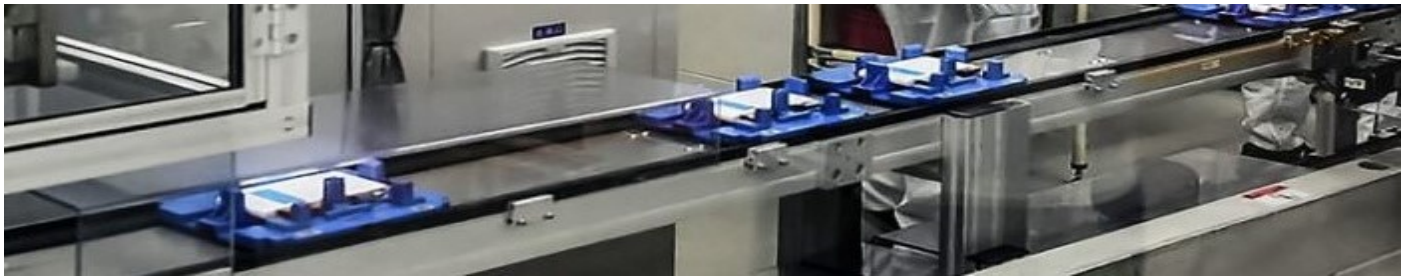


Plan Director de Seguridad
Para la implementación de un SGSI Basado en la Norma ISO 27001:2013
En la Empresa AABBDDEE A.S.

Programa Docente: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Área de Trabajo Fin de Máster: Sistemas de Gestión de la Seguridad de la Información

Estudiante: Javier Benitez Kaskajares

Profesor: Carles Garrigues Olivella

Profesor colaborador: Antonio José Segovia Henares

Fecha de Entrega: 21/12/2018

1 - Introducción

SGSI> Las Empresas deben ser conscientes de la importancia que tiene para su negocio, un de sus principales Activos, la Información.

SGSI> Los riesgos, las vulnerabilidades y amenazas están ahí, por lo tanto, es muy importante diseñar un SGSI para su aplicación en la Empresa bajo la norma ISO/IEC 27001 que permita obtener una visión global del estado de los sistemas de información y definen claramente las medidas de seguridad a aplicar para prevenir futuros incidentes.

SGSI> Es necesario involucrar a todo el personal de la compañía sin importar el área a la que pertenezcan, pues son ellos los que ayudarán a implementar los sistemas de gestión para evitar que se queden solo en documentos.

2 - Implementación de un SGSI

SGSI> La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), es una opción fundamental cuando se trata de proteger la información, ya que este tiene como objetivo esencial proteger dicho activo, a través de controles y políticas de seguridad, que deben ser aplicadas en una organización.

SGSI> Los ciberataques están experimentado un gran crecimiento motivados muchos de ellos por un aspecto económico y que conduce a una profesionalización de los atacantes, cada vez más organizados y con personal especializado en la búsqueda de brechas en la seguridad de los sistemas.

SGSI> Los pilares básicos de la seguridad de la información son: Confidencialidad, Integridad, Disponibilidad.

2 - Implementación de un SGSI

SGSI> La Norma ISO 27001 como parte de la implementación de la seguridad de la información es muy relevante ya que, toma como base todos los riesgos a los que se enfrenta la organización en su día a día.

SGSI> Tiene como objetivo principal establecer, implantar, mantener y mejorar de forma continua la seguridad de la información de la organización. Sin embargo, no debemos olvidar el papel que ocupan otras normas.

SGSI> La norma ISO 27002 es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013.

3 - Plan Director de Seguridad

SGSI> La falta de preparación y medios en las organizaciones para tratar los casos de incidentes de seguridad, desemboca en que el daño causado por los ataques sea aún mayor y más duradero en el tiempo.

SGSI> Para todo esto es necesario que la Empresa desarrolle de un Plan Director de Seguridad.

SGSI> Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.

4 - Perfil del Responsable de Seguridad

SGSI> **Uno de los perfiles más importantes en la implantación de un SGSI es el responsable de seguridad de la información.**

SGSI> **La Dirección de la entidad debe comprometerse con la implementación, establecimiento, operación, monitorización, mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información.**

5 - Hoja de Ruta

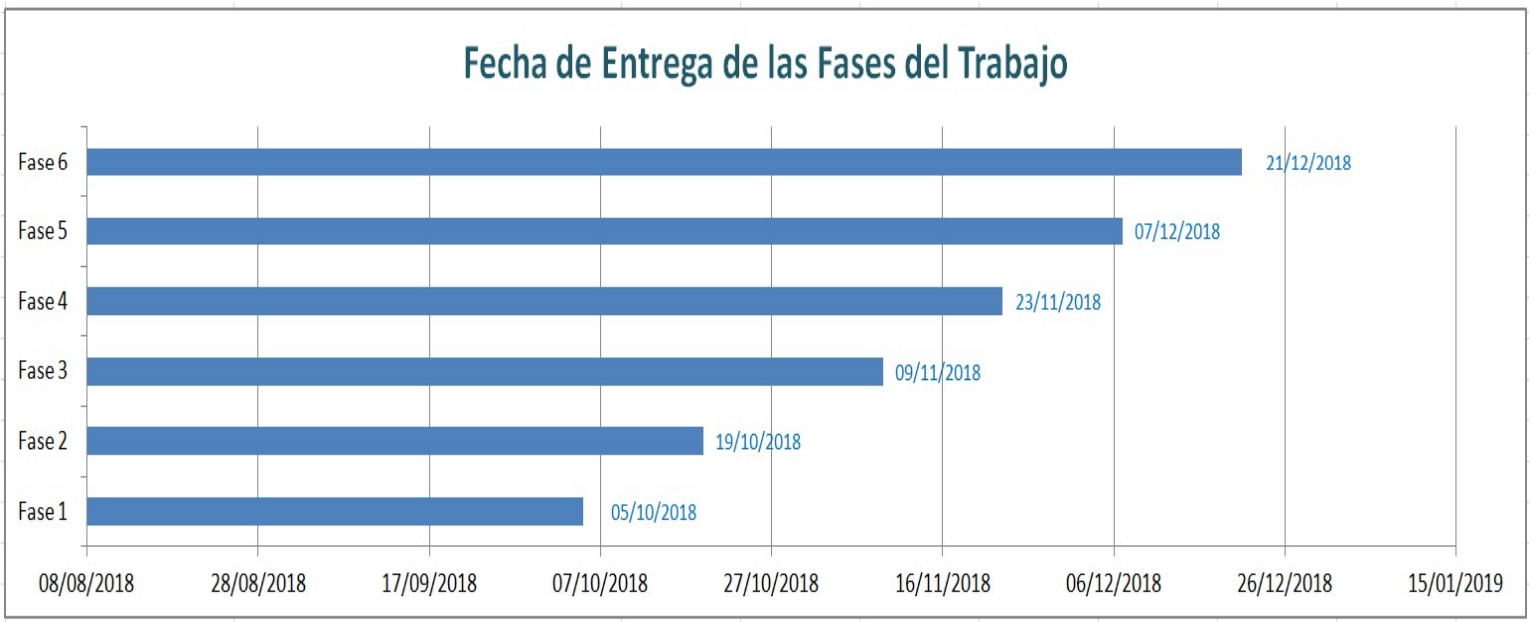
SGSI> **La falta de coordinación y gestión "hoja de ruta" de los esfuerzos para gestionar la seguridad, tienen un efecto negativo en el negocio y reducen la eficiencia de las operaciones y del personal técnico.**

6 - Planificación del Trabajo

- SGSI> **FASE 1 - Situación Actual: Contextualización, objetivos y análisis diferencial.**
- SGSI> **FASE 2 - Sistema de Gestión Documental.**
- SGSI> **FASE 3 - Análisis de Riesgos.**
- SGSI> **FASE 4 - Propuestas de Proyectos.**
- SGSI> **FASE 5 - Auditoría de Cumplimiento.**
- SGSI> **FASE 6 - Presentación de Resultados y Entrega de Informes.**

