Trabajo Final de Máster en Seguridad de las Tecnologías de la Información y las Comunicaciones

Desarrollo para el Plan Director en la Implementación de un Sistema de Gestión de la Seguridad de la Información

Autor: Ing. Andrea Arteaga Palacios
Director de TFM: Antonio José Segovia Henares
Universitat Oberta de Catalunya – UOC
Junio de 2019

Dedicatoria y agradecimientos

En primera instancia, deseo agradecer a dos mujeres admirables, luchadoras y fuertes: ***mi madre y abuela*****,** por brindarme siempre su apoyo, afecto y confianza, con los cuales he llegado a cumplir otro de los sueños de mi vida. A ***mi madre*** en especial, le agradezco por inculcar en mí, el ejemplo de esfuerzo y valentía, no temer a las adversidades y siempre, trabajar con dedicación, amor, determinación, perseverancia para obtener mis logros establecidos.

Quiero mostrar mis más sinceros agradecimientos, por el apoyo incondicional de personas muy especiales y grandes amigos, **doña Nelly, Juliana Londoño** y su esposo **Julián Velasco**, quienes me extendieron su mano, dedicaron una parte de su tiempo para ayudarme a seguir avante, y con ello, conseguir la culminación de este máster.

Por último pero no menos importante, quiero manifestar mi más sincero y respetuoso agradecimiento, a quien fue mi mentor durante dos semestres, cuando estaba en la asignatura de SGSI y en mi TFM, el ***profesor Antonio José Segovia Henares***, quien direccionó mi trabajo final de máster, siempre estuvo respondiendo oportunamente a mis numerosas inquietudes y brindándome mucho ánimo.

Mil gracias a todos.

Resumen

El desarrollo del estudio a tratar en este documento, atañe a la realización del Trabajo Final de Máster Interuniversitario en Seguridad de las Tecnologías de la Información y las Comunicaciones.

Con el Plan Director, se determina el grado de seguridad en el que se halla la empresa, cuando se realiza la evaluación pertinente para tal caso. Ello permite reducir los riesgos, aplicar las medidas correctivas (controles), para luego hacer un seguimiento de los mismos y de esta forma gestionar la confidencialidad, integridad y disponibilidad de los activos de información. Llevando a cabo un alineamiento con los objetivos, estrategias y políticas de la empresa.

En este estudio se realizó el análisis pertinente, teniendo como base los estándares de seguridad, como los son ISO/IEC 27001 e ISO/IEC 27002 y empleando las metodologías PDCA (Plan, Do, Check, Act) y Magerit para un proceso de mejora continua del negocio.

Palabras clave: Plan Director, riesgos, controles, activos de información, estándares de seguridad.

Summary

The aim of this study presented here concerns about the final work from Inter-university Máster's in Security of Information and Communications Technologies.

The level of security of the company is determined by the Master Plan when a relevant assessment is conducted. This allows to reduce risks, implement corrective actions (controls) and then tracking these, and in this way to manage confidentiality, integrity and availability of information assets. This with aim to achieve alignment of company objectives, strategies and policies.

In this study I did relevant analysis based on safety standards, such as ISO/IEC 27001and ISO/IEC 27002, and used the PDCA (Plan, Do, Check, Act) and Magerit methodologies for a process of continuous improvement.

Key words: Master Plan, risks, controls, information assets, safety standards.

Tabla de contenido

1. Situación actual

1.1 Introducción

Una parte de este capítulo tratará algunas normas de la ISO, las cuales tienen relación con el tema en cuestión, pero no se va a ser mucho énfasis en ellas, sin embargo se usarán como base en la realización de este trabajo.

También se presenta la situación actual de la empresa (objeto estudio), en materia de Seguridad de la Información, dentro de la cual se desglosan puntos relevantes, para conocer la posición en la que se encuentra esta organización.

En lo concerniente al proyecto, se estipula el tema de Plan Director con los criterios solicitados, como requerimientos expuestos en el documento Guía del TFM.

1.2 Planeación

1.2.1 Objetivos de Seguridad de la Información

1.2.1.1 Objetivo General

Conservar y salvaguardar el activo información de la organización, al igual del uso apropiado de los recursos, gestionar los riesgos para proteger la *integridad, confidencialidad y disponibilidad* de la información, junto con el hecho de brindar seguridad en la continuidad del negocio.

1.2.1.2 Objetivos Específicos

- Puntualizar los controles apropiados, para implementar una declaración de aplicabilidad, en la que se indique los objetivos de los mismos.

- Analizar y gestionar los riesgos de seguridad de la información, para informar a la empresa, así según su impacto y riesgo, sean asumidos, transferidos, minimizados y/o eliminados de una forma documentada, repetible, eficiente y adaptada a los cambios que se produzcan a nivel del entorno, la organización y tecnología.

- Determinar las políticas de seguridad de la información, que estén acorde a los procesos, lineamientos y requerimientos de la organización.

- Monitorear y originar reportes sobre los procesos que se ejecutan en la empresa, para conocer el nivel de cumplimiento, frente a lo planteado por las normas estándar ISO 27001 e ISO 27002.

- Efectuar un estudio de análisis y evaluación del riesgos, identificando los activos y recursos que se deben proteger.

- Fomentar en las áreas implicadas, las buenas prácticas y comportamientos seguros en el manejo de la información, mediante capacitaciones de sensibilización, con las que se espera mejorar el nivel de conciencia de las personas, frente a la necesidad de proteger los activos de información pertenecientes a la empresa.

1.3 Plan Director

1.3.1 Objetivos del Plan Director

- ✓ Conocer el contexto y liderazgo (compromiso de la Alta Dirección, políticas de la entidad, organización de los roles, responsabilidades, infraestructura tecnológica, funcionalidad de las redes: interna y externa, relación con los proveedores, etc.) sobre la compañía.

- ✓ Planear los objetivos de seguridad de la información y Plan Director, alineados con las estrategias, políticas, objetivos, metas, visión y misión de la empresa.

- ✓ Llevar una medición de las actividades a ejecutar, para conseguir los objetivos establecidos.

- ✓ Evaluar el nivel de cumplimiento, por medio del análisis diferencial con respecto a las normas estándar ISO/IEC 27001 e ISO/IEC 27002.

- ✓ Valorar los riesgos de seguridad.

- ✓ Hacer seguimiento sobre las propuestas de mejoras realizadas.

1.4 Marco normativo ISO de referencia

1.4.1 ISO/IEC 27001:2013

La norma ISO 27001 emitida por la Organización Internacional de Normalización, describe cómo *gestionar la seguridad de la Información en una empresa*, y ser implementada en cualquier tipo de entidad, con o sin fines de lucro, privada o pública, pequeña o grande.

Su función principal es proteger la confidencialidad, integridad y disponibilidad de la información, *así como de los sistemas que la procesan dentro de la compañía.* Dicha labor la lleva a cabo investigando, cuáles son los potenciales problemas que podrían afectar la información (evaluación de riesgos), para luego definir lo que es necesario realizar y así evitar, tales problemas se produzcan (mitigación o tratamiento del riesgo).

A partir de lo anterior se dice, la filosofía principal de la norma ISO 27001 se basa en la *gestión de riesgos: investigar dónde están los riesgos y tratarlos sistemáticamente.*

Figura 1. Estructura ISO 27001 [1]

Las medidas de seguridad o controles a implementar, se enseñan regularmente bajo la forma de políticas, procedimientos e implementación técnica (software y equipos). Pero en muchos sucesos, las implementaciones de ISO 27001 que se dan, tendrán conectividad con determinar las reglas organizacionales (redacción de documentos), las cuales son requeridas para prevenir violaciones de la seguridad.

ISO 27001 se divide en 11 secciones más el anexo A, en donde las secciones que van de 0 a 3 son introductorias (no son obligatorias para la implementación), por el contrario, las secciones que van de 4 a 10 son obligatorias; lo que conlleva, la empresa debe implementar todos sus requerimientos para cumplir con esta norma. Los controles que conforman el Anexo A, se implementan si corresponden en la Declaración de aplicabilidad.

- Sección 0 - Introducción.
- Sección 1 - Alcance.
- Sección 2 - Referencias normativas.
- Sección 3 - Términos y definiciones.
- Sección 4 - Contexto de la organización.
- Sección 5 - Liderazgo.
- Sección 6 - Planificación.
- Sección 7 - Apoyo.
- Sección 8 - Funcionamiento.
- Sección 9 - Evaluación de desempeño.
- Sección 10 - Mejora.

PDCA (Planificación, Implementación, Revisión y Mantenimiento)

Anexo A - Proporciona un catálogo de 114 controles, de acuerdo a la nueva versión (ISO 27001:2013).

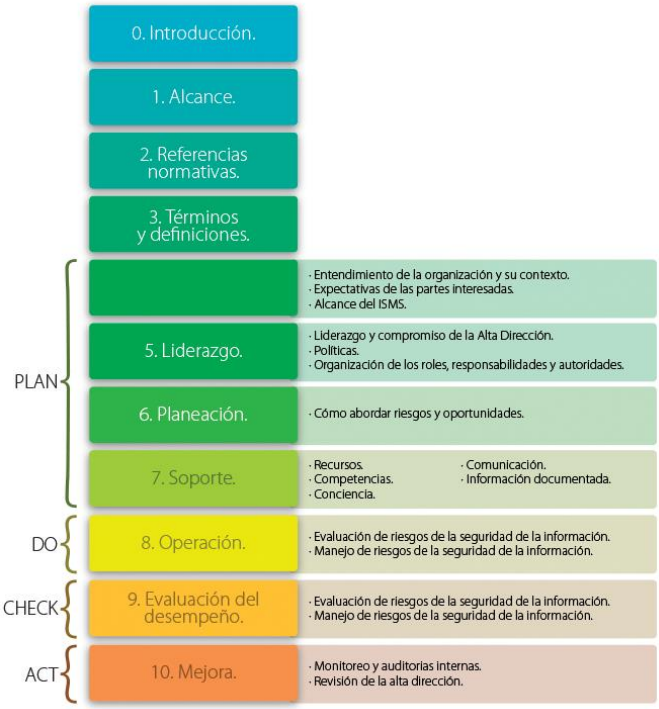


Figura 2. Estructura del estándar ISO/IEC 27001:2013 [4]

1.4.2 ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013 consta de principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una empresa.

Los objetivos de la norma brindan orientación general sobre los objetivos, comúnmente aceptados de la gestión de la seguridad de información. Además contiene las mejores prácticas de control de objetivos y controles. Los siguientes dominios son los que estructuran la norma ISO 27002:2013,

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad de los recursos humanos.
- Seguridad física y ambiental.
- Gestión de las Comunicaciones y operaciones.
- Control de acceso a la información.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes de seguridad de la información.
- Gestión de la continuidad del negocio.
- Conformidad. Aspectos de cumplimiento legal y normativo.

Tanto los controles como los objetivos de los mismos en ISO/IEC 27002:2013, se encuentran destinados hacer implementados, con el fin de cumplir los requisitos identificados por una evaluación de riesgos. *Es decir, no se requiere implantar todos los controles recomendados por esta norma, pues la organización es la que*

debe priorizar, y seleccionar los controles que se pueden alinear con su estrategia de riesgo.

1.4.3 ISO 27002: Complemento de ISO 27001

En el tema de seguridad de la información, la norma ISO 27001 se destaca por ser la base en el tratamiento de los riesgos de una organización. Tal norma se encarga de establecer, implantar, mantener y mejorar la seguridad de la empresa de una manera continua. Pero también está la norma ISO 27002, la cual contiene las buenas prácticas con la que se determinan controles y objetivos de estos, donde todos ellos se integran en la norma ISO 27001, relacionados con la temática de los riesgos.

Por lo expuesto anteriormente, se entiende bien la importancia de la norma ISO 27001 como **Sistema de Gestión de Seguridad de la Información.** Pero igual es de importante la labor que lleva a cabo la norma ISO 27002, como guía de buenas prácticas e implantando controles, con los cuales ofrece una aceptable garantía en la seguridad de la información, y junto con las recomendaciones dadas al respecto.

1.4.4 ISO 31000:2018

El día 14 de febrero de 2018, se publicó la nueva norma ISO 31000:2018 "Gestión del riesgo. Principios y directrices", con las que se reemplaza a la pasada versión de ISO 31000:2009. Esta norma ejerce de *referencia* para otros estándares, los cuales tengan relación con la Gestión de Riesgos. También complementa información de diferentes normativas, tratándose en diversos planos como: local, regional, nacional o incluso continental.

Su estructura se presenta a continuación, de manera muy resumida:

- Capítulos 1 y 2: Introducción y Campo de aplicación.
- Capítulo 3: Términos y definiciones.
- Capítulo 4: Principios.
- Capítulo 5: Marco de referencia.
- Capítulo 6: Proceso. [73]

La presente norma proporciona directrices en relación a la gestión del riesgo, por las cuales puede afrontar las organizaciones. Los procedimientos mencionados anteriormente, se pueden emplear en cualquier tipo de organización sin interesar su contexto.

Además ofrece un planteamiento usual, para gestionar sobre cualquier tipo de riesgo, de tal manera que no resulta ser específico de la industria o el sector.

ISO 31000 se emplea durante toda la vida de la organización, se enfoca en la gestión del riesgo en las empresas, apoya para fijar todos los objetivos alcanzables, se puede adaptar a cualquier actividad e incorporar, en la toma de decisiones basadas en hechos.

Las novedades que presenta ISO 31000 son:

i. Diversidad y pluralidad: El nuevo estándar admite la toma decisiones, planificación con respecto a las áreas de la organización como financiera y

contable, además de la operativa, producción y comercialización. Incluso puede abarcar los campos de operación, desde la producción de alimentos hasta planes complejos, para dispositivos de comunicaciones.

ii. Revisión ISO Guide 73: Ayuda a que la gestión de riesgos sea, más simple y claro para toda persona que labora en la empresa.

iii. Reducción del texto: Con su actualización se han obtenido nociones fundamentales, además de ser un escrito corto, preciso, definido, sencillo de asimilar, entender y emplear.

1.4.5 ISO 27005:2018

Es ineludible tener una visión sistemática, para la gestión de riesgos de seguridad de la información, reconocer las necesidades de la organización sobre los requerimientos concerniente a este tema, y así, generar un sistema eficiente con respecto a la gestión de seguridad de la información.

Ofrece directrices para la gestión de riesgos de seguridad de la información. Esta norma garantiza los conceptos generales dados en ISO/IEC 27001:2013, fue elaborada para brindar la implementación, cumplimiento con la seguridad de la información y la cual está realizada desde una perspectiva de gestión de riesgos.

Para una mejor comprensión de la norma ISO 27005:2018, se requiere conocer los modelos, conceptos, terminologías y procesos establecidos en ISO 27001 e ISO 27002.

Cabe señalar, esta norma se emplea en todas las clases de negocios existentes, donde coordinan los riesgos asociados, a la seguridad de la información de tal entidad.

1.5 Términos y definiciones

1.5.1 Plan Director

Es un documento oficial en el que los responsables de una organización (empresarial, institucional, no gubernamental, etc.), reflejan sus intenciones para el futuro de la organización a largo plazo, definiendo generalmente un período no inferior a 5 años.

Entre las características de este documento destacan que es **cualitativo** (no cuantitativo), **objetivo** (no subjetivo), y **atemporal**. Es cualitativo porque específica las futuras cualidades de la organización, como su estructura, su misión ante la sociedad, o su catálogo de servicios. Es objetivo, porque indica el fin por el que lucha la empresa, pero no entra en detalles de cómo conseguirlo. Es atemporal porque, independientemente de la duración del plan, no establece intervalos de tiempo que rijan las prioridades a llevar a cabo en el día a día.

1.5.2 SGSI

Es la abreviatura que hace referencia al *Sistema de Gestión de la Seguridad de la Información,* la cual es una parte del Sistema de Gestión General, tiene como base un enfoque de riesgo empresarial*, determinado para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.*

De acuerdo a la norma ISO 27001:2013, el SGSI se encarga de preservar la *confidencialidad, integridad y disponibilidad* de la información, así como de los sistemas relacionados con su tratamiento dentro de la empresa.

Para establecer y gestionar un SGSI, se emplea el ciclo de *PDCA (Plan-Do-Check, Act),* tal como se tratará posteriormente.

1.5.3 PDCA

El ciclo PDCA se conoce también como "Círculo de Deming", puesto que una de las primeras personas que usaron este esquema lógico, para la mejora de calidad fue el Dr. Williams Edwards Deming.

PDCA consta una *estrategia de mejora continua* de la calidad en cuatro pasos, el cual se utiliza en diferentes campos de las entidades, con el fin de tramitar argumentos como *salud y seguridad ocupaciones (ISO 45001), calidad (ISO 9000), inocuidad alimentaria (ISO 22000) o medio ambiente (ISO 14000).*

Las letras PDCA son una abreviatura de las palabras en inglés **Plan, Do, Check, Act,** en español quiere decir Planificar, Hacer, Verificar y Actuar.

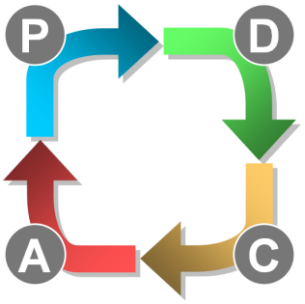


Figura 3. Mejora continua [5]. **Figura 4. Ciclo de vida PDCA [13].**

La anterior representación del ciclo PDCA indica: se debe **planificar** primero cómo conseguir lo que se desea adquirir, como segunda instancia se ejecutan las acciones que se han planificado (**hacer**), luego se confirma sobre lo que se ha hecho (**verificar**) y por último se establecen los cambios realizados, de esta forma minimizar los riesgos (**actuar**). Para una revisión se vuelve al punto de partida, pero en este caso se han agregado las mejoras hechas sobre anteriores estudios.

1.5.4 Confidencialidad, Integridad y Disponibilidad.

La gestión de la información se sustenta en tres pilares fundamentales: *Confidencialidad, Integridad y Disponibilidad.* La seguridad de la información emplea impedimentos y procesos, con los que resguardan el acceso a los datos y brindan este permiso, solamente a las personas con autorización para realizarlo.

Confidencialidad: necesita que la información sea accesible, es decir de forma única a las personas que están autorizadas para acceder a ella.

Integridad: la información debe mantenerse sin sufrir ningún tipo de alteración, frente accidentes o intentos maliciosos y, en caso de necesitar hacer modificaciones en los datos, solamente se realizarán con previa autorización.

Disponibilidad: implica que el sistema informático continúe funcionando, sin padecer alguna clase de degradación con respecto a accesos. La información estará disponible, solamente a personas autorizadas. [60]

1.5.5 Trazabilidad

Es una cualidad que permite, todas las acciones realizadas sobre la información o un sistema de tratamiento de la información, sean asociadas de modo inequívoco a un individuo o entidad. [65]

1.5.6 Autenticación

Provisión de una garantía de que una característica afirmada por una entidad es correcta. [65]

1.5.7 Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría, y evaluarlas objetivamente, determinando el grado en el que se cumplen los criterios de auditoría. [65]

1.5.8 Activo

Es un bien o derecho u otro recurso que la empresa dispone (ej; muebles, equipos informáticos, derechos de cobro por servicios, información, venta de bienes a clientes, entre otros), incluidos todos aquellos, de los cuales se espera adquirir un beneficio económico. [65]

1.5.9 Información

Se trata de un conjunto organizado de datos procesados, consta un mensaje que cambia el estado de conocimiento del sujeto, o sistema que acepta tal mensaje. La información permite resolver inconvenientes y tomar decisiones.

En otras palabras, la información es un recurso que ofrece significado o sentido a la realidad, como puede ser, mediante códigos y conjuntos de datos, con lo que se da origen al pensamiento humano o conocimiento.

1.5.10 Seguridad de la Información

Es el conjunto de medidas preventivas y reactivas, tanto de las organizaciones en si, como de los sistemas tecnológicos con los que se trata de resguardar, y proteger la información; de tal manera que se pueda mantener la confidencialidad, integridad y disponibilidad de la misma.

Pero se debe tener muy claro el concepto de seguridad de la información, no debe confundirse con el de seguridad informática, porque este último se ocupa de la seguridad, en el aspecto del medio informático; sin embargo, la información se halla en distintos medios y formas, no es solamente en medios informáticos.

1.5.11 Amenaza

Se trata de cualquier situación o eventualidad, que pueda generar daño a las empresas, impidiendo que estas o las personas que laboran, no les permita realizar sus actividades, donde afectaría de manera directa, tanto a la información como a los sistemas que se encargan de procesarla.

Dicho de otra manera, una *amenaza* solamente se presenta, si se genera una vulnerabilidad, la cual puede resultar aprovechable por una persona dañina, independientemente que comprometa o no, la seguridad de un sistema de información.

1.5.12 Vulnerabilidad

Es una debilidad o fallo en un sistema de información, con lo que se pone en riesgo la seguridad de la información, de tal manera, permita que un atacante pueda comprometer la disponibilidad, confidencialidad e integridad de la misma; por tal razón, es requerido encontrar la vulnerabilidad y eliminarla lo antes posible. [61]

1.5.13 Riesgo

Se define como la combinación entre la probabilidad que se genere un evento y sus consecuencias negativas.

Los factores que componen el riesgo son: amenaza y vulnerabilidad.

El riesgo se calcula de la siguiente manera:

Riesgo = Amenaza * Vulnerabilidad [63]

1.5.14 Impacto

El impacto se genera sobre un activo de información, de acuerdo a lo estipulado en la norma ISO 27001 y es la consecuencia dada, cuando se materializa una amenaza.

El impacto es, la diferencia entre las estimaciones del estado de seguridad del activo antes y después de materializar la amenaza. [64]

1.5.15 Salvaguardar

Es un concepto aplicado para referirse a la protección o defender la información, el cual resulta ser uno de los activos más relevantes de una entidad.

1.5.16 Control

Son aquellas políticas, procedimientos, prácticas y estructuras organizativas, concebidas para mantener los riesgos de seguridad de la información, por debajo del nivel de riesgo asumido. El concepto control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. [65]

1.5.17 Política

Se trata de un documento importante, en el que se **indican los objetivos marcados por la organización,** en materia de seguridad de la información y además, establece las **principales líneas de actuación que permite proteger,** todos los datos frente a las pérdidas, garantizando la integridad, confidencialidad y disponibilidad. [66]

1.5.18 Mitigar riesgo

Es el proceso de buscar tratamiento a los riesgos, los cuales fueron identificados en la evaluación de riesgos.

1.5.19 Red de comunicación

Conjunto de computadores conectados entre sí, se comunican para compartir datos y recursos, sin tener en cuenta la ubicación física de los diversos dispositivos.

Por medio de una red se ejecutan procesos en otro computador, o permitir el acceso a archivos, envío de mensajes, compartir programas, etc.

1.5.20 Seguridad de redes

Trata de las políticas y prácticas instauradas, con el fin de prevenir y supervisar el acceso no autorizado, el uso indebido, modificación o denegación de una red informática y sus recursos accesibles.

