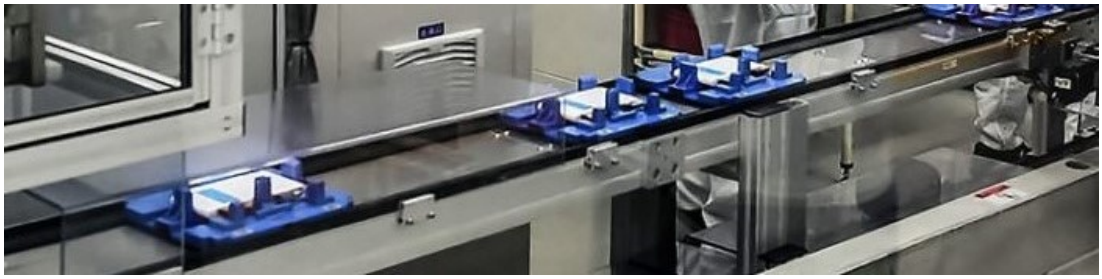


Plan Director de Seguridad
Para la implementación de un SGSI Basado en la Norma ISO 27001:2013
En la Empresa AABBDDEE A.S.

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

Índice

1 - Introducción.

1-1 - Justificación y contexto.

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

Proteger la información de una empresa consiste en poner barreras de protección para bloquear posibles ataques, es necesario proteger todos los assets de la empresa debido a que cada vez es más habitual es uso de internet y los sistemas de información, lo que convierte a las Empresas en focos más en vulnerable frente a los atacantes.

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.

Es necesario involucrar a todo el personal de la compañía sin importar el área a la que pertenezcan, pues son ellos los que ayudaran a implementar los sistemas de gestión para evitar que se queden solo en documentos. Algunos mecanismos para ello son las campañas de concientización sobre la seguridad de la información, la publicación de resultados, la verificación del cumplimiento de políticas y las auditorias de seguridad de la información.

Actualmente la Empresa AABBDDEE A.S., cuenta con diferentes procesos y procedimientos en el área de tecnología que están enfocados y basados en la Norma ISO 9001, con el transcurso del tiempo estos procesos no se han modificado y se crea la necesidad de evolucionar y actualizar estos procesos a una norma más actualizada y que este enfocada en la Seguridad de la Información.

Basados en la norma ISO 27001:2013 se evaluará el estado actual de los procesos relacionados con la seguridad de la información en la Empresa, realizándose un análisis de riesgos en miras a identificar y desarrollar los proyectos a generarse que le permitan la implementación de un sistema de Seguridad de la información.

1-2 - Implementación de un SGSI

1-2-1 - Objetivo.

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.

Se debe determinar el objetivo de la implementación de un SGSI, y qué parte de la organización va a ser objetivo del mismo, por ejemplo de entre: Procesos, Activos, Tecnología, Servicios, Personal, Relaciones con terceros.

Uno de los aspectos más importantes en el desarrollo de un SGSI es el establecimiento de los Objetivos Estratégicos de Seguridad y de los mecanismos necesarios para la medir y conocer cómo afectan a la seguridad de la información de la Empresa, las acciones de mejora que se realicen.

Estos datos permitirán tomar decisiones al respecto y realizar los ajustes necesarios para el logro de los objetivos.

1-2-2 - Beneficios.

Los beneficios de implantar un SGSI basado en la ISO 27001 podrían identificarse como los siguientes:

- Potenciar la aplicación de mejores prácticas de seguridad de la información en la Empresa.
- Aumentar la confiabilidad de los servicios ofrecidos a los clientes de la Empresa. Aumentar la confiabilidad de los servicios contratados a los proveedores de la Empresa.
- Aumentar el prestigio de la Empresa en el sector como una empresa comprometida con la seguridad de la información.
- Un beneficio claramente identificado en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en la Empresa, es la protección de uno de los activos más importantes de la Organización y de su futuro empresaria, es decir, la protección de su “Información”.

1-2-3 - Debe ser inherente a la propia Empresa

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.

Aumenta el número de ataques de día Cero es decir, aquellos que se producen antes de que se haga pública la existencia de la debilidad explotada. Los ataques se vuelven más complejos abarcando el aprovechamiento de debilidades no sólo tecnológicas, sino también operativas, ingeniería social, herramientas especializadas, etc.

Un volumen significativo de pérdidas económicas, de imagen, de oportunidades de negocio, etc., se deben a falta de políticas, procedimientos definidos y falta de control sobre el acceso a la información y a los sistemas.

Las Empresas con una estructura de Central y Delegaciones aumentan las necesidades de conexiones exteriores a las diferentes estructuras de sus sistemas, lo cual exige ir en paralelo con su seguridad.

Para la gestión de la seguridad de la información es habitual establecer o adoptar un modelo de la seguridad de la información partiendo de la información como activo central.

En este modelo se identificarán tanto los principios básicos que determinan la necesidad del nivel de seguridad en información como los actores que afectan a su estado tanto positivamente como negativamente.
Por esta razón, se debe establecer un compromiso mediante el desarrollo de un modelo de soporte para la gestión y la promoción de una cultura de seguridad, definiendo las responsabilidades por parte de su personal, clientes y usuarios, para la protección de la seguridad de sus activos de información.

Se considera que los pilares básicos de la seguridad de la información son:

- Confidencialidad:
  Sólo las personas autorizadas tienen acceso a la información sensible y/o privada. Por ejemplo a la información de un departamento de una Empresa solo podrán a acceder los miembros de ese departamento que hayan sido autorizados.

- Integridad:
  La información y sus métodos de procesamiento son exactos y completos, y no pueden ser manipulados sin autorización. Por ejemplo, la integridad de la

información digital de un análisis médico debe estar asegurada, ya que de lo contrario se podría poner en riesgo la salud de una persona.

- Disponibilidad:
  Los usuarios autorizados pueden acceder a la información cuando lo necesitan. Por ejemplo, la información que controla la gestión de la producción de una planta productiva que trabaja a tres turnos, no puede permitirse el lujo de que no esté disponible.

Aunque los anteriores paradigmas son los pilares básicos, tal como van evolucionando los entornos relacionados con la seguridad de la Información, también se deberían tener en cuenta los siguientes puntos:

- Autenticidad y no repudio:
  Existe garantía de la identidad de los usuarios, procesos que tratan la información, y de la autoría de una determinada acción.
- Trazabilidad:
  Es posible reproducir un histórico o secuencia de acciones sobre un determinado proceso y determinar quién ha sido el autor de cada acción.
- Privacidad:
  Que garantiza que sólo las personas autorizadas tienen acceso a información de carácter personal.

1-2-4 - La ISO/IEC 27002 como parte de la implementación

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. 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.

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.

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como la preservación de la confidencialidad, integridad y disponibilidad.

La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza, y a su vez se organiza en base a 14 dominios, 35 objetivos de control y 114 controles.

La norma ISO 27002 establece un catálogo de buenas prácticas que determina, desde la experiencia, una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en relación con el tratamiento de los riesgos.

La importancia de disponer de una actualizada, completa y veraz información es la clave para la correcta realización de todas las actividades de la organización, en todas sus áreas, campos y actividades. Sin embargo, es todavía mucho más importante mantener dicha información con seguridad para que no se pierda, se robe o se deteriore de cualquier forma.
La información y los datos de los que se dispone en la organización y que recopila en su día son uno de los activos más valiosos que pueden marcar el futuro de la organización.

De esta manera, es fácil comprender la importancia de la norma ISO 27001 como Sistema de Gestión de Seguridad de la Información. Sin embargo, es igual de importante el papel que ocupa dentro de todos los requisitos de la norma ISO 27002 como guía de buenas prácticas para implantar controles y que garantizarán la seguridad de la información gracias a sus recomendaciones.

La norma ISO 27002 se encuentra estructurada en 14 capítulos que describen las áreas que se deben considerar para garantizar la seguridad de la información de las que se dispone. El documento recomienda un total de 114 controles, si bien no hace falta cumplirlos todos, sí que hay que tenerlos en cuenta y considerar su posible aplicación, además del grado de la misma.

Revisión breve de cada uno de los 14 capítulos:

1. Políticas de Seguridad de la Información:
   Dentro de este capítulo se hace hincapié en la importancia que ocupa la disposición de una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

2. Organización de la Seguridad de la Información:
   Los controles indicados en este capítulo buscan estructurar un marco de seguridad eficiente tanto mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles.

Tenemos que tener presente que cada vez es mayor el peso que está ocupando el teletrabajo dentro de las empresas, y por ello, se deben tener en cuenta todas sus características especiales para que ningún momento la seguridad de la información de la que se dispone se vea afectada.

3. Seguridad relativa a los recursos humanos:
   Si analizamos los incidentes de seguridad que se producen en una organización nos daremos cuenta de que la gran mayoría de estos tienen su origen en un error humano. Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir.

4. Gestión de activos:
   Se centra en la atención en la información como activo y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, quiebras en la seguridad y en la alteración no deseada.

5. Control de acceso:
   Controlar quien accede a la información dentro de un aspecto relevante. Al fin y al cabo no todas las personas de una organización necesitan acceder para realizar su actividad diarias a todos los datos, sino que tendremos roles que necesitan un mayor acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, gestión de los privilegios de acceso, etc. siendo algunos de los controles que se incluyen en este apartado.

6. Criptografía:
   En el caso de que estemos tratando la información sensible o crítica puede ser interesante utilizar diferentes técnicas criptográficas para proteger y garantizar su autenticidad, confidencialidad e integridad.

7. Seguridad física y del entorno:
   La seguridad no es solo a nivel tecnológico sino también físico, es decir, una simple labor de no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles, por parte del personal externo los documentos con los que se están trabajando no sólo nos permitirán gestionar de forma adecuada la seguridad sino que se acabarán convirtiendo en hábitos que nos aportan eficiencia en la gestión.

8. Seguridad de las operaciones:
   Tiene un marcado componente técnico entrado en todos los aspectos disponibles como la protección del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc.

9. Seguridad de las comunicaciones:
   Partiendo de la base de que la gran mayoría de los intercambios de información y de datos en distintas escalas se llevan a cabo mediante las redes sociales, garantizar la seguridad y proteger de forma adecuada los medios de transmisión de estos datos clave.

10. Adquisiciones, desarrollo y mantenimiento de los sistemas de información:
    La seguridad no es un aspecto de un área en concreto, ni de un determinado proceso, abarca toda la organización y tiene que estar presente como elemento transversal clave dentro del ciclo de vida del sistema de gestión.

11. Relación de proveedores:
    Cuando se establecen las relaciones con terceras partes, como puede ser proveedores, se deben establecer medidas de seguridad pudiendo ser muy recomendable e incluso necesario en determinados casos.

12. Gestión de incidentes de seguridad de la información:
    No podemos hablar de controles de seguridad sin mencionar un elemento clave, los incidentes en seguridad. Se debe estar preparado para cuando estos incidentes ocurran, dando una respuesta rápida y eficiente, siendo la calve para prevenirlos en el futuro.

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio:
    No sabemos lo que necesitábamos un dato hasta que lo hemos perdido. Sufrir una pérdida de información relevante y no poder recuperarla de alguna forma puede poner en peligro la continuidad de negocio de la organización.

14. Cumplimiento:
    No podemos hablar de seguridad de la información, sin hablar de legislación, normas y políticas aplicables que se encuentre relacionadas con este campo y con las que conviven en las organizaciones. Debemos tener presente que ocupan un enorme lugar en cualquier sistema de gestión y se debe garantizar que se cumple y que están actualizados con los últimos cambios, siendo esencial para no llevarnos sorpresas desagradables.

1-3 - Plan Director de Seguridad.

1-3-1 - Introducción.

La Empresa debe ser consciente que la información es uno de los activos más importantes, por lo tanto debe proteger la información de los diferentes riesgos a los que se encuentra expuesta.

Dicha información está cada vez más compartida y accesible desde diferentes sistemas, lo cual aumenta su vulnerabilidad por lo tanto la Empresa debe proteger su activo más importante.

“La Online Trust Alliance (OTA) ha publicado su informe Cyber Incident & Breach Trends, un análisis anual que ha descubierto que los ciberataques dirigidos a negocios casi se duplicaron, de 82.000 en 2016 a 159.700 en 2017. Dado que la mayoría de los ciberincidentes no se denuncian, OTA cree que el número real en 2017 podría superar fácilmente los 350.000.”

Muchos incidentes son provocados por el propio personal interno de la organización, lo que hace ineficaces las medidas establecidas para proteger de los ataques procedentes del exterior.

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.

El crecimiento de los ataques diseñados específicamente para atacar objetivos determinados, la difusión de kits y la automatización que permiten realizar ataques sofisticados y masivos a personas sin conocimientos tecnológicos elevados, hace que el número de ataques haya crecido de manera enormemente significativa en los últimos años.

Debido a estos datos, las organizaciones necesitan proteger su información para asegurar que esté disponible cuando se necesite, que sea fiable y que su distribución esté controlada. Esta necesidad se ve agravada por el hecho de que la cantidad de información que maneja una organización y su complejidad crece de forma exponencial, dificultando los esfuerzos para su protección.
La Empresa debe establecer una disciplina que defina y gestione las variables, los procesos y los objetivos que intervienen el curso de cumplir con los requisitos o necesidades de seguridad TIC establecidos como aceptables para cualquier organización.

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

1-3-2 - Objetivo del plan director.

La evolución de las tecnologías de la información y comunicación nos ha permitido automatizar y optimizar muchas de las actividades que se llevan a cabo en la organización. Estas tecnologías han ido ocupando un lugar cada vez más importante, hasta el punto de que hoy en día, sin ellas, muchos de nuestros procesos de negocio no serían posibles.

La información es un activo importante para la Empresa, es fundamental para el negocio: facturas, informes, bases de datos de clientes, pedidos, etc. Podemos decir que la empresa basa su actividad en sistemas de información con soporte tecnológico (Ordenadores, Comunicaciones, página Web, etc.).

Por eso proteger los sistemas de información es proteger el negocio. Para garantizar la seguridad de la información del negocio se necesita llevar a cabo una gestión planificada de actuaciones en materia de Ciberseguridad, tal y como se realiza en cualquier otro proceso productivo de la organización.

Si sufrimos un incidente de seguridad informática, realmente no conocemos los riesgos a los que está expuesta la Empresa.

Si las herramientas tecnológicas y la información que dan soporte a los servicios y procesos productivos de la organización son de gran valor para la organización, debemos empezar a pensar en poner en práctica un Plan Director de Seguridad.

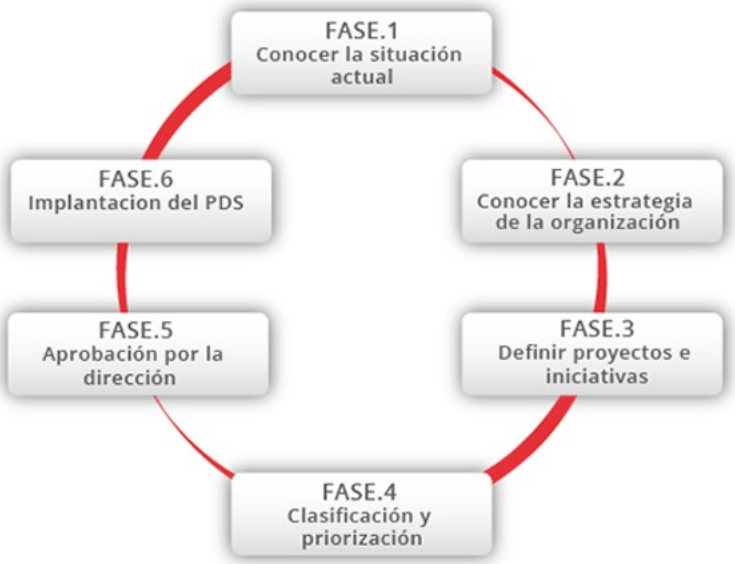
Plan Director de Seguridad:

- 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.

- Es fundamental para la realización de un buen Plan Director de Seguridad (PDS), que se alinee con los objetivos estratégicos de la empresa, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización así como terceros que colaboren con ésta.

- Se debe tener en cuenta que un Plan Director de Seguridad se basa en la mejora continua.

Para la elaboración y puesta en marcha de un Plan Director de Seguridad se siguen las siguientes fases o etapas:



Fases Plan Director de Seguridad.

Fuente: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

1-4 - Perfil del Responsable de Seguridad.

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

El responsable de seguridad de la información en un SGSI de una empresa, debe ser personal interno de la Empresa, ya que, tenemos que asumir que el Sistema de Gestión de Seguridad de la Información afecta a la gestión del negocio y requiere que todas las acciones futuras y las decisiones que se tomen solo las puedan desarrollar la alta dirección de la organización.

No podemos considerar que el Sistema de Gestión de Seguridad de la Información o SGSI sea una cuestión meramente tecnológica o técnica de los niveles inferiores de la

empresa sino todo lo contrario, la gerencia debe tener la responsabilidad de gestionar los riesgos y los impactos del negocio.

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.

Las funciones habituales del perfil del responsable de seguridad de la información en un SGSI, serán:

- Desarrollar una política de seguridad de la información.
- Garantizar el cumplimiento de planes y objetivos de Sistema de Gestión de Seguridad de la Información.
- Constituir roles y responsabilidades de seguridad de la información.
- Informar a la empresa la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad.
- Designar todos los recursos necesarios para llevar a cabo el SGSI.
- Determinar todos los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asignar los recursos suficientes para todas las fases del SGSI.
- Garantizar que se realizan todas las auditorías internas.
- Llevar a cabo revisiones periódicas del SGSI.
- Operar, establecer, implementar, monitorizar, revisar y mantener el Sistema de Gestión de Seguridad de la Información.
- Poder asegurar que todos los procedimientos de seguridad de la información apoyan a los requerimientos de negocio.
- Detallar todos los requerimientos necesarios para cumplir con la legislación vigente.
- Suministrar todos los controles implementados de una forma correcta.
- Desarrollar todas las revisiones cuando sea necesario.
- Mejorar la eficiencia del Sistema de Gestión de Seguridad de la Información.
- Decidir las competencias necesarias que debe tener cada trabajador de la empresa en función de las tareas que vaya a desempeñar.
- Complacer las necesidades mediante planes de formación.
- Analizar y evaluar la eficiencia de las acciones que ha desarrollado.
- Conservar todos los registros de estudios, formación, habilidades, experiencia y cualificación.
- Tomar las decisiones relativas y oportunas a:
    - Enriquecer y desarrollar la eficiencia del Sistema de Gestión de Seguridad de la Información.
    - Actualización del plan de tratamiento de riesgos y de la evaluación de riesgos.

- Cambiar los controles y procedimientos que afecten a la seguridad de la información. De esta forma, obtendremos como respuesta cambios internos o externos en los requisitos de los negocios.
- Necesidad de recursos.
- Mejorar la forma de medir la eficacia de los controles.

1-5 - Hoja de Ruta.

Los incidentes que surgen en la seguridad de la información, son algo común en los últimos años y se producen cada vez con una frecuencia mayor.

Esto supone la necesidad de establecer una disciplina de seguridad que proteja no sólo de las vulnerabilidades o debilidades conocidas, sino también de prevenir aquellas que sean posibles aunque sean desconocidas. Así mismo, supone la necesidad de reaccionar con rapidez y eficacia ante la publicación de nuevas vulnerabilidades, puesto que podrían empezar a ser explotadas en cualquier momento.