6 - Planificación del Trabajo

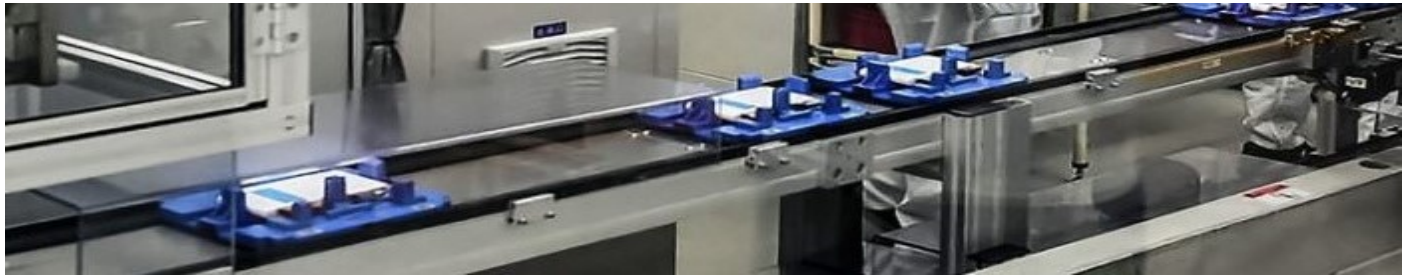
SGSI> **Esquema de la evolución del desarrollo de trabajo en el tiempo: desglosado en 6 fases:**



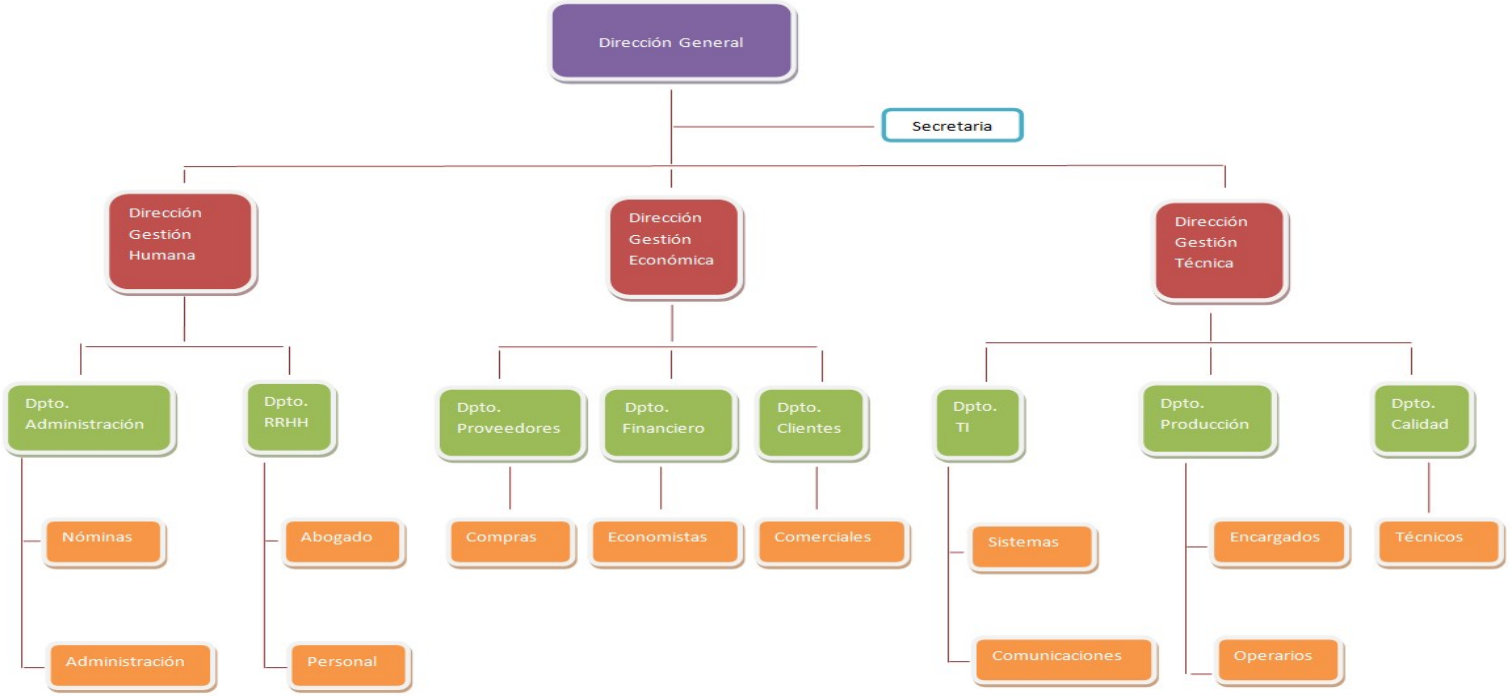
7 - Contextualización - Empresa AABBDDEE A.S.

- SGSI> **AABBDDEE A.S. Empresa ficticia objeto de este Trabajo**

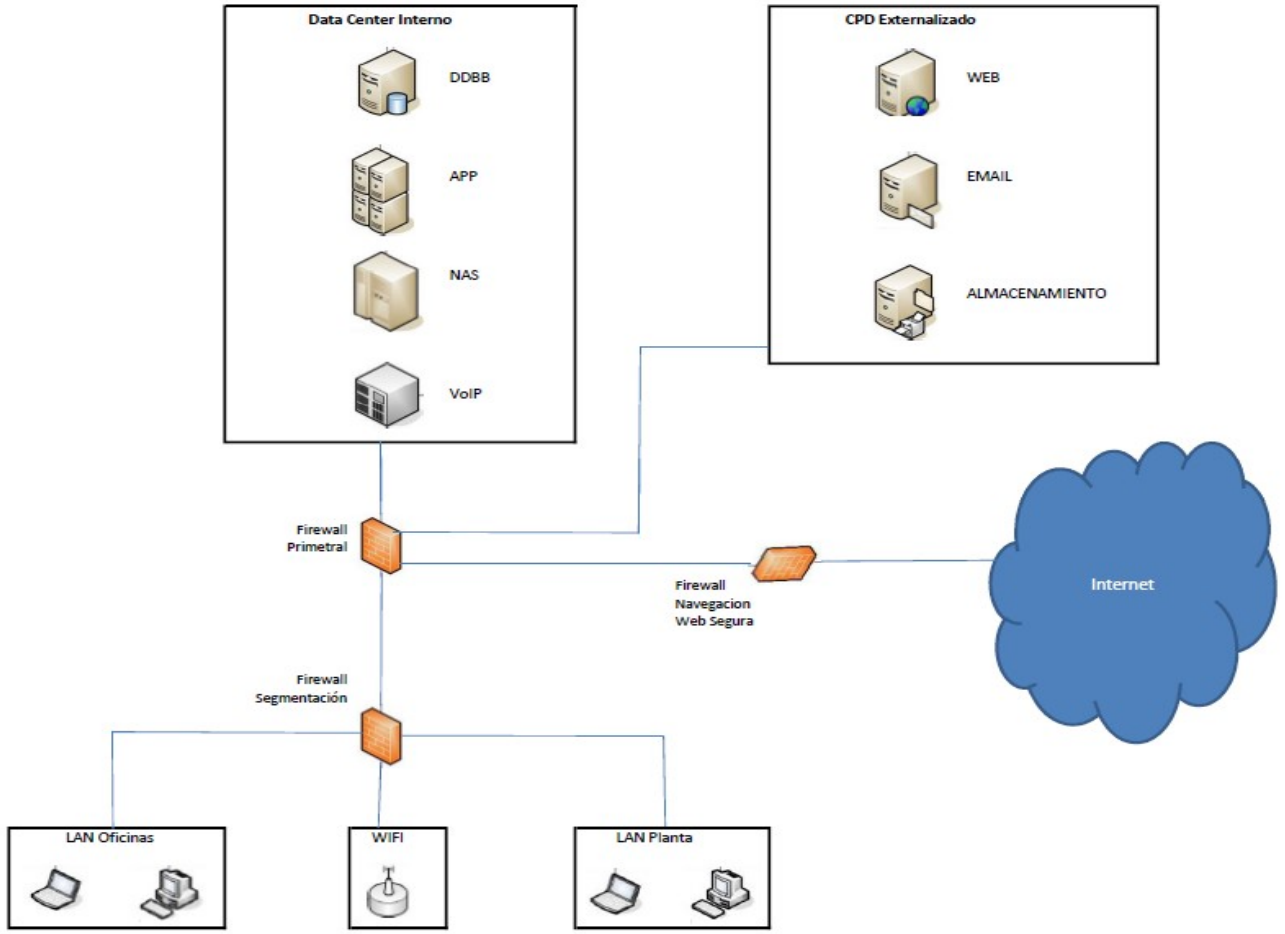
- SGSI> **AABBDDEE A.S. es una Empresa dedicada a los suministros industriales para las empresas de automoción.**