La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red.

1.5.21 Análisis de riesgo

El análisis de riesgo informático es un elemento, el cual forma parte del programa de gestión de continuidad del negocio.

Se necesita realizar el análisis de riesgo informático, para identificar si existen controles que ayudan a minimizar, la probabilidad de ocurrencia de la vulnerabilidad (riesgo controlado), de no existir, la vulnerabilidad será de riesgo no controlado.

El proceso de análisis de riesgo origina un documento, al cual se le conoce como matriz de riesgo. En este documento se muestran los elementos identificados, la manera en que se relacionan y los cálculos realizados. Este análisis de riesgos es indispensable, para lograr una correcta administración del riesgo.

1.5.22 Tratamiento de riesgos

Es un proceso de modificar el riesgo, mediante la implementación de controles. [65]

Para ISO 31000, este concepto define el proceso para modificar el riesgo. [68]

1.5.23 Riesgo residual

Es aquel riesgo que subsiste, después de haber implementado los controles. [68]

En otras palabras, el riesgo residual es aquél que permanece después, de que la dirección desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo permanente, una vez se han implantado de manera eficaz las acciones planificadas, por la dirección para mitigar el riesgo inherente. [67]

1.5.24 Riesgo Inherente

Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga a la actividad en particular y de la probabilidad, que un choque negativo afecte la rentabilidad y el capital de la compañía.

El riesgo inherente es propio del trabajo o proceso, que no puede ser eliminado del sistema, es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma. [67]

1.5.25 Evaluación de Riesgos

Proceso en el cual, una organización debe identificar los riesgos de seguridad de su información, luego determinar la probabilidad de ocurrencia y su impacto.

1.5.26 Nivel de Riesgos

Es la magnitud de un riesgo o de una combinación de varios. Se expresa en términos de combinación de la probabilidad, y las consecuencias de los mismos. [68]

1.5.27 Probabilidad

Para ISO 31000, la probabilidad es la oportunidad de que algo suceda. [68]

1.5.28 Declaración de Aplicabilidad

Por sus siglas en inglés *SoA (Statement of Applicability),* es un documento que si bien es un requisito de documentación en el estándar ISO/IEC 27001, porque es la principal declaración en la que se define, todo aquello que se desea realizar con la seguridad de los activos, pertenecientes a la empresa.

SoA se trata de un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar **ISO/IEC 27001** (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad). [59]

1.5.29 Ingeniería social

Es la práctica de obtener información confidencial, por medio de la manipulación de usuarios legítimos. El principio que sustenta la ingeniería social, es el que en cualquier sistema "los usuarios son el eslabón débil".

En síntesis, es un conjunto de técnicas empleadas por los cibercriminales, con el objetivo de engañar a los usuarios incautos, para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

1.6 Contexto de la organización

1.6.1 Descripción del negocio

La organización que será objeto de estudio, desarrolla aplicaciones informáticas basadas en Internet. Durante el tiempo que lleva realizando este trabajo, se ha especializado en la implementación de proyectos innovadores y relacionados con las tecnologías de la información.

Cuentan con la experiencia de implementaciones en manejo de tecnologías orientadas hacia internet, siendo muy fuertes en .NET, SQL Server, HTML 5.0 y ecosistemas móviles.

1.6.2 Objetivos

- Promover su industria.
- Saber el estado de desarrollo de tecnologías móviles en empresas punteras y su aplicabilidad.
- Interaccionar con la cultura e incentivar la colaboración de los países con los que se va a tratar.
- Seguir desarrollando sistemas de información que sean de gran innovación, con altos niveles de calidad y el compromiso de obtener, la satisfacción de los clientes.
- Entender los esquemas de cooperación empresarial.
- Fomentar mayor conocimiento de los competidores, para impulsar oportunidades de negocio y participación entre empresas.

1.6.3 Misión

Proveer soluciones y servicios prácticos e innovadores, soportados en sistemas de información desarrollados, bajo estándares internacionales de calidad, con el propósito de incrementar tanto la productividad como competitividad de los clientes, con un equipo de profesionales altamente capacitados, comprometidos con el crecimiento integral de la empresa y la región.

1.6.4 Visión

Estar posicionados a nivel nacional e internacional, como una compañía referente en la industria TI, por la calidad, investigación e innovación en sus productos y servicios, logrando la fidelización de clientes que garanticen la solidez empresarial.

1.6.5 Políticas de la organización

Las políticas establecidas en el momento por la entidad se listan a continuación:

- Procedimientos de inicio de sesión seguros.
- Sistema de gestión de contraseñas.
- Almacenar pruebas.

1.6.6 Organización de los roles y responsabilidades

	Funciones	Procesos agrupados	Procesos individuales
DIRECCIÓN TI	Planificación y coordinación TI	Gestión de la seguridad y del cumplimiento normativo.	
		Gestión de los procesos, la organización y los RRHH.	
		Gestión de proyectos y calidad.	Gestión de Proyectos. Gestión de Calidad.
		Gestión estratégica y financiera.	Gestión Estratégica. Gestión Financiera.
	Gestion de infraestructura TI.	Adquisición e Implementación de Aplicaciones.	
		Adquisición e Implementación de la infraestructura Hw, Sw y Comunicaciones.	Gestión de Hardware y Software base.
			Gestión de las Comunicaciones
	Gestión de los servicios TI.	Gestión de la producción.	Gestión de continuidad de servicios TI.
			Gestión de la capacidad.
			Gestión de la disponibilidad.
			Gestión de nivel del servicio.
		Soporte de los servicios TI.	Gestión de cambios y revisiones.
			Gestión de incidencias.
			Gestión de la configuración.
	Monitorización y evaluación TI.		

Tabla 1. Jerarquía de roles.

NOTA: La tabla anterior se encuentra como anexo al documento, en el archivo llamado ***1. Situación Actual.xls***, pestaña u hoja de cálculo ***1.5.6 Organización de los roles.***

ROLES	PUESTOS DE TRABAJO															
Dirección TI	JSP	JGTI	CGTI	TGTI	JS	JDMS	CT	AS	JO	OP	JDSC	TSC	JDDM	JP	AN	PR
b. Planificación y Coordinación TI																
b.1 Gestión de la seguridad y del cumplimiento normativo.	D	R	E		I						S	E				
b.2 Gestión de procesos, organización y RRHH.	I	D R	E	E	I	I					I		I			
b.3 Gestión de proyectos y calidad																
b.3.1 Gestión de proyectos	I	I	D		R	E					E			E		
b.3.2 Gestión de calidad	I	I	D		R	E					E			E		
b.4 Gestión Estratégica y Financiera																
b.4.1 Gestión Estratégica	D	R	E	E												
b.4.2 Gestión Financiera	D	R	E	E												

Tabla 2. Relación entre roles, puestos de trabajo y responsables.

c. Gestión de infraestructura TI	JSP	JGTI	CGTI	TGTI	JS	JDMS	CT	AS	JO	OP	JDSC	TSC	JDDM	JP	AN	PR
c.1 Adquisición e implementación de aplicaciones	I	I			D								R	S	E	E
c.2 Adquisición e implementación de la infraestructura Hw, Sw y la comunicación																
c.2.1 Gestión de Hw y Sw base	I	I			D	R	E									
c.2.2 Gestión de las comunicaciones	I	I			D	R					S	E				
d. Gestión de los servicios TI																
d.1 Gestión de la producción																
d.1.1 Gestión de de continuidad de servicios TI	I	I			D	R	S				E		E			
d.1.2 Gestión de la capacidad	I	I			D	E					E		E			
d.1.3 Gestión de la disponibilidad	I	I			D	R	S				E		E			
d.1.4 Gestión de nivel de servicio																
d.2 Soporte de los servicios TI																
d.2.1 Gestión de cambios y revisiones					I	D	R				E		E			
d.2.2 Gestión de incidencias					I	D	S				E		E			
d.2.3 Gestión de la configuración					I	D	R				E		E			
e. Monitorización y Evaluación TI	D	R			S	E					E		E			

Tabla 3. Continuación sobre la relación entre roles, puestos de trabajo y responsables.

Para una mejor comprensión sobre las anteriores tablas, se requiere establecer la correspondencia entre los ***Roles y Puestos de trabajo.*** Posteriormente se va a señalar cómo se comunica cada puesto en el rol.

Con lo cual se identifican los niveles de responsabilidades de la siguiente manera:

Puestos de trabajo	**Responsabilidades**
Director (D)	Responsable último rol o dada la equivalencia, entre rol y proceso establecido. Aprueba los trabajos correspondientes al rol, presentado por un responsable y proporciona los recursos técnicos, humanos y financieros para su ejecución.
Responsable (R)	Quien gestiona la ejecución de las responsabilidades correspondientes al rol. Presenta informes al Director.
Supervisor (S)	En determinado momento, un rol sea arduo, se puede requerir dividir responsabilidades en grupos, y fijarlas a los supervisores de grupo, con lo cual no se presume subdividir el rol.
Ejecutor (E)	Se encarga de realizar las tareas técnicas, ya que tiene los conocimientos precisos para ejercerlo.
Informado (I)	A nivel general, se informa a personas interesadas de las tareas realizadas en un proceso generado.

Tabla 4. Responsabilidades asignadas a los puestos de trabajo.

Para los puesto de trabajo determinados, se tratarán con abreviaturas, éstas se darán a continuación para tener mayor claridad y entendimiento de la tabla 5.

Puestos de trabajo	Abreviaturas
Jefe del Servicio de Producción	JSP
Jefe de Gabinete de Gestión TI	JGGTI
Consultor de Gestión TI	CGTI
Técnicos de Gestión TI	TGTI
Jefe de Sistemas	JS
Jefe del Departamento de Mantenimiento de Sistemas	JDMS
Consultor Técnico	CT
Administradores de Sistemas	AS
Jefes de Operación	JO
Operadores	OP
Jefe del Departamento de Seguridad y Comunicaciones	JDSC
Técnicos de Seguridad y Comunicaciones	TSC
Jefe del Departamento de Desarrollo y Mantenimiento	JDDM
Jefe de Proyectos	JP
Analistas	AN
Programadores	PR

Tabla 5. Puestos de trabajo y sus respectivas abreviaturas.

1.6.7 Valores

Innovación: Promover la generación de ideas para darle valor agregado a los productos y servicios, brindando así nuevas alternativas para los clientes.

Calidad: Tener el compromiso de desarrollar productos y servicios que cumplan con características específicas, para lograr la satisfacción del cliente.

Visión: Siempre estar proyectando cómo se desarrollará el entorno y cómo deberán realizarse las actividades en el futuro.

Integración: Trabajar articulados con otras entidades, con el fin de realizar proyectos de gran envergadura para lograr un objetivo común.

Liderazgo Empresarial: Contar con un gran sentido de pertenencia por la región, el cual se ve reflejado en la construcción permanente de proyecto, de alto impacto para el fortalecimiento tecnológico.

1.7 Liderazgo

1.7.1 Liderazgo y compromiso de la Alta Dirección

La Alta Dirección de la compañía brinda la orientación de la política, sobre la gestión de documentos y archivos para así:

- Certificar que los procesos del negocio y la documentación originada, son transparentes y claros.
- Legitimar a los interesados externos a la organización (tales como auditores, reguladores, etc.), que los documentos se tramitan de forma apropiada.
- Proporcionar congruencia entre las operaciones de la entidad, con referencia a la gestión de documentos.
- Con el liderazgo, apoyo, compromiso y responsabilidad de la Alta Dirección, se crea un ambiente en el que un sistema de gestión de documentos, se puede modular y proceder de manera eficiente. En donde tal documentación, puede ser usada por la alta dirección para consolidar su rol en la empresa.
- Asegurar que se establece, implementa y mantiene un sistema de gestión de documentos, archivos efectivo y eficiente para alcanzar los objetivos de la organización.
- Implicar a personas de la empresa, que tienen obligaciones en verificar y sancionar el cumplimiento de las normas.
- Revisar periódicamente el sistema de gestión y archivos de la organización.
- Asegurar que las responsabilidades, competencias en materia de gestión y archivos están definidas, asignadas y comunicadas a toda la compañía.
- Adoptar decisiones, estimular las acciones necesarias, para la mejora continua de la política de gestión y archivos.

1.8 Cronograma de actividades del proyecto

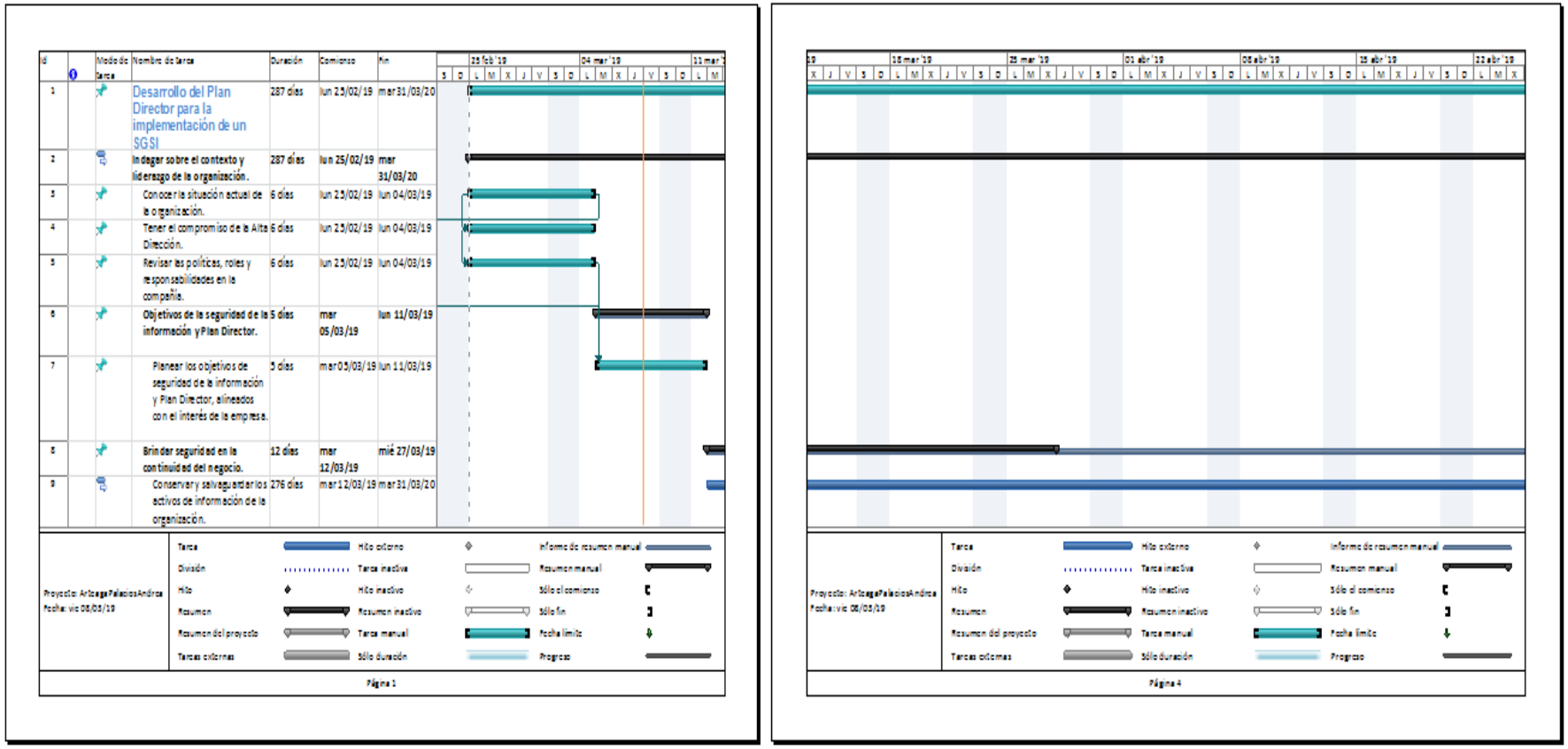


Figura 5. Cronograma de actividades - Diagrama de Gantt

<u>NOTA:</u> El cronograma completo se encuentra anexo al documento, el archivo es ***ArteagaPalaciosAndrea_TFM_SGSI.mpp***

1.9 Soporte

1.9.1 Recursos

Los documentos que reúnen el proceso de evidenciar, registrar, amparar y mantener la documentación relacionada con el SGSI trata:

- Indicadores de evaluación.
- Requisitos para un Sistema de Gestión de Documentos.
- Normalización y análisis de procesos.
- Guía control de acceso.

1.9.2 Personal competente

1.9.2.1 Talento Humano

Considerar el talento humano como capital más importante. La organización está conformado por un equipo interdisciplinario de profesionales, se caracterizan por responder a las metas de la organización de manera competente, personas íntegras que imprimen todo su conocimiento y pasión, en cada uno de los proyectos desarrollados.

Contar con profesionales, formados en áreas como Administración de Sistemas Informáticos, Gestión y desarrollo de Proyectos de Software, Dirección Estratégica en Tecnologías de Información, Dirección y Gestión de Proyectos.

1.9.2.2 Competencias emprendedoras

Creatividad e innovación: Sus fundadores demostraron tener este tipo de competencia, al implementar proyectos nuevos para satisfacer las necesidades de SI que se presentan en la región, y al indagar nuevas formas de calidad, pues así, asegurar su confiabilidad en el producto.

Pensamiento sistémico: Dicha competencia se desarrolla a lo largo del objeto social de innovación, el cual se encarga de adoptar nuevos productos a los cambios pertinentes en el entorno tecnológico, de esta forma se crea una estructura dinámica.

Orientación al logro: Puede ser la competencia más importante, a la hora de aceptarla en el desarrollo de la organización, las personas que crearon esta entidad pensaron que buscar nuevos métodos de calidad, generaban mayor confiabilidad en el software.

1.10 Operación

1.10.1 Evaluación del nivel de cumplimiento

La Gestión de Activos y Pasivos (GAP) es una función que debe enmarcar en la estructura de la empresa, y ofrecer una proporción dentro de las necesidades que presenta una entidad. Cuyo objetivo es medir, controlar los riesgos del mercado y trazar estrategias para ellos.

Cabe destacar que la GAP toca toda la organización, en un proceso de análisis y planeación, además de necesitar un fuerte apoyo por parte de la Alta Dirección, así ella puede tomar decisiones calculadas sobre los riesgos.

El proceso de GAP lo conforman 4 fases, las cuales se repiten en el momento de hacer seguimiento, de acuerdo a las decisiones que se hayan tomado y continuar con el refinamiento de las estrategias adquiridas.

- En la primera fase se identifica la situación de partida.
- Se calcula el efecto de los diferentes posibles escenarios.
- Se opta por la mejor estrategia.
- Implantación de las decisiones y vuelve a comenzar el ciclo.

Más adelante se mostrará el análisis diferencial, entre las normas estándar para la Seguridad de la Información (ISO/IEC 27001 e ISO/IEC 27002) y los criterios establecidos por la organización, referentes al mismo tema y así, se podrá conocer de manera global, el estado actual de la entidad frente a esta situación.

El objetivo de la realización de un análisis GAP (análisis diferencial), de controles implantados vs. controles necesarios no existentes, con respecto a la norma ISO/IEC 27002 (desarrolla un código de buenas prácticas, para la gestión de la seguridad de la información), es la verificación de la implantación, en lo concerniente a los procesos que se detectaron en el Plan Director de Seguridad (PDS). [81]

De acuerdo a lo estipulado por la ISO (International Organization for Standarization) y bajo sus normas, cabe señalar que un Sistema de Gestión se determina por un proyecto que consta de 4 etapas, como se puede observar a continuación:

Etapa	Descripción	Principales actividades
Planificar	Se instituye temas relacionados con los objetivos, políticas, procesos y procedimientos del SGSI, concernientes a la gestión de riesgo y mejorar por supuesto el área más relevante, Seguridad de la Información, de tal manera que se conseguirán resultados con respecto a los objetivos y políticas que se tratan en la compañía.	Establecer el SGSI.
Implementar	Efectuar y maniobrar con los procesos, políticas, procedimientos del SGSI y controles.	Implementar y operar el SGSI.
Medir	Valorar y en el caso que se requiera, medir el beneficio del proceso con respecto a la política del SGSI, junto con la práctica y sus objetivos. Después de haber realizado estas acciones, se da a conocer los resultados adquiridos para llevar a cabo su revisión.	Monitorear y revisar el SGSI.
Mejorar	Realizar acciones preventivas y correctivas, con la ayuda de la información obtenida, a través de los resultados generados por la realización de auditorías internas del SGSI, análisis de gestión o datos apreciables, para seguir con el progreso continuo del SGSI.	Mantener y mejorar el SGSI.

Tabla 6. Etapas que definen un proyecto para la implementación ISO 27001 en una organización.

La Metodología que se va emplear para los dos casos de análisis diferencial, con respecto a las normas ISO 27001 e ISO 27002, se trataron sobre el modelo de madurez, empleado para la valoración de los controles (COBIT) y basado en el CMM [81].

Las pautas que se trataron se describen en la siguiente tabla:

Valores asignados para el nivel de cumplimiento			Efectividad
Valor cuantitativo	***Valor cualitativo***	***Detalle***	
0	No existente	No existe certeza del estándar en la empresa.	0%
1	Inicial	Se han anexado normas a la medida de la compañía, pero presenta versatilidades.	10%
2	Repetible	La empresa tiene normas adaptadas, pero no tienen documentación al respecto.	50%
3	Definido	Existen normas acondicionadas a la organización, con la apropiada información registrada, pero no tienen medición.	90%
4	Administrado	Se miden de manera periódica los procesos de la entidad, y se realizan las mejoras necesarias.	95%
5	Optimizado	La entidad ha llevado a cabo todas las mejoras propuestas, cumpliendo así con las normas estándar y las buenas prácticas.	100%
6	No Aplica - N.A.		

Tabla 7. Valores asignados para el nivel de cumplimiento. (Ver archivo 1. Situación Actual.xls, hoja de cálculo: Criterios Análisis Diferencial)

Como se mencionó anteriormente, para esta caso de utilizaron:

- Evaluación: Se registró el valor cualitativo (Tabla 7), dependiendo de la situación actual de la empresa vs. control establecido por la norma ISO/IEC 27002:2013.

- Valor: Se utilizó el valor cuantitativo (Tabla 7), de acuerdo al valor determinado en el punto anterior (Evaluación).

- Total: Valor medio de los controles. Es este aspecto cabe destacar dos particularidades que se usaron, para una mayor claridad y entendimiento:
  - Los objetivos de los controles se representaron de color gris, en este espacio está el valor total, representado por el promedio de los valores asignados en cada control.
  - Mientras que los dominios de los controles, se trataron con el color naranja y en el campo "Total", se registró el valor acorde al promedio, de los valores dados en este campo, sobre los objetivos de los controles.

- Efectividad: Es el porcentaje utilizado, con relación a los conceptos que se determinaron en los ítems de “Evaluación” y “Valor”.