La falta de coordinación y gestión 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. Se necesitan herramientas de gestión que faciliten y automaticen los procesos necesarios para la toma de decisiones a nivel directivo basadas en la gestión de riesgos, el cumplimiento normativo y la coordinación de las auditorías. De este modo las organizaciones pueden reducir el esfuerzo en estas tareas e invertirlo en actividades de mejora e innovación.

1-6 - Enfoque y Método seguido.

El alcance del documento cubre la descripción e introducción a todos los conceptos, procesos y metodologías estandarizadas orientadas a la gestión de la seguridad de la información y por tanto a los SGSI.

En este documento se describirán los pasos de realización e implantación de los procesos orientados a la gestión de la seguridad de la información, y para ello, nos basamos en la metodología de implantación del SGSI bajo la Norma ISO/IEC 27001:2013 y nos apoyaremos en el estudio de la ISO/IEC 27002. Todo esto permitirá cuantificar y comparar los requisitos de seguridad de la información que debe cubrir la Empresa, mediante la implantación de las salvaguardas o controles adicionales necesarios para el cumplimiento de todos los requisitos.

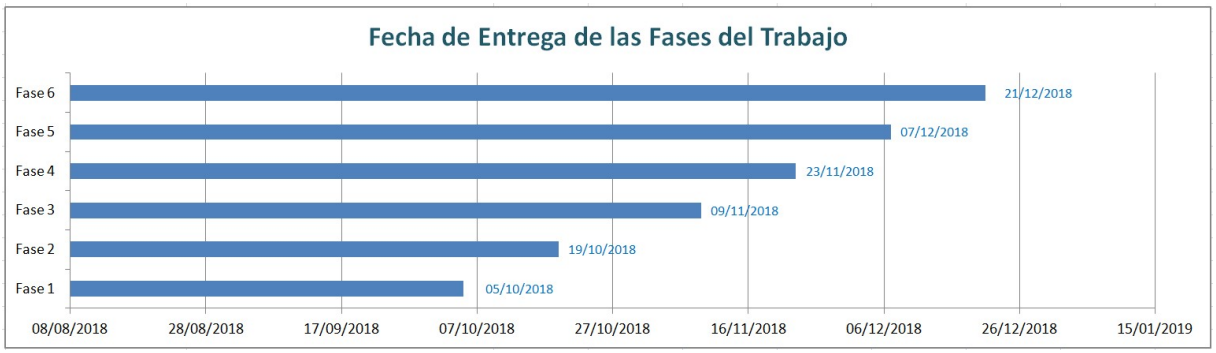
ISO 27001:2013 es la norma principal de la serie ISO 27000 y contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). Tiene su origen en el estándar ISO27001:2005. El nuevo estándar contiene 14 anexos con una mejor distribución de los controles y una simplificación hacia los aspectos que son realmente importantes en un SGSI para una empresa.

El SGSI se integrará con los procesos de gestión del negocio, apoyado la línea empresarial, a su vez asegurará la confidencialidad, integridad y disponibilidad de la Información, manteniendo este criterio a lo largo de la evolución de la Empresa.

La norma ISO27001:2013 comienza definiendo el sistema de gestión que servirá de base para administrar los riesgos: sistematizar el descubrimiento, tratamiento y mitigación de los riesgos, y su seguimiento a lo largo del tiempo. Después el Comité de Seguridad designado asignará recursos, verificará la implementación de los controles, proporcionará la mejora continua de los procesos, y marcará los ajustes de las políticas organizativas marcadas, que complementarán las medidas de seguridad incorporándolas a un plan de capacitación y concientización, para todos los actores involucrados en este ámbito.

1-7 - Planificación del Trabajo.

En el siguiente esquema se presenta la evolución del desarrollo de trabajo en el tiempo, desglosado en 6 fases:



Planificación en el tiempo de las Fases del Trabajo.

En cada fase se realizarán y documentarán los siguientes hitos, según la siguiente planificación:

- **FASE 1 - Situación Actual: Contextualización, objetivos y análisis diferencial.**
  Introducción al Proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto la ISO/IEC 27001+ISO/IEC 27002.

- **FASE 2 - Sistema de Gestión Documental.**
  Elaboración Política de Seguridad. Declaración de aplicabilidad y Documentación del SGSI.

- **FASE 3 - Análisis de Riesgos.**
  Elaboración de una metodología de análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

- **FASE 4 - Propuestas de Proyectos.**
  Evaluación de proyectos que debe llevar a cabo la Organización para alinearse con los objetivos planteados en el Plan Director. Cuantificación económica y temporal de los mismos.

- **FASE 5 - Auditoría de Cumplimiento.**
  Evaluación de controles, madurez y nivel de cumplimiento.

- **FASE 6 - Presentación de Resultados y Entrega de Informes.**
  Consolidación de los resultados obtenidos durante el proceso de análisis. Realización de los informes y presentación ejecutiva a la Dirección. Entrega del proyecto final.

2 - Situación Actual

2-1 - Contextualización- Empresa AABBDDEE A.S.

2-1-1 - Definición de la Empresa

AABBDDEE A.S. Empresa ficticia objeto de este Trabajo, es una Empresa dedicada a los suministros industriales para las empresas de automoción.

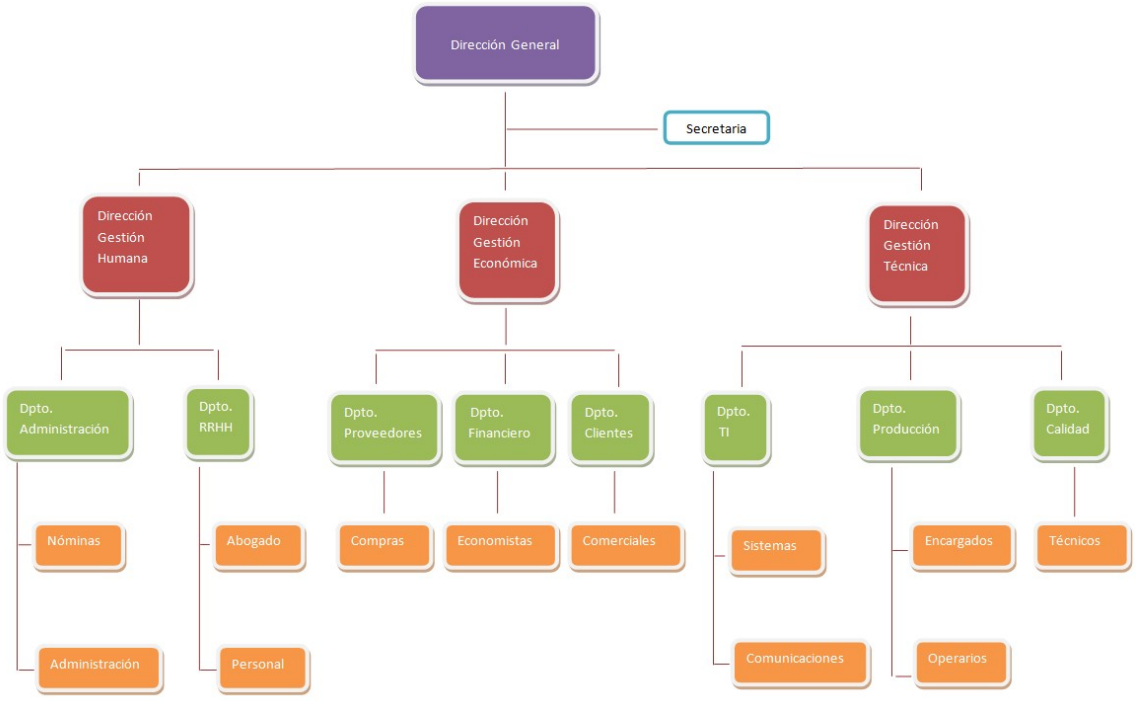
2-1-2 - Estructura y Jerarquía de la Organización

La Empresa AABBDDEE A.S está constituida por 46 personas, distribuidas en los siguientes departamentos y realizando los siguientes cometidos:

- 1 persona en la Dirección General.
- 1 persona en Secretaría.
- 3 personas en la Dirección de la Organización.
- 1 persona en Nóminas.
- 2 personas en Administración.
- 2 personas en RRHH.
- 2 personas en el departamento de Proveedores.
- 2 personas en el departamento Financiero.
- 2 personas en el departamento de Clientes.
- 6 personas pertenecen al departamento de TI.
- 22 personas trabajan en planta.
- 2 personas pertenecen al departamento de calidad.

A su vez la empresa tiene subcontratado el servicio de limpieza.

El siguiente esquema muestra la distribución funcional y jerárquica de la estructura de la Empresa AABBDDEE A.S:



Ver documento adjunto: Organigrama funcional de la Empresa AABBDDEE A.S.

2-1-3 - Infraestructura Tecnológica de la Empresa

A continuación se hace una descripción de la infraestructura tecnología relacionada con los sistemas IS/IT actuales:

- 1 CPD principal en la las oficinas físicas de la Empresa:
    - 12 servidores físicos:
        - 10 tienen Windows Server 2013:
            - 1 tiene instalada una base de datos Oracle con la información de clientes
            - 1 tiene instalada una base de datos Oracle con información de proveedores
            - 1 tiene instalada una base de datos Oracle con información de los productos de fábrica.

        - 2 tienen VMware para el uso de máquinas virtuales.

- 1 CPD secundario externalizado.

- 3 Firewall,s:
    - 1 protección para la navegación web segura.
    - 1 para la seguridad perimetral.
    - 1 para la segmentación.

- 2 Switches:
    - 1 de núcleo
    - 1 de distribución.

- 2 AP puntos de acceso Wifi.

- 1 unidad de cinta para las copias de seguridad (10 cintas LTO).

- 1 NAS para almacenamiento de información.

- En la empresa hay 30 portátiles.
    - 22 portátiles en oficinas
    - 8 portátiles en planta.
    - Los empleados tienen instalado en sus equipos el software habitual que tiene por defecto Windows 10.

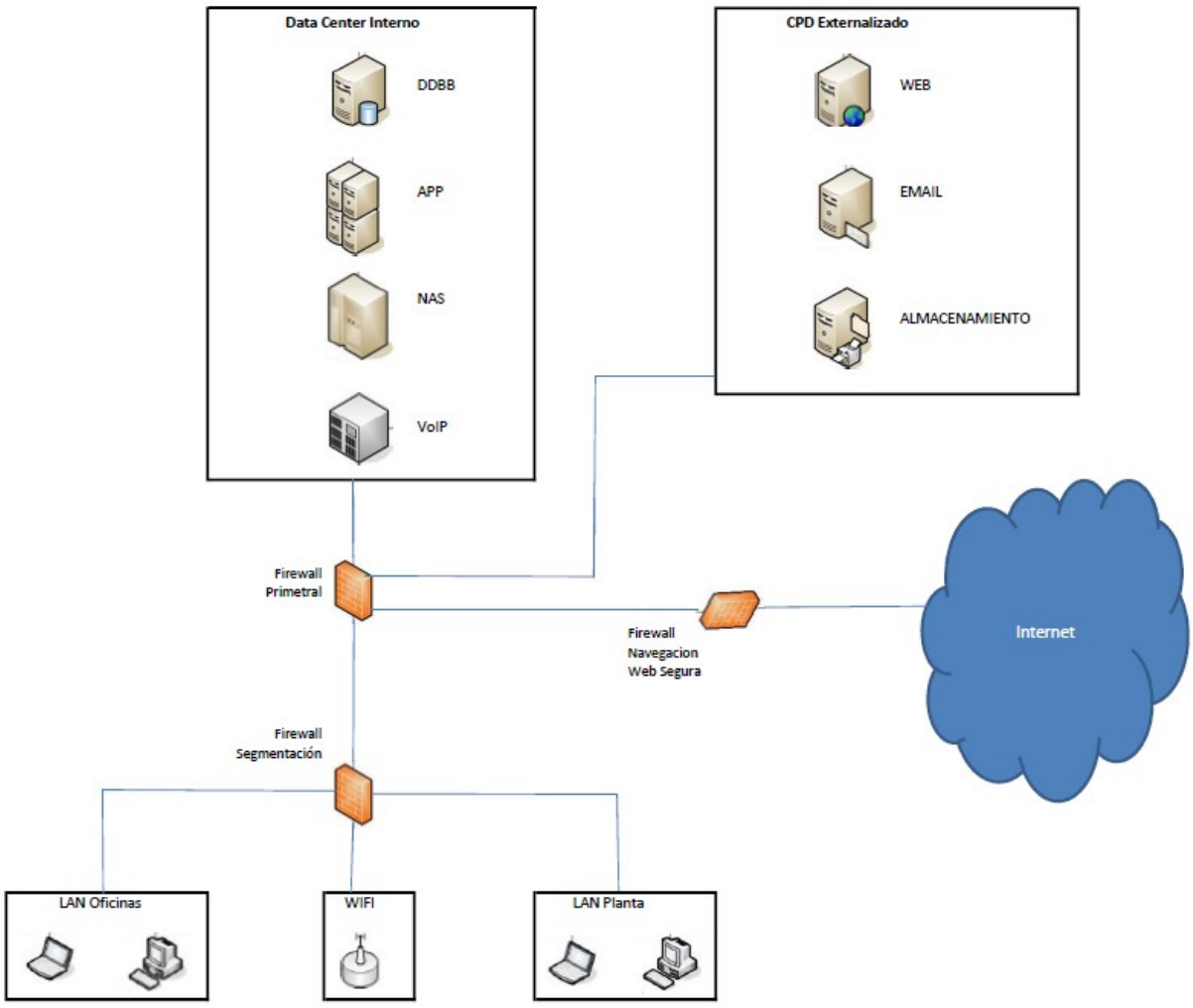
- En la empresa hay 20 PC´s.

- Todos los miembros de la empresa disponen de un dispositivo móvil (Smartphone).

- 1 medio de almacenamiento externo para compartir información con entidades externas.

- La empresa tiene subcontratado el hospedaje de la página web de la organización.

- La empresa tiene subcontratado el hospedaje del correo electrónico.



Ver documento adjunto: Diagrama de Red de la Infraestructura Tecnológica.

2-2 - Objetivos de la Seguridad de la Información.

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.

Objetivos específicos de seguridad alineados con el entorno de negocio de la Empresa AABBDDEE A.S.:

- La seguridad de la información debe estar en el mapa de riesgos de la Empresa.
- Debe ser tratada dentro del entorno de negocio de la Empresa.
- Reducir los tiempos de ejecución de los planes de continuidad de negocio.
- Priorizar los activos de información y los riesgos relacionados.
- Debe diferenciar entre datos, infraestructuras, aplicaciones y personas.
- Fortalecer la protección de la ciberseguridad para activos claves
- Debe ser holística con una gobernanza colaborativa
- Incluir y concienciar a todos los empleados
- Establecer características de seguridad en los sistemas TIC
- Debe construir defensas adaptativas
- Planificar y probar las respuestas e incidentes de la Seguridad de la Información.
- Conseguir reducir el número de incidentes de seguridad.
- Definir políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información.
- Definir las medidas de seguridad más apropiadas a aplicar.
- Mantener una cultura en Seguridad de la Información manteniendo un criterio de mejora continua y a su vez poder determinar el grado de su cumplimiento en el tiempo, con el seguimiento de los diferentes KPI´s, como pueden ser: objetivos estratégicos, indicadores del grado de efectividad, indicadores de medición del entorno y hostilidad, métricas de resultado obtenidos.

2-3 - Análisis diferencial.

AABBDDEE A.S. quiere imprentar un sistema de gestión de la seguridad de la información en su negocio, pero actualmente no tiene experiencia en la ISO 27001 como normativa para su desarrollo.

El objetivo del análisis es la verificación de la implantación, en relación a los procesos detectados en el Plan Director de Seguridad (PDS), de los controles establecidos en la Norma.

En estos momentos AABBDDEE A.S. documenta y gestiona ciertos controles en relación al ámbito de la seguridad de la información, que son:

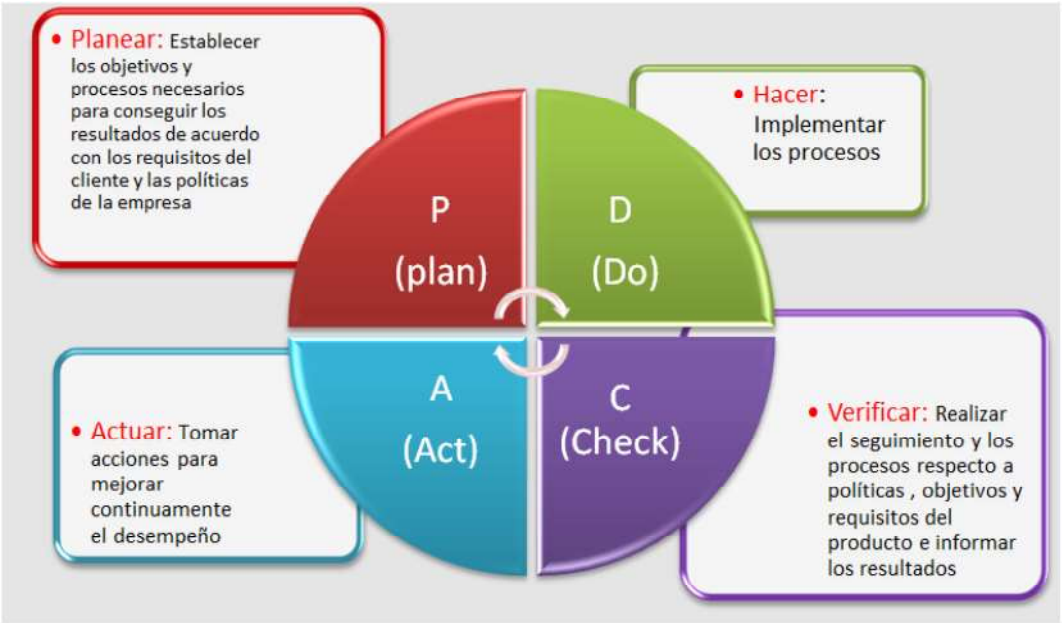
- Calendario y planing en las políticas de copias de seguridad.
- Procesos de gestión de cambios.
- Plan de continuidad de negocio.
- Plan de capacidad.
- Política de cifrado.
- Políticas de control de accesos.
- Procedimiento gestión de proveedores.

A su vez AABBDDEE A.S. tiene implementado otros controles no documentados, relacionados con la seguridad IS/IT que son:

- Entornos de desarrollo, pruebas y producción separados.
- Networking y controles de red para segmentación de los entornos de oficina IT y planta OT.
- Disposición de un sistema para la gestión de los incidentes de seguridad de la información.

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.

Tal como se planifica y redacta a continuación:



Etapas PDCA.

Fuente:https://www.google.es/search?q=imagenes+etapas+PDCA&tbm=isch&source=iu&ictx=1&fir=9oNkADoKt50eFM%253A%252CuTxbhNGEwJ_yoM%252C_&usg=AI4_-kSVebsnGDmxfG5rF9egxXZTrzEomw&sa=X&ved=2ahUKEwiZxfy5rYjeAhVIJ8AKHSL5C_cQ9QEwB3oECAYQEg#imgrc=9oNkADoKt50eFM:

- **Planificar - Establecer el SGSI**

En esta etapa se establecen los procesos necesarios para conseguir los resultados según las necesidades de los clientes y la política de seguridad de la organización.