8 - Estructura y Jerarquía de la Organización



9 - Infraestructura Tecnológica de la Empresa



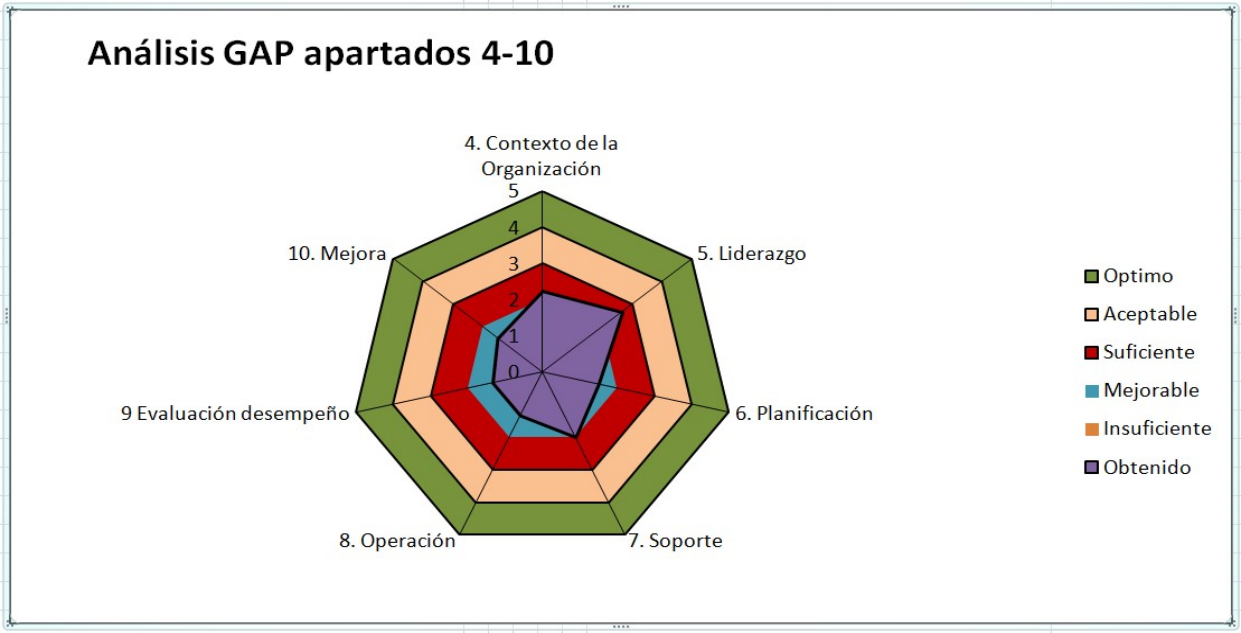
10 - Objetivos de la Seguridad de la Información

SGSI> **El objetivo general es diseñar e implementar un sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001 en la Empresa AABBDDEE A.S., enfocado en los procesos de las áreas necesarias de la empresa, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque.**

SGSI> **En la implantación del SGSI en la Empresa objeto de este trabajo es importante el estudio del PDCA (Plan - Do - Check - Act) bajo la norma ISO/IEC 27001, es decir antes de emprender acciones es necesario planificar, ver dónde estamos, adónde queremos ir, con qué medios contamos y sobre qué entorno queremos trabajar.**

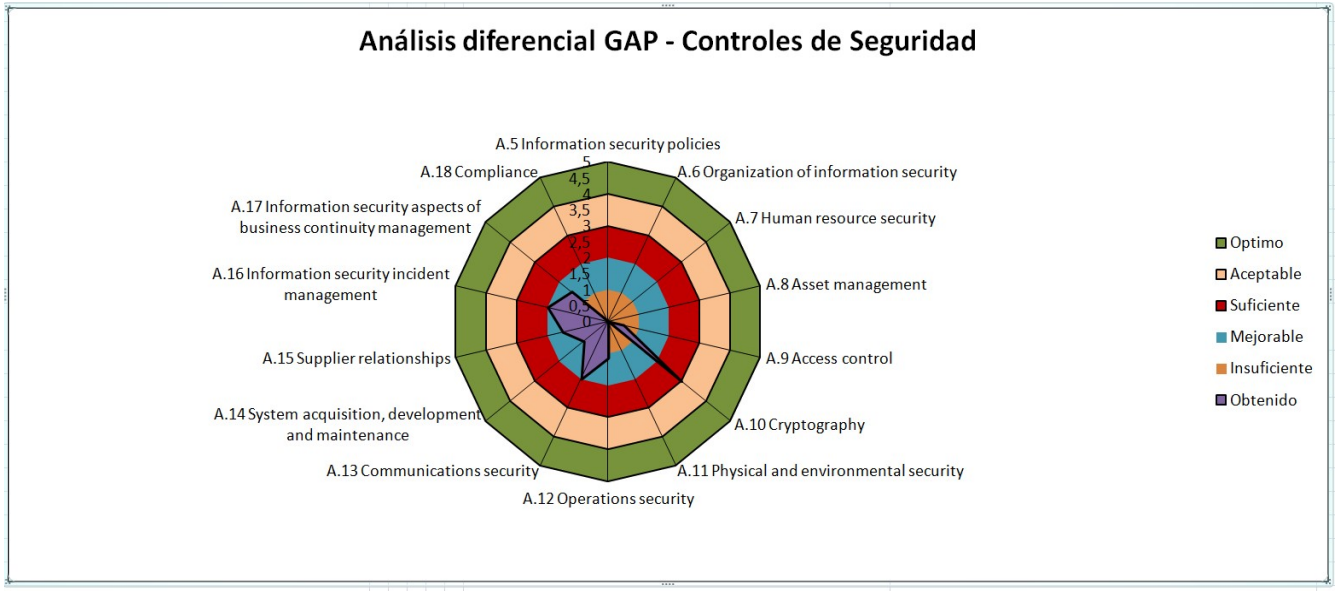
11 - Análisis diferencial

SGSI> **Ante este estudio y mediante la ejecución de un análisis GAP en relaciones a los apartados 4 al 10 identificados en la Norma ISO 27001, hemos obtenido los siguientes resultados (ver documento Análisis diferencial 4-10):**



12 - Análisis diferencial

SGSI> **A continuación, en el análisis diferencial, profundizaremos en los Controles de Seguridad mediante la ejecución del análisis GAP, con respecto a la norma ISO/IEC 27002, tras lo cual hemos obtenido los siguientes resultados (ver documento Análisis diferencial Controles de Seguridad):**



13 - Sistema de Gestión Documental

SGSI> **Mantener una documentación adecuada que gobierne la seguridad de la Empresa, mediante un SGSI perfectamente adaptado a los procesos de negocio de la Organización, es algo imprescindible para que el resto de Procesos engranen correctamente.**

SGSI> **En este plan de trabajo y para la Gestión Documental de la Empresa AABBDDEE A.S. nos centraremos en la realización de los siguientes DOCUMENTOS, exigidos en la implantación de un Sistema de Gestión de Seguridad de la Información, bajo la norma ISO 27001:2013:**

13 - Sistema de Gestión Documental

- SGSI> **Política de seguridad de la información:** Es un documento breve y de alto nivel que detalla el principal objetivo del SGSI.