Además se le aplicó un método de semáforo, para resaltar el grado de importancia y atención de cada control. Las pautas establecidas para priorizar fueron:

- Color rojo: Corresponde a 0 y 1. Los procesos en este color, son los urgentes de mejorar.
- Color amarillo: Corresponde a 2 y 3. Los procesos son deseables de mejorar tan pronto como sea posible.
- Color verde: Corresponde a 4 y 5. Indica la evolución de los procesos, con base al mejoramiento continuo. [80]

1.10.1.1 Análisis Diferencial con respecto a la norma ISO/IEC 27002

Para este análisis se listaron los 14 dominios, 35 objetivos de control y 114 controles, los cuales fueron evaluados con base a cuatro criterios, por lo tanto el análisis diferencial está compuesto por cuatro campos. Las reglas para ellos se establecieron, teniendo en cuenta el nivel de cumplimiento de la organización (situación actual), frente a la norma estipulada por ISO/IEC 27002:2013.

De esta manera se puede evaluar y determinar el análisis diferencial, tomando como base, el nivel de cumplimiento de la organización en los controles aplicados en la misma (de forma cualitativa y cuantitativa), con respecto a los controles fijados por la norma ISO 27002, así se pueden precisar los hallazgos fuertes y débiles en la empresa, además de recomendar mejoras sobre la misma, para mayor cumplimiento en esta situación.

El desarrollo de esta parte se puede verificar en el archivo adjunto llamado, ***1. Situación Actual.xls***, hojas de cálculo o pestañas: ***Análisis diferencial ISO 27002 y Criterios Análisis Diferencial.***

1.10.1.2 Análisis Diferencial con respecto a la norma ISO/IEC 27001

La metodología empleada fue la misma que se utilizó, en el “Análisis Diferencial con respecto a la norma ISO/IEC 27002:2013, pero se lleva a cabo sobre los apartados 4 a 10:

- 4. Contexto de la organización.
- 5. Liderazgo.
- 6. Planificación.
- 7. Apoyo.
- 8. Funcionamiento.
- 9. Evaluación de desempeño.
- 10. Mejora.

Ver el archivo *1. Situación Actual.xls,* hojas de cálculo o pestañas: *Análisis Diferencial ISO 27001 y Criterios Análisis Diferencial.*

1.11 Justificación

El Plan Director de Seguridad (PDS) es una herramienta útil para cualquier empresa, porque permite determinar las actividades (procesos) de ella, con respecto a la Seguridad de los Sistemas de Información, ya sea a corto, mediano o largo plazo y siempre teniendo muy en cuenta, el PDS esté alineado con las estrategias, objetivos, metas de la organización.

Con el PDS se busca analizar e indicar a una organización, el grado de seguridad en el que se encuentra y así, sugerir las medidas correctivas estructuradas en el tiempo, con las cuales se puede acreditar, el nivel de seguridad apropiado de acuerdo a lo que precise el negocio.

Posteriormente se dan las razones por las que se requiere de un PDS:

- La Seguridad de la Información se vuelve cada vez más relevante para una entidad.
- Surge la necesidad de un plan, en el que se fijen las directrices a seguir.
- Emergen requerimientos de seguridad en toda la compañía.
- Reunir proposiciones de manera separada con respecto a la seguridad.
- Discurrir la seguridad con una visión integral (legal, tecnológica, recursos humanos, organizativa, etc.).
- Determinar el nivel de seguridad de la compañía (fortalezas y debilidades), con el fin de distribuir esfuerzos y establecer un nivel de seguridad aceptable.
- Optimizar, reforzar y ajustar el actual SGSI implantado en la entidad, conforme a los estándares de seguridad.
- Precisar los procesos, directrices y políticas de seguridad.

2. Sistema de Gestión Documental

2.1 Definición

Un Sistema de Gestión Documental (SGD) o Document Management System (DMS) por sus siglas en inglés, se encarga de registrar de manera eficaz y ordenada, la elaboración, admisión, sostenimiento, uso y disposición de los documentos (ISO 15489-1: 2001 [E], Información y documentación - Gestión documental) [13].

Para tener un conocimiento más cercano del SGD, es pertinente conocer sus objetivos:

- Proteger y redimir la documentación que se genera de forma eficiente.
- Avalar el funcionamiento idóneo de la empresa, junto con el desempeño con respecto a la legislación vigente.
- Coordinar y regular las acciones exactas que lleguen a damnificar la creación, aceptación, localización, consentimiento y conservación de los documentos.

Además el sistema de gestión documental brinda apoyo en el momento de la toma de decisiones, y tiene un papel muy importante en la compañía por las siguientes razones:

- Previene el mal gasto de tiempo, cuando se quiere recobrar la documentación necesaria.
- Instaurar un ciclo de vida de la documentación, facilitando así, su destrucción segura y certificada.
- Impedir la pérdida de la documentación, pues los documentos se hallan unificados y registrados en un único sistema.
- Admitir el control de accesos, convicción sobre la información detallada en los documentos e imposibilitar su disposición a terceras personas.

2.2 Ventajas

- Digitalización de documentos: Con esta manera de almacenar la documentación, se guardarán en una localización central. Una digitalización de documentos bien organizada y planificada, resulta ser necesario para una adecuada utilización del sistema.

- Localización central: Con un sistema de gestión de este tipo, toda la información procedente del trabajo diario de la empresa, estará recopilada en un sitio central, por lo cual la empresa deberá seleccionar qué empleados podrán tener acceso a dichos documentos. Así la información supone acabar con la búsqueda ardua de documentación, por las redes de carpetas de la entidad, consiguiendo de esta forma una forma ágil de trabajar.

- Mejorar el flujo de trabajo: Utilizando el sistema de gestión documental, hará que los procesos de trabajo resulten ser más eficientes y productivos. Con ello, se brindará una imagen global de los procesos realizados en la organización. Poniendo en práctica este método, habrá un control en el

seguimiento de las labores inconclusas, conocer las que ya se han completado o automatizar tareas iterativas, las cuales ayudarán a la empresa, en cuanto ahorro de tiempo se refiere.

- Seguridad de la Información: Teniendo un Sistema de Gestión de Documentos, el riesgo de pérdida de la información disminuye de manera notable. Además la compañía podrá seguir laborando efectivamente, teniendo la confianza en que su documentación está segura en este sistema, y podrá recuperar los datos cuando sean requeridos.

- Compartir documentos: El Sistema de Gestión Documental brinda a sus usuarios, compartir la información necesaria en sus labores, permitiendo el acceso a los grupos tanto a nivel interno como externo (proveedores, clientes, etc.) de la organización.

- Colaboración documental: Existen sistemas, donde a diversas personas se les facilita trabajar un documento al mismo tiempo, por estar ubicado en un lugar central. De esta manera, los empleados podrán modificar ésta información en el instante que lo requieran. Sin embargo, con este sistema se pueden presentar inconvenientes, por tal razón existe una *Guía de Gestión Documental,* donde se hallan los problemas más frecuentes que a una entidad se le pueden presentar, pero con la guía se obtiene un alto rendimiento en esta clase de colaboración.

- Control de versiones: Los gestores documentales elaborar un historial de versiones, para proporcionar el medio de acceder a cualquier versión del texto y recuperar información, en caso tal de surgir un incidente y recuperar el trabajo que se venía realizando en la última versión.

2.3 Alcance del SGSI

Con base a lo estipulado por la norma ISO 27001:2013, en la que plantea, la organización debe trazar los límites del SGSI, para delimitar su alcance y alinearse con ésta.

El límite del SGSI está definido por los activos, con los que apoyan los diferentes procesos, asociados a la implementación de sistemas de información, orientadas a la Web para diferentes sectores y proyectos innovadores, relacionados con:

- *Gestión de la seguridad y del cumplimiento normativo.*
- *Gestión de los procesos, la organización y los R. H.*
- *Gestión de proyectos y calidad.*
- *Gestión estratégica y financiera,*
- *Gestión de infraestructura TI (Adquisición e Implementación de Aplicaciones, Adquisición e Implementación de la infraestructura hardware, software y comunicaciones).*
- *Gestión de los servicios TI (Gestión de continuidad de servicios TI, Gestión de cambios y revisiones, Gestión de incidencias, Gestión de la configuración).*
- *Monitorización y evaluación TI.*

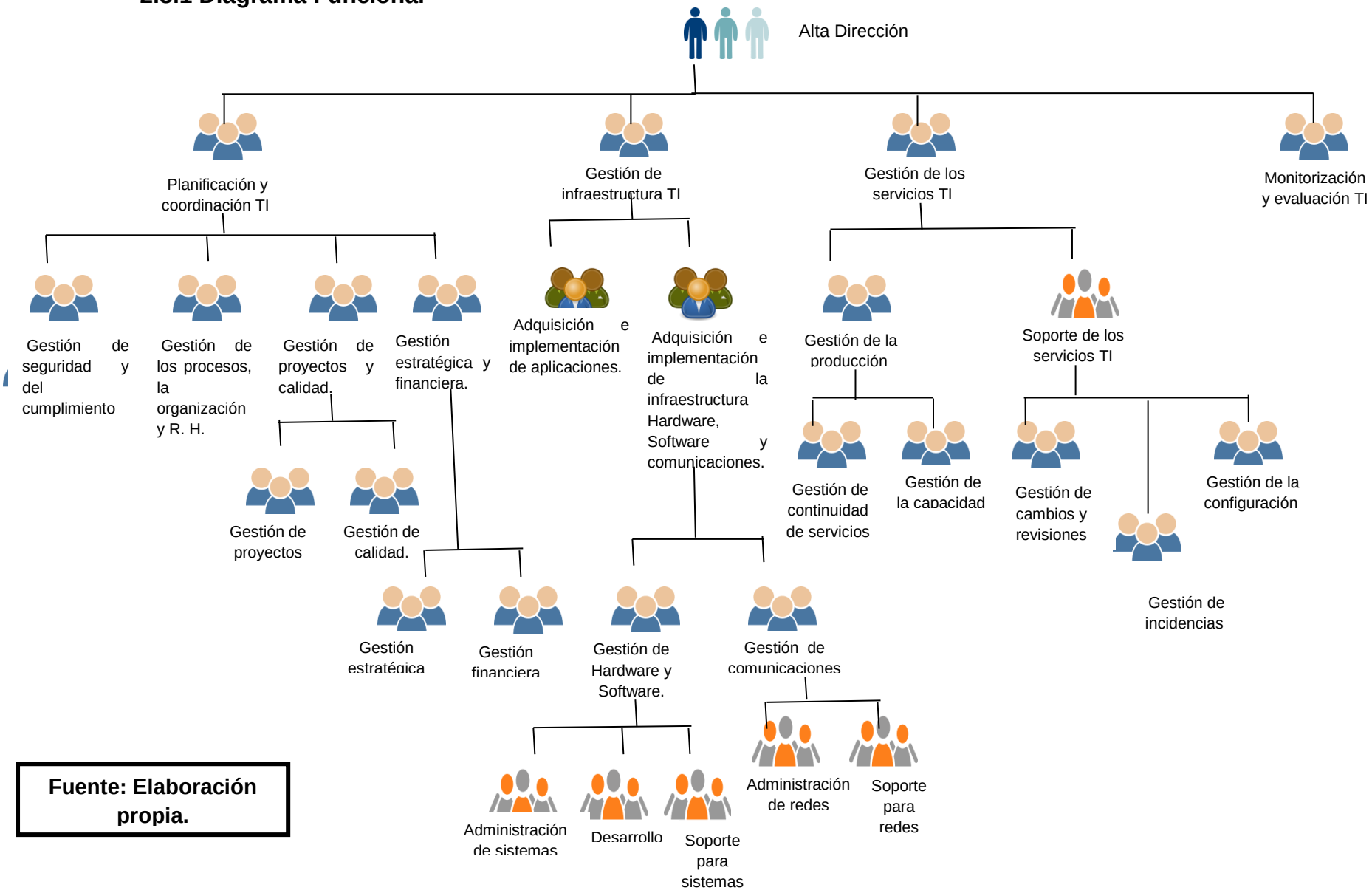
A partir de este planteamiento, afectará a todo el sistema, incluyendo la información con la que trata la compañía a diario. En pocas palabras, la Gestión de la Seguridad de la Información incorpora, tanto los soportes físicos como lógicos del manejo y uso de los datos. Tratando también la seguridad referente a las instalaciones, como lo pueden ser acceso físico y de la información (local).

Con lo que se quiere lograr, la mejora en la seguridad de los sistemas utilizados, por el personal interno de la empresa. Para ello se va a realizar una evaluación de los sistemas de información, descubrir sus vulnerabilidades, posibles amenazas y riesgos, para brindar propuestas, llevar un seguimiento de su continuidad y salvaguardar la información.

El SGSI está conformado por los sistemas de información que favorecen a los procesos de desarrollo, basados en el modelo internacional de calidad CMMI, el trabajo del equipo y la tecnología con la que se cuenta, para satisfacer las necesidades del cliente.

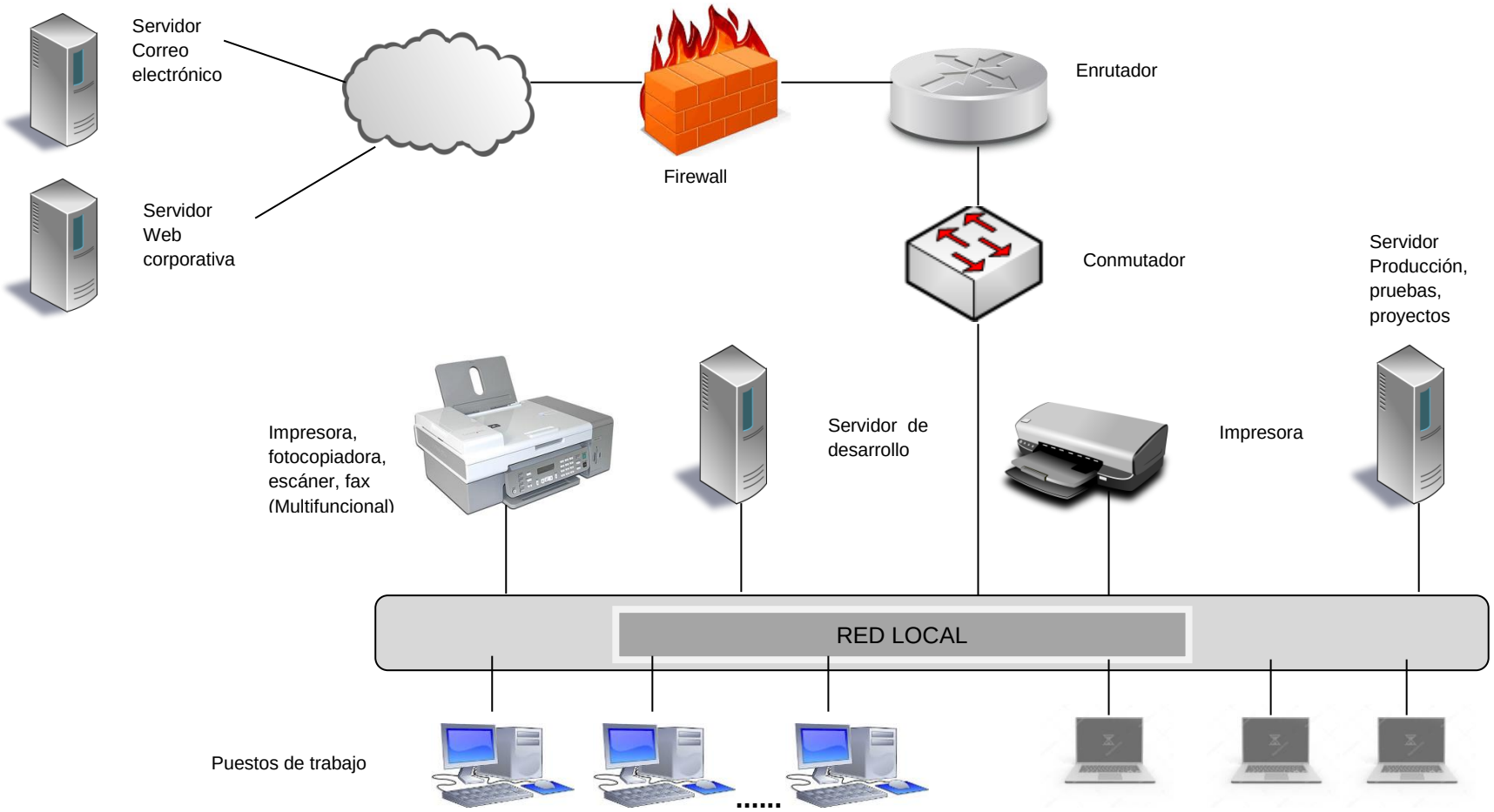
Llevando a cabo desarrollos de sistemas, para la toma de decisiones de entes territoriales, sistemas de información para el monitoreo del cumplimiento de metas, basados en indicadores de tipo social, económico de impacto en áreas de salud, educación, tránsito, entre otros.

2.3.1 Diagrama Funcional



Fuente: Elaboración propia.

2.3.2 Diagrama de red con la infraestructura tecnológica



Fuente: Elaboración propia

2.4 ISO 27001: Política de seguridad en la organización

La norma ISO 27001 brinda los medios necesarios, para la implementación del *Sistema de Gestión dela Seguridad de la Información* en una compañía, por lo cual, realizar una buena planificación en el tema que se atañe en este trabajo, crea una buena gestión estratégica para la organización. Donde esta estrategia precisa la aleación de políticas, operaciones y estructuras organizativas, con las que se quiere garantizar los planteamientos en la *Seguridad de la Información,* y esto conlleve a un alineamiento con los objetivos del negocio, la legislación vigente y las regulaciones que sean adaptables.

La política de seguridad hace referencia a un conjunto de documentos, los cuales se hallan sistematizados, de tal forma que propone normas, procedimientos y actuaciones para ser cumplidos por la empresa. Además se trata de un método, que trata los objetivos de seguridad de la organización a largo plazo.

Dentro del ámbito en el que será aplicada los empleados, proveedores, colaboradores de la entidad, deben conocer y cumplir esta política, teniendo el rol que cada uno tiene asignado, en el caso de utilizar la información de la organización.

La política de seguridad se fundamenta en las siguientes reglas y estándares:

- Estándar ISO/IEC 27001:2013.
- Legislación relacionada con la seguridad de la información referida a la normativa de seguridad.
- Legislación relacionada con la privacidad de datos personales (LOPD, GDPR). [22]

No hay una descripción precisa respectiva, a los elementos del cuerpo normativo de seguridad. Los aspectos que caben resaltar son:

- Normativas: Se refiere a que el desarrollo de la política, se lleva a cabo en áreas precisas de la compañía.

- Política: Está alineada con los objetivos de la organización, el compromiso y obligación por parte de la empresa.

- Procedimientos: Fija las condiciones que se empleará la norma en la entidad.

2.4.1 Política del SGSI

La Dirección de TI de la empresa objeto de este estudio, la cual está representada por la *Gestión de la Seguridad y del cumplimiento normativo,* estipula su estrategia concerniente a la Seguridad de la información, y por ende, los datos personales como un aspecto de mucha relevancia, para brindar la consecución de los objetivos y continuidad del negocio.

Además la misma Dirección se compromete a conducir y promover, a todos los niveles involucrados en la Seguridad de la Información, el acuerdo al planteamiento en esta política, tanto al personal interno como externo de la organización y origine un SGSI (Sistema de Gestión en la Seguridad de la Información), que se puede articular con temáticas como requisitos legales o reglamentarios, seguridad de la organización en la gestión de proyectos, restricción de acceso a la información, gestión de claves, copia de seguridad de la información, reporte de vulnerabilidades, almacenar pruebas, planificación e implementación de la continuidad, en cuanto a la seguridad de los datos, mejoramiento continuo en la Seguridad de la Información, gestión y análisis de los riesgos, monitoreo regular sobre los procesos de la empresa, fomentación e implicación de las personas relacionadas con el uso de la información, etc., dirija la protección en cuanto a la información de la entidad y la tecnología empleada para su procesamiento, además de la distribución de los activos encontrados en la empresa, así se puede compartir en la red corporativa, con el fin de que todos los empleados tengan un mejor conocimiento sobre esta información.

Siguiendo con la necesidad de avalar la óptima seguridad posible, dentro de los servicios que se ofrecen, tratándose de la integridad, disponibilidad y confidencialidad de los datos, sistemas y/o comunicaciones dirigidos por la organización empleada para el desarrollo de este trabajo.

La política de seguridad tratada en este apartado tendrá un seguimiento anual, además cabe indicar, se ha realizado con base a las pautas mencionadas en el ***alcance del SGSI, políticas y objetivos de la organización,*** fue aceptada por la *Gestión de la Seguridad y del cumplimiento normativo*, en donde ésta área de la organización, podrá modificar la política establecida, cuando lo crea pertinente hacer para la mejora continua de la empresa.

2.5 Declaración de Aplicabilidad

Se trata de un documento donde se listan, los objetivos y controles a implementar en la empresa; los cuales son requeridos por la misma, de igual manera consta de la justificación pertinente, sobre los controles que no serán implementados.

La Declaración de Aplicabilidad (DdA) se lleva a cabo, después del tratamiento de riesgos, la cual se realiza posteriormente a la evaluación de riesgos. En donde el tratamiento tiene como fin, la definición de las acciones a ejecutar, para mitigar los riesgos identificados y analizados al hacer estos estudios.

De acuerdo a lo anteriormente tratado, el objetivo de la DdA es definir cuáles de los 114 controles (medidas de seguridad), recomendados por el Anexo A de la norma ISO 27001 son lo que se implementarán.

Lo que se quiere alcanzar por medio de la implementación de controles (objetivos de control), se hallan incluidos implícitamente en los controles elegidos.

En tal caso de que la empresa llegara a solicitar la certificación ISO 27001, el auditor tomará como base la Declaración de Aplicabilidad, visitará la compañía y verificará si los controles han sido implementados, tal como se detallan en la DdA, ya que se trata de un documento esencial en la ejecución de la auditoría física.

Si se lleva a cabo una buena redacción de este documento (DdA), puede ser de gran ayuda en la reducción de otros documentos, es decir, en la situación de justificar un control, donde puede resultar ser muy conciso, éste puede ser admitido en la DdA.

Los motivos por los cuales es de suma relevancia este documento son:

- En el desarrollo del tratamiento de riesgos, se identifican los controles que deben implementarse, los riesgos que se necesitan minimizar. Aunque en el DdA también se conocen controles requeridos por otras razones; ejemplos de ellos pueden ser, motivos legales, requerimientos contractuales, etc.

- El informe acerca de la evaluación de riesgos puede originarse muy extenso, por lo cual, un documento de esta índole no resulte verdaderamente funcional en el uso operativo diario. Por ello, la Declaración de Aplicabilidad es sucinto, de tal manera que puede exponerse ante la Alta Dirección y actualizada.