A su vez se divide en las siguientes subetapas:

- Definir la política de seguridad:
  En esta subetapa de la planificación, se establecen los principios y líneas de actuación globales en cuestiones de seguridad de la información y siempre con alineación a los objetivos del negocio.
  Al final debe quedar constancia de una serie de políticas, normas, guías y estándares de segundo nivel.
  La política del SGSI es normalmente un documento muy general, una especie de "declaración de intenciones" de la Dirección.
- Definir el alcance:
  Donde se define el alcance del sistema de seguridad (sus límites), es decir, en a qué procesos, áreas organizativas, emplazamientos y activos de la organización queda limitado.
- Definir la organización de la seguridad de la información:

Es necesario tener definido un esquema de organización interno, donde todas las responsabilidades y funciones en materia de seguridad de la información estén correctamente asignadas.

- Definir las políticas de alto nivel:
  Donde se contemplan en conjunto todas las áreas de seguridad de la información.
- Definir los objetivos de seguridad:
  Donde se garantiza que todas las iniciativas en seguridad de la información estén coordinadas y orientadas en una misma dirección, y alineadas con los objetivos de negocio.
- Identificar los riesgos:
  Donde se identifican los activos de la información y se establecen los riesgos a los que están sometidos, según el impacto en caso de que produjera una falta de confidencialidad, privacidad, integridad o disponibilidad.
  La organización debe establecer un umbral de riesgo asumible por la organización y priorizar las acciones a tomar.
- Seleccionar Salvaguardas:
  Donde se seleccionan los controles o salvaguardas para mitigar los riesgos. Estas salvaguardas pueden ser controles técnicos, procedimientos operativos, normativas de usuario, cláusulas contractuales, etc.

- **Hacer - Implantar y operar el SGSI**

En esta etapa se implantan los procesos. Se especifica cómo se lleva a efecto las salvaguardas seleccionadas, cuándo se implementan, quién será responsable y con qué presupuesto se cuenta para su implementación y también cómo se medirá el éxito o fracaso de las acciones realizadas.

A su vez se divide en las siguientes subetapas:

- Implantar el plan de gestión del riesgo:
  Definido el Plan de Seguridad, se presenta a la dirección para su aprobación.
  Una vez aprobado por ésta, se conseguirá la dotación presupuestaria necesaria para arrancar los proyectos.
  En esta subetapa además se hace el seguimiento de los subproyectos que llevan a cabo la implementación de las medidas de seguridad que el análisis de riesgos ha determinado como necesarias en la etapa anterior.
- Seleccionar e implantar indicadores:
  Donde se establecen una serie de indicadores, que permitan controlar el funcionamiento de las medidas de seguridad de la información implantada, su eficacia y su eficiencia. Así como definir los mecanismos y la periodicidad de la medida de estos indicadores.

- **Verificar - Monitorizar y revisar el SGSI**

En esta etapa se revisan y se evalúan tanto lo servicios como los procesos comprándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.
Como mínimo se realizará una revisión anual del sistema de gestión global. Debe existir un procedimiento que describa cómo mantener actualizado el SGSI.

A su vez se divide en las siguientes subetapas:

  - Desarrollar procedimientos de Monitorización:
    Se recomienda la automatización de los procedimientos de monitorización, para facilitar y fiabilizar la generación de los informes del estado de la seguridad de la información y la generación de las alarmas de seguridad deficientes y que requieran actuación urgente.
  - Revisar regularmente el SGSI:
    La Dirección debe revisar el SGSI a intervalos planificados, para ratificar su conveniencia, adecuación y eficacia. Esta revisión debe ser como mínimo anual, aunque inicialmente se recomienda una periodicidad menor.
  - Auditar internamente el SGSI:
    Para comprobar la idoneidad del diseño e implantación del SGSI se realizan auditorías (internas o externas), la cuales deben ser planificadas para poder contar con la implicación de las personas necesarias.

- **Actuar - Mantener y mejorar el SGSI**

En esta etapa se mejorar la eficacia de las prestaciones y la gestión de los servicios.

A su vez se divide en las siguientes subetapas:

  - Implantar mejoras, acciones correctivas y preventivas:
    De las etapas anteriores (monitorización, revisión, resultados auditorías), se obtienen una serie de propuestas de mejora y acciones correctivas y preventivas que hay que planificar en el Plan de Seguridad de la información.
  - Mantener registros:
    Un registro es una evidencia de cualquier parte del SGSI. En ellos se establece los procedimientos para realizar la gestión de los registros: identificación, almacenamiento, protección, recuperación, eliminación, etc.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de ACTUAR lleva de nuevo a la fase de PLANIFICACIÓN para iniciar un nuevo ciclo de las cuatro fases.

Procedemos a continuación a realizar el análisis diferencial con respecto a los apartados del 4 al 10 identificados en la Norma ISO 27001:

4. Contexto de la Organización:

Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI:

- 4.1. Conocimiento de la organización y de su contexto
- 4.2. Comprensión de las necesidades y expectativas de las partes interesadas
- 4.3. Determinación del alcance del Sistema de Gestión de la Seguridad de la Información.
- 4.4. Sistema de Gestión de Seguridad de la Información.

5. Liderazgo:

Esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

- 5.1. Liderazgo y compromiso.
- 5.2. Política.
- 5.3. Roles, responsabilidades y autoridades en la organización.

6. Planificación:

Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

- 6.1. Acciones para tratar riesgos y oportunidades.
- 6.2. Objetivos de Seguridad de la información y planes para lograrlos.

7. Soporte:

Esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

- 7.1. Recursos.
- 7.2. Competencia.
- 7.3. Toma de conciencia.
- 7.4. Comunicación.
- 7.5. Información documentada.

8. Operación:

Esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

8.1. Planificación y control operacional.
8.2. Valoración de riesgos de la seguridad de la información.
8.3. Tratamiento de riesgos de la seguridad de la información.

9 Evaluación desempeño:

Esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

9.1. Seguimiento, medición, análisis y evaluación.
9.2. Auditoría interna.
9.3. Revisión por la dirección.

10. Mejora:

Esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

10.1. No conformidades y acciones correctivas.
10.2. Mejora continua.

Disponemos de la Siguiente Información de la Empresa AABBDDEE A.S.:

La Empresa en la situación actual entiende la necesidad de la implantación de un SGSI, aunque de momento no se llega a visualizar el alcance del ISMS.

El órgano de dirección de la Empresa manifiesta su compromiso por liderar el proceso marcando unos roles que lleven adelante las políticas necesarias para la implantación del SGSI, pero se manifiesta la necesidad de este trabajo para seguir una plan de ruta, que de alguna manera deje claramente marcado como planificar y abordar los riesgos y oportunidades.

Actualmente la empresa dispone de algunos documentos en relación a la seguridad de la información, pero de una manera no estructurada, por lo tanto se ve la carencia de la existencia en un soporte que identifique los recursos, competencias, conciencia, comunicación, información documentada, los cuales se identificarán y

documentarán en lo evolución de este plan director de la implantación de SGSI para esta Empresa.

A partir de este punto será preciso y necesario realizar una evaluación de riesgos de la seguridad de la información de la Empresa, trabajo no realizado hasta ahora en la organización.

Tras la realización de la evaluación de riesgos será necesario marcar un umbral aceptable y determinar las técnicas a aplicar para el manejo de dichos riesgos en beneficio de la Empresa y cumplimento del SGSI desarrollado.

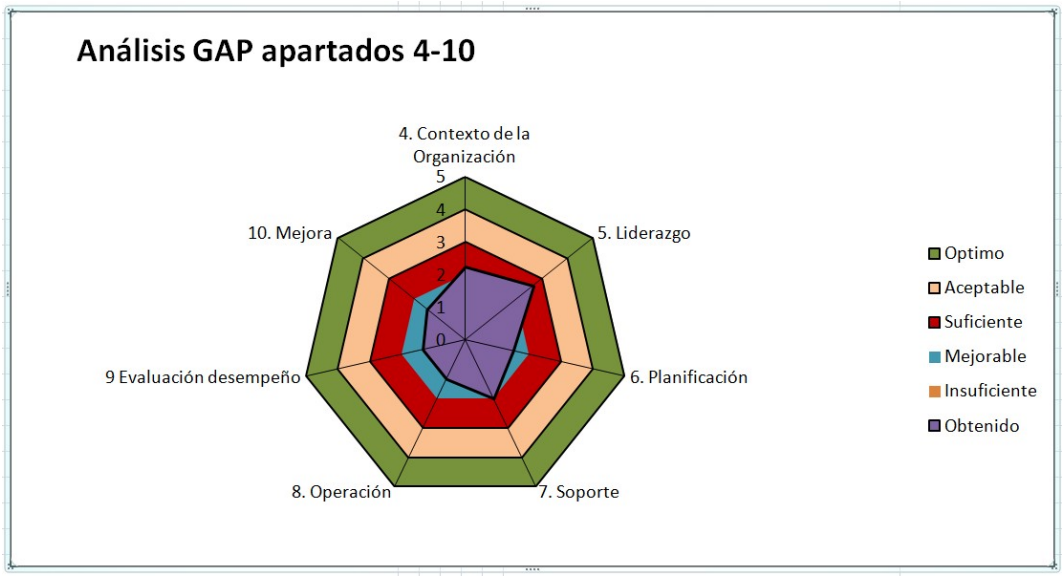
Como ya se ha indicado anteriormente, la implantación del SGSI no es un proceso estático, sino que será necesario que se realicen periódicamente, en la Empresa, auditorías internas al respecto y que los resultados sean revisados por la Dirección de la Organización, para que se apliquen las correcciones que sean necesarias.

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):

Ver documento adjunto:
Análisis diferencial apartados 4-10.

	Valor
4. Contexto de la Organización	2,25
5. Liderazgo	2,666
6. Planificación	1,5
7. Soporte	2
8. Operación	1,333
9 Evaluación desempeño	1,333
10. Mejora	1,5

Resumen análisis diferencial apartados 4-10.



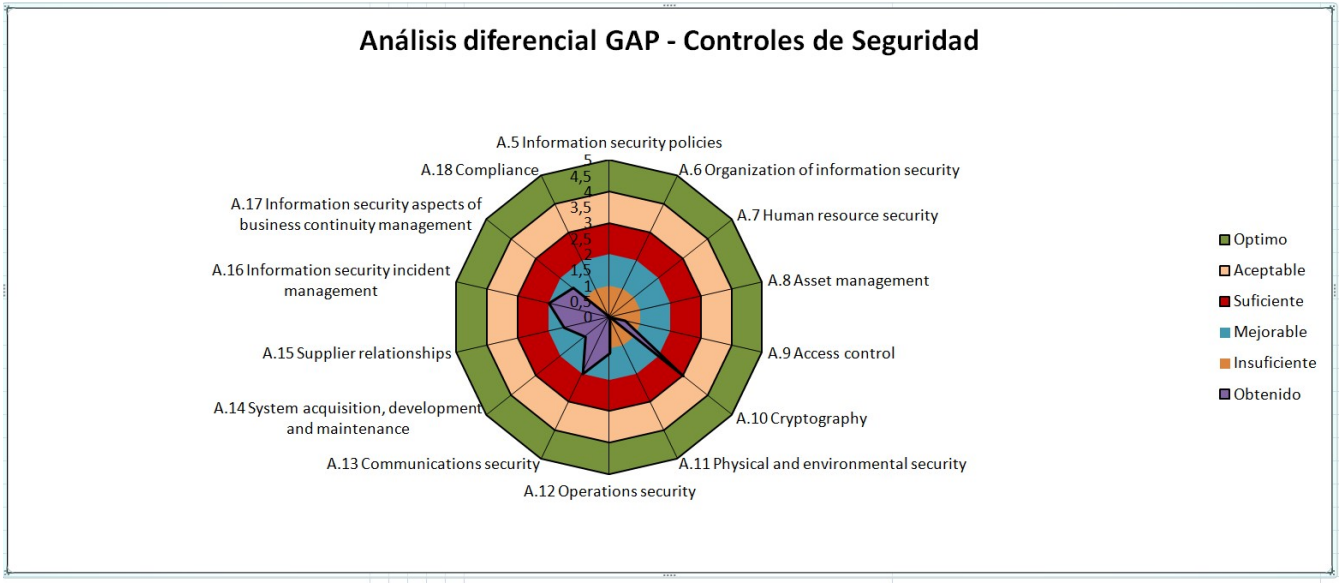
Análisis GAP apartados 4-10.

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):

Ver documento adjunto: ***Análisis diferencial Controles de Seguridad.***

	Valor
A.5 Information security policies	0
A.6 Organization of information security	0
A.7 Human resource security	0
A.8 Asset management	0
A.9 Access control	0,5
A.10 Cryptography	3
A.11 Physical and environmental security	0
A.12 Operations security	1,14
A.13 Communications security	2
A.14 System acquisition, development and maintenance	1
A.15 Supplier relationships	1,5
A.16 Information security incident management	2
A.17 Information security aspects of business continuity management	1,5
A.18 Compliance	0

Resumen análisis diferencial Controles de Seguridad.



Análisis GAP Controles de Seguridad.

3 - Sistema de Gestión Documental.

3-1 - Introducción.

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.

Se debe conocer qué documentación, o información documentada en el lenguaje simplificado de las normas ISO, es formal y estrictamente necesaria para que el Sistema de Gestión de Seguridad de la Información (SGSI) de una organización cumpla con la ISO 27001:2013.

En la siguiente lista de verificación se identifican los Documentos obligatorios y Registros requeridos por la ISO 27001:2013:

Documentos obligatorios:

- **El alcance del sistema de gestión de seguridad de la información (cláusula 4.3)** Este documento es, habitualmente, bastante corto y se redacta al inicio de la implementación de ISO 27001. En general, se trata de un documento independiente, aunque puede ser unificado con una política de seguridad de la información.

- **Política de seguridad de la información y objetivos (cláusulas 5.2 y 6.2)** La política de seguridad de la información generalmente es un documento breve y de alto nivel que detalla el principal objetivo del SGSI. Los objetivos para el SGSI, en general, se presentan como un documento independiente, pero también pueden ser unificados en la política de seguridad de la información. Contrariamente a la revisión 2005 de ISO 27001, ya no se necesitan ambas políticas (Política del SGSI y Política de seguridad de la información); solo hace falta una política de seguridad de la información.

- **Metodología de evaluación y tratamiento de riesgos (cláusula 6.1.2)** La metodología de evaluación y tratamiento del riesgo es, habitualmente, un documento de 4 a 5 páginas y debe ser redactado antes que se realice la evaluación y el tratamiento de riesgos. El informe de evaluación y tratamiento de riesgos debe ser redactado una vez que se realizó la evaluación y el tratamiento de riesgos, y allí se resumen todos los resultados.

- **Declaración de aplicabilidad (cláusula 6.1.3 d)**
  La Declaración de aplicabilidad (o DdA) se redacta en base a los resultados del tratamiento del riesgo; es un documento clave dentro del SGSI porque describe no sólo qué controles del Anexo A son aplicables, sino también cómo se implementarán y su estado actual. También debería considerar a la Declaración de aplicabilidad como un documento que describe el perfil de seguridad de su empresa.

- **Plan de tratamiento de riesgo (cláusula 6.1.3 e y 6.2)**
  Este es, básicamente, un plan de acción sobre cómo implementar los diversos controles definidos por la DdA. Este documento se desarrolla en función de la Declaración de aplicabilidad y se utiliza y actualiza activamente a lo largo de toda la implementación del SGSI.

- **Informe sobre evaluación de riesgos (cláusula 8.2)**
  Este es, básicamente, el informe sobre la evaluación de riesgos. Identificar, controlar, reducir o eliminar las fuentes de riesgo antes de que empiecen a afectar al cumplimiento de los objetivos.

- **Definición de roles y responsabilidades de seguridad (cláusulas A.7.1.2 y A.13.2.4)**
  El mejor método es describir estas funciones y responsabilidades en todas las políticas y procedimientos de la forma más precisa posible. Evite expresiones como "debería hacerlo"; en cambio, utilice algo como "el Jefe de seguridad realizará xyz todos los lunes a las zxy horas". Algunas empresas prefieren detallar las funciones y responsabilidades de seguridad en sus descripciones del trabajo; sin embargo, esto puede generar mucho papelerío.

- **Inventario de activos (cláusula A.8.1.1)**
  Si no contaba con un inventario de este tipo antes del proyecto ISO 27001, la mejor forma de hacerlo es directamente a partir del resultado de la evaluación de riesgos ya que allí, de todos modos, se tienen que identificar todos los activos y sus propietarios; entonces, simplemente puede copiar el resultado desde ese instrumento.

- **Uso aceptable de los activos (cláusula A.8.1.3)**
  Habitualmente, este documento se confecciona bajo la forma de una política y puede cubrir un amplio rango de temas porque la norma no define muy bien este control. Probablemente, la mejor forma de encararlo es la siguiente: déjelo para el final de la implementación de su SGSI y todas las áreas y controles que no haya cubierto con otros documentos y que involucran a todos los empleados, inclúyalos en esta política.

- **Política de control de acceso (cláusula A.9.1.1)**
  En este documento usted puede cubrir sólo la parte comercial de la aprobación de acceso a determinada información y sistemas, o también puede incluir el aspecto técnico del control de acceso. Además, puede optar por definir reglas para acceso lógico únicamente o también para acceso físico. Debería redactar este documento solamente después de finalizado su proceso de evaluación y tratamiento de riesgos.

- **Procedimientos de operación para gestión de TI (cláusula A.12.1.1)**
  Puede crear este procedimiento como un único documento o como una serie de políticas y procedimientos; si se trata de una empresa pequeña, debería tener menor cantidad de documentos. Normalmente, aquí puede abarcar todas las áreas de las secciones A.12 y A.13: gestión de cambios, servicios de terceros, copias de seguridad, seguridad de red, códigos maliciosos, eliminación y destrucción, transferencia de información, supervisión del sistema, etc. Este documento se debería redactar solamente una vez que finalice su proceso de evaluación y tratamiento de riesgos.

- **Principios de ingeniería de sistemas seguros (cláusula A.14.2.5)**
  Este es un nuevo control en ISO 27001:2013 y requiere que se documenten los principios de ingeniería de seguridad bajo la forma de un procedimiento o norma y que se defina cómo incorporar técnicas de seguridad en todas las capas de arquitectura: negocio, datos, aplicaciones y tecnología. Estos principios pueden incluir validación de datos de entrada, depuración, técnicas para autenticación, controles de sesión segura, etc.

- **Política de seguridad para proveedores (cláusula A.15.1.1)**
  Este también es un control nuevo en ISO 27001:2013, y una política de este tipo puede abarcar un amplio rango de controles: cómo se realiza la selección de potenciales contratistas, cómo se ejecuta la evaluación de riesgos de un proveedor, qué cláusulas incluir en el contrato, cómo supervisar el cumplimiento de cláusulas contractuales de seguridad, cómo modificar el contrato, cómo cerrar el acceso una vez cancelado el contrato, etc.