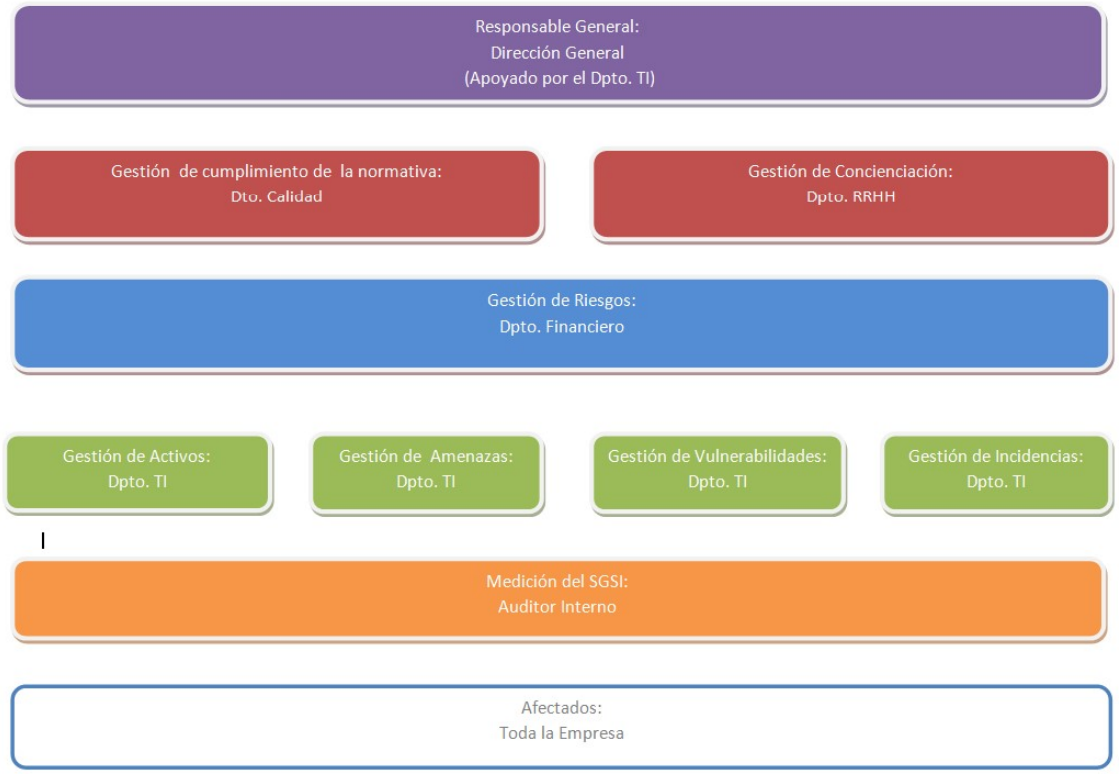
- SGSI> **Procedimiento de Auditorías Internas:** El programa de auditoría interna estará definido a través de un plan anual donde se marquen los periodos de realización de las auditorías.

- SGSI> **Gestión de Indicadores:** Se deben medir los controles de seguridad implantados para la obtención de resultados tras las auditorias.

- SGSI> **Procedimiento Revisión por Dirección:** La Dirección de la Organización debe revisar anualmente y de una manera activa, los aspectos más importantes que han sucedido en relación al Sistema de Gestión de Seguridad de la Información.

13 - Sistema de Gestión Documental

SGSI> **Roles y Responsabilidades:** La norma ISO 27001 establece los requisitos a cumplir por los roles, responsabilidades y autoridades de la Organización:



13 - Sistema de Gestión Documental

SGSI> **Metodología de Análisis de Riesgos:** Este análisis permite identificar y analizar cada uno de los procesos del negocio y determinar los riesgos a los cuales están expuestos cada uno de ellos, a su vez se consigue identificar amenazas y vulnerabilidades.
La metodología seleccionada para la evaluación de riesgos es MAGERIT.

SGSI> **Declaración de Aplicabilidad:** Documento clave dentro del SGSI porque describe no sólo qué controles son aplicables, sino también cómo se implementarán y su estado actual.

14 - Análisis de Riesgos

- SGSI> **Inventario de los Activos:** Un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

- SGSI> **Valor de los Activos:** La valoración de Activos se realizará bajo una estimación cuantitativa y según la siguiente clasificación: Alto, Medio, Bajo, que se identificarán para los siguientes pilares básicos de la seguridad de la información son: Confidencialidad, Integridad, Disponibilidad.
  Se valorarán los activos según su criticidad en: Crítico y No Crítico.

- SGSI> **Amenazas:** Todas las causas de las amenazas permiten ser clasificadas por su naturaleza.

14 - Análisis de Riesgos

- SGSI> **Vulnerabilidades:** es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información.

- SGSI> **Probabilidad que se materialicen las Amenazas:** La calificación de riesgo global que indica la probabilidad de que una vulnerabilidad potencial puede materializarse dentro de la construcción del entorno de las amenazas asociadas.

- SGSI> **Establecimiento de Impactos en la Organización de la materialización de las Amenazas:** Se debe determinar los efectos adversos, impactos, resultantes al potencializarse una amenaza.

14 - Análisis de Riesgos

- SGSI> **Riesgo Residual:** Después de identificar los controles adecuados para reducir un riesgo especifico al nivel considerado aceptable, debe evaluarse cuanto los controles, si se implementan reducirán el riesgo. Esta reducción de riesgo es el denominado "riesgo residual".

- SGSI> **Cálculo del nivel de riesgo:** La determinación final de la misión de riesgo se obtiene multiplicando las calificaciones asignadas por la probabilidad de la amenaza y el impacto de la amenaza.

15 - Propuestas de Proyectos

SGSI> Se deberá identificar los proyectos que se deben llevar a adelante para implementar las salvaguardas necesarias para tratar los Riesgos identificados en el proceso de análisis de Riegos en la Empresa.

SGSI> Una vez conocido el nivel de riesgo actual en la organización se debe determinar el denominado umbral de riesgo, que será el punto a partir del cual todo riesgo debería ser reducido por lo menos hasta situarse en el punto justamente inferior al marcado por cada organización.

SGSI> Se deberá elegir entre alguna de las siguientes opciones: Aceptarlo, Asignarlo a terceros o Compartirlos, Minimizarlos o evitarlos.

15 - Propuestas de Proyectos

- SGSI> Una vez identificados los riesgos que hay que mitigar (riesgos no asumibles) y los objetivos de seguridad que se desea alcanzar, se deberán seleccionar los controles o salvaguardas necesarias. Estas salvaguardas pueden ser controles técnicos, procedimientos operativos, normativas de usuario, cláusulas contractuales, etc. La selección de estos controles se sugiere hacerla a partir de la norma ISO 27002.

- SGSI> Dentro de cada Proyecto elegido se marcarán diferentes Acciones en función de la envergadura del proyecto seleccionado.

- SGSI> En función de las necesidades para la implementación de los Proyectos decididos para la mitigación de los Riesgos detectados, se ha definido la siguiente clasificación de Acciones:

15 - Propuestas de Proyectos

- SGSI> **Definir nuevas reglas:**

  - SGSI> **Reglas que se encuentran documentadas mediante planes**
    Objetivo: Implementar mecanismos de seguridad para la prevención de fuga, daño o pérdida de información.

  - SGSI> **Reglas que se encuentran documentadas mediante políticas**
    Objetivo: Formar y realizar Auditorías internas del Sistema de Gestión de seguridad de la información, que permitan generar políticas para subsanar las deficiencias detectadas.

15 - Propuestas de Proyectos

- SGSI> **Definir nuevas reglas:**

  - SGSI> **Reglas que encuentran documentadas mediante procedimientos**
    Objetivo: Desarrollar alineamientos, directrices y procedimientos de seguridad, que permitan brindar pautas para el control de acceso IT, el desarrollo seguro de software y aplicaciones, evaluaciones de seguridad.

  - SGSI> **Reglas que se encuentran documentadas mediante instrucciones**
    Objetivo: Implementar mecanismos de auditoría, seguridad y protección sobre la información de las BBDD core del negocio.

