de tiempo.**
- **Y dejar establecidos los mecanismos para determinar el incremento de la madurez de la SI, en base a poder estimar los efectos de la ejecución de los proyectos en base a la afectación directa sobre cláusulas y controles de seguridad; y actuando sobre los propios riesgos detectados.**
  - **Asociando los proyectos sobre los requisitos y controles de seguridad sobre los que actúan, así como la cuantificación en el incremento de madurez resultante.**
  - **Estableciendo sobre el catálogo de amenazas la relación de controles que pueden interactuar para reducir/mitigar el riesgo; y estableciendo un coeficiente de atenuación para estimar la mejora en la efectividad de los controles aplicados y como consecuencia la mitigación de los riesgos actuales.**

Gracias