- Por último, el DdA debe documentar si cada control aplicado está implementado o no. Puede mostrarse como una estrategia eficaz, ya que la mayoría de los auditores buscan, describir cómo se *implementa cada control aplicable, como puede ser, refiriéndose a un documento (política, procedimiento, instrucciones de funcionamiento, etc.), otra forma es simplemente indicando el procedimiento vigente o el equipo que se utiliza.*

La DdA puede ser en realidad muy útil, porque ayuda a la organización a pensar en cómo implementar sus controles, tales como: comprar nuevos equipos, modificar un procedimiento, contratar empleados, entre otros. Éstas son algunas decisiones relevantes y a veces costosas, por tal razón, no es de asombrarse que se necesite de mucho tiempo para tomarlas.

En síntesis este documento facilita obtener una visión amplia, sobre lo que una empresa está llevando a cabo para salvaguardar su información, de acuerdo a lo que se determina en la norma ISO 27001:2013.

2.6 Procedimiento de Auditorías Internas

Algunos de los procesos más relevantes a realizar sobre el SGSI son: evaluar, realizar seguimiento del sistema (revisiones) y las mejoras que se van implementando. Para lo cual se concreta, con la ayuda de las ***auditorías internas*** que permiten hacer tal análisis.

De acuerdo a lo establecido en la norma ISO 27001, Anexo A, en donde se indica que está conformado por 114 controles, realizar una auditoría de forma correcta, se requiere de tiempo para auditar completamente un área de la empresa.

El sistema de gestión implantado con esta norma, ha de llevar a cabo una auditoría interna de manera regular, en la que se corrobore su adecuación, frente a los requisitos de la norma periódica, normalmente una vez al año.

Para este proceso no hay reglas de tiempo asignado, ya que depende de diversos factores, en donde se incluye la madurez del SGSI, tamaño de la compañía y la cantidad de hallazgos encontrados en la auditoría.

Esta labor puede ser ardua, de tal manera que existe una manera de hacer una auditoría eficaz, si se comparten responsabilidades de las auditorías ISO 27001, entre los diferentes auditores del equipo, como dividiéndose los controles entre ellos, de acuerdo a sus habilidades y puntos fuertes.

- 9 Control de acceso.
- 10 Criptografía.
- 11 Seguridad física y ambiental.
- 12 Seguridad operacional.
- 13 Seguridad de las comunicaciones.
- 14 Adquisición, desarrollo y mantenimiento del sistema.

O encargarse de requisitos más generales:

- 5 Políticas de seguridad de la información.
- 6 Organización de la seguridad de la información.
- 7 Seguridad de los recursos humanos.
- 8 Gestión de activos.
- 15 Relaciones del proveedor.
- 16 Gestión de incidentes de seguridad de la información.
- 17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.
- 18 Cumplimiento.

Algunos puntos claves para la preparación previa a la auditoría interna son:

- Cerciorarse de tener acceso a la información que sea necesite (hallazgos, procedimientos y políticas anteriores a la auditoría).
- Elaborar un listado de verificación de auditoría.
- Hacer un plan de auditoría.
- Establecer los tiempos para estar con los auditados, realizar el informe y fijar una reunión de seguimiento con los representantes del departamento.
- Requiere de una comprensión profunda de lo que se necesita en el Anexo A y en la organización.

Para lo cual, la auditoría interna puede realizarse por parte de un auditor interno o un auditor externo con experiencia. En este propósito, la norma en su versión 2013, elimina el requerimiento de "los auditores no deben auditar su propio trabajo", ubicando este punto en la cláusula 9.2.e, donde se fija que en el momento de elegir un auditor, se deben "asegurar la objetividad e imparcialidad del proceso de auditoría". [70]

La dirección de la empresa da la aprobación al plan de auditoría, y para su puesta en ejecución, razón por la cual, antes de realizar la visita a la organización, es preciso comunicar el plan y los objetivos de la sesión por adelantado, al igual que se debe informar a todos los departamentos a auditar, y a los mismos auditores internos. La forma contraria, no es una buena manera de iniciar una auditoría.

Se necesita comprobar, los auditados tienen claro la importancia que tiene el hecho, de realizar auditorías ISO 27001; lo cual es fundamental en el mantenimiento del SGSI.

Para cumplir con la auditoría, se necesita llevar un procedimiento documentado, donde se incluyen las responsabilidades de cada una de las partes, junto con los requisitos que se han de acatar en la auditoría interna, y los registros que se generan con la producción de la misma.

En síntesis, una auditoría interna al SGSI, se trata de hacer un análisis de las medidas de seguridad, considerada para la gestión de la misma, comprobando así, el funcionamiento de este sistema de gestión, donde a su vez, los resultados obtenidos de esta auditoría, serán las entradas para la verificación, por parte de la dirección acerca del SGSI. Donde su principal resultado, es el informe originado por el auditor interno, del cual se producirán acciones que ayudarán a eliminar las no conformidades detectadas, que redunden en un SGSI más seguro y gestiona eficazmente, la información con la que trabaja la empresa. [31]

Una vez se culmine la auditoría, el representante del departamento en cuestión debe determinar, una serie de medidas correctivas y programar, un seguimiento de la efectividad de la acción que se eligió para hacerse. [69]

Con base a ello, cabe indicar que la función primordial de la auditoría interna de un SGSI, el cual está basado en la ISO 27001 es, contribuir a la mejora continua del sistema y la gestión responsable de la información.

2.6.1 Objetivo de la Auditoría

Conocer el nivel de cumplimiento del SGSI en la empresa objeto de estudio académico, sobre los controles de las normas ISO 27001:2013 e ISO 27002:2013.

2.6.2 Alcance de la Auditoría

El alcance del SGSI se ha determinado de la siguiente manera: “Apoyo al proceso de Gestión de Seguridad de la Información”.

2.6.3 Áreas auditadas

Los ámbitos a auditar para la realización de este proceso, se listan a continuación:

- Tecnología
- Redes
- Administración
- Sistemas
- Recursos humanos

2.6.4 ¿Quién puede realizar una auditoría Interna ISO 27001?

Aunque la norma ISO 27001:2013 no establece los *requisitos* que debe cumplir un auditor interno, para la realización de una auditoría, la norma exige claramente, es la organización que se encarga de seleccionar a los auditores. De acuerdo a lo expuesto anteriormente, la misma empresa es la que determina los requisitos, puesto que si no se establecen, cualquier persona auditaría un SGSI.

Por lo tanto, los requisitos mínimos para un auditor interno ISO 27001 son:

Experiencia: Es recomendable que el auditor cuente con la experiencia precisa, además del conocimiento demostrable en Seguridad de la Información. Tomando como base lo anterior, por ser la norma ISO 27001 muy joven, existe la dificultad de hallarse auditores internos, con más de cinco años de experiencia demostrable, de ahí que se ha encontrado otra manera de dar una valoración en este tema, trata de estimar el número de sistemas implementados por el auditor líder, el cual como mínimo deberían ser tres proyectos.

Conocimientos: Obtener un amplio conocimiento de la norma ISO 27001 y los procesos de seguridad de la información. Estos conocimientos pueden ser adquiridos, a través de la formación y cursos a nivel de implementador, de la norma ISO 27001 deseablemente.

Seleccionando al Auditor Interno ISO 27001: Por lo tratado antes, se ha dado la necesidad de asentar requisitos para el equipo auditor de la norma ISO 27001. Lo cual permite avalar, que el auditor interno tenga la capacidad y experiencia requerida, para ejecutar de manera eficiente el trabajo por el que fue contratado. Tales conocimientos mencionados a evaluar, pasan por el dominio del ciclo de PDCA, basado en la norma ISO 27001, junto con los temas relacionados a la gestión de riesgos, y controles para la seguridad de la información. Sin embargo, no se debería descartar, la realización de evaluaciones para los candidatos, a ser una labor tan relevante.

En la práctica: En esta parte, se han presentado organizaciones, las cuales se limitan a exigir certificaciones, pero hay profesionales que no tienen estos documentos, sin embargo, tienen mucha experiencia debido a que ejecutan auditorías diariamente. Así que también resulta ser muy importante definir la experiencia, formación y conocimiento demostrable del auditor interno ISO 27001. [70]

2.6.5 Auditoría Interna de los controles en un SGSI

La auditoría interna se ha de planear, ejecutar, asegurando los objetivos de la empresa e imparcialidad, con base a lo considerado en el plan de auditoría de cada organización (preparación de la auditoría, realización de la auditoría, conclusiones de la auditoría, seguimiento, independencia de los auditores, responsabilidades de cada una de las partes y requisitos que se han de cumplir para la planificación de la auditoría), y lo indicado en la norma ISO 27001:2013. A partir de ahí, establecer si los controles y procedimientos del SGSI cumplen con:

- Requisitos tales como, la norma, legislación y normativa aplicables.
- Implantación y sostenimiento eficiente de los controles, generando el resultado esperado.
- Determinar los requisitos de seguridad de la información. [32]

De acuerdo como se establece en el punto A.18 Cumplimiento, apartado A.18.2 Revisiones de seguridad de la información, sección A.18.2.1 Revisión independiente de la seguridad de la información, indicado por la norma estándar antes mencionada.

El fin de la auditoría interna es verificar el funcionamiento del SGSI y esto conlleva, a obtener resultados que serán parte de las entradas, para el correspondiente análisis de la Dirección en el sistema y con lo cual, ayudará a una toma de decisiones.

2.6.6 Generación de hallazgos de auditoría

Con la ejecución de la auditoría, se van obteniendo hallazgos que ocasionan: no conformidades, conformidades, oportunidades de mejora u observaciones relacionadas con el tema de interés.

A continuación se tratarán en detalle las temáticas mencionadas anteriormente:

- No conformidades: Hace referencia al *incumplimiento* de un requerimiento estipulado por la norma estándar. Esta labor se debe verificar con una persona que representa al auditado, para que de esta forma, se adquiera el reconocimiento y se encuentren fundamentadas en las evidencias de la auditoría. De las cuales se derivan:

  - ***No Conformidad Menor:*** Desviación menos crítica con respecto a la *no conformidad mayor,* sin embargo, se debe tratar como ésta y cerrarla en un tiempo prudencial. Un caso de ello es el incumplimiento de uno o muchos controles, de un dominio de la norma por parte de la entidad.

- ***No Conformidad Mayor:*** En este aspecto, se trata de una desviación crítica, la cual se debe atender y cerrar de manera obligatoria, tomando como base las evidencias originadas. Esta no conformidad será adquirida por la empresa, en el caso de incumplir un apartado completo establecido por la norma.

- Conformidades: En esta parte se emplea el concepto de conformidad, vinculado al cumplimiento de un requisito de la norma. Se deben dar de manera breve, señalando las ubicaciones, funciones o requisitos que hayan sido auditados, en el momento de no contemplar no conformidades.

Un apunte relevante y que se debe tener en cuenta es, el auditor debe apartarse de una sección, en la que ha descubierto una no conformidad u observación, sin dar una justificación a la persona u organización auditada, y de esta forma, tener la completa certeza de una buena comprensión en lo expuesto.

- Observaciones: La observación es un poco menos crítica con respecto a la no conformidad menor. En caso de que el auditado quiera adquirir la certificación, este hallazgo no es obligatorio tratarlo, se atiende sólo como una sugerencia y en una nueva oportunidad, es decir, una próxima auditoría, el personal encargado de ella la puede emplear como ***no conformidad menor,*** pero esto ya lo decide el personal auditor.

- Oportunidades de mejora: Estas hacen alusión a circunstancias, en las que el auditor comprende, son un apoyo al sistema; por lo cual, no se admite como incumplimiento con los requisitos de la norma, frente a la situación que se está analizando. Van dirigidas a propuestas, de tal manera, la compañía decide si las acepta o no. El hecho de no considerar una oportunidad de mejora, no significa que se interprete como una no conformidad en la siguiente auditoría, ni siquiera aunque se trate de una observación.

2.7 Gestión de Indicadores

En esta sección se presentará una serie de indicadores, utilizados para la organización que está siendo objeto de este estudio, de tal forma que permita medir la efectividad, eficacia y eficiencia de la Seguridad de la Información en la empresa.

El fin de utilizar los indicadores para este análisis es, detectar y prevenir eventos e incidentes de seguridad.

2.7.1 Objetivo de la medición

Medir la efectividad, eficacia y eficiencia de los componentes de implementación y gestión. Donde los indicadores servirán como insumo, para el componente de mejora continua, permitiendo de esta forma, adoptar toma de decisiones para la mejora.

Los objetivos de los anteriores procesos de medición, en seguridad de la información son:

- Comunicar valores de seguridad a la entidad.
- Suministrar estados de seguridad que puedan ser empleados, como guía para las revisiones futuras, así, permita hacer mejoras concernientes a seguridad de la información y sirvan de apoyo, como nuevas entradas a auditar.
- Evaluar la efectividad de la implementación de los controles de seguridad.
- Valer como insumos, al plan de análisis y tratamiento de riesgos.

2.7.2 ¿Qué aporta un indicador?

Un indicador es una métrica general de evaluación, con respecto a la eficiencia o riesgo de un SGSI implementado, de acuerdo a lo establecido por la norma estándar ISO/IEC 27001. Permitiendo así, que el indicador lleve a cabo un seguimiento del compromiso, de la Alta Dirección en el tema de seguridad de la información.

Con esta labor se quiere presentar a la Alta Dirección un informe, en el tiempo establecido por la misma (mensual, trimestral o anual), para la gestión de la seguridad de la información y los sistemas que se encargan de operarla

Los indicadores más apropiados y que interesan a la organización, son aquellos vinculados a los dominios establecidos en el Anexo A y en sí, con la norma estándar ISO/IEC 27001:

- Continuidad del negocio.
- Respuesta ante incidentes.
- Documentación de las políticas, procesos, guías e instrucciones técnicas.
- Concienciación de los empleados.
- Gestión de riesgos.
- Control de la información saliente/entrante.
- Planes de seguridad.
- Mantenimiento y actualización del hardware y software. [33]

NOTA: El desarrollo de este punto está como anexo a este documento, se encuentra en el archivo ***2. Sistema de Gestión Documental****,* hoja de cálculo o pestaña llamada ***2.7 Gestión de Indicadores****.*

2.8 Revisión por parte de la Dirección

De acuerdo a lo establecido por la norma estándar ISO 27001:2013, la Alta Dirección tiene como compromiso, revisar de manera regular (no anual) el Sistema de Seguridad de la Información, en períodos flexibles, planificado de acuerdo a las políticas de cada empresa, como requisito y necesidad que surge para la seguridad de la información de la misma, como resultado después de la ejecución en el estudio de análisis de la gestión (monitorización, medición y auditoría interna), a su vez, obtener la certeza de su permanente correlación, vigencia y efectividad.

Los aspectos fundamentales que debe tener en cuenta la Dirección, en el momento de llevar a cabo esta revisión son:

- Revisión de los objetivos de seguridad de la información.
- Documentación y registro de los resultados obtenidos.
- Revisión de la política de seguridad de la información. [34]

La revisión por la Dirección debe contemplar las siguientes entradas:

- El **estado de las anteriores revisiones.** Efectuar una revisión sobre los compromisos que se adquirieron en las revisiones pasadas, para luego tomar las decisiones adecuadas dirigidas a su acatamiento.

- La **retroalimentación del rendimiento de la seguridad de la información,** como puede ser la retroalimentación de los usuarios, con quienes se pueden detectar los aspectos de incidencias relevantes, donde éstas afecten la prestación del servicio y ayude, en la definición de las acciones para la mejora en el incremento, de conformidad en los usuarios. Incluyendo también información referente a: no conformidades y acciones correctivas, medición de la monitorización y los resultados, resultados de auditoría y cumplimiento de los objetivos de seguridad.

- **Desempeño del Sistema de Seguridad.** Se hace una revisión con la ayuda del análisis de indicadores, u otros métodos de medición sobre los subsistemas integrados al SGSI, con respecto a la obtención de las metas planeadas y las acciones, con las cuales modificar las desviaciones que surjan. De la misma forma, se aprovecha para establecer la conformidad de los procesos.

- **Acciones correctiva y preventivas.** Identificar el estado de las dos clases de acciones (correctivas y preventivas) en su implementación, de acuerdo a los resultados generadas en las no conformidades reconocidas, y de esta manera, servir de guía en la toma de decisiones.

- **Cambios que conciernen al Sistema de Gestión.** Verificar los cambios que puedan alterar, a los subsistemas que conforman el Sistema, donde se deciden los actos a seguir para enfrentar tales cambios que se presentan.

- **Oportunidades para la mejora.** Precisar las proezas en la mejora constante del Sistema de Gestión.

- **Revisiones tanto de la política como de los objetivos del Sistema.** Se lleva a cabo un análisis para la confirmación en el cumplimiento de las políticas, objetivos y con base a los indicadores considerados en el estudio. [35]

En el siguiente apartado se da a conocer de manera resumida, la información de entradas para la revisión por parte de la Dirección:

A. INFORMACIÓN DE ENTRADAS PARA LA REVISIÓN
A.1 Estado de los compromisos de revisiones anteriores.
A.2 Contexto de la organización: Estado y Actualización.
A.3 Desempeño de los procesos y conformidad del servicio (trabajo para el cliente).
A.4 Información sobre el desempeño y eficiencia del SGSI.
A.4.1 Satisfacción del cliente y retroalimentación de las partes interesadas, incluido los requisitos legales.
A.4.2 Nivel en que se han obtenido los objetivos del SGSI.
A.4.3 Idoneidad de los procesos y conformidad del servicio.
A.4.4 Información de las no conformidades y acciones correctivas del período analizado.
A.4.5 Resultados del seguimiento y la medición.
A.4.6 Resultados de auditorías internas.
A.5 Operatividad de las acciones tomadas para afrontar riesgos y oportunidades en el sistema.
A.6 Condición de incidentes, acciones preventivas y correctivas.
A.7 Estados variables en el SGSI de índole legal.
A.8 Determinar las oportunidades de mejora para la próxima revisión.

Tabla 8. Entradas de revisión por parte de la Dirección.

2.9 Metodología de Análisis y Gestión de Riesgos

El análisis de riesgos estima los siguientes componentes:

- Activos: Elementos del sistema de información, o relacionados con el mismo y son de apoyo, para cumplir los objetivos, metas, misión de la organización.

- Amenazas: Hechos que afectan a los activos de la empresa.

- Protección: Son medidas para preservar los activos de las amenazas.

Con los componentes mencionados anteriormente, se considera lo siguiente:

- Impacto: Hace relación con los sucesos que puedan ocurrir.

- Riesgo: Peligro al que se está expuesto. [44]

La realización del procedimiento de análisis de riesgos, concede el estudio de los anteriores componentes de una manera planificada, para que así se puedan obtener resultados con argumentos, y continuar con la parte de tratamiento de los riesgos. Dicho en otras palabras, la *gestión de la seguridad de un sistema de información,* tiene relación directa con la *gestión de riesgos* y de esta forma, concede al análisis la comprobación de esta gestión.

2.9.1 Metodologías de análisis de riesgos

Las metodologías de análisis de riesgos se fraccionan de la siguiente manera:

I. *Metodologías de gestión del riesgo:* Están dirigidas a identificar, valorar y aplicar tratamiento de los riesgos, detectados durante el análisis.

II. *Métodos cualitativos:* Es el método más utilizado a nivel de análisis de riesgos, en la toma de decisiones sobre proyectos de compañías.
Es posible usarlos en caso de que el nivel de riesgo sea bajo, no haya necesidad de justificar el tiempo ni precisar de los recursos, para llevar a cabo un análisis completo.

III. *Métodos semi cuantitativos:* Se hace uso de una clasificación, en donde se tratan con términos como alto, medio, bajo o descripciones con más detalle de la probabilidad y la consecuencia.

IV. *Método cuantitativo:* En esta clase de métodos, se fijan valores de ocurrencia a los riesgos encontrados, con ello se calcula el nivel de riesgo.

V. *Metodologías de cuantificación:* El enfoque en este caso va orientado a las herramientas que tratan la cuantificación de riesgos, aplicando indicadores, de tal manera, permite medir el impacto que tienen los riesgos en las empresas, posteriormente se realizan acciones coordinadas para su tratamiento, gestión o eliminación. [73]

Entre las metodologías de cuantificación se encuentra ***Magerit,*** la cual fue preparada por el Consejo Superior de Administración Electrónica. Magerit es una metodología práctica, para tratar los riesgos (*análisis y gestión*) del Sistema de Información, conocido también con el nombre de ***"Proceso de Gestión de los Riesgos".***

Las siglas ***Magerit*** hacen referencia, a la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administración, para lo cual, comprende la fase AGR (Análisis y Gestión de Riesgos).

Magerit fue diseñada para las organizaciones que trabajan, con información digital y servicios informáticos. Por tal razón se incluyó en el análisis, para el desarrollo de este trabajo. Se destaca, la función esencial de esta metodología es, evaluar cuánto valor afronta una empresa, con respecto a un proceso y cómo lo protegerá. Además brinda apoyo en la planificación de tratamientos, y proyecta a las compañías en la auditoría, para los procesos de certificación o acreditación. [73]

El fin de Magerit se encuentra relacionado de manera directa, con la generalización del uso sobre los medios electrónicos, informáticos y telemáticos, los cuales son de gran ayuda en determinadas actividades, pero también presenta algunos riesgos, donde se busca mitigarlos con las respectivas medidas de seguridad. [53]

Magerit tiene como objetivos:

<u>Directos</u>

- Hacer que las personas encargadas de los sistemas de información, tomen conciencia sobre los riesgos que se pueden generar, y la necesidad de minimizarlos o eliminarlos.
- Brindar un método con el que se realice un análisis para estos riesgos.
- Encontrar y planear las respectivas medidas de seguridad, y así tener los riesgos controlados, es decir, en un estado aceptable.

<u>Indirectos</u>

- Dar apoyo a la empresa en procedimientos tales como auditoría, certificación o acreditación y evaluación.

Con lo mencionado anteriormente, se ha tratado de dar una homogeneidad en el tema referente a los informes, dentro de los cuales se recopila datos que servirán, de gran ayuda para la organización, llegar a determinaciones en un estudio de análisis y gestión de riesgos (modelo de valor, mapa de riesgos, evaluación de salvaguardas, estado de riesgo, informe de insuficiencias y plan de seguridad). [53]

Para el uso de procedimiento, existe la herramienta **PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos),** la cual fue desarrollada por el Centro Nacional de Inteligencia - Centro Criptológico Nacional, consta de librerías que posibilita la aplicación de Magerit, de tal manera que se pueda llevar a cabo el análisis y gestión de los riesgos en el marco de los criterios. [51]

El *análisis de riesgos* es parte de la *planificación* y se toman decisiones de tratamiento. Luego se materializa en la etapa de *implantación,* lleva a cabo monitores para evaluar que las medidas aplicadas, han sido las apropiadas para minimizar, controlar los riesgos y actuar de manera oportuna ante incidencias, dentro de un círculo de mejora continua. En otras palabras, esta metodología apoya en el estudio de los riesgos, los cuales soportan los Sistemas de Información y sugiere, las medidas apropiadas que deben adaptarse para controlar los riesgos.