15 - Propuestas de Proyectos

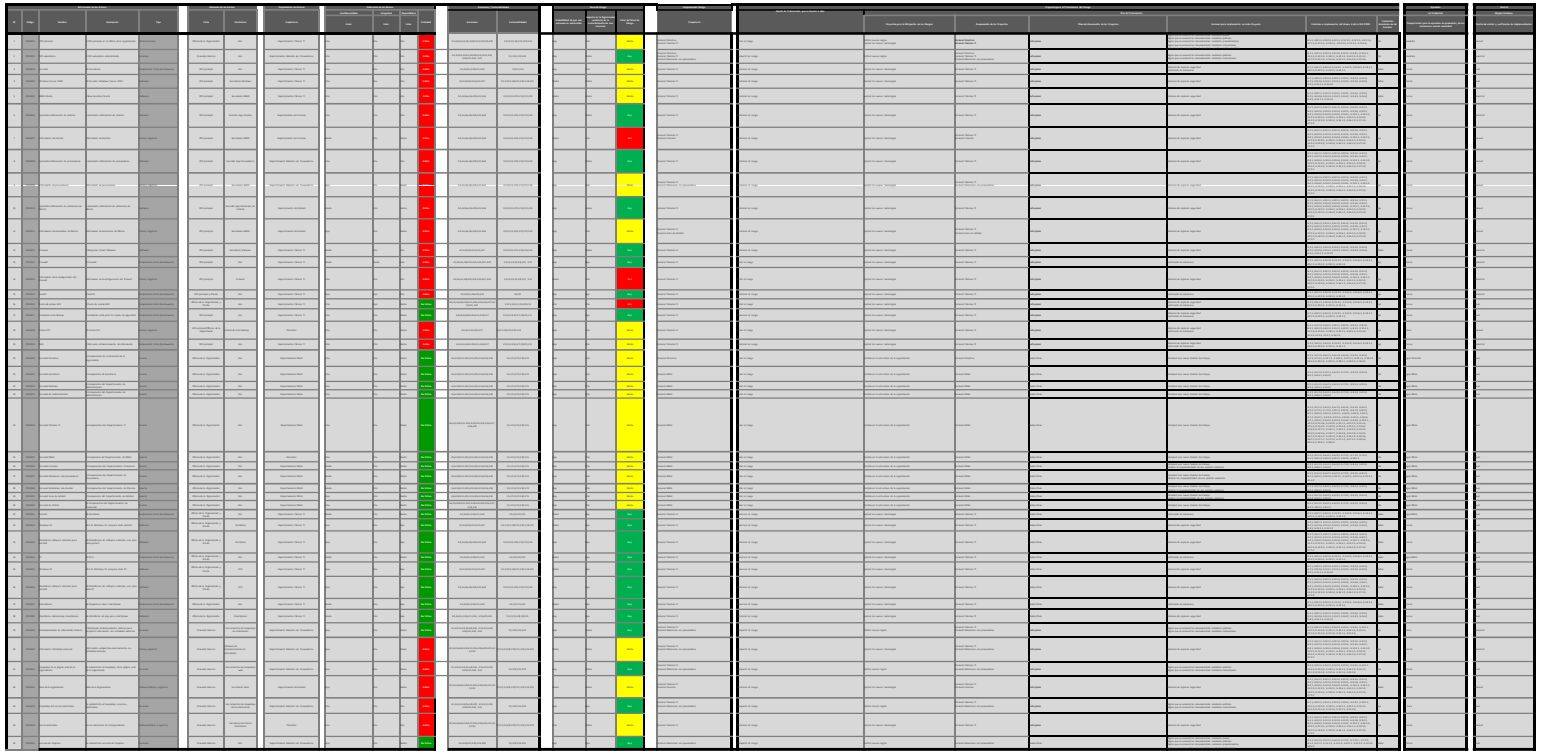
- SGSI> **Aplicar las nuevas tecnologías:**
  - SGSI> **Ubicaciones de recuperación de desastres para Centros de Datos**
    Objetivo: Adquirir servicios avanzados de monitoreo SOC para prevenir y afrontar desastres en los centros de datos y sus ámbitos de gestión.
  - SGSI> **Sistemas de copia de seguridad**
    Objetivo: Desarrollar una política de Backup.
  - SGSI> **Sustitución de Hardware**
    Objetivo: Implementar mecanismos de Alta Disponibilidad para garantizar los niveles de servicio y funcionamiento de servidores de aplicaciones, bases de datos, almacenamientos, comunicaciones, switches, routers.

15 - Propuestas de Proyectos

- **Cambio en la estructura de la organización:**
  - **Introducir una nueva función de trabajo**
    Objetivo: Realizar formación de seguridad de la información a todos los empleados de la compañía, por grupos objetivos.
  - **Cambiar la responsabilidad de una posición existente**
    Objetivo: Realizar documentos de Roles y Matriz de Responsabilidades sobre la implementación y seguimiento del SGSI en la estructura de la Empresa.

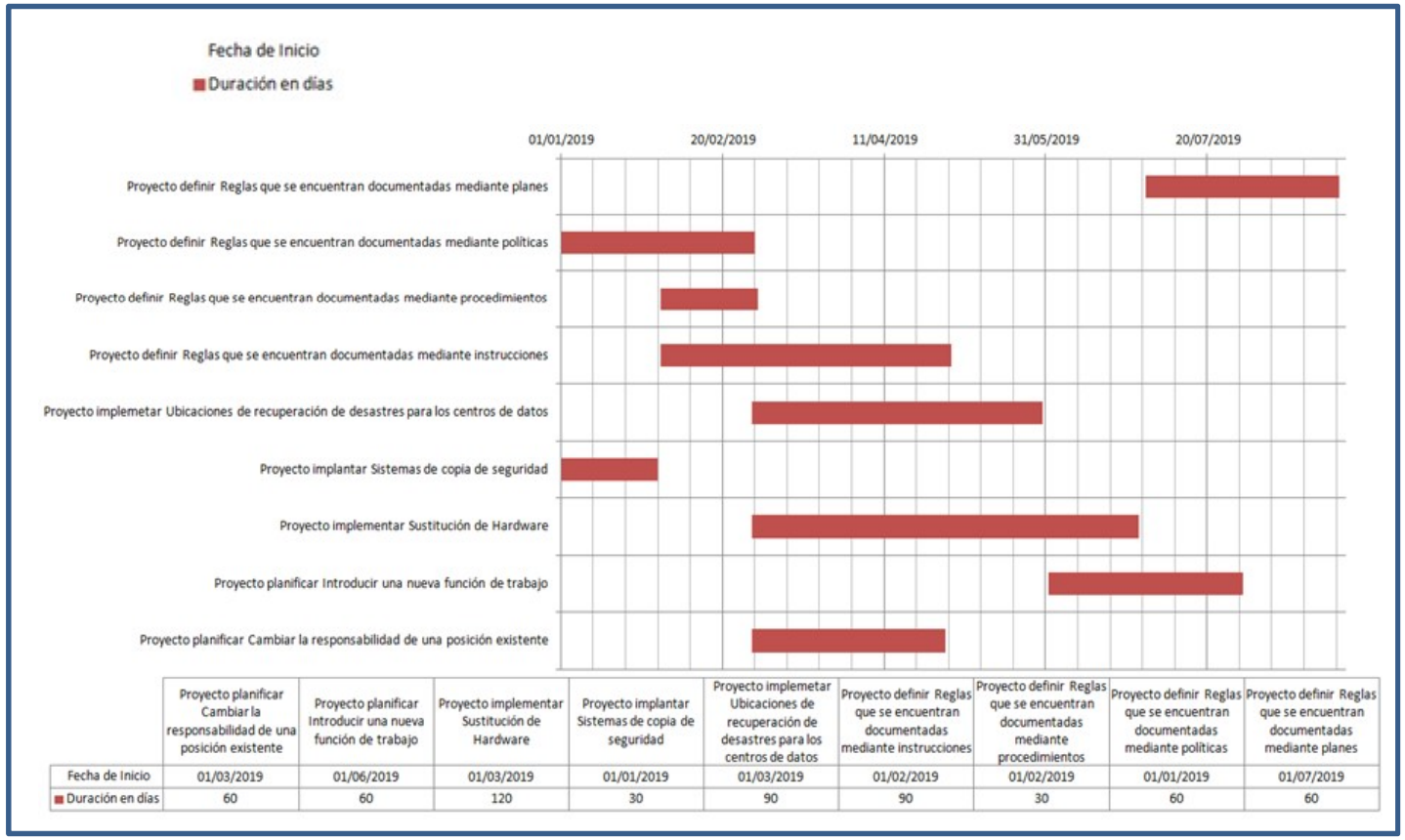
15 - Propuestas de Proyectos

SGSI> **Acciones que se implementaran en la Empresa según tabla de "Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento":**



15 - Propuestas de Proyectos

SGSI> Planificación de los Plazos de Consecución de los Proyectos:



	Proyecto planificar Cambiar la responsabilidad de una posición existente	Proyecto planificar Introducir una nueva función de trabajo	Proyecto implementar Sustitución de Hardware	Proyecto implantar Sistemas de copia de seguridad	Proyecto implemetar Ubicaciones de recuperación de desastres para los centros de datos	Proyecto definir Reglas que se encuentran documentadas mediante instrucciones	Proyecto definir Reglas que se encuentran documentadas mediante procedimientos	Proyecto definir Reglas que se encuentran documentadas mediante políticas	Proyecto definir Reglas que se encuentran documentadas mediante planes
Fecha de Inicio	01/03/2019	01/06/2019	01/03/2019	01/01/2019	01/03/2019	01/02/2019	01/02/2019	01/01/2019	01/07/2019
Duración en días	60	60	120	30	90	90	30	60	60