- **Procedimiento para gestión de incidentes (cláusula A.16.1.5)**
  Este es un procedimiento importante que define cómo se informan, clasifican y manejan las debilidades, eventos e incidentes de seguridad. Este procedimiento también define cómo aprender de los incidentes de seguridad de la información para que se puedan evitar en el futuro. Un procedimiento de esta clase también puede invocar al plan de continuidad del negocio si un incidente ha ocasionado una interrupción prolongada.

- **Procedimientos de Continuidad de negocio (cláusula A.17.1.2)**
  Generalmente se trata de planes de continuidad del negocio, planes de respuesta ante incidentes, planes de recuperación para el sector comercial de la organización y planes de recuperación ante desastres (planes de recuperación para infraestructura de TI). Estos procedimientos se describen con mayor detalle en la norma ISO 22301, la principal norma internacional para continuidad del negocio.

- **Requerimientos legales, regulatorios y contractuales (cláusula A.18.1.1)**
  Este listado debe confeccionarse en la etapa más temprana posible del proyecto porque muchos documentos tendrán que ser desarrollados de acuerdo a estos datos. Este listado debe incluir no sólo las responsabilidades para el cumplimiento de determinados requerimientos, sino también los plazos.

Registros obligatorios:

- **Registros de formación, habilidades, experiencia y calificaciones (cláusula 7.2)**
  Es el departamento de recursos humanos el que generalmente se encarga de llevar estos registros. Si usted no tiene un sector de este tipo, cualquier persona que habitualmente se encargue de los empleados debería ser quien realice este trabajo. Básicamente, sería suficiente una carpeta en la que se encuentren todos los documentos.

- **Seguimiento y resultados de medición (cláusula 9.1)**
  La forma más sencilla de describir cómo se miden los controles es a través de políticas y procedimientos que definan a cada control. En general, esta descripción puede ser realizada al final de cada documento, y cada descripción tiene que definir los tipos de ICD (indicadores clave de desempeño) que es necesario medir para cada control o grupo de controles.
  Una vez que se estableció este método de control, usted debe realizar la medición en función de dicho método. Es importante reportar los resultados de esta medición en forma regular a las personas que están a cargo su evaluación.

- **Programa de auditoría interna (cláusula 9.2)**
  El programa de auditoría interna no es más que un plan anual para realizar las auditorías; para las empresas más pequeñas, puede tratarse solamente de una auditoría, mientras que para las organizaciones más grandes puede ser una serie de, por ejemplo, 20 auditorías internas. Este programa debe definir quién realizará las auditorías, los métodos que se utilizarán, los criterios que se aplicarán, etc.

- **Resultados de auditorías internas (cláusula 9.2)**
  Un auditor interno debe generar un informe de auditoría, que incluye los resultados de la auditoría (observaciones y medidas correctivas). Este informe

debe ser confeccionado dentro de un par de días luego de realizada la auditoría interna. En algunos casos, el auditor interno tendrá que verificar si todas las medidas correctivas se aplicaron según lo esperado.

- **Resultados de la Revisión por Dirección (cláusula 9.3)**
  Estos registros se presentan, normalmente, bajo la forma de actas de reunión y deben incluir todo el material tratado durante la reunión de la dirección, como también todas las decisiones que se tomaron. Estas actas pueden ser en papel o en formato digital.

- **Resultados de acciones correctivas (cláusula 10.1)**
  Generalmente, estos son incluidos en los formularios para medidas correctivas (FMC). Sin embargo, es mucho mejor agregar estos registros en alguna aplicación que ya esté en uso en la organización; por ejemplo, la Mesa de ayuda, porque las medidas correctivas no son más que listas de actividades a realizar con responsabilidades, tareas y plazos bien definidos.

- **Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3)**
  Habitualmente se llevan de dos formas: (1) en formato digital, generados en forma automática o semiautomática como registros de diversas TI y de otros sistemas, y (2) en papel, donde cada registro se hace manualmente.

Con la realización correcta de estos documentos la Organización consigue procedimientos a nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

También se debe mantener un control de estos documentos generados, para establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión sobre los mismos:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.

- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

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:

3-2 - Política de seguridad de la información

La política de seguridad de la información generalmente es un documento breve y de alto nivel que detalla el principal objetivo del SGSI. Los objetivos para el SGSI, en general, se presentan como un documento independiente, pero también pueden ser unificados en la política de seguridad de la información. Contrariamente a la revisión 2005 de ISO 27001, ya no se necesitan ambas políticas (Política del SGSI y Política de seguridad de la información); solo hace falta una política de seguridad de la información.

La Política de Seguridad es establecida por la Dirección de la empresa y tiene de contemplar que:

- Tiene que alinearse a la estrategia de la empresa.
- Debe reflejar los objetivos de seguridad de la Información y una guía para conseguirlo.
- Se debe reflejar el compromiso por parte de los afectados de dicha política.
- Deberá estar disponible y constantemente comunicada a los afectados por la misma.

La Organización en relación a la política de Seguridad se posiciona en:

- Asegurar los fundamentos de confidencialidad, integridad y disponibilidad de la información.
- Profundizar los requisitos de protección de la información, tanto operativamente como legalmente.

- Se compromete a participar, marcar responsabilidades, implantar y mantener en el tiempo el resultado del desarrollo de este documento que abarca la seguridad de la información de la Empresa.
- Concienciar e informar a los afectados por este plan.

Ver documento adjunto: ***Política de Seguridad de la Información.***

3-3 - 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, asegurando el seguimiento del plan desarrollado, de una manera interna a lo largo del tiempo, que garantice su cumplimiento, objetivos marcados y observando los puntos:

- El análisis de riesgos: cómo la compañía analiza sus riesgos y el criterio empleado para determinar si un riesgo es o no significativo.
- La declaración de aplicabilidad.
- Los objetivos que persigue la organización.
- Cómo se monitoriza y mide.
- Cómo se informa y mejora.
- Las revisiones realizadas sobre el SGSI.
- El grado de implicación de la Dirección de la compañía.
- La coherencia entre la política, el análisis de riesgos, los objetivos, responsabilidades, normas, procedimientos, datos de indicadores, revisiones realizadas y criticidad de la información afectada.

Las auditorías internas se realizaran periódicamente, por el equipo dirigido por el auditor seleccionado, el cual deberá tener en posesión un título universitario TIC, y estar formado en el entorno SGSI.

Entre las misiones del Auditor responsable estarán:

- Coordinar el equipo seleccionado para la realización de las auditorias.
- Preparar las auditorias.
- Verificar que el SGSI es conforme con la norma y se mantiene actualizado.
- Registrar los elementos auditables.
- Analizar los resultados de las auditorías.
- Realizar informes de los resultados de la auditoria.

La Auditoría completa se realizará cada año, divida en secciones que se realizarán trimestralmente según la siguiente planificación:

Primer Trimestre:

- Auditoría de las Políticas de Seguridad.
- Auditoría de la Organización de la Seguridad de la Información.
- Auditoría de la Seguridad relacionada con Recursos Humanos.
- Auditoría de la Gestión de Activos.

Segundo Trimestre:

- Auditoría del Control de de accesos.
- Auditoría del Cifrado.
- Auditoría de la Seguridad Física y Ambiental.
- Auditoría de la Seguridad de la Operativa.

Tercer Trimestre:

- Auditoría de la Seguridad de las Comunicaciones TIC.
- Auditoría de la Adquisición y mantenimiento de los Sistemas de Información.
- Auditoría de la Relaciones con Proveedores.

Cuarto Trimestre:

- Auditoría de la Gestión de Incidentes en la Seguridad de la Información.
- Auditoría de la Gestión de la Continuidad de Negocio en relación con la Seguridad de la Información.
- Auditoría del Cumplimiento.

A continuación se adjunta la plantilla base que servirá de guía para la realización de las auditorias:

Ver documento adjunto: Plantilla del modelo de Informe de Auditoría.

3-4 - Gestión de Indicadores

Se deben medir los controles de seguridad implantados para la obtención de resultados tras las auditorias, para lo cual se deben definir unos indicadores.

A través de estos indicadores se podrá evaluar la implementación del SGSI en la Organización y su correcto seguimiento:

- A.7.2.2 Concienciación, educación y capacitación en seguridad de la información

Nombre indicador	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información
Descripción	Medida de conocimiento de la implantación de la seguridad de la información
Fórmula de medición	Número de respuestas afirmativas con respecto al número de personas de la empresa
Unidades de medida	Respuestas / Personas
Valor objetivo	100%
Valor umbral	<75%

- A.8.1.3 Uso aceptable de los activos

Nombre indicador	A.8.1.3 Uso aceptable de los activos
Descripción	Medida que marca la correcta utilización de los activos inventariados para la seguridad de la información
Fórmula de medición	Número de activos correctamente utilizados con respecto al total
Unidades de medida	Activos / Activos
Valor objetivo	100%
Valor umbral	<80%

- A.11.1.2 Controles físicos de entrada

Nombre indicador	A.11.1.2 Controles físicos de entrada
Descripción	Control del funcionamiento del procedimiento de acceso de personas
Fórmula de medición	Número de accesos contralados con respecto a los acceso realizados
Unidades de medida	Accesos / Accesos
Valor objetivo	100%
Valor umbral	<100%

- A.12.6.1 Gestión de las vulnerabilidades técnicas

Nombre indicador	A.12.6.1 Gestión de las vulnerabilidades técnicas
Descripción	Control de las vulnerabilidades técnicas detectadas en un periodo de tiempo
Fórmula de medición	Número de vulnerabilidades en un mes
Unidades de medida	Vulnerabilidades / tiempo
Valor objetivo	0%
Valor umbral	< 2 %

- A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Nombre indicador	A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
Descripción	Revisión de KPI´s de control de la implantación y continuidad de la de la seguridad de la información
Fórmula de medición	Suma resultados KPI con respecto al máximo de la suma de los KPI,s
Unidades de medida	Resultado KPI / Resultado KPI
Valor objetivo	80%
Valor umbral	< 70%

3-5 - 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, en este ámbito la normativa ISO 27001 establece que:

- Se deben tener en cuenta los cambios en la empresa que afecten al SGSI.
- Compromiso de gestionar la información documentada de forma detallada.
- Revisar el cumplimiento de los objetivos de calidad y seguridad de la información.
- Revisar el cumplimiento de la implementación de los planes definidos para el tratamiento de los riesgos identificados, así como de las vulnerabilidades y amenazas.
- Valorar la retroalimentación del desempeño de la Seguridad de la Información y la aplicación de las acciones correctivas resultado de las auditorias y revisiones realizadas, así como revisar y asegurar el cumplimiento de objetivos de Seguridad de la Información.

Tras la revisión por Dirección, se pueden considerar como salidas positivas, las decisiones relacionadas con oportunidades de mejora del entorno de la Seguridad de la información y posibles cambios de estrategia, todo lo cual va dirigido a la propia mejora del negocio de la propia Empresa.

A continuación se adjunta la plantilla base que servirá de guía para el registro de las revisiones que realice la Dirección

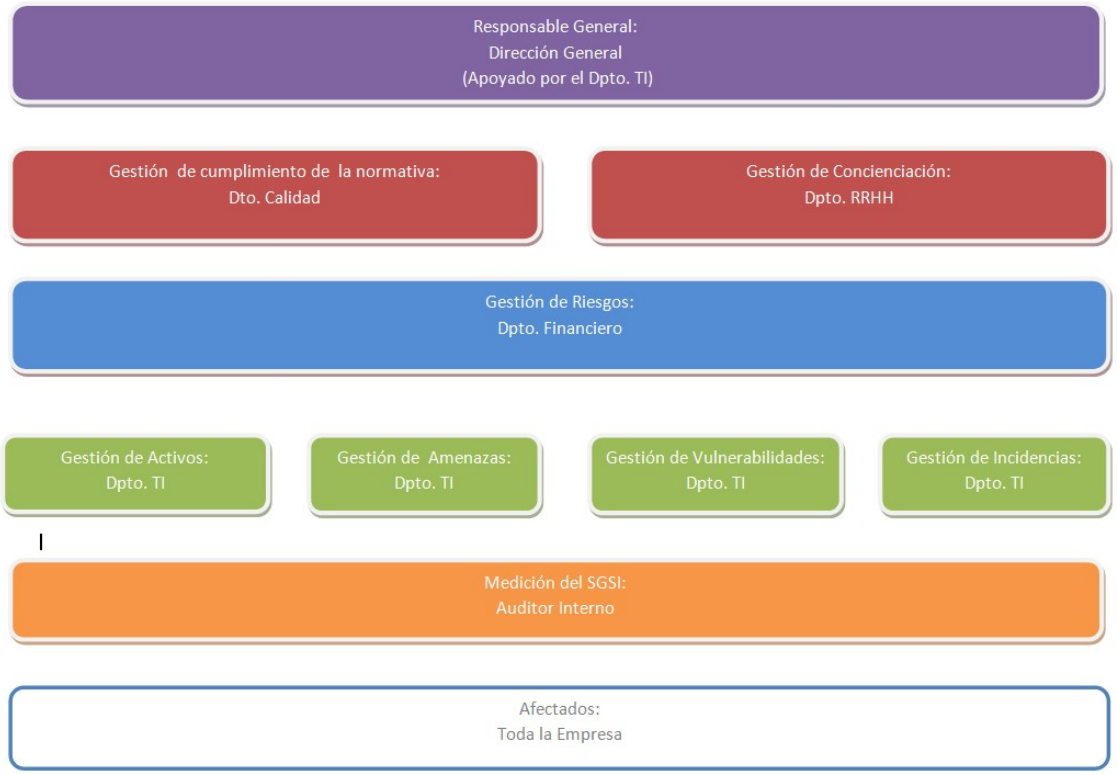
Ver documento adjunto: ***Plantilla del modelo de Registro de Revisión de la Dirección.***

3-6 - Roles y Responsabilidades

La norma ISO 27001 establece que los roles, responsabilidades y autoridades en la organización han de cumplir los siguientes requerimientos:

- La Dirección ha de asegurar la comunicación y asignación de roles dentro de la organización.
- La Dirección debe asignar responsabilidades y autoridad para asegurar la conformidad del SGSI con la normativa ISO 27001.
- La Dirección ha de asignar responsabilidad y autoridad para tener una fuente que reporte sobre el desempeño del SGSI

La Dirección de la Empresa ha marcado los distintos Roles y Responsabilidades relacionadas con la implantación, cumplimento y seguimiento del Sistema de Gestión de la Seguridad de la Información en la Empresa, en función del siguiente esquema:



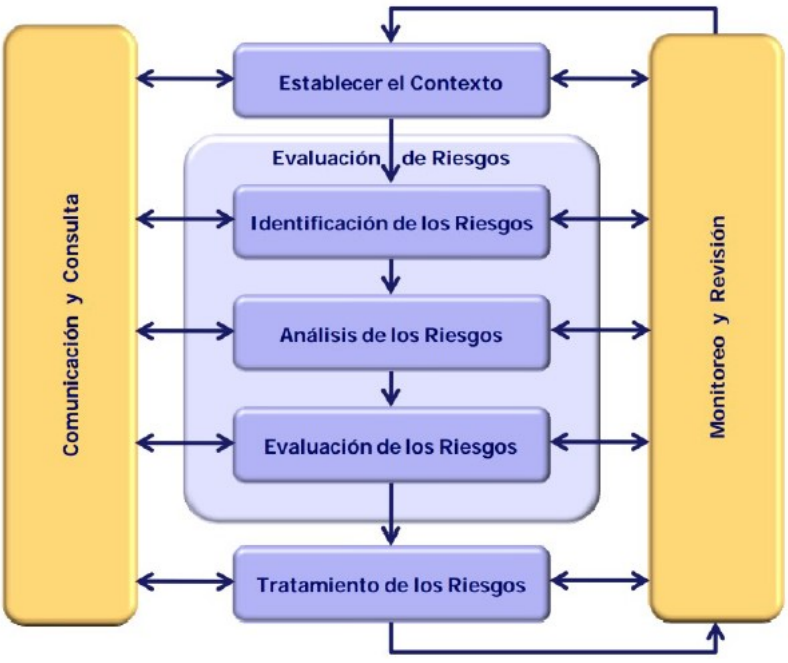
Ver documento adjunto: Esquema Roles y Responsabilidades del SGSI en la Empresa.

3-7 - Metodología de Análisis de Riesgos

3-7-1 - Proceso de Gestión 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.

El siguiente diagrama muestra el proceso de gestión de riesgo y la interrelación entre sus diferentes componentes:



Proceso de gestión de Riesgos

Fuente: https://exacato.files.wordpress.com/2015/01/capturadepantalla-2015-01-28-a-las-10-28-06.png?w=362&h=317

3-7-2 - Metodología seleccionada: Magerit

La metodología seleccionada para la evaluación de riesgos es MAGERIT.

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.

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT permite saber cuánto valor está en juego y ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Previamente para poder llevar a cabo el análisis de riesgo es imprescindible hacer previamente un Inventario de todos los Activos (todo a aquello que su perdida, daño o modificación pueda afectar al negocio), relacionados con las IS/IT.

METODOLOGÍA	CARACTERÍSTICAS Y OBSERVACIONES
MAGERIT	Son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). [3] Es elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. [4] Consiste en investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. [5]

PASO A SEGUIR	DESCRIPCIÓN
1 - Caracterización de los activos	Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia. El resultado de esta actividad es el informe denominado "modelo de valor". Adicionalmente incluye unas Sub-tareas: a. Tarea MAR.11: Identificación de los activos b. Tarea MAR.12: Dependencias entre activos c. Tarea MAR.13: Valoración de los activos [6]
2 – Caracterización de las amenazas	Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación). El resultado de esta actividad es el informe denominado "mapa de riesgos". Adicionalmente incluye unas Sub-tareas: a. Tarea MAR.21: Identificación de las amenazas Tarea b. MAR.22: Valoración de las amenazas. [6]

3 – Caracterización de las salvaguardas	Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar. El resultado de esta actividad se concreta en varios informes: • Declaración de aplicabilidad. • Evaluación de salvaguardas. • Insuficiencias (o vulnerabilidades del sistema de protección). Incluye las siguientes Sub-tareas: a. Tarea MAR.31: Identificación de las salvaguardas pertinentes. b. Tarea MAR.32: Valoración de las salvaguardas [6]
4 – Estimación del estado de riesgo	Esta actividad procesa todos los datos recopilados en las actividades anteriores para: • Realizar un informe del estado de riesgo: estimación de impacto y riesgo. • Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas Incluye las siguientes Sub-tareas: • Tarea MAR.41: Estimación del impacto. • Tarea MAR.42: Estimación del riesgo. [6]
5 – Caracterización de los activos	Esta actividad consta de tres sub-tareas: • MAR.11: Identificación de los activos • MAR.12: Dependencias entre activo • MAR.13: Valoración de los activos [6]

3-7-3 - Fases para la implementación:

1. Establecimiento de Parámetros:
   Se deben identificar los parámetros que se utilizarán durante todo el proceso de análisis de riesgos.

2. Análisis de Activos:
   Identificar cuáles son los activos que posee la empresa y que necesita para llevar a cabo sus actividades; debe ir acorde con el alcance definido. Los activos se pueden clasificar en: físicos, lógicos, de personal, de entorno e infraestructura, intangibles. Se efectuará su valoración de acuerdo a los parámetros descritos anteriormente.