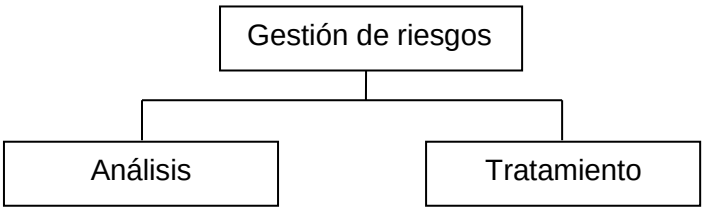


Figura 6. Gestión de riesgos. [44]

En la **figura 6** se muestra la fusión de las actividades de análisis y tratamiento en el proceso Gestión de Riesgos.

METODOLOGÍA	CARACTERÍSTICAS Y OBSERVACIONES
MAGERIT	En primera instancia, se trata de las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, tal método cubre la fase AGR (Análisis y Gestión de Riesgos). [36] Se realiza por el Consejo Superior de Administración Electrónica, en respuesta a la percepción de la Administración, y la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. [37] Trata en investigar los riesgos que soportan los SI y recomienda las medidas acertadas que deberían tenerse en cuenta para controlar estos riesgos. [38]
PASO A SEGUIR	**DESCRIPCIÓN**
I. 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: ◆ Tarea MAR.11: Identificación de los activos ◆ Tarea MAR.12: Dependencias entre activos ◆ Tarea MAR.13: Valoración de los activos [38]

II. Caracterización de las amenazas	Dicha actividad se encarga de identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación). De esta actividad se obtiene el informe de "mapa de riesgos". Adicionalmente incluye unas Sub-tareas: - Tarea MAR.21: Identificación de las amenazas - Tarea MAR.22: Valoración de las amenazas. [38]
III. 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: - Insuficiencias (o vulnerabilidades del sistema de protección). - Declaración de aplicabilidad. - Evaluación de salvaguardas Incluye las siguientes Sub-tareas: - Tarea MAR.31: Identificación de las salvaguardas pertinentes. - Tarea MAR.32: Valoración de las salvaguardas [38]
IV. Estimación del estado de riesgo	Esta actividad procesa todos los datos recopilados en las actividades anteriores para: - Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas - Realizar un informe del estado de riesgo: estimación de impacto y riesgo. Incluye las siguientes Sub-tareas: - Tarea MAR.41: Estimación del impacto. - Tarea MAR.42: Estimación del riesgo. [38]

Tabla 9. Metodología de análisis y gestión de riesgos seleccionada para este trabajo

A continuación se presenta un esquema de manera general para, señalando los pasos para el análisis de riesgos:

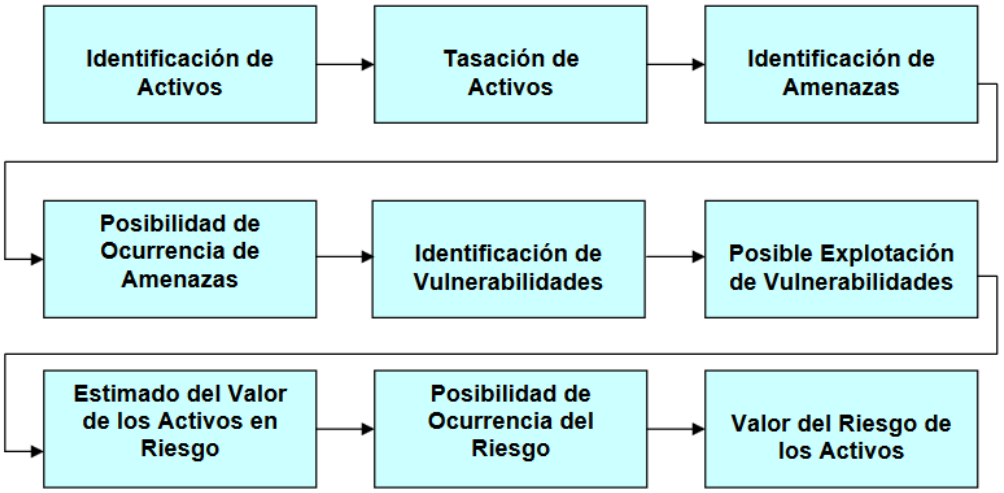


Figura 7. Metodología para el análisis de riesgos. [62]

2.9.2 Relación entre la norma ISO 31000:2018 y la metodología Magerit

De acuerdo a la norma **ISO 31000:2018**, en la que hace énfasis sobre la *condición dinámica de la gestión de riesgos,* lo cual requiere constantes revaloraciones y modificaciones para hacer esta labor más eficiente.

Con ello se ha observado, la norma proporciona los principios, las directrices para la identificación, el análisis y evaluación de riesgos, tiene mayor claridad en lo que tratan. Pero este nuevo estándar, no señala las herramientas o procedimientos exactos, puesto que el contexto de la empresa y la gestión de riesgos deben estar alineados. [45]

La norma ISO 31000:2018 constituye una serie de buenas prácticas, para brindar eficacia en la gestión de riesgos sobre todos los niveles, básicamente operativo, de gobierno y la confianza de los interesados.

Es claro, la norma ISO 31000:2018 es un procedimiento de aprendizaje, pues de esta forma la empresa podrá consolidar su desempeño y fortaleza. [72]

Magerit se encarga de implementar tal proceso, dentro de un marco de trabajo para la toma de decisiones, con respecto a los riesgos provenientes por la utilización de Tecnologías de la Información (TI), y siguiendo la normativa ISO 31000. Donde el propósito de esta norma es, aplicar y adaptar al público, ya sea que se trate de una entidad privada o pública, comunidad, asociación, grupo o individuo. En este aspecto cabe destacar, la norma ISO 31000 no tiene un propósito de certificación, pues simplemente aporta algunas directrices, para la implementación de una cultura organizacional; por ello, esta norma no es prescriptiva y su base la trata en la realidad de la organización: contexto interno/externo, objetivos, prácticas existentes y desempeño. [72]

En la Gestión de la Seguridad de la Información existe una parte esencial, la cual es conocer y controlar los riesgos encontrados, como una manera de salvaguardar la información de la empresa. De tal manera que las compañías

indagan sobre la manera de implementar, modelos de gestión de seguridad, adaptando así metodologías, las cuales ofrezcan un marco de trabajo definido, para agilizar la administración de riesgos y facilite su mejora.

Para tal caso, las normas ISO 27005 (coordina los riesgos asociados a la seguridad de la información de una entidad. *Apartado 1.4.5 ISO 27005:2018 de este informe)* e ISO 31000 son los estándares más conocidos para la gestión de riesgos, encontrándose alineados con elementos del marco de referencia de la entidad (comprensión de la gestión de la organización, contexto y objetivos), para proporcionarle un enfoque, en cuanto a la implementación de herramientas y metodologías, que pueden solventar las necesidades fundamentales, de la administración de riesgo en sus sistemas de información. [71] [72]

El enfoque basado en riesgos de la ISO 31000:2018, evalúa y adapta continuamente la gestión de riesgos.

Con respecto a su proceso, la norma determina:

- Establecer el contexto.
- Definir los criterios de los riesgos.
- Realizar una evaluación estructurada de los riesgos.
- Identificar el tratamiento apropiado para los riesgos.

De esta manera, ayuda a mejorar el desempeño del sistema de gestión y a su vez la organización, en cuanto a su alcance y objetivos se refiere. [72]

Es un complemento para las demás normas establecidas, de tal forma, contribuye a la gestión de riesgos e incremento en la seguridad.

2.9.3 Visión general del proceso de gestión de riesgos

Se conoce que la gestión de riesgos, está distribuida en una serie de pasos organizados en las normas ISO.

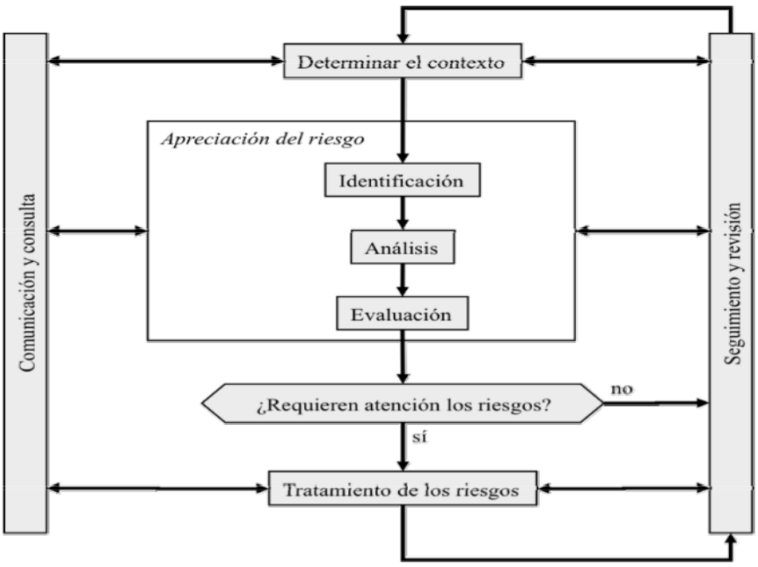


Figura 8. Proceso de gestión de riesgos (Fuente ISO 31000). [44]

- Comunicar y consultar: Hace referencia al trato con los interesados tanto a nivel interno como externo, dependiendo de cada etapa del proceso de gestión de riesgos.

- Establecer el contexto: Determinar los contextos interno y externo de este proceso, en donde se ejecutará el resto del mismo.

- Identificar riesgos: Corroborar los interrogantes ***qué, por qué y cómo*** pueden manifestarse las circunstancias, para emplearse en el siguiente análisis.

- Analizar riesgos: Establecer controles existentes y considerar los riesgos, en términos de consecuencias y probabilidades dentro del contexto de los controles.

- Evaluar riesgos: Realizar una confrontación entre niveles estimados de riesgos y criterios preestablecidos.

- Tratar riesgos: En caso de riesgos de poca relevancia, aceptarlos y monitorearlos. Hecho contrario, realizar las acciones de desarrollo e implementación de un plan de gestión preciso, en los que se admita consideraciones y reducción de posibles pérdidas.

- Monitorear y revisar: Se requiere hacer un seguimiento efectivo, en todas las etapas del proceso de gestión de riesgos, ya que es de gran relevancia para la mejora continua. [43]

Un desglose del proceso de gestión de riesgos, para las decisiones que se dan en caso del tratamiento de riesgos, se muestra a continuación:

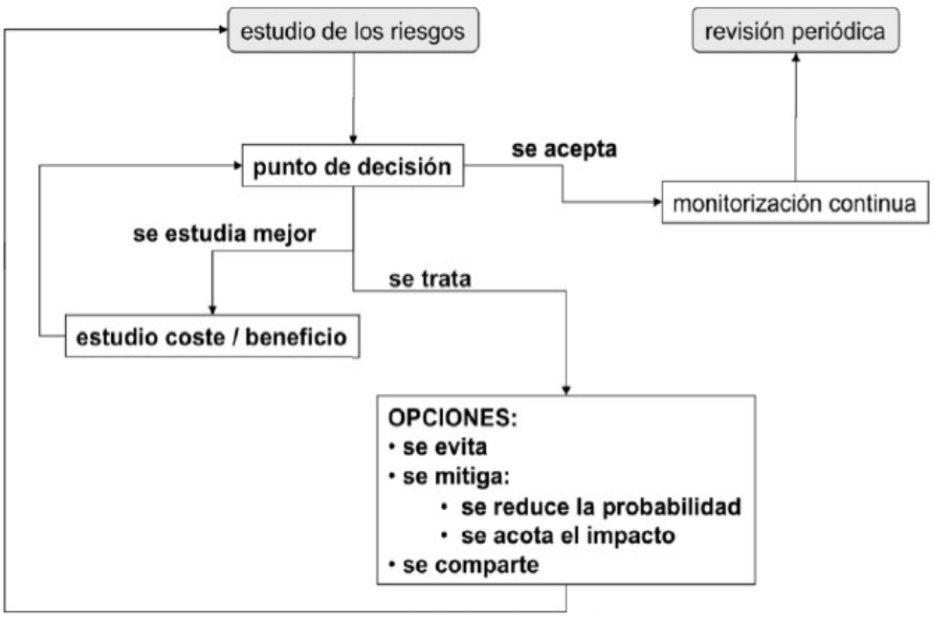


Figura 9. Decisiones de tratamiento de los riesgos. [51]

2.9.4 Aplicación de la metodología, métodos y procesos para el análisis de riesgos en este caso

Dado que los riesgos no presentan el mismo origen ni la misma naturaleza, surgen diversas estrategias para su gestión. Aunque existen otros factores, los cuales inciden significativamente como lo pueden ser: tamaño de la entidad, número de empleados, estructura, actividad de producción y el sector en el que se desenvuelven.

Esto ha hecho, se desarrollen metodologías de análisis propias de un sector o especialidad, cuyo objetivo es la identificación, valoración, tratamiento y monitoreo de los riesgos asociados a una actividad, función o proceso.

Teniendo en cuenta, el análisis de riesgos es una aproximación metódica y un apoyo para establecer el riesgo. [10]

Como se mencionó anteriormente, la metodología seleccionada para la realización del análisis de riesgos es ***Magerit,*** y teniendo esta metodología como base, se siguieron los pasos planteados por la misma:

a. Identificación de los activos de la organización (Caracterización de los activos – Tabla 7 – Metodologías de análisis de riesgos), los cuales se dividen en los siguientes grupos:

   - *Activos de información.* Datos digitales, activos tangibles, activos intangibles, software de aplicación, sistemas operativos.
   - *Activos físicos.* Infraestructura de TI, controles de entorno de TI, hardware de TI, activos de servicios de TI.
   - *Activos humanos.* Empleados, externos.

b. Valoración de activos (Caracterización de los activos), donde se utilizan campos como:

   - Identificador: Código que permite identificar de manera unívoca el activo.
   - Nombre: Nombre del activo.
   - Descripción: Breve descripción del activo o función que desempeña.
   - Tipo: Clasificación de los activos (aplicación, datos, software, lógico, físico, hardware, servicio).
   - Clasificación.
   - Responsable: Persona en concreto o departamento, responsable del activo que está utilizando.
   - Valor: Número equivalente a la definición, de acuerdo al criterio estipulado en la escala para valoración de activos.

Para este último, se emplea el método semi cuantitativo (ver 2.9.1 Metodologías de análisis de riesgos), determinando los siguientes valores, de acuerdo a sus respectivos criterios planteados para cada uno:

- Muy Alto. 10. Perjuicio muy grave a la organización.
- Alto. 7 a 9. Agravio grave a la organización.
- Medio. 4 a 6. Daño importante a la organización.
- Bajo. 1 a 3. Daño menor a la organización.
- Muy Bajo. 0. Pérdida irrelevante para la organización.

Con esta estimación, se busca conocer los activos más vulnerables, los cuales puedan perjudicar a la empresa, de manera muy considerable, significativa o moderada, ya que estos criterios se determinan como los más relevantes, respecto a la continuidad del negocio y tal valoración, sea un gran apoyo en este estudio y determinante, en las decisiones de la Alta Dirección.

c. Identificación de amenazas (Caracterización de las amenazas – Tabla 7) Las amenazas son "cosas que suceden", de todo lo que puede presentarse, existe el interés por los activos, en tal caso de ocurrirles algo y causar daño, además están expuestos los activos de la organización. Para tal caso, las amenazas se agrupan de la siguiente manera:

    - Desastres Naturales: Fuego, Daños por agua, Desastres Naturales.
    - Origen Industrial: Corte de suministro eléctrico, Condiciones Inadecuadas de temperatura y/o humedad, Fallo de servicios de comunicación.
    - Errores y fallos no intencionados: Errores de los usuarios, Errores del administrador, Errores de monitorización, Errores de configuración, Difusión de software dañino, Alteración de la información, Introducción de información incorrecta, Destrucción de la información, Alteración de la información, Introducción de información incorrecta, Destrucción de información, Vulnerabilidades de los programas (Software), Caída del sistema por agotamiento de recursos.
    - Ataques intencionados: Manipulación de la configuración, Suplantación de la identidad del usuario, Abuso de privilegios de acceso, Difusión de software dañino, Acceso no autorizado, Análisis de tráfico, Modificación de la información, Introducción de falsa información, Corrupción de la información, Destrucción de la información, Divulgación de información, Manipulación de programa, Robo, Ataque destructivo, Extorsión e Ingeniería social.

d. Valoración de las amenazas (Caracterización de las amenazas – Tabla 7) Hace referencia, cuando un activo termina siendo víctima de una amenaza, no resulta afectado en todas sus dimensiones ni en el mismo costo.
Posteriormente el estudio que se hace en este apartado se trata, por los anteriores grupos de amenazas mencionados anteriormente, valorando cada uno con base a una escala en relación con el método cuantitativo (2.9.1 Metodologías de análisis de riesgos), donde se asignan valores cualitativos, de acuerdo a la frecuencia de la amenaza:

    - *Extremadamente frecuente*: Una vez al día.
    - *Muy frecuente*: Una vez cada 15 días.
    - *Frecuente*: Una vez cada dos meses.

- *Poco frecuente*: Una vez cada seis meses.
- *Muy poco frecuente*: Una vez al año.
- *Nada frecuente*: Menos de una vez al año.

e. Valoración de vulnerabilidades (Caracterización de las salvaguardas. Tabla 7) Consiste en realizar una estimación de las insuficiencias, o vulnerabilidades del sistema encontradas durante el análisis, las cuales se trataron con valores cuantitativos, teniendo como guía dos criterios que se aplicaron:
    - 10: Muy alta. Daño muy grave a la organización.
    - 7-9: Alta. Daño grave a la organización.
    - 4-6: Media. Daño importante a la organización.
    - 1-3: Baja. Daño menor a la organización.
    - 0: Muy baja. No es irrelevante a efectos prácticos.

f. Declaración de aplicabilidad – Statement of Applicability. SoA (Caracterización de las salvaguardas. Tabla 7-2.5 Declaración de Aplicabilidad). Conjunto de salvaguardas, donde se muestra si son aplicables al sistema de información bajo estudio, o son de interés.

Es un informe en el que se recopilan, las contramedidas que se contemplan necesarias, para defender el sistema de información, el cual está siendo objeto de estudio. [10]

Con lo mencionado anteriormente, se puede indicar brevemente, el SoA reúne qué controles aplican en la organización y cuáles no.

Donde aquellos controles que sí aplican, se deben incluir los objetivos de control, descripción, razón para su selección/aplicación y la referencia al documento en el que se desarrolla su implantación.
Los controles que no aplican, es necesario señalar el motivo de su exclusión. Este apartado suele ser relevante, puesto que en la fase de certificación del sistema, éste será uno de los documentos que revisará el auditor con mucho cuidado.

Para seleccionar un control, se debe tener en cuenta los siguientes aspectos:

- Coste del control, con respecto al coste del impacto que afectaría al activo a salvaguardar, en caso de ser dañado y el valor del activo en esta circunstancia.
- La necesidad de disponibilidad del control.
- Qué controles ya existen.
- Qué supondría su implantación y mantenimiento, en los aspectos económico y humano.

Una vez se hayan tomado las respectivas decisiones, el paso a seguir es el de implantación, la cual es una fase que necesita tiempo y recursos de la organización.

Por lo tanto, la implantación de los controles y las salvaguardas más técnicas, van a requerir apoyo del personal encargado de tales funciones. Ya que los controles

organizativos se encarga la Alta Dirección, con la toma de decisiones correspondientes.

De los controles seleccionados, no resulta ser fundamental, desarrollar un procedimiento o documento para cada uno de ellos, en tal caso lo más recomendable es agrupar diversos controles para sacar más provecho al sistema.

Los controles implantados deben ser monitoreados, para corroborar su funcionamiento y obtener los resultados deseados. Esta revisión se tiene que ejecutar por parte de la persona encargada del activo, de manera regular en función de la criticidad y el valor que representa, el mismo para la empresa.

Resulta de gran relevancia, determinar previamente objetivos e indicadores, con los que se podrán hacer las mediciones de un buen funcionamiento, respecto al correcto desempeño de los controles implantados. [75]

g. Evaluación de riesgos (Estimación del estado de riesgo. Tabla 7). Apoya en el estudio de comparativa, entre los niveles de riesgos detectados y los criterios de riesgo predispuestos. Se prosigue con la priorización de los riesgos hallados. En esta parte, se establece la "probabilidad" de materializarse el riesgo, con lo cual se quiere indicar, la valoración del riesgo incluye un análisis en donde intervienen, la probabilidad de ocurrencia y el efecto en los resultados. Estos últimos pueden darse en valores cualitativos o cuantitativos, pero en el caso de realizarse en términos de costo, llevar a cabo esta labor con una evaluación cualitativa es más sencilla y económica. [55]

Este punto se lleva a cabo de la siguiente manera:

- Se continúa agrupando por tipo de amenaza, pues de esta forma se podrá comprender, qué desastre(s) se deben priorizar para un mayor control y mantener en estado aceptable el sistema, en cuanto a los riesgos que resultan ser la parte vulnerable para la empresa y los cuales necesitan de un pronto tratamiento.
- Se asignan los campos de probabilidad, impacto y riesgo.
- A su vez, el campo de probabilidad tendrá otros subcampos, de acuerdo a la escala con la que se trabaja en esta sección. Alto=3; Medio=2; Bajo=1.
- Para obtener el impacto del activo, se asigna los anteriores valores de la escala, a las dimensiones: A (Autenticación), C (Confidencialidad), I (Integridad), D (Disponibilidad), T (Trazabilidad), se hace la suma correspondiente de todos y luego se divide por el total de dimensiones, 5 (obteniendo así, el promedio de riesgo con respecto a los criterios establecidos: A, C, I, D, T), para obtener el *Total Cuantitativo* y *Total Cualitativo,* esto con el fin de clasificar los riesgos para priorizarlos y la Alta Dirección tenga claridad en la toma de decisiones.

Total Cuantitativo= (Valor(A) + Valor(C) + Valor(I) + Valor(D) + Valor(T)) / 5

(3.4.7 Evaluación de riesgos. Tabla 21. Dimensiones de la seguridad de la información. Fundamentado en la metodología Magerit [41].)

Total Cualitativo -> Bajo (Si total cuantitativo es 1)
Medio (Si total cuantitativo es 2)
Alto (Si total cuantitativo es 3)

Y con estos datos, realizar los cálculos para conocer el *Riesgo.*

NIVEL DE RIESGO = IMPACTO * PROBABILIDAD.

Llegado a este punto, se evalúa el riesgo y de acuerdo al impacto que recibe el mismo, se clasifica de la siguiente manera: Riesgo <=4 (el riesgo se considera de poco impacto); Riesgo > 4 (el riesgo se considera de alto impacto y debe tratarse inmediatamente).