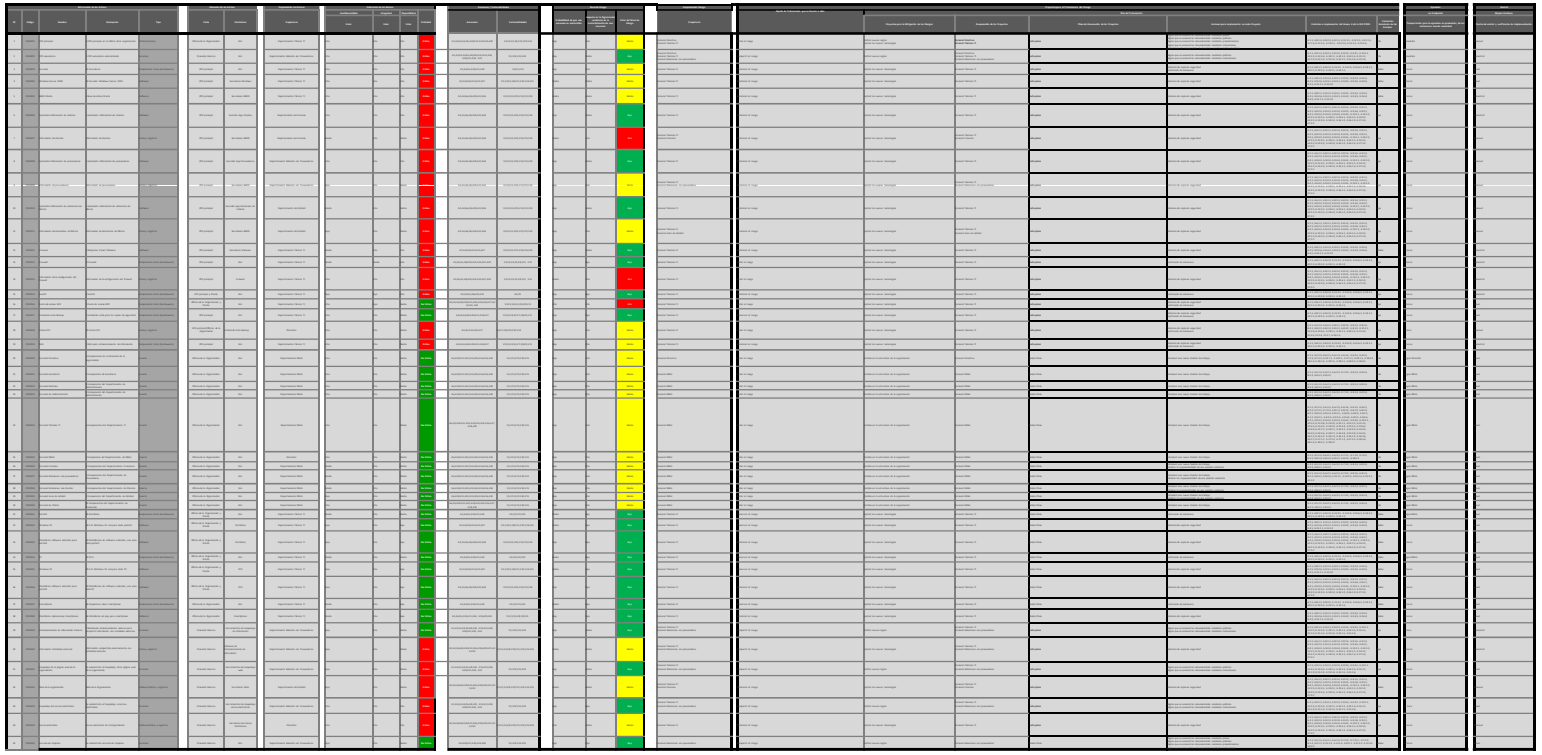
15 - Propuestas de Proyectos

- **Verificación de la Implementación de los Puntos de Control:**
  - Siguiendo normativas de buenas prácticas y en el cumplimiento de un correcto plan de implementación de un Sistema de Gestión de Seguridad de la Información, se introducen en este estudio, puntos de control para hacer un seguimiento de la correcta implantación, funcionamiento y conocimiento de los proyectos o acciones a realizar.
  - Según se muestra en la tabla del "Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento"

15 - Propuestas de Proyectos

SGSI> **Verificación de la Implementación de los Puntos de Control:**

Según los parámetros de la siguiente tabla:



16 - Auditoría de Cumplimiento

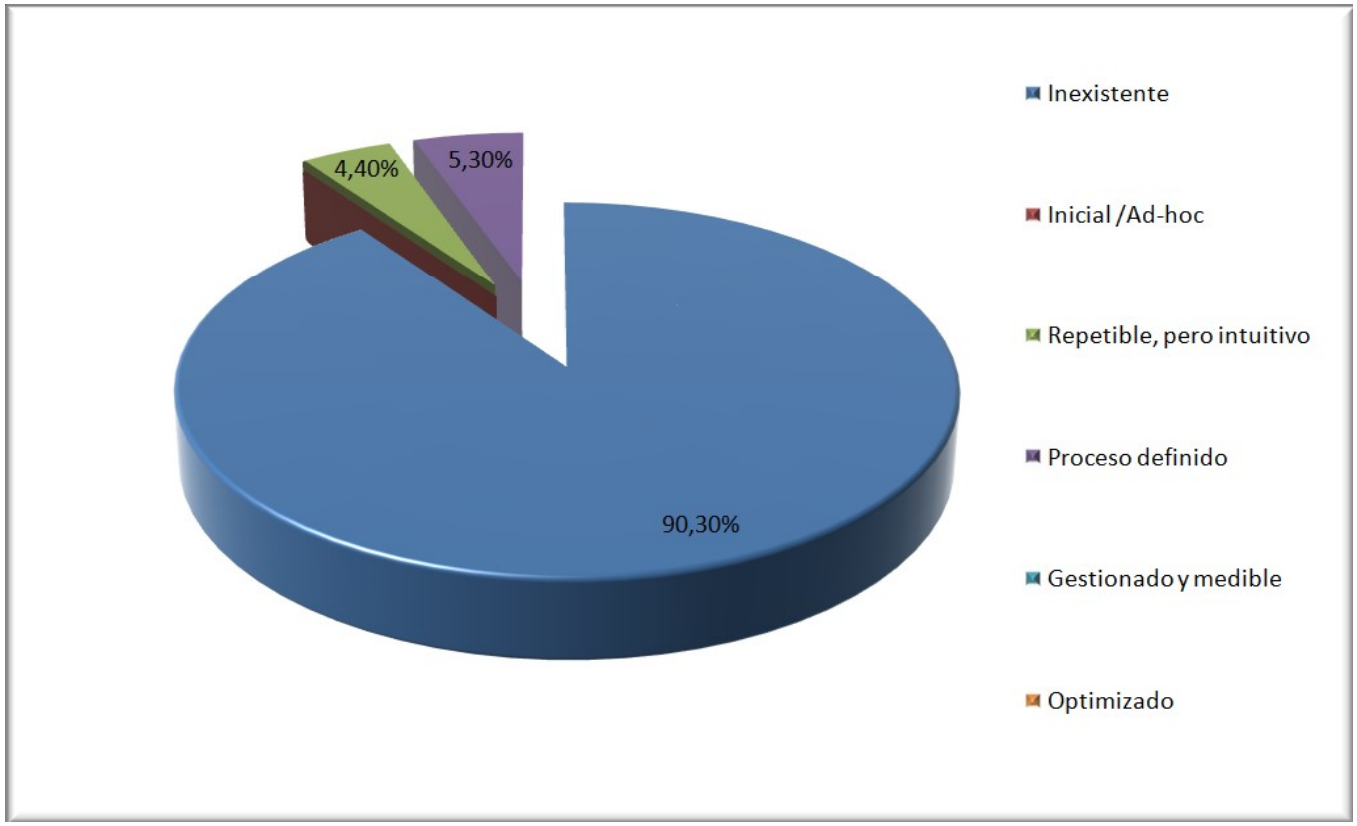
SGSI> **El proceso de Auditoria de complimiento es necesario para determinar hasta qué punto la Empresa cumple o no cumple con los requerimientos del estándar en materia de seguridad, basándonos en la ISO/IEC 27002:2013 como marco de control de la seguridad.**

SGSI> **Madurez CMM de los controles ISO:**

El objetivo de este proceso es determinar si el nivel de madurez que ha establecido la Empresa, es adecuado en función de lo analizado y comprobado durante la auditoria, en lo que respecta a los diferentes dominios de control y los 114 controles planteados por la ISO/IEC 27002:2013.