   Se debe identificar:

   - Inventario de los Activos
   - Valor de los Activos
   - Criticidad de los Activos

3. Análisis de las Amenazas:
   Amenazas son aquellas situaciones que podrían llegar a darse en una organización y que resultarían en un problema de seguridad. Se clasifican en:

   - Accidentes: situaciones no provocadas voluntariamente y que generalmente no pueden evitarse. Pueden ser de los siguientes tipos: accidente físico, avería, interrupción de servicios esenciales, accidentes mecánicos o electromagnéticos.
   - Errores: situaciones cometidas de forma involuntaria, por el desarrollo de las actividades propias de la empresa, ya sea por desconocimiento o descuido del personal o terceros. Dentro de estos se pueden encontrar: errores en la utilización de los sistemas, en el desarrollo de aplicaciones, de actualización en los sistemas o aplicaciones, en la monitorización, de compatibilidad entre aplicaciones, inesperados (virus, troyanos, etc.).
   - Amenazas intencionales presenciales: provocadas por el personal de la empresa de forma voluntaria, al realizar acciones que saben que provocan un daño ya sea físico o lógico. Se pueden encontrar las siguientes: acceso físico no autorizado, acceso lógico no autorizado, indisponibilidad de recursos, filtración de datos a terceros.
   - Amenazas intencionales remotas: provocadas por personas ajenas a la empresa y que consiguen dañarla. Se pueden encontrar, entre otras, las siguientes: acceso lógico no autorizado, suplantación del origen en una comunicación, gusanos, denegación de servicio.

4. Establecimiento de las Vulnerabilidades:
   Vulnerabilidades son aquellos agujeros que se tienen en la seguridad de una empresa y que permiten que una amenaza pueda dañar un activo. Se debe tener claro que, sin vulnerabilidad, la amenaza no puede dañar un activo y que las vulnerabilidades por sí mismas no provocan daños, sino que estos son siempre provocados por las amenazas.

5. Establecimiento de Impactos:
   Los impactos son las consecuencias que provoca en la empresa el hecho de que cierta amenaza, aprovechando una vulnerabilidad, afecte un activo. Al analizar los impactos, se deben tener en cuenta los siguientes aspectos: el resultado de la agresión de una amenaza sobre un activo, el efecto sobre cada activo, el valor económico de las pérdidas producidas en cada activo, las pérdidas cuantitativas o cualitativas.

6. Nivel de Riesgo:
   Después de identificar los controles adecuados para reducir un riesgo específico al nivel considerado aceptable, debe evaluarse cuanto los controles, si se implementan reducirán el riesgo.

3-8 - Declaración de Aplicabilidad

La Declaración de aplicabilidad, o DdA, se redacta en base a los resultados del tratamiento del riesgo; es un documento clave dentro del SGSI porque describe no sólo qué controles son aplicables, sino también cómo se implementarán y su estado actual. También debería considerar a la Declaración de aplicabilidad como un documento que describe el perfil de seguridad de su empresa.

Ver documento adjunto:

Plantilla del documento de Declaración de Aplicabilidad.

4 - Análisis de Riesgos.

4-1 - Establecimiento de parámetros

Establecimiento de parámetros: se deben identificar los parámetros que se utilizarán durante todo el proceso de análisis de riesgos, los cuales son:

- Valor de los activos: se asigna una valoración económica a todos los activos de la Entidad. En esta valoración se debe tener en cuenta: valor de reposición, valor de configuración, valor de uso del activo, valor de pérdida de oportunidad. Se utiliza una escala de valores: alta, media, baja; y a cada rango se le asigna un valor económico.

- Vulnerabilidad: es la frecuencia con la que una organización puede sufrir alguna amenaza en concreto. Se recomienda también la utilización de una escala de valores, que puede ser por ejemplo: alta (una vez al día), media (una vez cada dos meses), baja (una vez cada seis meses), esta valoración se convierte a número que significa la estimación anual de ocurrencia.

- Impacto: el porcentaje del valor del activo que se pierde en el caso que sucede un incidente sobre él; en este parámetro también se realiza una estimación por rango de impactos, por ejemplo: alto (75%), medio (50%), bajo (20%).

- Efectividad del control de seguridad: la influencia que tendrán las medidas de protección ante los riesgos que se van a detectar; es decir, cómo las medidas de seguridad que se implanten, reducirán el riesgo detectado.

Se debe tener presente que los parámetros deben ser utilizados tal y como se definan en un principio, durante todo el análisis de riesgos, si se hace una modificación en mitad del proceso, los resultados no serán adecuados.

4-2 - Análisis de Activos

4-2-1 - 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.

La ISO 27001 tiene como objetivo proteger los activos de la información de cualquier organización. Toda organización posee información importante que desea proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización es lo que se denomina activo.

Los activos de información pueden ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Tras el estudio realizado en la Empresa AABBDDEE A.S. en este ámbito se plasman los resultados en el documento adjunto “Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo”.

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Información de los Activos					Ubicación de los Activos	
Nº	Código	Nombre	Descripción	Tipo	Física	Electrónica
1	CDO-001	CPD principal	1 CPD principal en la oficina de la organización	Infraestructuras	Oficina de la Organización	N.A.

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

4-2-2 - 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:
  Sólo las personas autorizadas tienen acceso a la información sensible y/o privada.
- Integridad:
  La información y sus métodos de procesamiento son exactos y completos, y no pueden ser manipulados sin autorización.
- Disponibilidad:
  Los usuarios autorizados pueden acceder a la información cuando lo necesitan.

Tras el estudio realizado en la Empresa AABBDDEE A.S. en este ámbito se plasman los resultados en el documento adjunto "Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo".

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Valoración de los Activos			
Confidencialidad	Integridad	Disponiblidad	
Valor	Valor	Valor	Criticidad
Alto	Alto	Alto	Crítico

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

4-2-3 - Criticidad de los Activos

Tras identificar los activos se debe realizar la valoración de los mismos. Dicha valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio. Esta valoración nos permitirá a posteriori valorar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuesto.

Se valorarán los activos según su criticidad en:

- Crítico
- No Crítico

Tras el estudio realizado en la Empresa AABBDDEE A.S. en este ámbito se plasman los resultados en el documento adjunto "Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo".

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Valoración de los Activos			
Confidencialidad	Integridad	Disponiblidad	
Valor	Valor	Valor	Criticidad
Alto	Alto	Alto	Crítico

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

4-3 - Análisis de las Amenazas

Amenazas:

Todas las causas de las amenazas permiten ser clasificadas por su naturaleza. Podemos emplear estas cuatro causas amenazadoras:

No humanas:

A1 - Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.
A2 - Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen.
A3 - Accidente físico de origen natural, riada, fenómeno sísmico o volcánico.
A4 - Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.
A5 - Accidentes mecánicos o electromagnéticos.

Humanas:

A6 - Errores de utilización ocurridos durante la recogida y transmisión de datos.
A7 - Errores de diseño existentes desde los procesos de desarrollo del software.
A8 - Errores de ruta, secuencia o entrega de la información durante el tránsito.
A9 - Errores de monitorización, trazabilidad o registros del tráfico de información.
A10 - Sabotaje internos o externos (conductas dirigidas a causar daños al hardware o software: accesos no autorizados, daño o modificación sin autorización al software.
A11 - Negligencia en aplicación de políticas de seguridad.
A12 - Errores involuntarios o voluntarios en el uso de la tecnología informática.
A13 - Ingeniería Social

Humanas intencionales que necesitan presencia física:

A14 - Acceso físico con inutilización.
A15 - Acceso lógico con intercepción pasiva simple de la información.
A16 - Acceso lógico con alteración o sustentación de la información en tránsito, o reducir la confidencialidad para aprovechar los bienes o servicios.
A17 - Acceso lógico con corrupción o destrucción de información de configuración, o con reducción de la integridad y la disponibilidad del sistema sin provecho directo.
A18 - No se encuentran disponibles de recursos humanos.

Humana intencional que proceden de un origen remoto:

A19 - Acceso lógico con intercepción pasiva.
A20 - Acceso lógico con corrupción de información en tránsito o de configuración.
A21 - Acceso lógico con modificación de información en tránsito.
A22 - Suplantación de origen o de identidad.
A23 - Repudio del origen o de la recepción de información en tránsito.

Algunas amenazas provocan:

- Se puede Contraer virus.
- Se pueden Dañar equipos de cómputo.
- Se puede acceder sin autorización a los sistemas de información.
- Se pueden presentar inundaciones.
- Se pueden presentar interrupciones en el servicio.
- Pueden Fallar los equipos de computo.
- Se pueden presentar desastres naturales.

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Amenazas / Vulnerabilidades	
Amenazas	**Vulnerabilidades**
A1,A2,A3,A4,A5,A10,A11, A12,A14,A20	V1,V4,V5,V6,V12,V14, V16

4-3-1 - Probabilidad que se materialicen las Amenazas

Para obtener una 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, los siguientes factores deben ser considerados:

- Fuente de amenaza
- Naturaleza de la vulnerabilidad
- Existencia y eficacia de los controles actuales.

La probabilidad de que una vulnerabilidad potencial pueda suceder por una fuente de amenaza puede ser definida como alto, medio o bajo.

Nivel de Probabilidad	Definición de la probabilidad
Alta	La fuente de amenaza es altamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes.
Media	La fuente de amenaza es motivada y capaz. Los controles pueden impedir el éxito de que la vulnerabilidad suceda.
Baja	La fuente de amenaza carece de motivación. Los controles están listos para prevenir o para impedir significativamente que la vulnerabilidad suceda.

Tras el estudio realizado en la Empresa AABBDDEE A.S. en este ámbito se plasman los resultados en el documento adjunto "Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo".

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Nivel de Riesgo		
Probabilidad de que una amenaza se materialice	**Impacto en la Organización resultante de la materialización de una amenaza**	**Valor del Nivel de Riesgo**
Bajo	Alto	Medio

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

4-4 - Establecimiento de las Vulnerabilidades

Vulnerabilidades:

La vulnerabilidad de un activo de seguridad es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información.

Clasificación de vulnerabilidades:

- La vulnerabilidad intrínseca del activo respecto del tipo de amenaza sólo depende de ambas cantidades.
- La vulnerabilidad efectiva del activo tiene en cuenta las salvaguardas aplicadas en cada momento a dicho activo, como un factor en el que se estima la eficacia global de dichas salvaguardas.

Atributos de las vulnerabilidades:

- Potencialidad autónoma respecto al activo de seguridad que se encuentre amenazado.
- Potencialidad derivada de la relación entre activo y amenaza.
- Factores subjetivos generadores de más o menos fuerza.
- Oportunidad de acceso al dominio si se tiene la suficiente capacidad y los recursos necesarios, que son cuatro: Accesibilidad física presencial, accesibilidad física cualificada, accesibilidad lógica competencial y accesibilidad lógica instrumental.

Tipos de vulnerabilidades:

V1 - Mala ubicación del centro de cómputo.
V2 - Software mal configurado.
V3 - Software desactualizado.
V4 - Falta de Hardware o hardware obsoleto.
V5 - Falta de controles de acceso lógico.
V6 - Falta de controles eléctricos.
V7 - Inexistencia de un control de soportes magnéticos.
V8 - Falta de cifrado en las comunicaciones
V9 - Ausencia de copias de seguridad o copias de seguridad incompletas
V10 - Ausencia de seguridad en archivos digitales o archivos físicos confidenciales.
V11 - Cuentas de usuario mal configuradas.
V12 - Desconocimiento y/o falta de socialización de normas o políticas a los usuarios por los responsables de informática.
V13 - Dependencia exclusiva de un proveedor de servicio técnico externo.
V14 - Ausencia de documentación de la operación de las aplicaciones.
V15 - Pantalla en un sistema de información sin bloqueo por el usuario o sin protector de pantalla.
V16 - Centro de computo sin UPS

Tras el estudio realizado en la Empresa AABBDDEE A.S. en este ámbito se plasman los resultados en el documento adjunto “Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo”.

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Amenazas / Vulnerabilidades	
Amenazas	Vulnerabilidades
A1,A2,A3,A4,A5,A10,A11, A12,A14,A20	V1,V4,V5,V6,V12,V14, V16

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

4-5 - Establecimiento de Impactos en la Organización de la materialización de las Amenazas

Se debe determinar los efectos adversos resultantes al potencializarse una amenaza. Antes de comenzar el análisis de impacto, es necesario tener la información de:

- Misión del sistema (por ejemplo, los procesos realizados por el sistema informático)
- Criticidad del sistema y los datos (por ejemplo, el valor del sistema o de importancia para una organización).
- Sensibilidad del sistema y los datos.

Esta información puede ser obtenida a partir de la documentación existente de la organización, tales como el informe del impacto del análisis de la misión o el informe de evaluación de criticidad de activos.

La siguiente lista ofrece una breve descripción de cada objetivo de seguridad y su consecuencia (o impacto) de los que no se cumplan:

- Pérdida de integridad. La integridad del sistema y los datos se refiere a la exigencia de que información sea protegida. Si la pérdida de la integridad del sistema o los datos no se corrige, el uso continuado de los datos dañados podría dar lugar a inexactitudes, errores, fraude o decisiones erróneas. Además, la violación de la integridad puede ser el primer paso en un ataque exitoso contra la disponibilidad o confidencialidad del sistema. Por todas estas razones, la pérdida de integridad reduce la garantía de un sistema informático.

- Pérdida de la disponibilidad. Si algo crítico de un sistema de TI no está disponible para sus usuarios finales, la misión de la organización puede verse afectada. Pérdida de funcionalidad del sistema y la eficacia operativa, por ejemplo, puede resultar en pérdida de tiempo productivo.

- Pérdida de la confidencialidad. La confidencialidad del sistema y los datos se refieren a la protección de información de su divulgación no autorizada. Este impacto puede ir desde la puesta en peligro de seguridad nacional a la divulgación de la Ley de privacidad de los datos.

Algunos impactos tangibles se pueden medir cuantitativamente, como con la pérdida de ingresos, el costo de la reparación de los sistemas, o el nivel de esfuerzo requerido para corregir los problemas causados por una acción de amenaza exitosa.

Otros impactos (por ejemplo, la pérdida de la confianza del público, la pérdida de credibilidad, el daño a una organización de interés) no se pueden medir en unidades específicas, pero puede ser calificado o descrito en términos de alta, mediano y bajo impacto.

Magnitud del impacto	Definición del impacto
Alta	La vulnerabilidad ejercida: 1. Puede resultar en la pérdida de un alto costo de los principales activos tangibles o recursos 2. De manera significativa puede violar, dañar, o impedir la misión de una organización, la reputación o los intereses 3. Puede resultar en la muerte humana o lesiones graves.
Media	La vulnerabilidad ejercida: 1. Puede resultar en la pérdida costosa de activos materiales o recursos 2. Pueda violar, dañar, o impedir la misión de una organización, la reputación o los intereses 3. Puede resultar en lesiones.
Baja	La vulnerabilidad ejercida: 1. puede resultar en la pérdida de algunos bienes, materiales o recursos 2. Puede afectar notablemente la misión de una organización, la reputación o los intereses.

Algunos factores adicionales que se deben considerar para determinar la magnitud del impacto son:

- Una estimación de la frecuencia del ejercicio de la amenaza de código de la vulnerabilidad durante un período de tiempo determinado (por ejemplo, 1 año)

- El costo aproximado para cada ocurrencia de la amenaza teniendo en cuenta la fuente de la vulnerabilidad

- Un factor de ponderación sobre la base de un análisis subjetivo del impacto relativo de una determinada amenaza en una vulnerabilidad específica.

Tras el estudio realizado en la Empresa AABBDDEE A.S. en este ámbito se plasman los resultados en el documento adjunto “Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo”.

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Nivel de Riesgo		
Probabilidad de que una amenaza se materialice	Impacto en la Organización resultante de la materialización de una amenaza	Valor del Nivel de Riesgo
Bajo	Alto	Medio

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

4-6 - Nivel de Riesgo

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”.

Si el riesgo residual es inaceptable, una decisión comercial debe ser tomada sobre cómo se irá a manejar la situación. Una opción es la de seleccionar más controles para finalmente reducir los riesgos a un nivel aceptable. Es una buena práctica no tolerar riesgos inaceptables, pero muchas veces no es posible o financieramente factible reducir todos los riesgos al nivel aceptable.

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.
La fórmula que emplearemos para la determinación final de la misión de riesgo será:

Nivel de riesgo = Probabilidad de que una amenaza se materialice
X
El impacto en la organización resultante de la materialización de una amenaza

Escala de riesgo:

- Alto: 50 – 100
- Medio: 10 – 50
- Bajo: 1 – 10

Probabilidad de amenaza	Impacto		
	Bajo (10)	Medio (50)	Alto (100)
Alto (1.0)	10 x 1.0 = 10 (Bajo)	50 x 1.0 = 50 (Medio)	100 x 1.0 = 100 (Alto)
Medio (0.5)	10 x 0.5 = 5 (Bajo)	50 x 0.5 = 25 (Medio)	100 x 0.5 = 50 (Alto)
Bajo (0.1)	10 x 0.1 = 1 (Bajo)	50 x 0.1 = 5 (Bajo)	100 x 0.1 = 10 (Medio)

En la siguiente tabla se describen los niveles de riesgo. Esta escala de riesgo, con las calificaciones de Alta, media y baja, representa el grado o nivel de riesgo a que un sistema informático, instalación o procedimiento podría estar expuesto si una vulnerabilidad determinada se materializa.

En la escala de riesgo también se presentan acciones que las personas de la alta gerencia deben tomar para cada nivel de riesgo.

Nivel de Riesgo	Descripción del riesgo y acciones necesarias
Alta	Si una observación es evaluada como alto riesgo, hay necesidad de una fuerte necesidad de medida correctiva. Un sistema existente puede continuar la operación, pero el plan de acción correctiva debe llevarse a cabo lo más pronto posible
Media	Si una observación es categorizada como un riesgo medio, hay necesidad de acciones correctivas y de incorporar un plan para llevar a cabo esas acciones dentro de un periodo de tiempo razonable.
Baja	Si una observación es descrita como un riesgo bajo, se debe determinar si se requieren acciones correctivas o se acepta el riesgo

Tras el estudio realizado en la Empresa AABBDDEE A.S. en este ámbito se plasman los resultados en el documento adjunto "Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo".

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Nivel de Riesgo		
Probabilidad de que una amenaza se materialice	**Impacto en la Organización resultante de la materialización de una amenaza**	**Valor del Nivel de Riesgo**
Bajo	Alto	Medio

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

Propietario del Riesgo:

El propietario o responsable del riesgo es una persona o entidad a la que se ha dado la autoridad para valorar y gestionar un riesgo en particular, por lo que debe rendir cuentas por ello.

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio.

Nivel de Riesgo			Propiedad del Riesgo
Probabilidad de que una amenaza se materialice	Impacto en la Organización resultante de la materialización de una amenaza	Valor del Nivel de Riesgo	Propietario
Bajo	Alto	Medio	Personal Directivo Personal Técnicos TI

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento.

5 - Propuestas de Proyectos.

5-1 - Proyectos para el Tratamiento del Riesgo

En este punto se identificarán 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.

5-1-1 - Opciones de Tratamiento

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.