Ver 3.4.7 Evaluación de riesgos. Tabla 20. Criterios de aceptación del riesgo. [41]

h. Nivel de riesgo aceptable (Estimación del estado de riesgo). Trata de que un riesgo sea estimado o mitigado, la organización considera, pueda continuar con estos riesgos (no tratarlos) y por ello, terminan aceptándolos, pues no generarán perjuicio alguno. Dependiendo de que se encuentre o no en el umbral de aceptación, si están sobre este valor, se tratarán (*Tratamiento de riesgos).* Para lo cual, la Alta Dirección toma la decisión de fijar el nivel de riesgo aceptable. En este caso se ha optado porque el nivel de riesgo aceptable sea de 3, así que, todo riesgo <=3 es aceptado. (*3.4.9 Nivel del riesgo aceptable).*

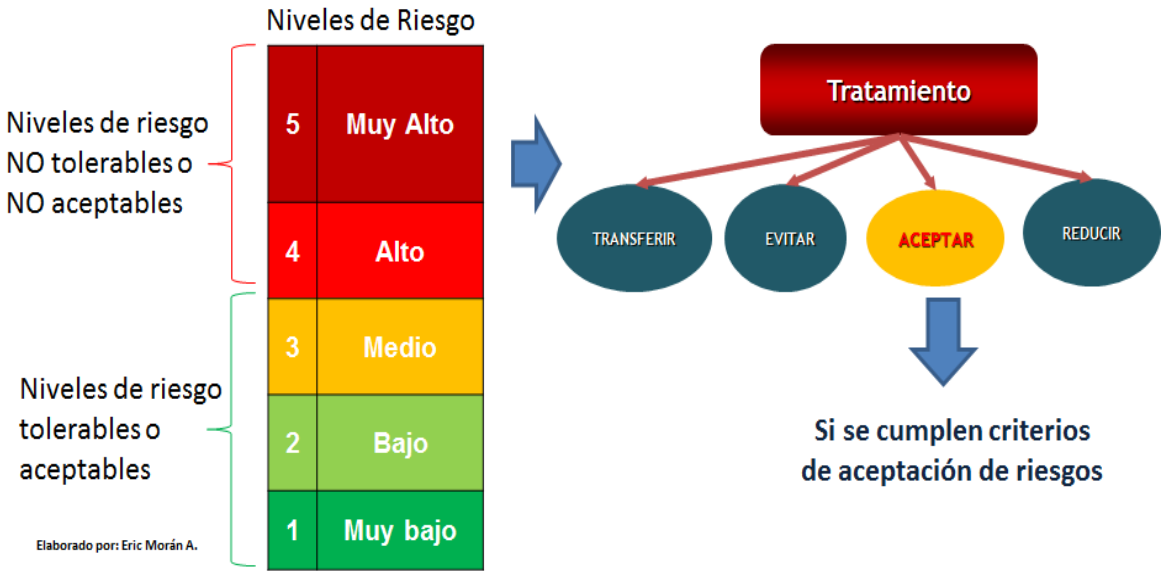


Figura 10. Niveles de riesgo. [52]

i. Tratamiento de riesgos (Ver Estimación del estado de riesgo. Tabla 7. Metodologías de análisis de riesgos) Consiste en definir el tratamiento y/o monitoreo, respecto a los riesgos determinados anteriormente y al nivel de aceptación fijado por la entidad, desarrollando e implementando estrategias y planes de acción precisos, para mantener el riesgo dentro del umbral o nivel de riesgo de aceptación.

Magerit como metodología, facilita un tratamiento sistemático y homogéneo, con lo que resulta primordial, para comparar opciones alternativas y seguir la evolución de los sistemas.

Cuando se ha realizado la valoración correspondiente, con el fin de establecer la eficacia de los controles fijados, para mitigar los riesgos hallados.

Así que, cuando los controles sean más eficientes y la gestión de riesgos resulte de manera afirmativa, el valor del riesgo neto tenderá a minimizar.

Para este caso, se sigue trabajando por grupos de amenazas, como se ha podido observar antes, para cuyos campos a tratar son:

- Amenazas (Grupo). Con el objetivo de tener siempre en cuenta los indicios de mayor impacto, para los activos de la organización, de acuerdo a la clasificación estipulada en el punto 3.4.3 Identificación de amenazas.

- Riesgo. Pues de esta manera se irá dando prioridad a los riesgos que la necesitan, para actuar de manera inmediata.

- Dominios de los controles. Tener una claridad qué dominio se vuelve más común, para clasificarlos de tal manera que se pueda tratar los riesgos y reconocer, los controles necesarios que ayudarán en la mitigación. Es decir, se puede dar el caso, varios controles de un mismo dominio o se puedan emplear controles comunes, para diversos riesgos.

- Objetivos de los controles. Reconocer y constatar, los propósitos de aplicar tales controles para dichos riesgos.

- Controles (Anexo A, ISO 27001:2013). Es la manera de establecer los salvaguardas sobre cada riesgo.

- Responsable (Departamento o persona directa). Es una manera de contactar con la persona o departamento encargado, del área en donde se presenta el riesgo y acordar el tratamiento que se va aplicar.

- Acciones a ejecutar. Son las actividades que se van a llevar a cabo, para tratar la amenaza generada, con base a los objetivos y controles que se van aplicar.

- Recursos a necesitar. Una vez determinada las acciones, se necesita conocer los recursos necesarios, para desempeñar las actividades mencionada antes.
- Opción para tratar el riesgo. Se refiere a las opciones del tratamiento de riesgo, las cuales son: transferir, mitigar, eliminar y aceptar. Esto de acuerdo a las decisiones que tome la Alta Dirección.

j. Riesgo residual (Ver Estimación del estado de riesgo. . Tabla 7. Metodologías de análisis de riesgos). Este es el último paso a realizar, de acuerdo a lo que está establecido por la metodología Magerit. Consiste entre la relación del grado de manifestación de los riesgos inherentes (o simplemente riesgo), y la gestión de mitigación de riesgo determinada por la Alta Dirección.

Tomando como base el análisis y el riesgo residual, se pueden tomar decisiones como la de seguir o declinar la actividad, de acuerdo a lo señalado por el nivel de riesgo, reforzar o si es necesario implantar nuevos controles.

A continuación se indica la forma en que se ejecutó este cálculo.

- Se determinaron parámetros como: Riesgo y el grupo de amenaza, en donde se encuentran los riesgos que están por encima del umbral (nivel de riesgo aceptable), el cual fue definido por la decisión tomada de la Alta Dirección (3).
- Luego está el nivel de riesgo (riesgo inherente), porque se requiere conocer, para el cálculo del riesgo residual.
- Sigue el tipo de medida de control, en el que se puntualizan los controles aplicables al riesgo, puesto que se necesitan para la valoración, la cual se ubica en el campo “efectividad”.
- El siguiente término a utilizar es, “promedio”, en el que se coloca el valor resultante, entre la sumatoria de efectividad de los controles y se divide por el número total de los mismos.
- Por último, el parámetro de riesgo residual, cuyo cálculo resulta después de dividir el nivel de riesgo con el promedio.

Por último se tuvo como referencia la norma ISO 31000:2018, para la realización del análisis o proceso de gestión de riesgos, para ir marcando directrices junto con la metodología Magerit.

Debido a que la norma se enfoca, en la gestión del riesgo en las organizaciones y es un apoyo, para establecer todos los objetivos alcanzables, tomando decisiones basadas en hechos.

La implementación de un Sistema de Gestión de Riesgos, por tanto, debe seguir una serie de pasos para que sea eficaz y cumpla con los objetivos trazados. [73]

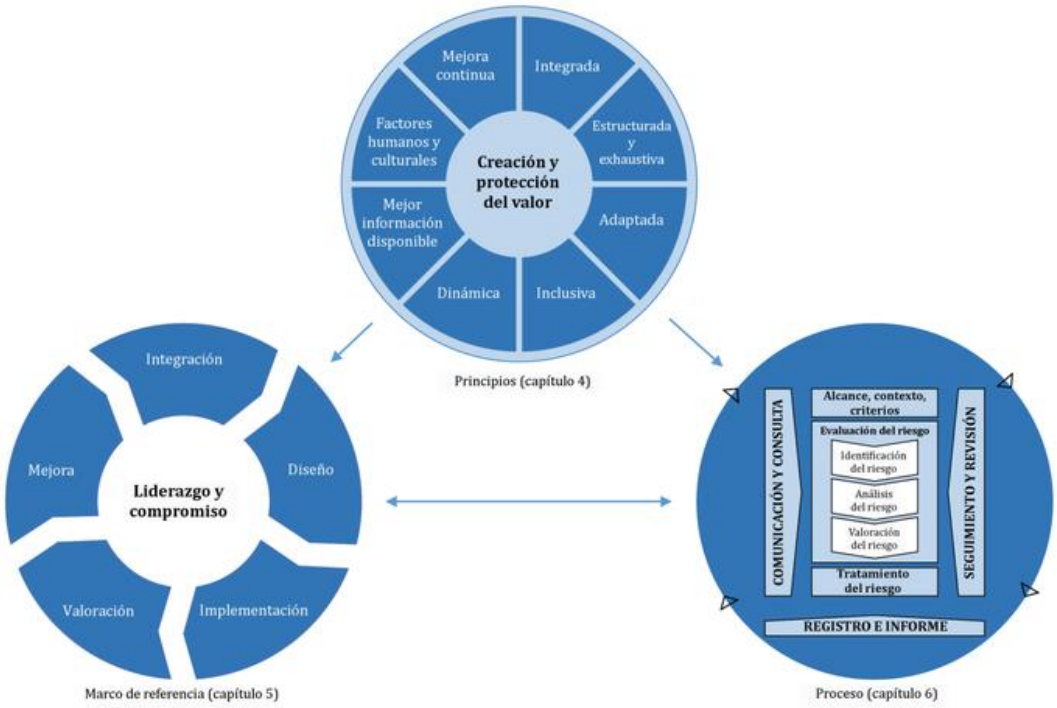


Figura 11. Principios, marco de referencia y proceso. ISO 31000:2018 [74]

Es necesario conocer la documentación formal y exacta, requerida para la implementación de un SGSI en una compañía, además cumpla con el estándar referente al tema de interés en este trabajo.

Con base a la última revisión de la norma ISO/IEC 27001:2013, se tratarán en la siguientes listas los documentos obligatorios y aquellos que comúnmente se suelen utilizar, en la implementación ISO 27001.

2.10 Documentación del SGSI

2.10.1 Documentos y registros requeridos por la ISO 27001:2013

La cuantía y precisión con respecto a la documentación requerida en esta gestión, se desarrolla de acuerdo al tamaño y exigencias de seguridad de la empresa, en otras palabras, puede ser que una docena de documentos sea apto al tratarse de una entidad pequeña, por otro lado, quizás para una organización grande resulte idóneo, tener cientos de documentos en su SGSI.

Sin embargo para el estudio académico en cuestión y con base a la norma ISO 27001:2013, los documentos que se desarrollan son:

- ✓ Alcance del SGSI.
- ✓ Política del SGSI.
- ✓ Metodología de evaluación y tratamiento de riesgos.
- ✓ Declaración de aplicabilidad.
- ✓ Tratamiento de riesgo.
- ✓ Definición de roles y responsabilidades.
- ✓ Inventario de activos.

- ✓ Procedimiento de Auditorías Internas.
- ✓ Gestión de Indicadores.
- ✓ Políticas y objetivos de la organización.
- ✓ Análisis y gestión de riesgos.

A continuación se listan los documentos y registros que son solicitados por la norma estándar ISO 27001:2013, pero cabe recordar, como se mencionó antes, la documentación necesaria depende de los requerimientos de la empresa.

Documentos	***ISO 27001:2013 (Cláusulas)***
Alcance del SGSI.	4.3
Política y objetivos de la empresa.	5.2 y 6.2
Metodología de evaluación y tratamiento de riesgos.	6.1.2
Declaración de aplicabilidad.	6.1.3.d
Plan de tratamiento de riesgo.	6.1.3.e y 6.2
Informe sobre evaluación y tratamiento de riesgos.	8.2 y 8.3
Definición de roles y responsabilidades de seguridad.	A.7.1.2 y A.13.2.4
Inventario de activos.	A.8.1.1
Uso aceptable de los activos.	A.8.1.3
Política de control de acceso.	A.9.1.1
Procedimientos de operación para gestión de TI.	A.12.1.1
Principios de ingeniería de sistemas seguros.	A.14.2.5
Política de seguridad para proveedores.	A.15.1.1
Procedimiento para gestión de incidentes.	A.16.1.5
Procedimientos de Continuidad de negocio.	A.17.1.2
Requerimientos legales, regulatorios y contractuales.	A.18.1.1

Tabla 10. Documentos requeridos en la ISO 27001:2013 [24].

Registros	***ISO 27001:2013 (Cláusulas)***
Registros de formación, habilidades, experiencia y calificaciones.	7.2
Seguimiento y resultados de medición.	9.1
Programa de auditoría interna.	9.2
Resultados de auditorías internas.	9.2
Resultados de la Revisión por Dirección.	9.3
Resultados de acciones correctivas.	10.1
Registros de las actividades de usuario, excepciones y eventos de seguridad.	A.12.4.1 y A.12.4.3

Tabla 11. Registros obligatorios en la ISO 27001:2013 [24].

2.10.2 Documentos no obligatorios

También existen documentos, aunque resultan ser no obligatorios, se pueden usar en la implementación de la ISO 27001, principalmente para el caso de los controles de seguridad del ***anexo A.***

Se reconoce que tales documentos no son de obligatoriedad, pero son los que regularmente se utilizan en el caso expuesto anteriormente:

Documentos	***ISO 27001:2013 (Cláusulas)***
Procedimiento para control de documentos.	7.5
Controles para la gestión de registros.	7.5
Procedimiento para auditoría interna.	9.2
Procedimiento para acciones correctivas.	10.1
Política BYOD (Bring Your Own Device = Trae tu propio dispositivo).	A.6.2.1
Política de dispositivo sobre dispositivos móviles y tele-trabajo.	A.6.2.1
Política de clasificación de la información.	A.8.2.1, A.8.2.2 y A.8.2.3
Política de claves.	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 y A.9.4.3
Política de eliminación y destrucción.	A.8.3.2 y A.11.2.7
Procedimientos para trabajo en áreas seguras.	A.11.1.5
Política de pantalla y escritorio limpios.	A.11.2.9
Política de gestión de cambios.	A.12.1.2 y A.14.2.4
Política de Copias de seguridad.	A.12.3.1
Política de transferencia de información.	A.13.2.1, A.13.2.2, y A.13.2.3
Análisis de impacto en el negocio (BIA).	A.17.1.1
Plan de pruebas y verificación.	A.17.1.3
Plan de mantenimiento y revisión.	17.1.3
Estrategia de continuidad de negocio.	A.17.2.1

Tabla 12. Documentos no obligatorios [24].

3. Análisis de riesgos (Risk analysis)

Sin duda alguna, para comenzar a trabajar en la seguridad de la información de una empresa, el *análisis de riesgos* es una de las secciones más importantes para ejecutar, concerniente a los temas como definición de proyectos y la mejora de seguridad.

Desde hace mucho tiempo se tiene conocimiento, con respecto a que la ***Información*** es el activo de más alta importancia para cualquier organización. Pero debido al avance de la tecnología, para ofrecer eficacia y facilitar la realización de los procesos, en un tiempo muy corto, la empresas se hallan propensas a un alto nivel de riesgo y amenazas, por el uso necesario tanto de las tecnologías de la información como de las comunicaciones.

A partir de aquí se ha podido aprehender, la importancia que se requiere determinar métodos para establecer, analizar, valorar y clasificar los riesgos, de tal manera que se puedan llevar a cabo procedimientos, los cuales sirvan de apoyo para controlar y reducir los riesgos que se presentan.

En otras palabras, la gestión de riesgos es un proceso utilizado, que ayuda a proteger la información de una entidad, y para cumplir con ello, debe realizarse de manera periódica, de esta forma, mitigar los costos operacionales originados con la interrupción de labores, y pérdida del activo mencionado antes. [41]

Las medidas a tener en cuenta en el proceso de ***gestión de riesgos,*** están definidas de la siguiente manera:

Figura 12. Proceso de análisis o gestión de riesgos [41]

3.1 ¿Qué es y por qué hacer un Análisis de riesgos?

La definición más apropiada sobre el concepto de ***análisis de riesgos*** se encarga de indicar, como el proceso para entender la esencia del riesgo y así, fijar el nivel del mismo. [40]

También se considera una herramienta de gestión, que sirve de apoyo a la Alta Dirección en la toma de decisiones. [44]

Se sabe bien que una parte del SGSI lo conforma el análisis de riesgos, con el que se conoce las principales vulnerabilidades de sus activos de información, y se identifica las amenazas que explotan a dichas irregularidades. Así la organización podrá formalizar tanto medidas preventivas como correctivas viables, que ayuden a garantizar buenos niveles de seguridad de la información en la empresa.

Para analizar riesgos, existen muchas metodologías, pero se tiene claro que todas inician a partir de *la identificación de activos de información,* donde esta operación trata los recursos involucrados en la seguridad de la información, la cual empieza por los datos, hardware, sigue hasta llegar con los documentos escritos y recurso humano. De tal manera, es sobre ellos que se procede a la determinación de amenazas o riesgos y vulnerabilidades.

Dado esto, se define el concepto de ***amenaza,*** como un hecho que puede de una u otra manera, afectar el activo de información de la compañía y tiene mucha analogía, ya sea con el recurso humano, fallas técnicas o sucesos naturales. Tales acontecimientos pueden presentarse como: ataques informáticos externos, infecciones con virus (malware), tormentas eléctricas, errores u omisiones del personal que trabaja en la entidad, terremotos, entre otros casos.

Siguiendo con los términos que se relacionan con el análisis de riesgos, está también el criterio de ***vulnerabilidad,*** consiste en una singularidad sobre un activo de información, la cual traza un riesgo ligado a la protección de este. Tal es el caso en el que surgen amenaza y vulnerabilidad, así se llega a exponer la pérdida de este activo para la entidad.

Frente a esta situación, se debe considerar un análisis y así, establecer qué riesgos son los que requieren de atención prioritaria para la organización. Dicho análisis se demarca, en conceptos de *posibilidad de ocurrencia del riesgo* e *impacto.* Este último se evalúa en función de factores como: pérdida económica, reputación de la empresa o nivel de daño debido a pérdida de la información.

Una vez identificadas las amenazas en el análisis de riesgos, es relevante señalar los *controles,* tanto para reducir la posibilidad de ocurrencia de la amenaza como su impacto.

Tras este análisis de reconocimiento en riesgos, la organización los puede tratar asignando cualquiera de los siguientes estados: ***aceptar, transferir, mitigar o evitar.*** Es así, en caso de que un riesgo no sea altamente crítico para la compañía, el estado de control estipulado podría ser manejado como **aceptado,** con lo cual se da a conocer, está presente un riesgo y es necesario hacer un seguimiento. Pero si tal riesgo significa una grave amenaza para el activo de la información, la decisión es **transferir o mitigar** dicho riesgo.

El fin del análisis de riesgos es asegurar a la entidad, la certeza de conocer tales riesgos y controles para tratarlos, con esta acción se podrá saber las medidas a tomar frente a un evento materializado, o evitar que se concrete. [42]

3.2 ¿Cuándo procede analizar y gestionar los riesgos?

Se aconseja realizar el análisis de riesgos sobre cualquier tipo de empresa, donde su trabajo necesite de los sistemas de información y comunicaciones, para el desarrollo de sus objetivos y metas planteadas. La organización puede ser a nivel público o privado.

El análisis de riesgos permite a la Dirección, tomar decisiones pertinentes y aplicar la medidas correspondientes en su gestión.

La ejecución del análisis de riesgos es arduo y dispendioso. Para llevar a cabo la identificación y valoración de activos, se necesita la cooperación de muchas personas que laboran en la empresa, empezando por la gerencia hasta los técnicos, de tal manera, se puede establecer una homogeneidad de criterios, así se consigue cifrar los riesgos más relevantes a tratar, ya que por lo general en el análisis de riesgos surgen altas cantidades de datos. Sin embargo, si los riesgos no se encuentran bien organizados, va a ser imposible realizar su interpretación.

Debido a ello, la forma de enfrentar este caso es enfocándose en lo más importante (***máximo impacto*** y ***máximo riesgo***), omitiendo lo que resulte poco significativo. Por lo anterior, demanda esfuerzo y coordinación, además debe ser planificada y justificada. [44]

3.3 Análisis y Evaluación del Riesgo

Cuando se halla identificado los activos de la información, el siguiente paso es, determinar cuáles serán protegidos para mitigar su riesgo y se prosigue a definir el *Riesgo Residual* (el riesgo con el que la organización se decide a convivir). [62]

3.4 Desarrollo del Análisis de Riesgos - Metodología Magerit

Con base a lo visto hasta el momento, cabe señalar que el análisis de riesgos es un acercamiento sistemático, el cual permite establecer el riesgo siguiendo los siguientes pasos:

a. Fijar los activos relevantes para la empresa, su correspondencia y valor.
b. Establecer a qué amenazas se enfrentan los activos.
c. Indicar qué aseguramientos existen y cuán eficientes resultan ser, respecto a los riesgos que se presentan.
d. Evaluar el impacto específico, que se originó mediante el daño presentado en el activo, cuando se ha llevado a efecto la amenaza.
e. Valorar el riesgo, una vez haya surgido como el impacto ponderado con la tasa de ocurrencia de la amenaza. [44]

3.4.1 Identificación de activos

El primer paso a realizar es la identificación de activos, los cuales resultan ser parte esencial del Sistema de Seguridad de los Sistemas de Información, para luego continuar con la valoración de los mismos y amenazas.

A continuación se listarán los activos identificados, los cuales se encuentran agrupados por categorías y la manera en que se encuentran: [46]

ACTIVOS DE INFORMACIÓN
Datos Digitales: • Bases de datos. • Investigación y desarrollo. • Estratégicos. • Correo electrónico. • Backups (copias de seguridad). • Clientes. • Código fuente de programa.
Activos tangibles: • Correo electrónico. • Personales. • Legales. • Investigación y desarrollo. • Otros medios para almacenar información. • Otras formas para hacer backups.
Activos intangibles: • Patentes. • Marca. • Conocimientos técnicos. • Licencias. • Productividad.
Software de aplicación: • Herramientas de bases de datos. • Gestión de la información. • Planificación de recursos organizacionales. • Middleware. • Utilidades. • Cliente. • Aplicaciones de desarrollo. • Aplicaciones de administración.
Sistemas operativos: • Computadores de escritorio. • Servidores. • Dispositivos de mano.

Tabla 13. Activos de información

ACTIVOS FÍSICOS
Infraestructura de TI: • Oficinas. • Escritorios. • Cajones. • Sala para almacenar medios físicos. • Archivadores. • Habitación de servidores. • Edificio.
Controles de entorno de TI: • Sistemas de alimentación no ininterrumpida. • Alarma contra incendio.
Hardware de TI: • Estaciones de trabajo. • Servidores. • Dispositivos de comunicación (Dispositivos de red). • Computadores portátiles. • Computadores de escritorio. • Dispositivos de almacenamiento. • Cableado de datos para estaciones de trabajo. • Cableado de datos para servidores. • Access Point. • Dispositivos de mano. • PC.
Activos de servicios de TI: • Firewalls • Routers. • Anti-spam. • Correo electrónico. • Servicio Web. • Antivirus. • Spyware.