16 - Auditoría de Cumplimiento

SGSI> **Diagrama de Madurez CMM de los controles ISO:**



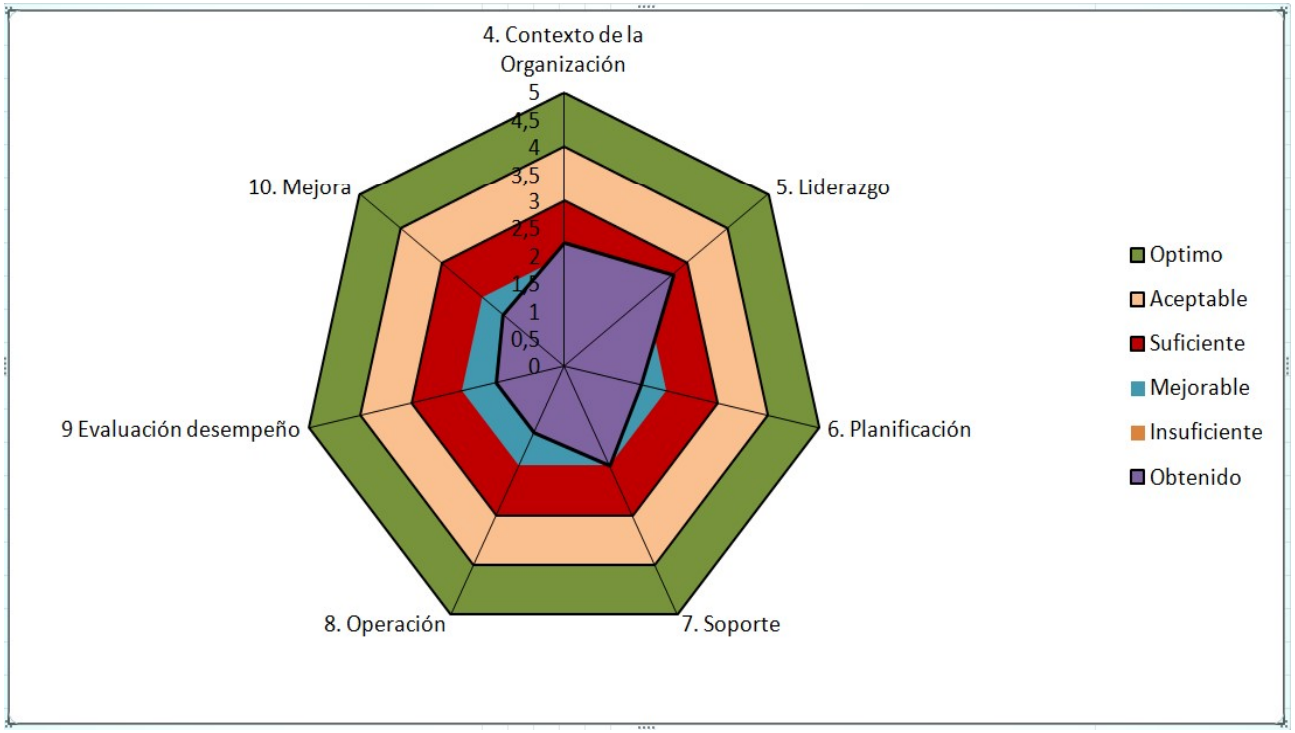
16 - Auditoría de Cumplimiento

SGSI> **Nivel de cumplimiento de los requisitos de la ISO 27001 que vienen definidos entre los apartados 4 al 10:**

Con el estudio de los siguientes diagramas de Radar conseguimos obtener una visión más detallada del nivel de cumplimiento de los requisitos de la ISO 27001 que vienen definidos entre los apartados 4 al 10.

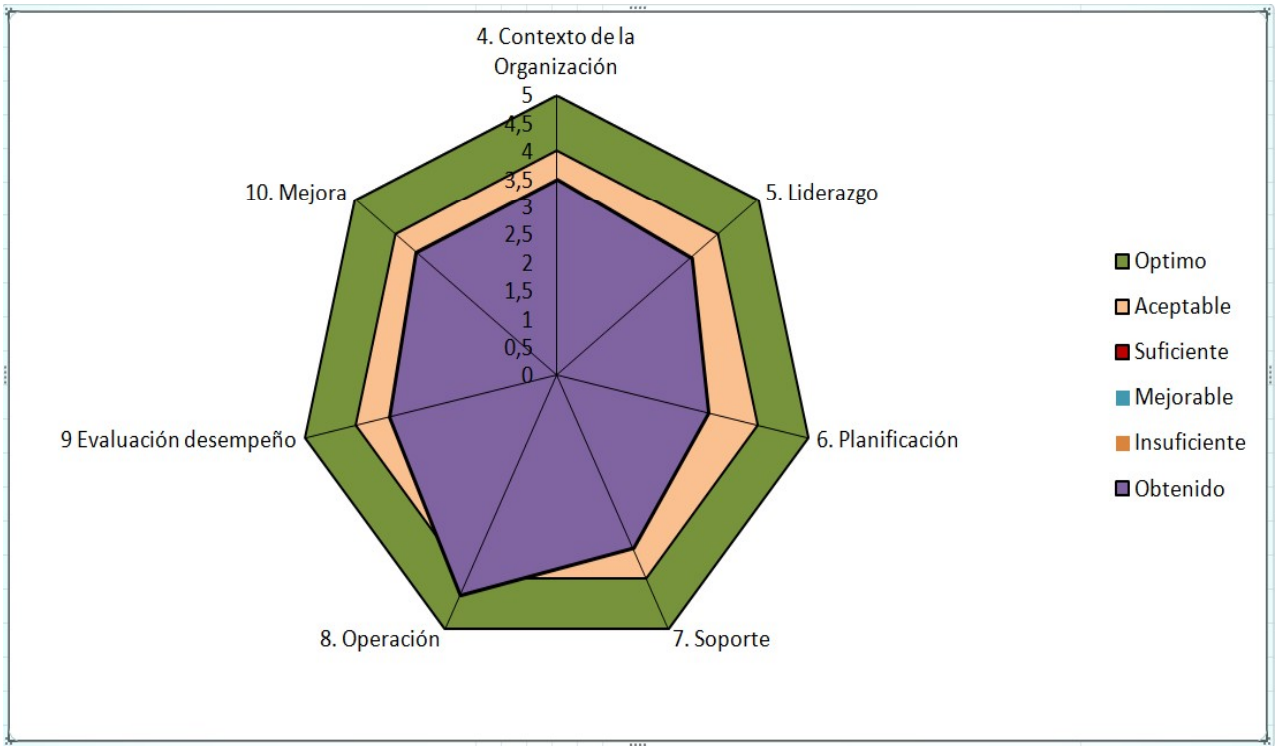
16 - Auditoría de Cumplimiento

SGSI> **Diagrama Radar de estado actual de cumplimiento de los requisitos de la ISO 27001 que vienen definidos entre los apartados 4 al 10:**



16 - Auditoría de Cumplimiento

SGSI> **Diagrama Radar de cumplimiento deseado de los requisitos de la ISO 27001 que vienen definidos entre los apartados 4 al 10:**