Se deberá elegir entre alguna de las siguientes opciones:

- Aceptarlo:
  Esta decisión consiste en que la organización ha detectado que se encuentra expuesta a un riesgo importante que debería ser reducido por debajo del umbral de riesgo marcado. Para ello debería invertir una serie de recursos, pero la protección frente al riesgo detectado representa un coste tan elevado, y su probabilidad de que llegue a suceder es tan improbable, que no resulta posible la inversión para protegerse ante esta situación. La decisión es que la organización trabaje aceptando que está expuesta al riesgo y, llegado el caso de que se produzca un incidente, improvisando una respuesta.

- Asignarlo a terceros o Compartirlos:
  Corresponde a la situación en la que una organización determina que tiene algún riesgo por encima de su umbral de riesgo. Además, considera que no puede asumirlo, por su gravedad, pero que a su vez no puede reducirlo, ya sea porque no tiene la capacidad de hacerlo o porque no tiene los recursos necesarios. En estos casos, se decide contratar a un tercero que sí posea esa capacidad para reducir y gestionar el riesgo de tal modo que quede por debajo del umbral de riesgo.

- Minimizarlos o evitarlos:
  Corresponde a la situación en la que una organización ha detectado un riesgo elevado, por encima de su umbral de riesgo, y decide implantar algún control o salvaguarda para reducirlo; al menos, hasta situarlo por debajo del umbral de riesgo determinado. Sin ningún género de dudas, lo ideal siempre es tratar de evitar o reducir un riesgo, ya que supone que la propia organización controla y dispone de las medidas de seguridad adecuadas que le permitan tratar de evitar dichos riesgos.

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.

A partir del resultado del análisis de riesgos se debe elaborar un plan de acción, que indique qué decisión se tomará con cada riesgo identificado, la cual puede ser una de las siguientes: reducir, transferir o aceptar el riesgo; dicho plan contendrá lo siguiente:

- Establecimiento de prioridades: se designan aquellos riesgos que tendrán que ser reducidos en primer lugar debido a que son los más elevados para la organización.

- Planteamiento del análisis de coste/beneficio: se estudian, para cada una de las medidas que se pueden implantar, qué coste le supondría a la organización y en qué porcentaje reduciría los riesgos detectados.

- Selección de controles definitivos: después de analizar el coste/beneficio de todos los controles, hay que seleccionar definitivamente los que tendrá que implantar la empresa para reducir los riesgos hasta situarlos por debajo de su umbral de riesgo.

- Asignación de responsabilidades: se asignan los responsables dentro de la empresa de llevar a cabo la implantación de los controles.

- Implantación de controles: se realiza la implantación de los controles de seguridad designados. Los controles que se implanten no son obligatoriamente técnicos, sino que podrían ser controles organizativos o procedimentales.

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio:

Proyectos para el Tratamiento del Riesgo			
Opción de Tratamiento que se llevará a cabo	Plan de Tratamiento		
	Proyectos para la Mitigación de los Riesgos	Responsable de los Proyectos	Plazo de Consecución de los Proyectos
Evitar el riesgo	Definir nuevas reglas Aplicar las nuevas tecnologías	Personal Directivo Personal Técnicos TI	Corto plazo

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-1-2 - Responsable de los Proyectos

Se identificaran los responsable de los diferentes Proyectos dentro de la Organización para depurar responsabilidades en casos de no realización de los mismo.

Dentro del análisis realizado en esta Empresa para determinar los posibles responsables de los proyectos que se plantean en cada capítulo serán:

- Personal Directivo
- Personal Técnicos TI
- Personal Relaciones con proveedores
- Personal RRHH

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio

Proyectos para el Tratamiento del Riesgo			
Opción de Tratamiento que se llevará a cabo	Plan de Tratamiento		
	Proyectos para la Mitigación de los Riesgos	Responsable de los Proyectos	Plazo de Consecución de los Proyectos
Evitar el riesgo	Definir nuevas reglas Aplicar las nuevas tecnologías	Personal Directivo Personal Técnicos TI	Corto plazo

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-1-3 - Proyectos para la Mitigación de los Riesgos

Para la mitigación de los diferentes Riesgos identificados en el estudio y análisis de los mismos, se han planificado para su consecución, una serie de Proyectos que cubrirán estos objetivos y que han sido clasificados en unos bloque genéricos, que luego a su vez, cada uno de ellos, se desglosará en la realización de diferentes Acciones, las cuales se identifican más adelante, con la intención de desglosar los proyectos para de esta manera poder reutilizar las acciones a realizar y estructurar la organización de la Empresa en cuento a personal y disponibilidad económica.

Se ha definido la siguiente clasificación:

- Definir nuevas reglas
- Aplicar las nuevas tecnologías
- Cambio en la estructura de la organización

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio:

	Proyectos para el Tratamiento del Riesgo		
Opción de Tratamiento que se llevará a cabo	Plan de Tratamiento		
	Proyectos para la Mitigación de los Riesgos	Responsable de los Proyectos	Plazo de Consecución de los Proyectos
Evitar el riesgo	Definir nuevas reglas Aplicar las nuevas tecnologías	Personal Directivo Personal Técnicos TI	Corto plazo

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-1-4 - Acciones y Puntos de Control para implementar en cada Proyecto

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

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:

- Definir nuevas reglas
    - Reglas que se encuentran documentadas mediante planes
        - Objetivo:
            - Implementar mecanismos de seguridad para la prevención de fuga, daño o pérdida de información
        - Puntos de control:
            - Identificar y clasificar la información de procesos core a ser monitoreados.
            - Implementar reglas y parámetros para monitorear la información.
            - Implementar reglas de monitoreo y bloqueo sobre web.
            - Implementar reglas de monitoreo y bloque sobre correo electrónico.
            - Implementar reglas de monitoreo y bloqueo sobre periféricos de almacenamiento como USB.
            - Definir alertas y escalamiento de notificaciones.
    - 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.
        - Puntos de control:
            - Realizar la selección y formación de Auditores internos de seguridad de la información.
            - Determina el programa y planes de auditorías.
            - Determinar No conformidades del SGSI.
            - Determinar Planes de acción para cerrar no conformidades y generar políticas que lo garanticen.

- Reglas que se 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.
  - Puntos de control:
    - Desarrollar, implementar y publicar la Política de Control de Acceso de IT, y desarrollar el procedimiento para la solicitud, baja y revisión de accesos.
    - Desarrollar la política de desarrollo de software seguro.
    - Desarrollar Política y guía para el desarrollo de análisis de vulnerabilidades, que garanticen su evaluación continua.

- Reglas que se encuentran documentadas mediante instrucciones
  - Objetivo:
    - Implementar mecanismos de auditoría, seguridad y protección sobre la información de las BBDD core del negocio.
  - Puntos de control:
    - Implementar soluciones que permitan brindar protección sobre la información de las BBDD.
    - Implementar políticas de auditorías sobre la información, consultas, modificaciones, eliminación.
    - Implementar políticas de acceso y trazabilidad sobre los administradores.

- Aplicar las nuevas tecnologías

  - Ubicaciones de recuperación de desastres para los 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.
    - Puntos de control:
      - Implementar análisis de eventos de Firewall.
      - Implementar análisis de eventos de servidores de aplicación.
      - Implementar análisis de eventos de Bases de Datos.
      - Implementar eventos de control de accesos de Directorio Activo.
      - Implementar eventos de IPS

- Implementar eventos de malware y amenazas informáticas.
- Desarrollo de procedimientos para la gestión de alertas y escalamiento de eventos e incidentes.

- Sistemas de copia de seguridad
  - Objetivo:
    - Desarrollar una política de Backup.
  - Puntos de control:
    - Implementar una política de backup, con copias incrementales diarias de Lunes a Jueves, y completada con una copia total y encriptada los Viernes, que es custodiada fuera de las instalaciones.

- 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.
  - Puntos de control:
    - Se realizarán pruebas de Alta Disponibilidad de cada uno de los elementos objeto de implementación para garantizar la Alta Disponibilidad de los Servicios y Sistemas.
    - Para la infraestructura de Networking como Routers, Switches, se deberán implementar mecanismos de alta redundancia y realizar pruebas que permitan evidenciar la entrada y funcionamiento normal en caso de fallos.
    - Para los servidores se deberán implementar clusters de Servidores.

- 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.
    - Puntos de control:
      - Realizar plan de formación en seguridad de la información para la Alta Dirección.

- Realizar curso de formación en SGSI para usuarios de las áreas de seguridad de la información y seguridad IT.
- Realizar formación para usuarios finales.

- 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.
  - Puntos de control:
    - Verificar la correcta implantación del SGSI y cumplimento de responsabilidades al respecto por los miembros afectados.

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio:

Proyectos para el Tratamiento del Riesgo		
Plan de Tratamiento		
Responsable de los Proyectos	**Plazo de Consecución de los Proyectos**	**Acciones para implementar en cada Proyecto**
Personal Directivo Personal Técnicos TI	Corto plazo	Reglas que se encuentran documentadas mediante planes Reglas que se encuentran documentadas mediante políticas Reglas que se encuentran documentadas mediante procedimientos Reglas que se encuentran documentadas mediante instrucciones Ubicaciones de recuperación de desastres para los centros de datos

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-1-5 - Valoración Económica de las Acciones

Para determinar una valoración económica de lo que supone a la Empresa la implantación de las acciones necesarias, se ha determinado una escala cuantificada según los siguientes valores:

- Alto: > 100.000
- Medio: > 10.000 y < 100.000
- Bajo: < 10.000

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio:

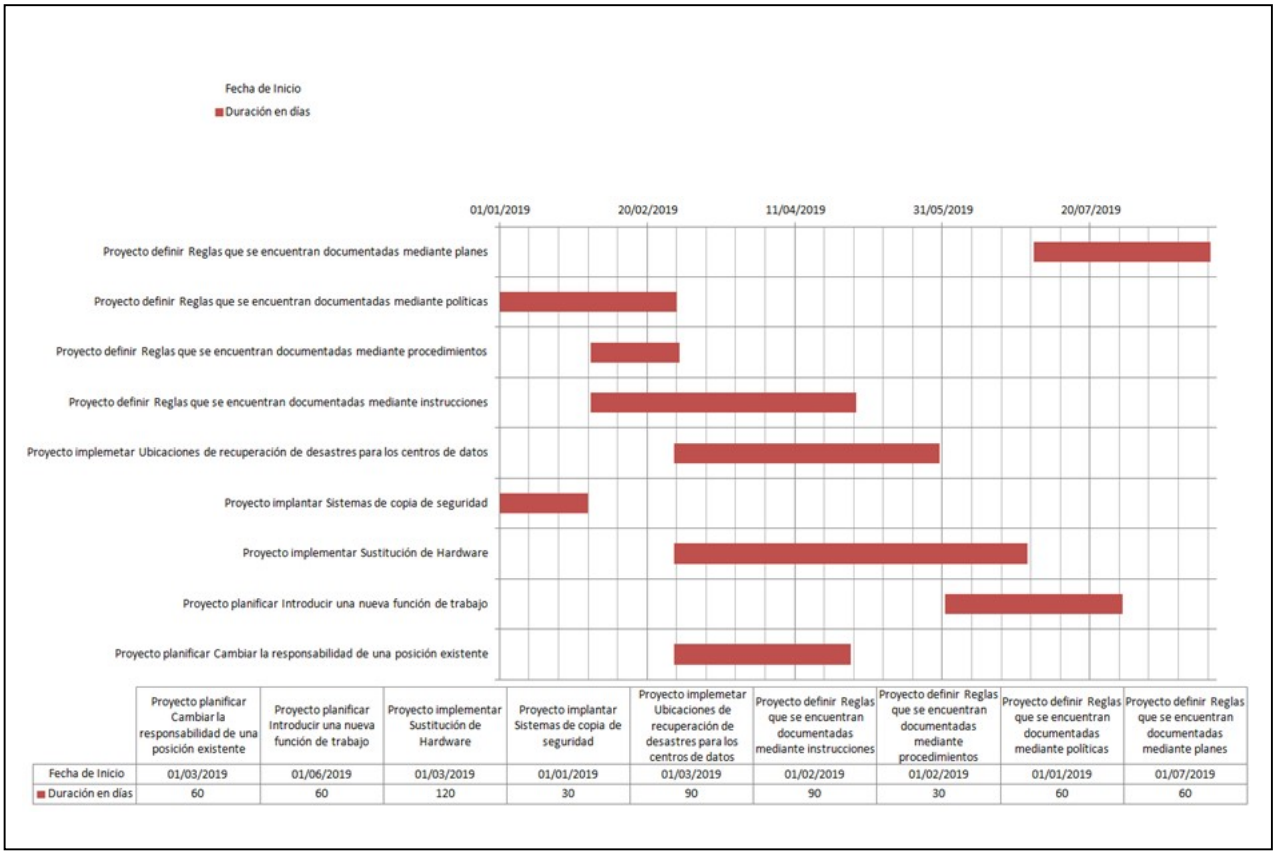
tamiento del Riesgo		
Plan de Tratamiento		
Plazo de Consecución de los Proyectos	**Acciones para implementar en cada Proyecto**	**Valoración Económica de las Acciones**
Corto plazo	Reglas que se encuentran documentadas mediante planes Reglas que se encuentran documentadas mediante políticas Reglas que se encuentran documentadas mediante procedimientos Reglas que se encuentran documentadas mediante instrucciones Ubicaciones de recuperación de desastres para los centros de datos	Alto

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-1-6 - Plazo de Consecución de los Proyectos

Los diferentes Proyectos planteados para el tratamiento de los diferentes Riesgos identificados, deben planificarse en el tiempo, en función de su urgencia o importancia, y estableciendo plazos de consecución de sus objetivos.

A continuación se muestra un diagrama de Gantt donde se puede ver de manera gráfica la planificación de la ejecución de todos los proyectos identificados en este Plan:



	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

Diagrama de Gantt de la planificación de ejecución de Proyectos

Ver documento adjunto:
Diagrama de Gantt de la Planificación de ejecución de Proyectos

La clasificación de los plazos se identificaran en:

- Corto plazo
- Medio plazo
- Largo plazo

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio:

Proyectos para el Tratamiento del Riesgo			
Opción de Tratamiento que se llevará a cabo	Plan de Tratamiento		
	Proyectos para la Mitigación de los Riesgos	Responsable de los Proyectos	Plazo de Consecución de los Proyectos
Evitar el riesgo	Definir nuevas reglas Aplicar las nuevas tecnologías	Personal Directivo Personal Técnicos TI	Corto plazo

Ver documento adjunto:

Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-2 - Tiempo límite para la ejecución en producción de las Acciones.

Una vez definidos los Proyectos y las Acciones necesarias para cada tratamiento de los diferentes riesgos detectados y analizados, haberse establecido los plazos de consecución de los objetivos de cada uno de ellos y comprobado que se han realizado, marcamos un tiempo límite para la ejecución en producción, de estas las acciones, en caso de necesidad tras la materialización de una amenaza.
Según el estudio realizado en esta Empresa se ha determinado como válida la siguiente clasificación:

- Inmediata
- 1 horas
- 2 horas
- 3 horas
- 4 horas
- Según Dirección
- Según RRHH

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio:

		Ejecución en Producción
Acciones para implementar en cada Proyecto	Valoración Económica de las Acciones	Tiempo límite para la ejecución en producción, de las acciones en caso de necesidad
Reglas que se encuentran documentadas mediante planes Reglas que se encuentran documentadas mediante políticas Reglas que se encuentran documentadas mediante procedimientos Reglas que se encuentran documentadas mediante instrucciones Ubicaciones de recuperación de desastres para los centros de datos	Alto	Inmediata

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-3 - 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.

A su vez estos contrales forman parte del proceso de Mejora Continua de todo este proyecto.

Los puntos de control se basarán en el resultado de los KPI,s marcados y en la temporalidad de cada control.

Según las siguientes escalas:

- Resultado de KPI,s Rechazable
- Resultado de KPI,s Aceptable
- Resultado de KPI,s Destacable

Periodicidad de los controles:

- Mensual
- Semestral
- Anual

Tabla diseñada para la clasificación y documentación de los valores extraídos del análisis de la Empresa AABBDDEE A.S. en relación a este ámbito de estudio:

	Ejecución	Control
	en Producción	Mejora Continua
Valoración Económica de las Acciones	Tiempo límite para la ejecución en producción, de las acciones en caso de necesidad	Puntos de control y verificación de Implementación
Alto	Inmediata	Mensual

Ver documento adjunto:
Análisis de Inventario de Activos-Valoración-Amenazas-Impacto-Riesgo-Tratamiento

5-4 - Evolución de los dominios de la norma ISO/IEC 27002

5-4-1 - Antes de la realización de los Proyectos planificados

A continuación se muestra de forma gráfica la evolución de los diferentes dominios y su cumplimiento antes de la realización de los diferentes Proyectos:

Ver documento adjunto:

Diagrama de radar antes de la realización de los Proyectos.

	Valor
A.5 Information security policies	0
A.6 Organization of information security	0
A.7 Human resource security	0
A.8 Asset management	0
A.9 Access control	0,5
A.10 Cryptography	3
A.11 Physical and environmental security	0
A.12 Operations security	1,14
A.13 Communications security	2
A.14 System acquisition, development and maintenance	1
A.15 Supplier relationships	1,5
A.16 Information security incident management	2
A.17 Information security aspects of business continuity management	1,5
A.18 Compliance	0

Resumen del análisis antes de la realización de los Proyectos.

Diagrama Radar antes de la realización de los Proyectos.

5-4-2 - Después de la realización de los Proyectos planificados

A continuación se muestra de forma gráfica la evolución de los diferentes dominios y su cumplimiento después de la realización de los diferentes Proyectos:

Ver documento adjunto:

Diagrama de radar después de la realización de los Proyectos.

	Valor
A.5 Information security policies	3
A.6 Organization of information security	5
A.7 Human resource security	3,33
A.8 Asset management	10,3
A.9 Access control	5,75
A.10 Cryptography	3
A.11 Physical and environmental security	14
A.12 Operations security	5,43
A.13 Communications security	8
A.14 System acquisition, development and maintenance	6
A.15 Supplier relationships	6,5
A.16 Information security incident management	16
A.17 Information security aspects of business continuity management	4
A.18 Compliance	2

Resumen del análisis después de la realización de los Proyectos.