Tabla 14. Activos físicos

ACTIVOS HUMANOS
Empleados: • Arquitectos de software y desarrolladores. • Auditor. • Personal y directivos. • Administradores de sistemas. • Administradores de red.
Externos: • Proveedores. • Trabajadores temporales.

Tabla 15. Activos humanos

3.4.2 Valoración de activos

Partiendo de la anterior identificación de activos, la valoración de los mismos se realizará en el contexto de este trabajo (*Desarrollo del Plan Director para la Implementación de un SGSI),* con respecto a la dimensión de seguridad de dichos activos y recordando, las propiedades de la seguridad de la información (disponibilidad, integridad y confidencialidad).

La manera como se estructuró la *escala de valoraciones*, como las cuantías aplicadas en esta evaluación, se encuentran en el archivo ***3. Análisis de riesgos.xls,*** pestaña u hoja de cálculo ***Escala de valoraciones-Activos,*** el desarrollo está en ***3.4.2 Valoración de activos.***

3.4.3 Identificación de Amenazas

La amenaza trata de un hecho que se origina por un percance en la empresa, lo cual provoca daños materiales o pérdidas de su activo **Información,** debido a ello el SGSI está formado con base a los criterios estipulados en la norma ISO 27001:2013, lo cual sirve de apoyo para controlar las amenazas que se presentan.

Teniendo claro esta definición, hay que recordar, se debe examinar el **Impacto.** [47]

Después de haber identificado y valorado los activos de la organización, el paso siguiente es la identificación de amenazas, de acuerdo a lo establecido por la metodología **Magerit.**

Con base a esta metodología, las amenazas son de cuatro tipos:

Tipo de amenaza	Descripción
Desastres Naturales (N)	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial (I)	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
Errores y fallos no intencionados (E)	Fallos no intencionales causados por las personas.
Ataques Intencionados (A)	Fallos deliberados causados por las personas.

Tabla 16. Tipos de amenazas - Magerit [48]

Para cada amenaza se representará de la siguiente forma:

(Código) Descripción sucinta de lo que puede pasar	
Tipos de activos: Se pueden ver afectados, por esta clase de amenaza.	**Dimensiones:** Seguridad que se pueden ver afectadas, por este tipo de amenaza, ordenas de más a menos relevante
Descripción: Complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado, con las consecuencias indicadas.	

Tabla 17. Representación general de una amenaza - Magerit [48]

Con base a lo visto en la tabla 11, tipos de amenazas, cada una está conformada por una lista de alternativas y sus respectivos códigos, según la amenaza:

Desastres Naturales (N)

- Fuego (N.1)
- Daños por agua (N.2)
- Desastres naturales (N.*)

Origen Industrial (I)

- Fuego (I.1)
- Daños por agua (I.2)
- Desastres Industriales (I.*)
- Contaminación mecánica (I.3)
- Contaminación electromagnética (I.4)
- Avería de origen físico o lógico (I.5)
- Corte del suministro eléctrico (I.6)
- Condiciones inadecuadas de temperatura y/o humedad (I.7)
- Fallo de servicios de comunicaciones (I.8)
- Interrupción de otros servicios y suministros esenciales (I.9)
- Degradación de los soportes de almacenamiento de información (I.10)
- Emanaciones electromagnéticas (I.11)

Errores y fallos no intencionados

- Errores de los usuarios (E.1)
- Errores del administrador (E.2)
- Errores de monitorización (log) (E.3)
- Errores de configuración (E.4)
- Deficiencias en la organización (E.7)
- Difusión de software dañino (E.8)
- Errores de (re-)encaminamiento (E.9)
- Errores de secuencia (E.10)
- Escapes de información (E.14)
- Alteración de la información (E.15)
- Introducción de información incorrecta (E.16)
- Degradación de información (E.17)
- Destrucción de información (E.18)
- Divulgación de información (E.19)
- Vulnerabilidades de los programas (E.20)
- Errores de mantenimiento / actualización de programas (software) (E.21)
- Errores de mantenimiento / actualización de equipos (hardware) (E.23)
- Caída del sistema por agotamiento de recursos (E.24)
- Indisponibilidad del personal (E.28)

Ataques intencionados (A)

- Manipulación de la configuración (A.5)
- Suplantación de la identidad del usuario (A.5)
- Abuso de privilegios de acceso (A.6)
- Uso no previsto (A.7)
- Difusión de software dañino (A.8)
- (Re-)encaminamiento de mensajes (A.9)
- Alteración de secuencia (A.10)
- Acceso no autorizado (A.11)
- Análisis de tráfico (A.12)
- Repudio (A.13)
- Interceptación de información (A.14)
- Modificación de la información (A.15)
- Introducción de falsa información (A.16)

- Corrupción de la información (A.17)
- Destrucción de la información (A.18)
- Divulgación de información (A.19)
- Manipulación de programas (A.22)
- Denegación de servicio (A.24)
- Robo (A.25)
- Ataque destructivo (A.26)
- Ocupación enemiga (A.27)
- Indisponibilidad del personal (A.28)
- Extorsión (A.29)
- Ingeniería social (A.30)

NOTA: El desglose de la identificación de amenazas, se encuentra en el archivo adjunto, ***3. Análisis de riesgos.xls,*** pestaña u hoja de cálculo ***3.4.3 Identi. de Amenazas.***

3.4.4 Valoración de Amenazas

Para la valoración de amenazas, primero se tomó una tabla en donde se asignaron valores de acuerdo a las frecuencias, que pueden presentar las diferentes amenazas en rangos de días, meses, un año:

Valor	Frecuencia
Extremadamente Frecuente (EF)	Una vez al día
Muy Frecuente (MF)	Una vez cada 15 días
Frecuente (F)	Una vez cada dos meses
Poco Frecuente (PF)	Una vez cada seis meses
Muy Poco Frecuente (MPF)	Una vez al año
Nada Frecuente (NF)	Menos de una vez al año

Tabla 18. Valores asignados para la evaluación de las amenazas identificadas

En segunda instancia, se prosiguió a la valoración de las amenazas identificadas, sobre los activos reconocidos de la organización.

NOTA: El desarrollo de este apartado se encuentra desarrollado en el archivo ***3. Análisis de riesgos.xls,*** pestaña u hoja de cálculo ***3.4.4 Valoración de amenazas*** y en seguida está la pestaña ***Valores Amenazas y Vulnerabili.***

3.4.5 Identificación de Vulnerabilidades

En primera instancia, se debe tener claro el concepto de *vulnerabilidad,* para una mejor comprensión de este apartado.

Vulnerabilidad: Se trata de las debilidades que se dan en la seguridad de la información en una organización, donde lo más probable, esto se dé para que una amenaza dañe los activos de la empresa.

En otras palabras, vulnerabilidad es toda aquella debilidad que es aprovechada por una amenaza, con respecto a la falta de protección sobre los activos de una entidad. [10]

El hecho de existir una vulnerabilidad, ayuda con el cálculo en la probabilidad de riesgo.

El objetivo de identificar las vulnerabilidades, es listar las vulnerabilidades (debilidades o defectos) que se presentan sobre los activos identificados anteriormente, los cuales pueden ser explotados por atacantes.

A continuación se presenta la identificación de las vulnerabilidades de manera un poco más detallada y sencilla:

- Medio Ambiente e Infraestructura: Son las vulnerabilidades que se encuentran amenazadas por el medio ambiente físico.

Medio Ambiente e Infraestructura
1.0 Protección física inapropiada - Habitación de servidores
1.1 Control de acceso desacertado - Sala para almacenar medios físicos
1.2 Control de acceso inadecuado - Habitación de servidores
1.3 Abastecimiento de energía eléctrica poco estable
1.4 Desastre natural
1.5 Desastre originado por el ser humano
1.6 Inadecuada prevención contra incendio
1.7 Inadecuada prevención contra inundación

Tabla 19. Vulnerabilidades ante el medio ambiente e infraestructura. [49]

- Personal: Se trata de vulnerabilidades estrictamente laborales, de acuerdo a los roles establecidos, a las personas que trabajan en la empresa.

Personal
2.0 Definición roles no definidas apropiadamente
2.1 Falta de conciencia de seguridad de la información
2.2 Falta de técnicas para monitorear
2.3 Falta en la determinación de políticas / reglamentos
2.4 Poca comunicación para divulgar las políticas de la organización
2.5 Personas altamente cualificadas
2.6 Prestar suficiente atención cuando se está haciendo el trabajo

Tabla 20. Vulnerabilidades en el personal de la organización. [49]

Hardware: Son las vulnerabilidades encontradas en los equipos electrónicos, a los cuales se les ha identificado amenazas.

Hardware
3.0 Almacenamiento de información inapropiado
3.1 Falta de mantenimiento programada
3.2 Falta de control de acceso con privilegios
3.3 Actualización de equipos
3.4 Suministro eléctrico
3.5 Conexión de equipos no autorizados
3.6 Falta de restricción en algunos equipos (servidores, estación de trabajo)
3.7 Falta de buen uso y cuidado de hardware

Tabla 21. Vulnerabilidades en el hardware. [49]

Redes de comunicaciones: Se tratan de vulnerabilidades relacionadas con las redes implantadas, su infraestructura, intercepción y hurto de información, acceso a la red por personas sin autorización, errores y fallas en la disponibilidad del servicio.

Redes de comunicaciones
4.0 Falta de restricción
4.1 Contraseñas poco robustas
4.2 Uniones de cables inapropiados
4.3 Líneas de comunicación desprotegidas
4.4 Red perimetral externa (DMZ) desprotegida
4.5 Políticas de autenticación sin implantar
4.6 Falta políticas sobre el uso de dispositivos de almacenamiento
4.7 No hay monitorización en el tráfico de la red
4.8 Falta revisiones periódicas en las medidas de seguridad
4.9 Capacidad inadecuada de la red
4.10 Access Point, estación de trabajo un poco desprotegidos

Tabla 22. Vulnerabilidades en las redes de comunicaciones

Software: Las vulnerabilidades que se tratan en esta sección, están relacionadas con el proceso de desarrollo, implementación y uso del software.

Software
5.0 Uso no controlado
5.1 Administración de configuración inadecuado
5.2 Contraseñas poco robustas
5.3 Testeo insuficiente
5.4 Instalación / Desinstalación no controlado
5.5 Falta de documentación
5.6 Control de acceso inadecuado
5.7 Administración poco eficiente de contraseñas
5.8 Falta mayor protección contra virus y malware (código malicioso)
5.9 Control de material de origen
5.10 Políticas de uso no aplicadas

Tabla 23. Vulnerabilidades a nivel de software. [49]

Información / Documentos: Vulnerabilidades dirigidas a la manipulación y protección de la información.

Información / Documentos
6.0 Control inapropiado de base de datos
6.1 Disponibilidad de datos respaldados
6.2 Ubicación de la sala para almacenar medios físico poco protegida
6.3 Información / documentos no retirados de los discos duros locales
6.4 Cuidado de daño en almacenamiento de medios
6.5 Almacenamiento de información / documentos no organizados adecuadamente.

Tabla 24. Vulnerabilidades en el campo de la información / documentos. [49]

3.4.6 Valoración de Vulnerabilidades

Esta herramienta brinda a los administradores del sistema, o personal de seguridad de la red, una apreciación con respecto a la valoración de los riesgos de seguridad. La información originada por la valoración de vulnerabilidades, presenta una guía clara en la resolución de vulnerabilidades conocidas, y proteger los activos de la empresa.

La información determinada con esta acción, asegura que se traten y monitoricen los riesgos más graves. Además es un soporte para justificar el costo o mano de obra requeridas, para fortalecer la seguridad de los activos.

NOTA: El detalle de este apartado se encuentra desarrollado en el archivo ***3.Análisis de riesgos.xls,*** pestaña u hoja de cálculo ***3.4.6 Valora. de Vulnerabilidad.***

3.4.7 Evaluación de riesgos

Con el apoyo de la norma ISO 27001 para realizar esta gestión, ofrece la posibilidad de llevar a cabo un cálculo simple sobre el riesgo, si se tiene pocas variables y por el contrario resultará complejo. [50]

Para llevar a cabo la evaluación de los riesgos, se puede tomar como base el uso de tablas para obtener resultados. El riesgo es calculado sobre un activo, teniendo en cuenta:

- El impacto sobre un activo debido a una amenaza
- La probabilidad de amenaza. [41]

NIVEL DE RIESGO = IMPACTO * PROBABILIDAD

Rango	Descripción
Riesgo <= 4	El riesgo se considera de poco impacto.
Riesgo > 4	El riesgo se considera de alto impacto y debe tratarse inmediatamente.

Tabla 25. Criterios de aceptación del riesgo. [41]

A	Autenticación	Asegurar la identidad u origen de los datos.
C	Confidencialidad	La información es accesible solamente para los usuarios autorizados.
I	Integridad	Información precisa y completa.
D	Disponibilidad	Los usuarios tienen acceso cuando se necesite y en los tiempos adecuados.
T	Trazabilidad	Determinar en todo momento, quién hizo qué y en qué momento.

Tabla 26. Dimensiones de la seguridad de la información. Fuente fundamentado en la metodología Margerit [41]

Para obtener el impacto del activo, se hizo la suma de los valores sobre las dimensiones tratadas en la tabla anterior, para luego dividirlo por los cinco dominios presentados (A, C, I, D, T), Bajo (1), Medio (2), Alto (3), partiendo de la tabla de valoración que se emplea para calcular el riesgo.

TOTAL CUANTITAVO = (VALOR(A) + VALOR(C) + VALOR(I) + VALOR(D) + VALOR(T)) / 5

Valor	Descripción
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

Tabla 27. Estimación de probabilidad. Fuente fundamentado en la metodología Margerit [41]

TOTAL CUALITATIVO - > Bajo (Si total cuantitativo es 1)
Medio (Si total cuantitativo es 2)
Alto (Si total cuantitativo es 3)

Valor	Descripción
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Tabla 28. Estimación de impacto. Fuente fundamentado en la metodología Margerit [41]

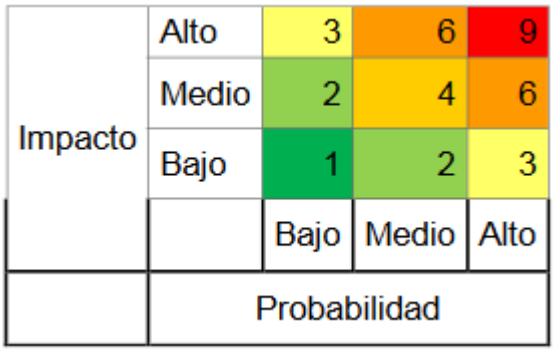


Figura 13. Estimación del riesgo. [41]

NOTA: El desglose de esta sección, se encuentra desarrollado en el archivo ***3. Análisis de riesgos.xls,*** hoja de cálculo o pestaña ***3.3.7 Evaluación de riesgos.***

3.4.8 Declaración de Aplicabilidad

Con base a los resultados arrojados por la evaluación de riesgos (ver punto 3.3.7), se han seleccionado los controles de la norma ISO 27001:2013, para la realización de esta parte y a su vez, la DdA será una base para el posterior desarrollo en el tratamiento de riesgos.

Este documento ofrece ventajas como:

- Consultar durante las auditorías al SGSI, como una forma global de conocer los controles de seguridad, aplicados en la empresa para salvaguardar sus activos.
- La organización puede implantar mejores prácticas.
- Resumir en un documento las amenazas reconocidas y examinadas durante la evaluación de riesgos.
- Llevar a cabo un análisis GAP. [59]

La Declaración de Aplicabilidad es un documento necesario a realizar, porque es la principal declaración en la que se define, todo aquello que se desea llevar a cabo con la seguridad de los activos pertenecientes a la empresa. La DdA es un resumen perfecto, con relación a qué se debe hacer, por qué se debe hacer y cómo se debe hacer.

De manera precisa, existen algunos salvaguardas implementados, funcionando no completamente ni de forma adecuada en la organización; pero la empresa ha contemplado definir, planificar los controles faltantes, para que a largo plazo, se puedan desarrollar, poner en funcionamiento de manera correcta, tal como se establece en la norma estándar ISO 27001:2013.

Tal documento se encuentra adjunto a este informe, en un archivo llamado ***3. Análisis de riesgos.xls,*** hoja de cálculo o pestaña ***3.4.8 DdA.***

3.4.9 Nivel del riesgo aceptable

Trata del nivel donde la Alta Dirección considera como margen, en el caso de que un riesgo sea estimado o haya que disminuir. Dichos riesgos que se encuentren en el umbral serán aceptados, aquellos que estén sobre este valor deberán de ser tratados (este tema se expondrá más adelante, en la parte de *Tratamiento de riesgos).*

En este caso, la Dirección ha decidido optar porque el nivel de riesgo aceptable es de 3, por lo cual, todo riesgo aquel, sea <= 3 será aceptado.

(Ver 2.9.4 Aplicación de la metodología, métodos y procesos para el análisis de riesgos en este caso).

Los detalles están desarrollados, en el archivo ***3. Análisis de riesgos.xls,*** hoja de cálculo o pestaña ***3.4.9 Nivel de riesgo aceptable.***

3.4.10 Tratamiento de riesgos

Una vez calculado el riesgo y haber analizado cuáles de ellos, son aceptados por la organización, el paso a seguir es precisar su tratamiento y/o monitoreo, en donde se ejecuten estrategias y controles para mantener tales riesgos, dentro del nivel de aceptación por la empresa. De tal forma, se continua con la evaluación de la "calidad de gestión", con lo cual se pueda indicar cuán eficaces son los controles, que se han fijado por la compañía y minimizar los riesgos encontrados.

Con esta acción se espera, el hecho de aplicar los controles necesarios sean eficientes, así obtener un indicador de riesgo inherente neto (riesgo residual) que vaya disminuyendo. Es decir, con el tratamiento de riesgos se recopilarán las salvaguardas y medidas que se van aplicar, para minimizar los riesgos que se encuentran por encima del umbral aceptado (nivel de riesgo).

A medida que los controles establecidos sean eficaces, junto con una gestión de riesgos pro-activa, el riesgo residual se irá reduciendo.

Para el tratamiento de riesgos se cuenta con las siguientes opciones a tratar:

- **Reducir el riesgo** (aplicando controles).
- **Asumir el riesgo** (en caso tal de que la organización no disponga de los recursos económicos para afrontar el riesgo).
- **Eliminar el riesgo** (como puede ser, eliminando el activo).
- **Transferir el riesgo** (traspasar el riesgo a una entidad externa, como una aseguradora).

Siguiendo con el Plan de tratamiento de riesgos, se aplicarán los controles necesarios del *Anexo A* de la norma estándar *ISO 27001:2013,* junto con las acciones que van a poner en práctica sobre los controles, recursos y plazos.

El desglose elaborada para este apartado, se encuentra adjunto en el archivo ***3. Análisis de riesgos.xls,*** hoja de cálculo o pestaña ***3.4.10 Tratamiento de riesgos.***

Con base al tratamiento elaborado, la opción a tratar que se ha tomado es la de ***Reducir los riesgos,*** pues son tratables por la organización y se hará mejoras con ello.

3.4.11 Riesgo residual

En este apartado se calculará el riesgo neto o riesgo residual, el cual se da por la relación entre los riesgos (riesgos inherentes) y la gestión realizada para minimizar los riesgos dados, en la sección anterior llamada "Evaluación de riesgo".

A partir de aquí y los resultados del riesgo residual, la Alta Dirección puede tomar la decisión de seguir o abandonar la actividad, de acuerdo a lo que indique el nivel de riesgos, o puede implantar nuevos controles u otras decisiones. [55]

Para desarrollar el riesgo neto o residual, se va a tratar con una tabla escala de valoración de efectividad sobre los controles, como se puede observar:

Control	Efectividad
Ninguno	1
Bajo	2
Media	3
Alto	4
Destacado	5

Tabla 29. Escala de valoración de efectividad de los controles para riesgo residual. [55]

Las operaciones realizadas para desarrollar este apartado, se encuentran detallados en el archivo ***3. Análisis de riesgos.xls,*** pestaña u hoja de cálculo ***3.4.11 Riesgo residual***.

Los cálculos generales que se aplicaron fueron:

PROMEDIO = (Efectividad Control 1+Efectividad Control 2+Efectividad Control N) / N
RIESGO RESIDUAL = (Nivel de riesgo / Promedio)
RIESGO RESIDUAL TOTAL = (Riesgo residual 1+Riesgo residual 2+Riesgo residual N) / N

4. Propuesta de Proyectos

4.1 Introducción

Con base al *análisis de riesgos* llevado a cabo en el punto anterior, se realizará el *tratamiento de riesgos,* con el planteamiento de la propuesta de proyectos, el cual requiere ejecutar la organización y en donde estén, alineados con el *Plan Director.* (1.3.1 Objetivos del Plan Director)

- ✓ Conocer el contexto y liderazgo (compromiso de la Alta Dirección, políticas de la entidad, organización de los roles y responsabilidades) sobre la compañía.

- ✓ Planear los objetivos de seguridad de la información y Plan Director, alineados con las estrategias, políticas, metas, visión y misión de la empresa.

- ✓ Llevar una medición de las actividades a ejecutar, para conseguir los objetivos establecidos.

- ✓ Evaluar el nivel de cumplimiento, por medio del análisis diferencial con respecto a las normas estándar ISO/IEC 27001 e ISO/IEC 27002.

- ✓ Valorar los riesgos de seguridad.

- ✓ Hacer seguimiento sobre las propuestas de mejoras realizadas.

De esta manera se van alcanzar niveles estables de seguridad, por parte de la empresa (es decir, cumplimiento con los requisitos de la norma, de acuerdo a las necesidades de la compañía), los cuales requieren una pronta atención de acuerdo a un nivel de riesgo, no tolerable o no aceptable y la organización, ha optado por mitigar estos riesgos.

Teniendo en cuenta los resultados de este análisis, el efecto obtenido es una propuesta de los proyectos identificados, en donde estarán integrados: su valor económico, planificación requerida, recursos, tiempo necesario para la ejecución, y con los que se pretende brindar apoyo para minimizar los riesgos generados.

Así como se indica en los objetivos del *Plan Director,* tales mejoras podrán ser evaluadas de acuerdo a las normas establecidas, por la ISO 27001 e ISO 27002, también en hacer seguimiento sobre dichas propuestas, a manera de continuar realizando mejoras.

Se ha dispuesto no plantear un número extenso de proyectos, pues la idea es tratar los riesgos de mayor prioridad y de suma urgencia para la empresa, los cuales, la organización aceptó tratarlos para mitigar sus riesgos y/o amenazas. Además se ha pensado en el número de personas cualificadas, que laboran en la empresa y las cuales, estarían disponibles a dedicar su tiempo de trabajo en los proyectos, sin que ellos desatiendan sus otras funciones.