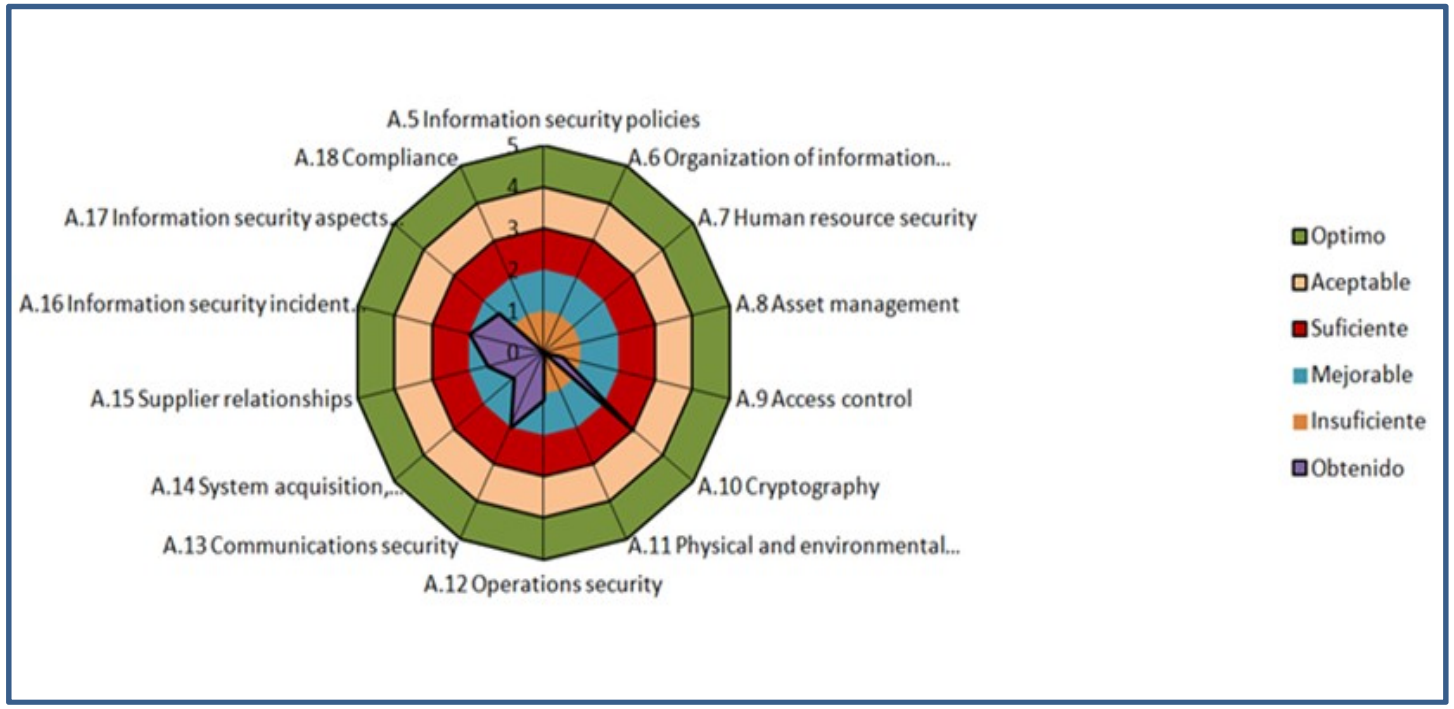
16 - Auditoría de Cumplimiento

SGSI> **Nivel de cumplimiento de los requisitos de la ISO 27001 que vienen definidos en el Anexo A:**

Con el estudio de los siguientes diagramas de Radar conseguimos obtener una visión más detallada del nivel de cumplimiento de los requisitos de la ISO 27001 que vienen definidos en el Anexo A.

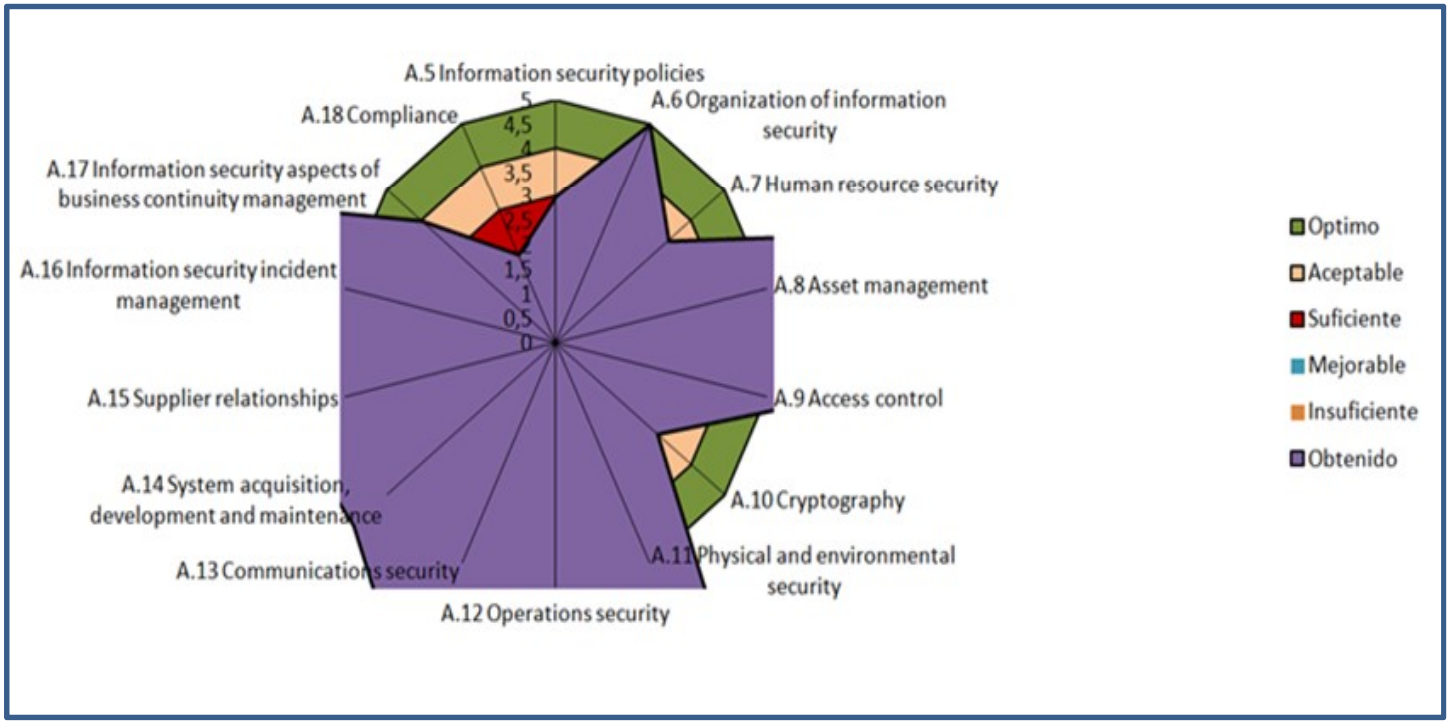
16 - Auditoría de Cumplimiento

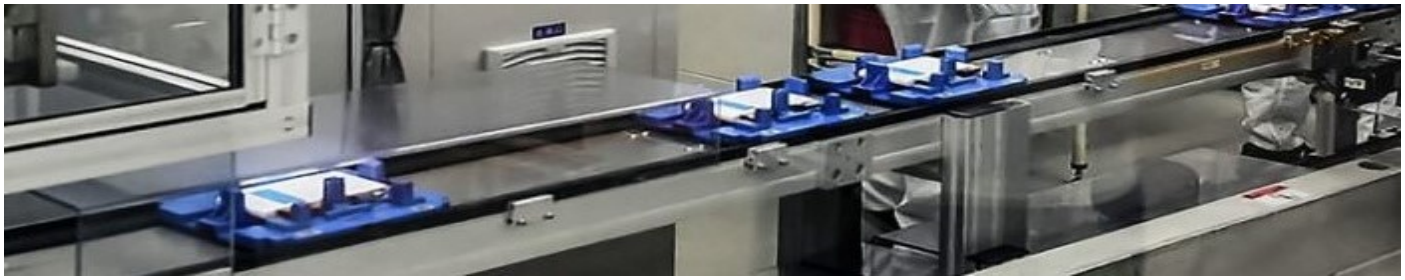
SGSI> **Diagrama Radar de estado actual de cumplimiento de los requisitos de la ISO 27001 que vienen definidos en el Anexo A:**



16 - Auditoría de Cumplimiento

SGSI> **Diagrama Radar de cumplimiento deseado de los requisitos de la ISO 27001 que vienen definidos en el Anexo A:**





Plan Director de Seguridad
Para la implementación de un SGSI Basado en la Norma ISO 27001:2013
En la Empresa AABBDDEE A.S.