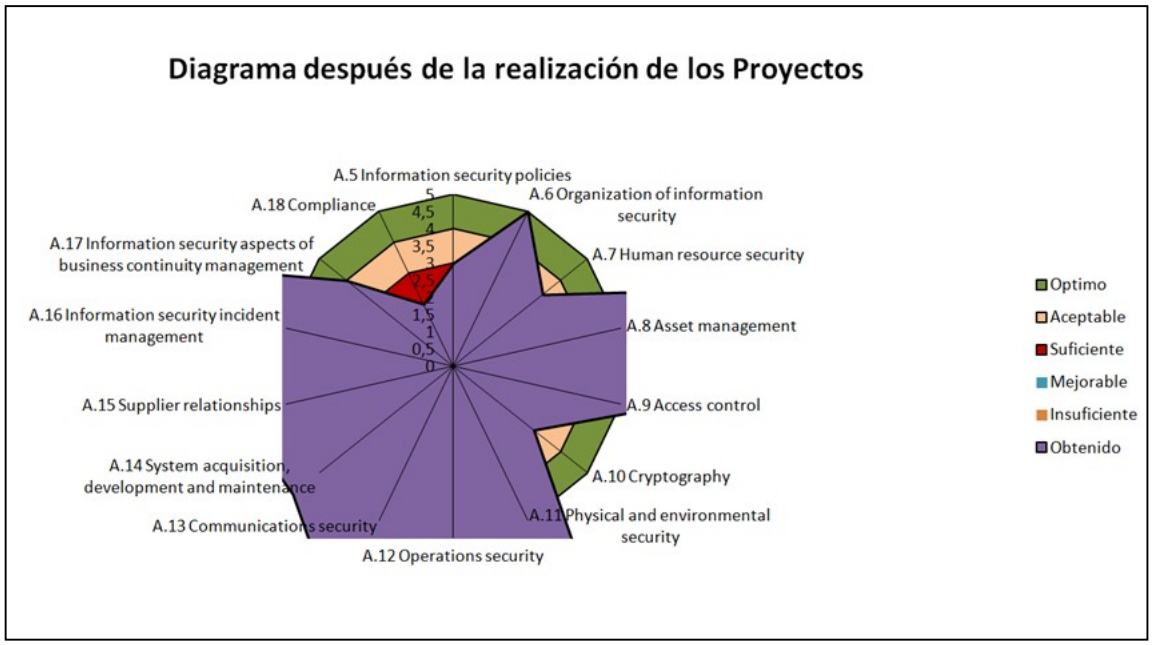


Diagrama Radar después de la realización de los Proyectos.

6 - Auditoría de Cumplimiento.

6-1 - Introducción

Este 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.

Estudiaremos los 114 controles o salvaguardas sobre buenas prácticas para la gestión de la seguridad de la Información organizados en 14 dominios y 35 objetivos de control.

6-2 - 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.

Esta estimación la realizaremos según la siguiente tabla, que se basa en el modelo de Madurez de la Capacidad (CMM):

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla modelo de la Madurez de la Capacidad (CMM)

En el siguiente diagrama se determina si el nivel de madurez que ha determinado la Empresa, es adecuado en función de los datos analizados:

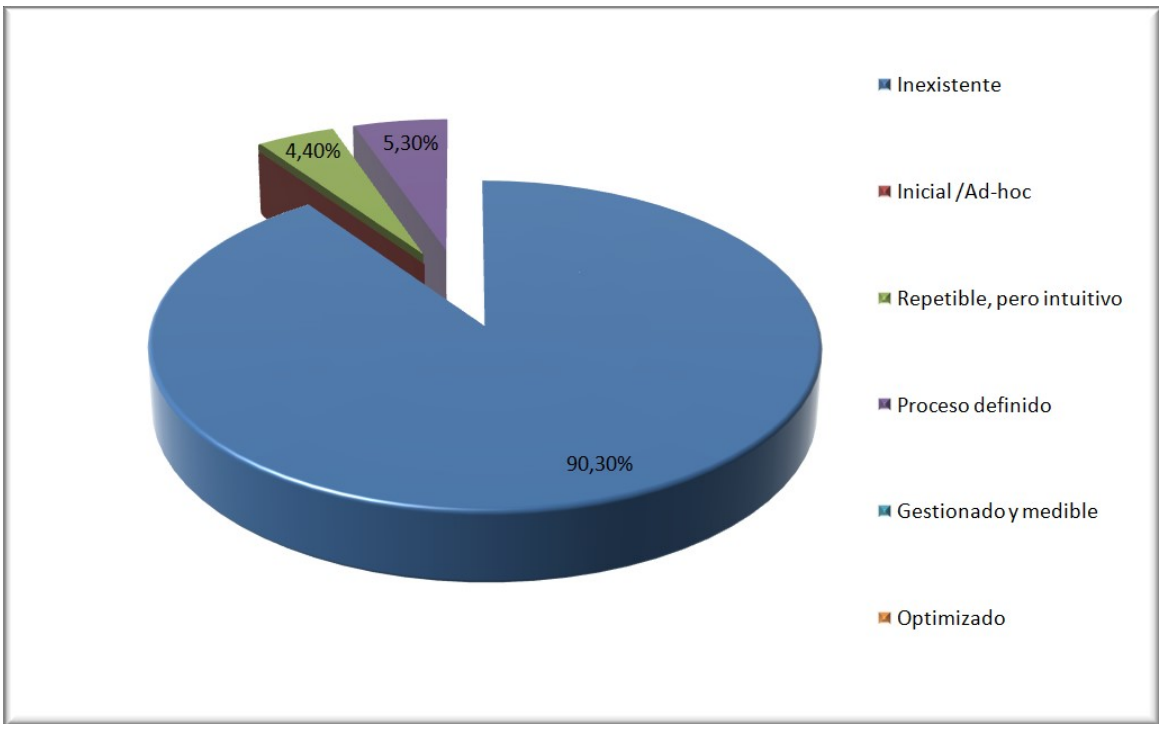


Diagrama de Madurez CMM de los controles ISO

Ver documento adjunto:
Diagrama de Madurez CMM de los controles ISO

6-3 - Nivel de cumplimiento de los Requisitos de la ISO 27001

6-3-1 - 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.

- **Estado actual de cumplimiento:**

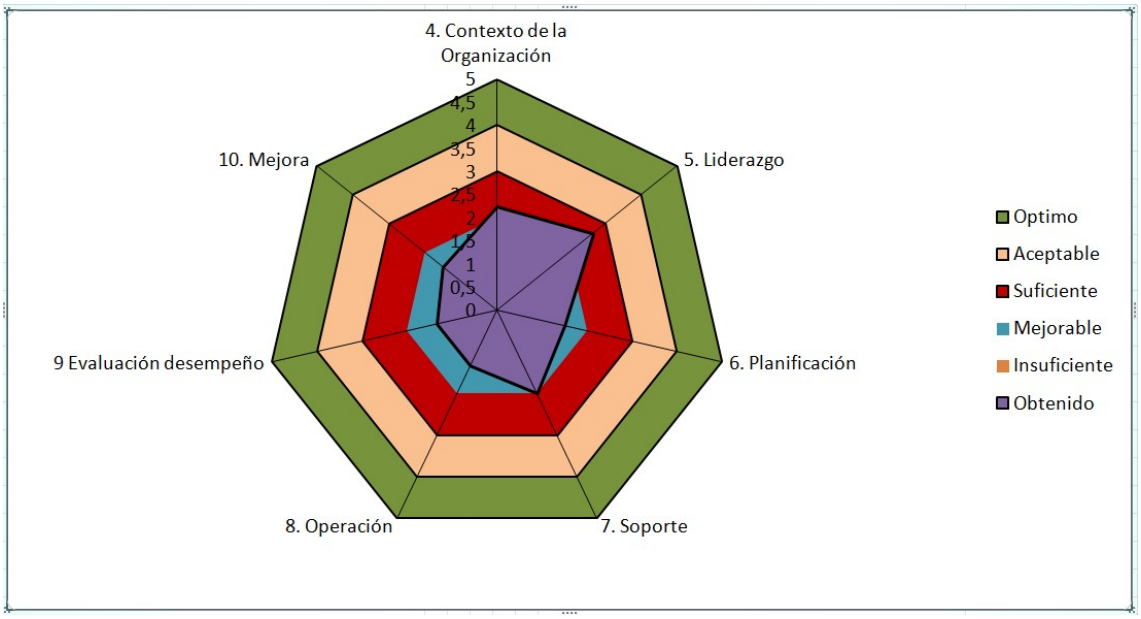


Diagrama Radar de estado actual de cumplimiento de los requisitos de la ISO 27001 que vienen definidos entre los apartados 4 al 10

Ver documento adjunto:

Análisis diferencial apartados 4-10.

- **Estado de cumplimiento deseado:**

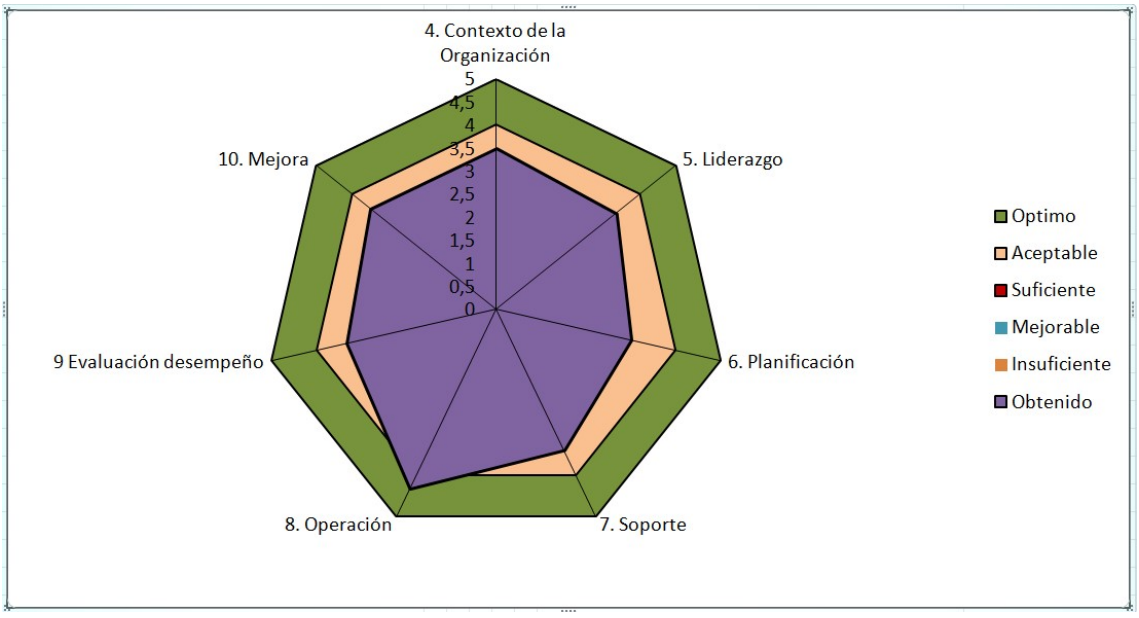


Diagrama Radar de cumplimiento deseado de los requisitos de la ISO 27001 que vienen definidos entre los apartados 4 al 10

Ver documento adjunto:

Estado de cumplimiento deseado apartados 4-10.

6-3-2 - 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.

- **Estado actual de cumplimiento:**

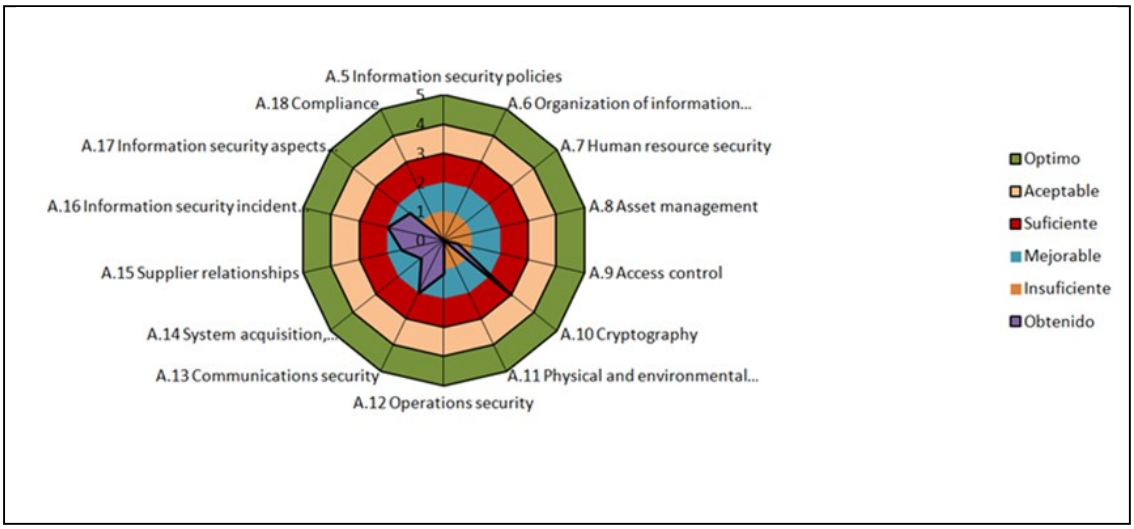


Diagrama Radar de estado actual de cumplimiento de los requisitos de la ISO 27001 que vienen definidos en el Anexo A

Ver documento adjunto:

Diagrama de radar antes de la realización de los Proyectos.

- **Estado de cumplimiento deseado:**

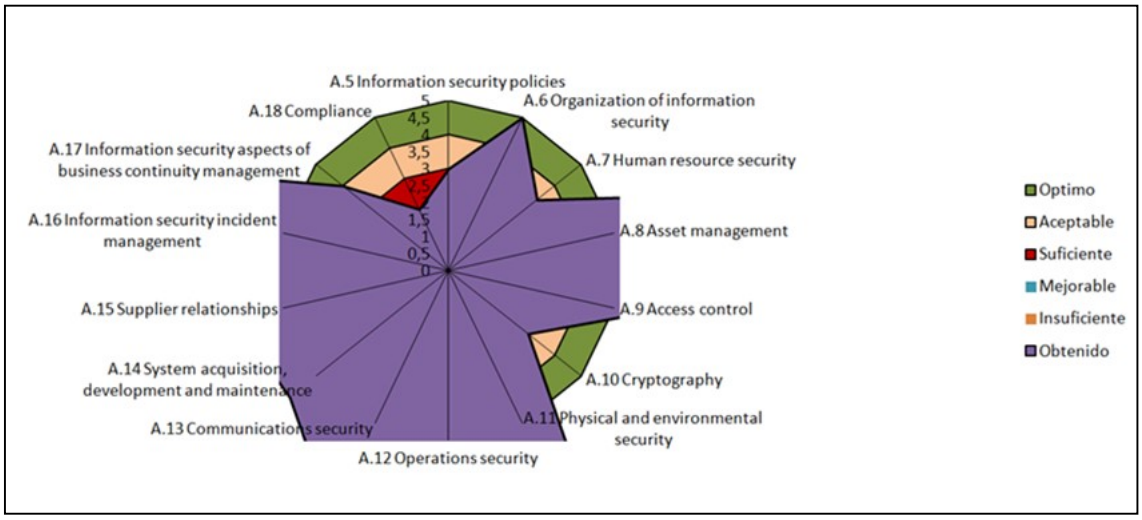


Diagrama Radar de cumplimiento deseado de los requisitos de la ISO 27001 que vienen definidos en el Anexo A

Ver documento adjunto:

Diagrama de radar después de la realización de los Proyectos.

7 - Conclusiones - Resumen

Introducción:

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

Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI):

La implementación de un SGSI, es una opción fundamental cuando se trata de proteger la información, ya que este tiene como objetivo esencial proteger los activos, a través de controles y políticas de seguridad, que deben ser aplicadas en una organización.

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.

Plan Director de Seguridad:

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.

Perfil del Responsable de Seguridad:

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

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.

Hoja de Ruta:

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.

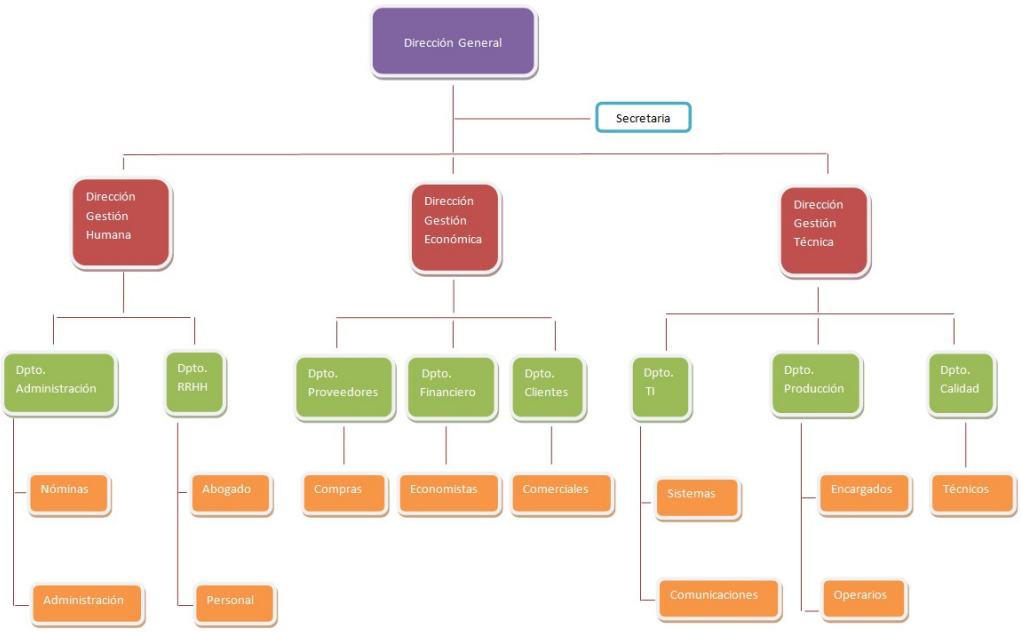
Planificación del Trabajo:

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

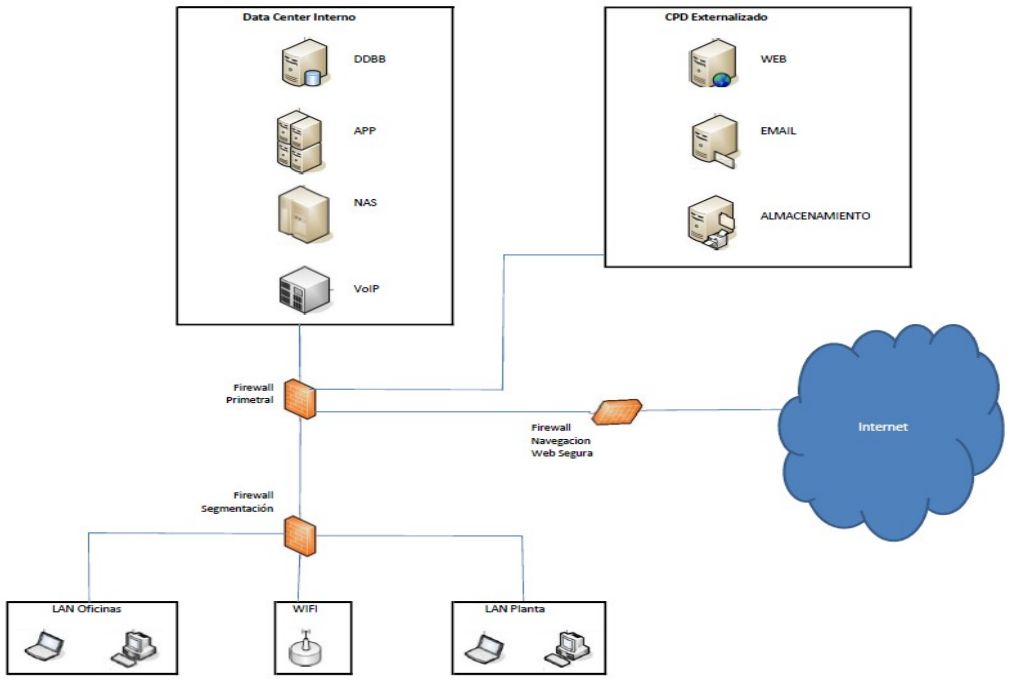
Contextualización - Empresa AABBDDEE A.S.:

AABBDDEE A.S. Empresa ficticia objeto de este Trabajo, es una Empresa dedicada a los suministros industriales para las empresas de automoción.

Estructura y Jerarquía de la Organización:



Infraestructura Tecnológica de la Empresa:



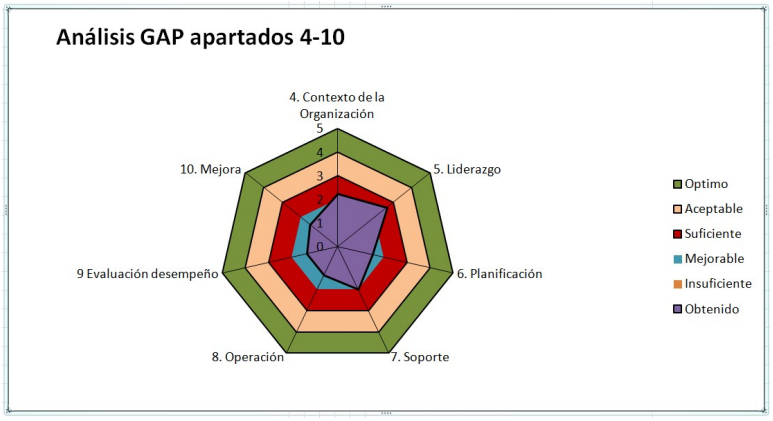
Objetivos de la Seguridad de la Información:

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.

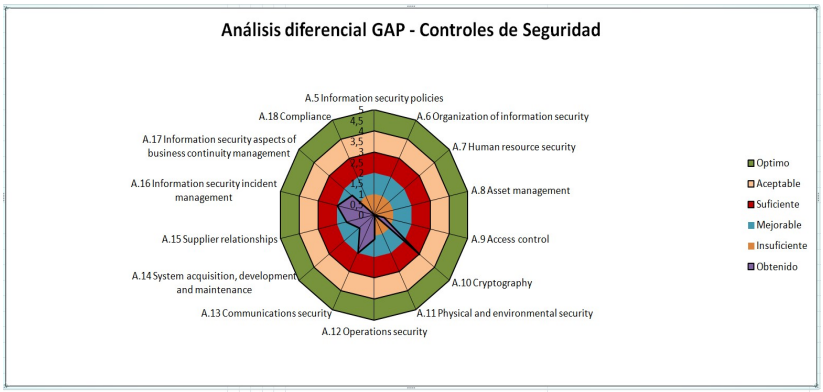
En la implantación del SGSI en la Empresa objeto de este trabajo es importante el estudio del PDCA (Plan - Do - Check - Act) bajo la norma ISO/IEC 27001.

Análisis diferencial:

En el análisis GAP en relación a los apartados 4 al 10 identificados en la Norma ISO 27001, hemos obtenido los siguientes resultados:



En el análisis GAP en relación a los controles de seguridad, con respecto a la norma ISO/IEC 27002, hemos obtenido los siguientes resultados:



Sistema de Gestión Documental:

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:

- **Política de seguridad de la información**.
- **Procedimiento de Auditorías Internas.**
- **Gestión de Indicadores**.
- **Procedimiento Revisión por Dirección**.
- **Roles y Responsabilidades.**
- **Metodología de Análisis de Riesgos: La metodología seleccionada para la evaluación de riesgos es MAGERIT.**
- **Declaración de Aplicabilidad.**

Análisis de Riesgos:

- **Inventario de los Activos.**
- **Valor de los Activos.**
- **Amenazas.**
- **Vulnerabilidades.**
- **Probabilidad que se materialicen las Amenazas.**
- **Establecimiento de Impactos en la Organización de la materialización de las Amenazas.**
- **Riesgo Residual.**
- **Cálculo del nivel de riesgo.**

Propuestas de Proyectos:

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.

Una vez conocido el nivel de riesgo actual en la organización se debe determinar el denominado umbral de riesgo.

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:

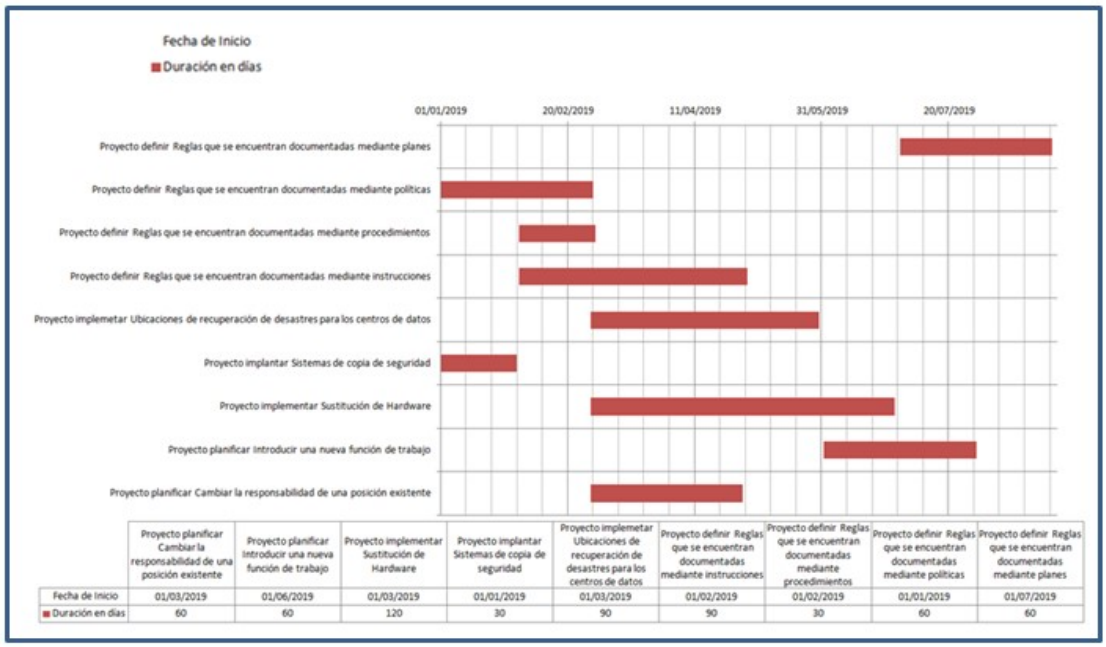
- Definir nuevas reglas
    - Reglas que se encuentran documentadas mediante planes
    - Reglas que se encuentran documentadas mediante políticas
    - Reglas que se encuentran documentadas mediante procedimientos

- Reglas que se encuentran documentadas mediante instrucciones

- Aplicar las nuevas tecnologías
  - Ubicaciones de recuperación de desastres para los centros de datos
  - Sistemas de copia de seguridad
  - Sustitución de Hardware

- Cambio en la estructura de la organización
  - Introducir una nueva función de trabajo
  - Cambiar la responsabilidad de una posición existente

Planificación de los Plazos de Consecución de los Proyectos:



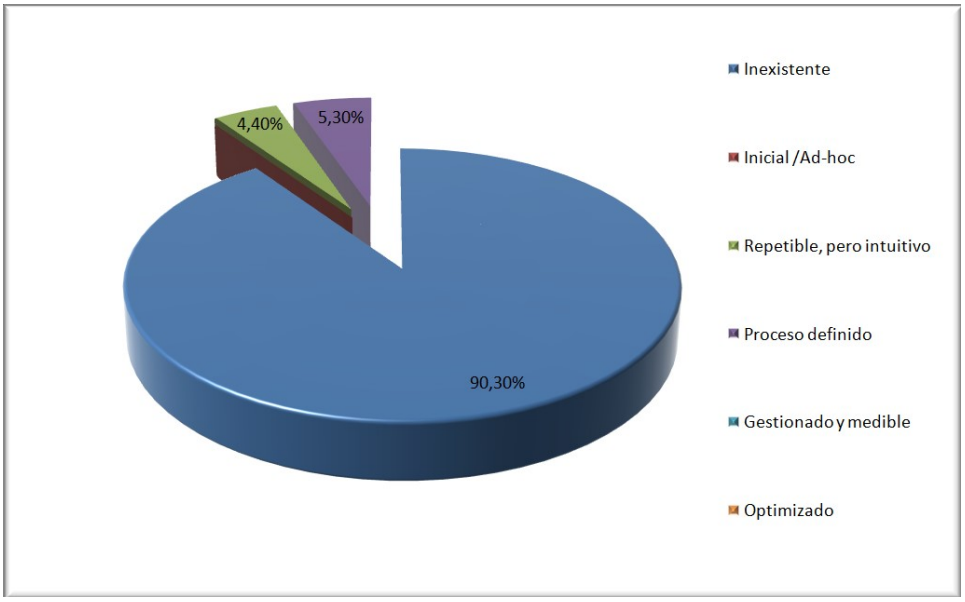
	Proyecto planificar Cambiar la responsabilidad de una posición existente	Proyecto planificar Introducir una nueva función de trabajo	Proyecto implementar Sustitución de Hardware	Proyecto implantar Sistemas de copia de seguridad	Proyecto implemetar Ubicaciones de recuperación de desastres para los centros 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

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:

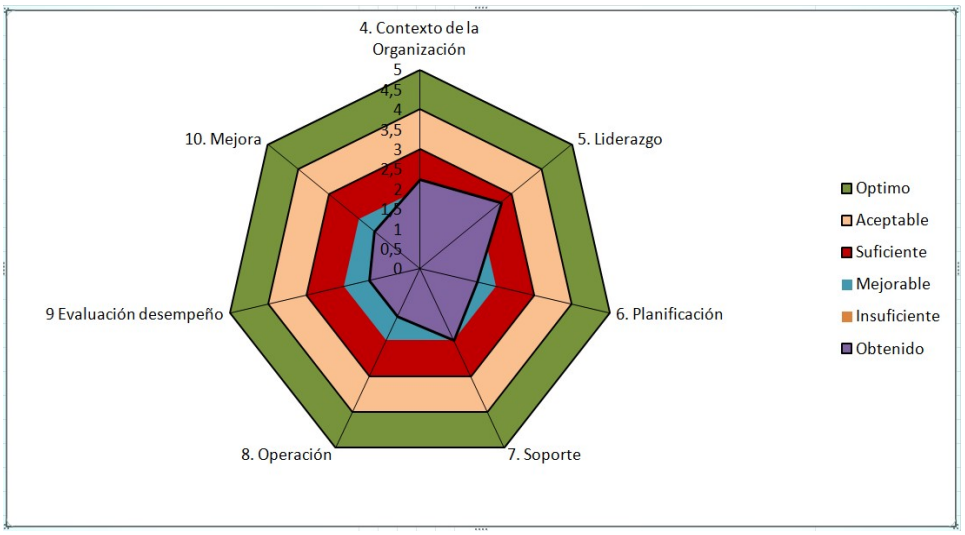
Auditoría de Cumplimiento:

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.

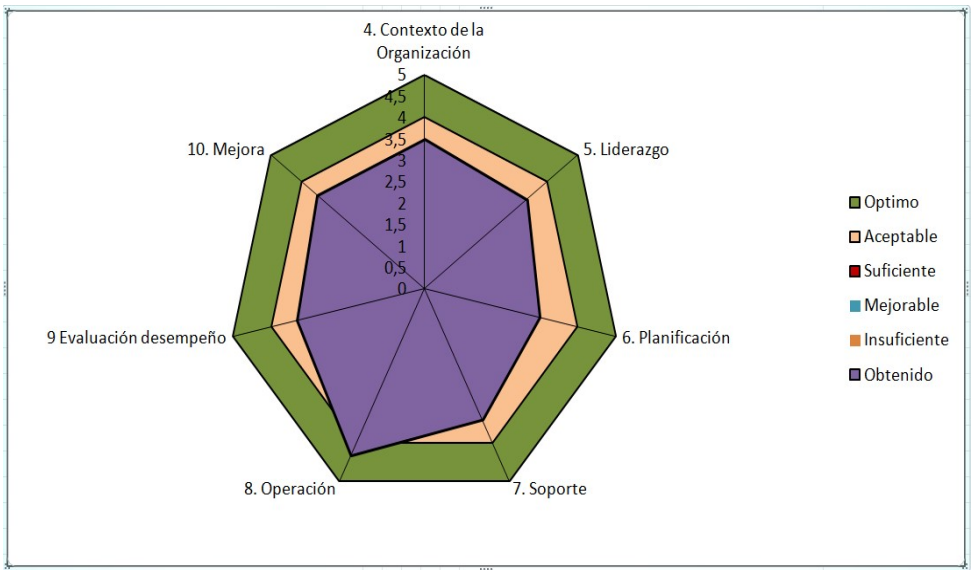


Nivel de cumplimiento de los requisitos de la ISO 27001 que vienen definidos entre los apartados 4 al 10:

Cumplimiento Actual:

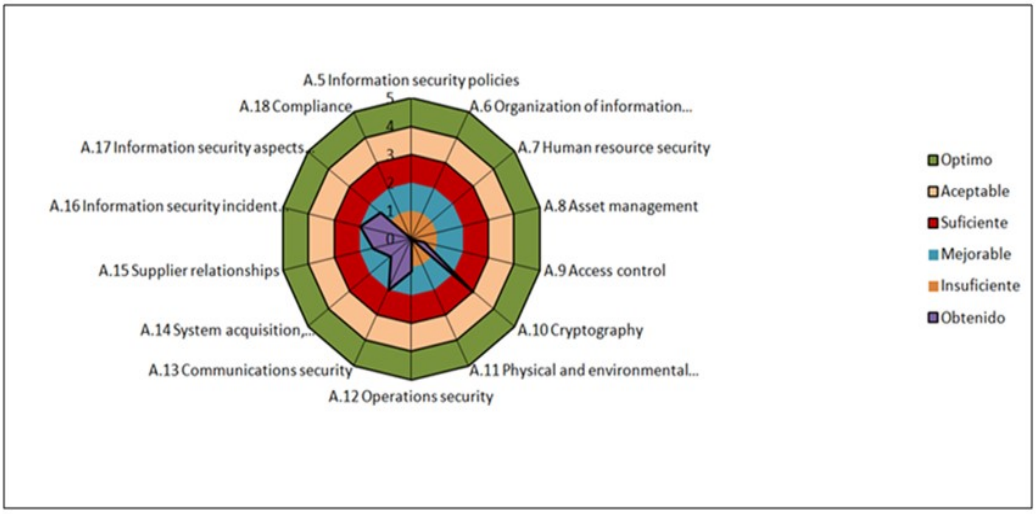


Cumplimiento deseado:

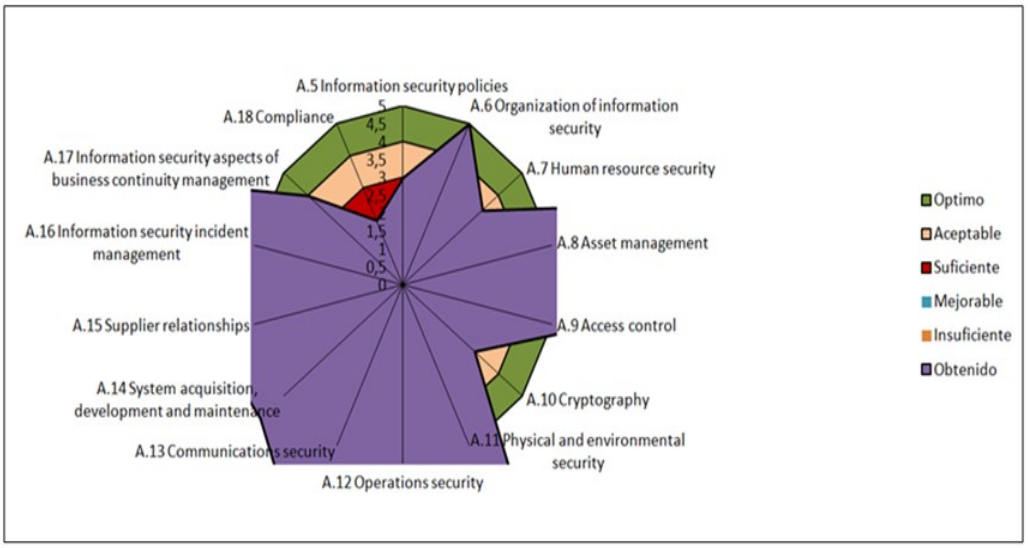


Nivel de cumplimiento de los requisitos de la ISO 27001 que vienen definidos en el Anexo A:

Cumplimiento Actual:



Cumplimiento deseado:



8 - Referencias.

https://www.pmg-ssi.com

https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

https://www.incibe.es

https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

https://www.pmg-ssi.com

https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

www.uoc.edu

http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/Análisis+diferencial#Attachments

http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/Análisis+y+gestión+de+riesgos

https://elperiodicodelaenergia.com

https://elperiodicodelaenergia.com/la-china-catl-construira-una-fabrica-de-celulas-de-baterias-para-vehiculos-electricos-en-alemania/

https://www.itdigitalsecurity.es

https://www.itdigitalsecurity.es/actualidad/2018/01/la-cifra-de-ciberataques-a-empresas-en-2017-podria-superar-los-350000

https://administracionelectronica.gob.es

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.W74gtvZuJQ8

https://www.google.es/search?q=imagenes+etapas+PDCA&tbm=isch&source=iu&ictx=1&fir=9oNkADoKt50eFM%253A%252CuTxbhNGEwJ_yoM%252C_&usg=AI4_-kSVebsnGDmxfG5rF9egxXZTrzEomw&sa=X&ved=2ahUKEwiZxfy5rYjeAhVIJ8AKHSL5C_cQ9QEwB3oECAYQEg#imgrc=9oNkADoKt50eFM:

https://www.sigea.es

https://www.sigea.es/isabes-cuantos-apartados-tiene-la-nueva-iso-27001/

https://www.sigea.es/wp-content/uploads/2013/09/iso270012013.png

http://www.iso27000.es

http://www.iso27000.es/sgsi_implantar.html

http://www.iso27000.es/download/doc_sgsi_all.pdf

http://www.hackplayers.com

http://www.hackplayers.com/2013/12/principales-certificaciones-seguridad-hacking.html?m=1

Seguridad de la Información

https://cursos.com/seguridad-informacion-profesion-futuro/

ISO 27001: El papel de la alta dirección en un SGSI

https://www.isotools.org/2015/02/04/iso-27001-papel-alta-direccion-sgsi/

Seguridad y privacidad de la información

https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Metodologías Para el Análisis de Riesgos en los SGSi

http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Auditoria Informática

https://es.slideshare.net/simondavila/clase-riesgosamenazasvulnerabilidades

shd.gov.co

www.shd.gov.co

27001 Academy

https://advisera.com/27001academy/es/knowledgebase/lista-de-documentos-obligatorios-exigidos-por-la-norma-iso-27001-revision-2013/

http://www.iso27000.es

http://www.iso27000.es/sgsi_implantar.html

Metodologías Para el Análisis de Riesgos en los SGSi

http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

ISO TooLS

https://www.pmg-ssi.com/norma-27001/

Metodologia-Magerit

http://metodologia-magerit.blogspot.com/

9 - Anexos.