4.2 Sugerencias para la realización de proyectos

En este apartado se van a plantear y dar detalles sobre los proyectos a proponer, para fortalecer salvaguardas generados en el análisis de riesgos (capítulo anterior), y que se encuentran alineados tanto con los objetivos de la organización, como los contenidos en el Plan Director.

El fin de estas propuestas es mitigar en lo máximo los riesgos actuales, presentados en el estudio anterior y mejorar, conforme al cumplimiento de la norma ISO 27001:2013 hasta obtener niveles aceptables (estabilidad en los riesgos, acorde con las normas).

Con lo cual el único deseo es aportar recomendaciones, para optimizar la gestión de seguridad, gestión de procesos y tecnologías establecidas en la entidad, además de encontrar un buen rendimiento en sus recursos.

La lista de los proyectos propuestos, se indican a continuación:

PROPUESTA DE PROYECTOS	
Proyecto 1	Capacitación al personal en Seguridad de la Información.
Proyecto 2	Implementación de controles de detección y prevención, sobre accesos a los sistemas de información.
Proyecto 3	Emplear controles para mantener estables, tanto la red de comunicaciones como los servicios que se ofrecen.
Proyecto 4	Establecer políticas de seguridad de la información.
Proyecto 5	Implementar controles en producción de proyectos de software.
Proyecto 6	Determinar procesos de documentación, relacionada con el SGSI.
Proyecto 7	Fijar políticas de acceso físico no autorizado, a instalaciones de procesamiento de información de la entidad.

Tabla 30. Lista de la propuesta de proyectos.

Para ver con más detalle los proyectos de la anterior lista, se encuentra adjunto a este documento, en un archivo llamado ***4. Propuesta de Proyectos.xls,*** en la primera pestaña u hoja de cálculo ***4.2 Sugerencias prop. de proyec.***

4.3 Estimación en costos de los proyectos propuestos

Para calcular el coste de mano de obra de los proyectos recomendados, se cuenta con la nómina de la empresa, pues al ser uno de sus servicios, tratarse de una compañía desarrolladora de software, se trabajarán con los mismos empleados, quienes de acuerdo a su contratación de tiempo completo (40 horas semanales), se les ha aplicado un porcentaje requerido para apoyar en la ejecución de las propuestas, donde el tiempo de dedicación para estas, se encuentran dentro del horario estipulado en sus contratos. Es decir, los empleados que realizan dichos proyectos, no están en horario completo en los respectivos proyectos, razón por la cual solo dedicarán el tiempo establecido en el documento, referente a su jornada laboral, mientras llevan a cabo las tareas propias de su trabajo.

Los equipos de hardware que se requieren, después de indagar y analizar, se han dado sus respectivos costos, con la referencia respectiva y el sitio donde se encuentran. Lo mismo se realizó con un software que se sugirió, para determinado proyecto, pero también lo puede desarrollar la compañía, en caso tal de quererlo así.

De tal manera, la empresa tendrá que hacer una mínima inversión en hardware, ya que la mayor parte de los trabajos son mano de obra y ésta, la paga la misma organización por nómina, contando con el tiempo (horarios laborales contratados) y desarrollo de funciones (estipulado en sus contratos).

El documento desarrollado se entrega junto con este informe, en un archivo llamado ***4. Propuesta de Proyectos.xls***, pestaña u hoja de cálculo ***4.3 Estimación proyec. propuest***

4.4 Cronograma de tiempos para los proyectos recomendados

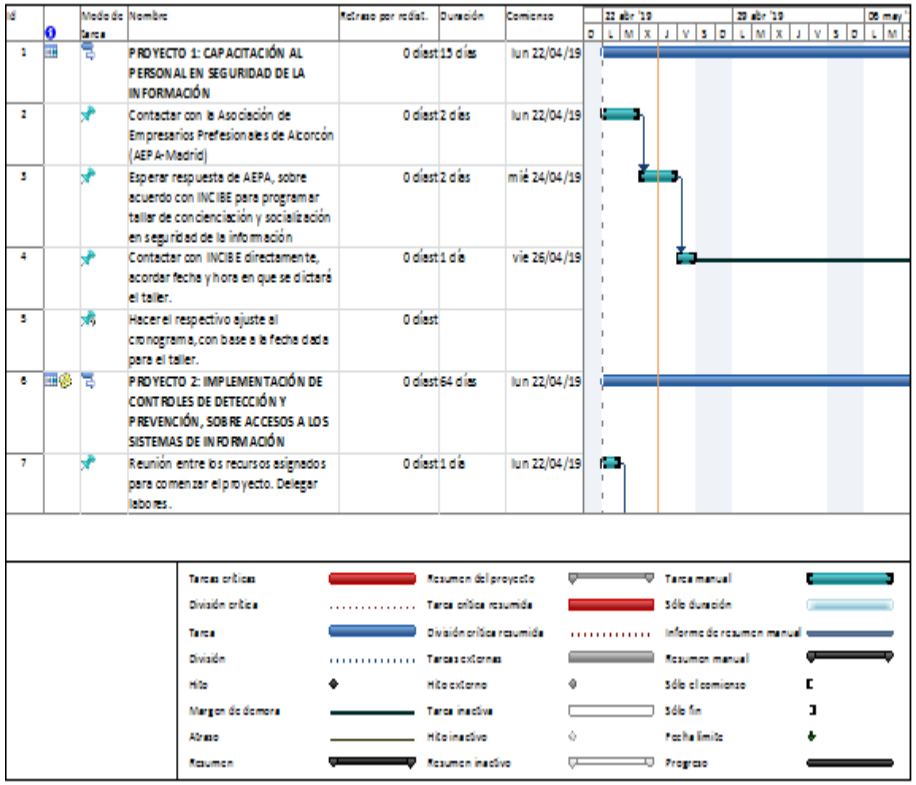
En este apartado se hizo el desglose de las actividades concerniente a la propuesta, que se van a realizar en cada proyecto, con sus respectivas estimaciones de tiempo y fechas.

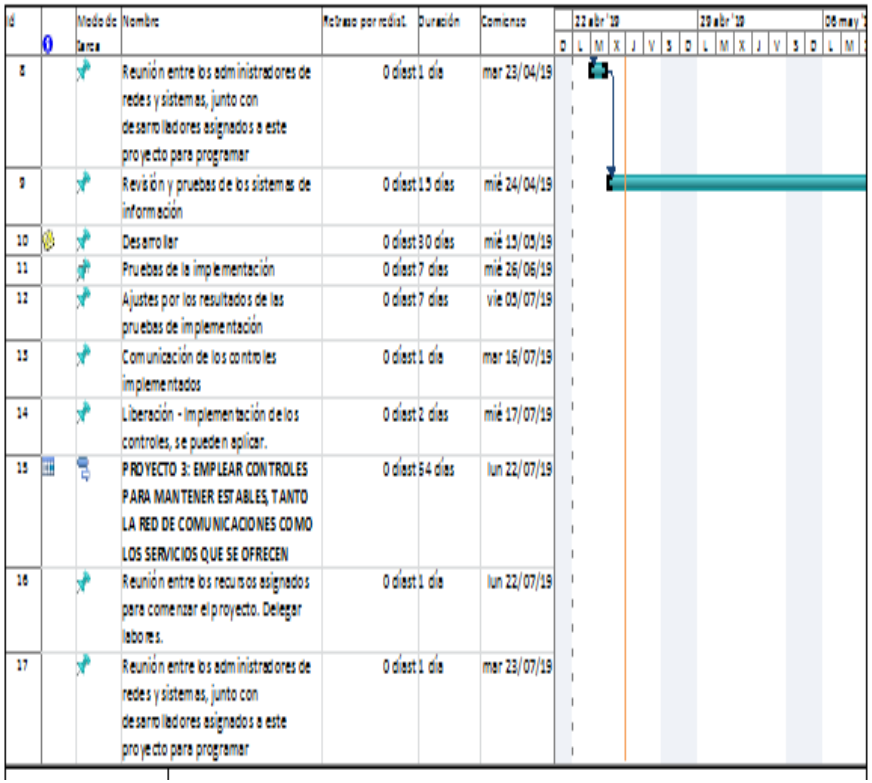
Con base a los anteriores análisis realizados, se hizo un bosquejo de la propuesta de proyectos a nivel temporal, el cual puede necesitar de algunos ajustes, pues en el caso del taller de capacitación, depende de la entidad que asigne a la persona especialista en el tema de seguridad de la información, fecha y hora, puede cambiar el cronograma en este aspecto.

De acuerdo a lo planeado en el cronograma, los tiempos para cada proyecto fueron:

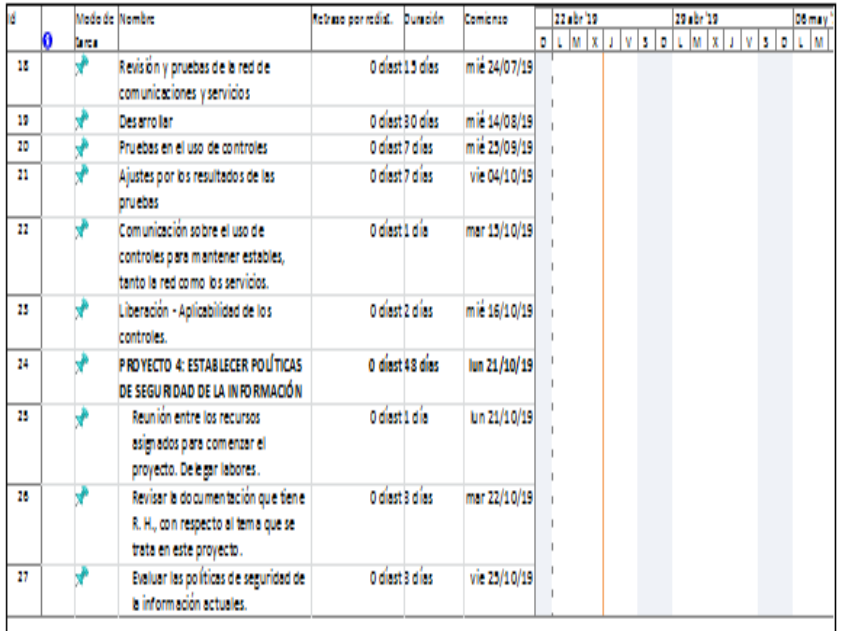
- Proyecto 1: 15 días
- Proyecto 2: 64 días
- Proyecto 3: 64 días
- Proyecto 4: 48 días
- Proyecto 5: 33 días
- Proyecto 6: 37 días
- Proyecto 7: 15 días

Lo cual quiere decir, el tiempo para ejecutar los 7 proyectos, está estimado en 276 días.

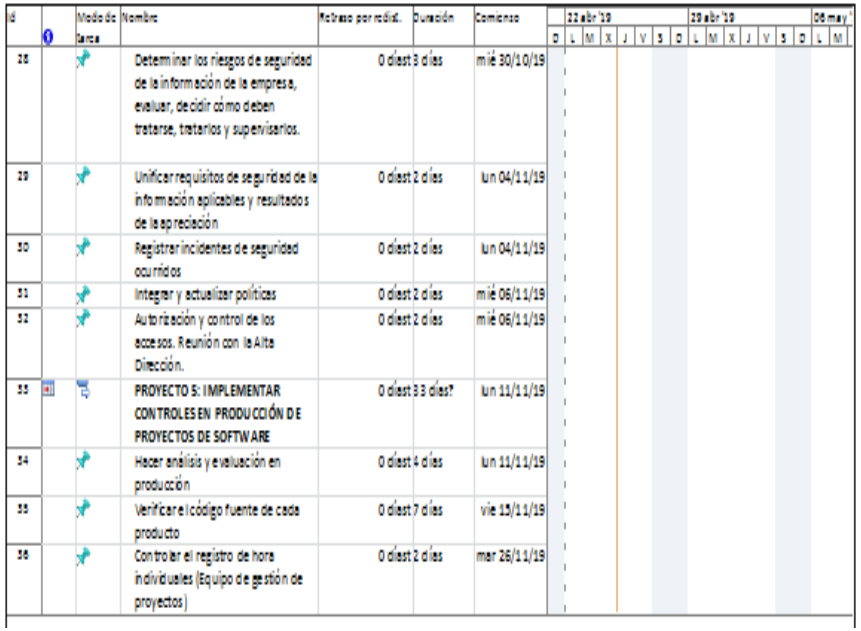




Figuras 14 y 15. Cronograma de estimación en tiempos para los proyectos propuestos.



Id	Modo de tarea	Nombre	Retraso por nivel.	Duración	Comienzo
18		Revisión y pruebas de la red de comunicaciones y servicios	0 días	15 días	mié 24/07/19
19		Desarrollar	0 días	30 días	mié 14/08/19
20		Pruebas en el uso de controles	0 días	7 días	mié 25/09/19
21		Ajustes por los resultados de las pruebas	0 días	7 días	vie 04/10/19
22		Comunicación sobre el uso de controles para mantener estables, tanto la red como los servicios.	0 días	1 día	mar 15/10/19
23		Liberación - Aplicabilidad de los controles.	0 días	2 días	mié 16/10/19
24		**PROYECTO 4: ESTABLECER POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	0 días	48 días	lun 21/10/19
25		Reunión entre los recursos asignados para comenzar el proyecto. Delegar labores.	0 días	1 día	lun 21/10/19
26		Revisar la documentación que tiene R. H., con respecto al tema que se trata en este proyecto.	0 días	3 días	mar 22/10/19
27		Evaluar las políticas de seguridad de la información actuales.	0 días	3 días	vie 25/10/19



Id	Modo de tarea	Nombre	Retraso por nivel.	Duración	Comienzo
28		Determinar los riesgos de seguridad de la información de la empresa, evaluar, decidir cómo deben tratarse, tratarlos y supervisarlos.	0 días	8 días	mié 30/10/19
29		Unificar requisitos de seguridad de la información aplicables y resultados de la apreciación	0 días	2 días	lun 04/11/19
30		Registrar incidentes de seguridad ocurridos	0 días	2 días	lun 04/11/19
31		Integrar y actualizar políticas	0 días	2 días	mié 06/11/19
32		Autorización y control de los accesos. Reunión con la Alta Dirección.	0 días	2 días	mié 06/11/19
33		**PROYECTO 5: IMPLEMENTAR CONTROLES EN PRODUCCIÓN DE PROYECTOS DE SOFTWARE**	0 días	33 días?	lun 11/11/19
34		Hacer análisis y evaluación en producción	0 días	4 días	lun 11/11/19
35		Verificar el código fuente de cada producto	0 días	7 días	vie 15/11/19
36		Controlar el registro de hora individuales (Equipo de gestión de proyectos)	0 días	2 días	mar 26/11/19

Figuras 16 y 17. Continuación Cronograma de estimación en tiempos para los proyectos propuestos.

El documento completo, perteneciente a este punto se halla en el archivo adjunto con este informe, llamado ***4. Cronograma de tiempos para los proyectos recomendados.mpp*** (Ms. project)

5. Auditoría de Cumplimiento V1.0

Se ha tomado como marco de referencia para dicha tarea, emplear el *Código de Buenas Prácticas ISO/IEC 27002:2013.* De tal forma, se pueda precisar qué controles serán implementados y cuáles no lo serán, con el fin de apoyar en el mejoramiento del SGSI de la organización y salvaguardar a la información, el cual representa uno de los activos con mayor relevancia de cualquier entidad, influyendo directamente en el desempeño de la misma.

La Auditoría de Cumplimento se realizará orientada a los elementos de *Seguridad de la Información en el SGSI,* haciendo uso de técnicas y herramientas para establecer posibles falencias, brindando de esta forma opciones de solución.

Debido a que en la compañía no se habían realizado auditorías, antes de hacer este trabajo, se presentará la versión 1.0 para esta actividad.

5.1 Objetivo

Evaluar el nivel de cumplimiento sobre los controles implementados, iniciativas de seguridad de la información, proceso de implementación en la actualidad y validar la madurez de la empresa.

5.2 Alcance

Esta labor de Auditoría se llevará a cabo en:

- Sistemas (Desarrollo, equipos de procesamiento de la información, entre otros).
- Instalaciones de la organización (seguridad dentro de la empresa, áreas de almacenamiento de información, equipos, sistemas con acceso restringido, etc.).
- Infraestructuras de hardware y software.
- Servicios de comunicaciones (redes, servicios web, correo electrónico, etc.)
- Producción.

5.3 Metodología

Para cumplir con lo establecido en el alcance anterior, se desarrollará siguiendo el procedimiento de Auditoría Interna ISO 27001:2013. Se indica que una auditoría, trata de un proceso para hacer una evaluación de las pruebas existentes, donde se hace referencia a la definición, en el grado de cumplimiento de los criterios establecidos. (Ver 2.6.6 Generación de hallazgos de auditoría).

Así que, el hecho de llevar a cabo una auditoría interna, teniendo como base a la norma ISO 27001, los resultados generados por esta, ayudan a dar respuesta con respecto a los siguientes interrogantes:

- ¿La organización cumple con todos los requisitos que se consideren pertinentes?
- ¿Se encuentran definidas las garantías de seguridad de la información de manera correcta?
- ¿Se consiguen los resultados esperados en cuanto a la seguridad de la información?

Teniendo en cuenta lo planteado por la norma ISO 27001, señala que la auditoría interna debe establecerse como una manera sistemática, con la cual se pueda planificar, hacer, comprobar y mejorar de forma continua, conocida y definida, trabajando con personal cualificado, ya sea que se trate de una contratación interna o externa.

En la auditoría se emplean diferentes tipos de desviaciones, los cuales son una manera de apoyar, en la valoración de los controles. Ellas se encuentran: *las No Conformidades (No Conformidad Mayor y No Conformidad Menor), Observación* y *Oportunidad de mejora.* [79]

- Las No Conformidades: Se generan en el momento que la empresa, no cumple con lo establecido en la norma ISO 27001:2013, por su propia documentación o terceros.

A continuación se ejemplifican algunas no conformidades:

- Falta de un riesgo específico requerido por la organización.
- Práctica habitual adoptada y mantenida por la organización, la cual no se encuentra documentada.
- Por último está un proceso que es requerido por la norma ISO 27001:2013, y no se está realizando de manera apropiada.

Frente a una No Conformidad, de acuerdo a lo estipulado por la norma ISO 27001:2013, la empresa debe:

- Responder de una forma idónea para controlarlos y corregirlos.
- Ocuparse de las consecuencias.
- Considerar las necesidades de eliminar las causas, de la No Conformidad.
- Implementar acciones correctivas, para afrontar las causas.
- Comprobar la eficacia de las acciones correctivas.
- Modificar el SGSI de la entidad, siempre que sea requerido.

Las No Conformidades se clasifican como:

- *No Conformidad Mayor*: No se cumple una sección completa del estándar. Ejemplo: No se ha realizado el análisis de riesgos.

- *No Conformidad Menor:* Es una desviación, con la cual no compromete la gestión del SGSI, es decir, se incumple un punto de un apartado referente al estándar. Ejemplo: No se ha definido, un propietario para los riesgos.

- Observación: No supone un incumplimiento del estándar, pero en caso de no realizarse la corrección pertinente, en el futuro puede dar lugar a una No Conformidad. Ejemplo: Todos los riesgos tienen asignado un propietario, excepto un riesgo a un nuevo activo, el cual fue incluido hace poco tiempo a la empresa.

- Oportunidad de mejora: Se trata de la situación, desde el punto de vista del auditor, la compañía aumenta la idoneidad, adecuación o eficacia de su

SGSI. En otras palabras, es solamente una recomendación, la cual nunca supondrá un incumplimiento del estándar. Algunos ejemplos sobre la oportunidad de mejora son:

- Incorporación de tecnologías nuevas o actualizadas.
- Exclusión de las actividades en los procesos de negocio.
- Se recomienda que la organización amplíe el alcance de su SGSI, a todas las áreas de la misma.

Para cumplir con el objetivo anterior, se utiliza como referencia el ***CMM (Capability Maturity Model - Modelo de Capacidad de Madurez),*** es un modelo para evaluar los procesos de la empresa.

Al comienzo se desarrolló para los procesos relativos al software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute). El SEI se trata de un centro de investigación y desarrollo, este es patrocinado por el Departamento de Defensa de los Estados Unidos de América, y coordinado por la Universidad mencionada anteriormente. "CMM" es una marca registrada del SEI.

Tal modelo precisa un conjunto de prácticas o procesos fundamentales, agrupados en Área Clave de Proceso (KPA, Key Process Area), para la evaluación y mejora de los procesos de desarrollo, implementación y mantenimiento. Donde cada área de proceso, establece un conjunto de buenas prácticas como se indica a continuación:

- Especificadas en un proceso documentado.
- Provistas (empresa) de los medios y formación necesarios.
- Efectuadas de una forma sistemática, global y homogéneo (institucionalizadas).
- Medidas.
- Verificadas. [76]

El CMM puede ser extendido a sistemas de gestión para valorar el nivel de madurez del sistema tratado.

Los niveles del CMM que se van a utilizar en este análisis, para estimar la madurez del Sistema de Gestión de este estudio son:

Efectividad	CMM	Nivel	Descripción
0%	L0	Inexistente	El proceso no utiliza funcionalidad de un sistema homologado. ◆Carencia completa de cualquier proceso reconocible. ◆ No se ha reconocido siquiera, que existe un problema a resolver.
10%	L1	Inicial / Ad-hoc	El proceso está parcialmente implementado en un sistema homologado, o usa desarrollo propio, habiendo funciones estándares o su uso es inadecuado, o no corresponde a una Best Practice. ◆ 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	El proceso está soportado, en gran medida, por la funcionalidad de un sistema homologado, pero no está estandarizado y no tiene gobernabilidad. ◆ Los procesos similares, se realizan de forma similar por distintas personas con la misma tarea. ◆ Se normalizan las buenas prácticas, con base a la experiencia y el método. ◆ Depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	El proceso está soportado por la funcionalidad de un sistema homologado, no está estandarizado, pero tiene gobernabilidad. ◆ La organización entera, participa en el proceso. ◆ Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado y medible	El proceso está completamente soportado por la funcionalidad, de un sistema homologado, tanto en la operación (transacciones) como en la gestión (analytics), los procesos de negocios están estandarizados par las distintas filiales y permite garantizar, los procesos operan de acuerdo diseños y normativas. ◆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 eficiencia.
100%	L5	Optimizado	Los proceso de negocios se han refinado, hasta un nivel de mejora práctica, se basan en los resultados de mejoras y continuas. ◆Los procesos están en constante mejora. ◆En base a criterios cuantitativos, se determinan las desviaciones más comunes, y se optimizan los procesos.

Tabla 31. Criterios de evaluación del modelo de madurez del SGSI. [77] [80]

A esta escala también se le ha agregado un semáforo, para ser más específicos, resaltar pronto el grado de importancia de cada criterio. De tal manera, las directrices que se tomaron para ello son:

- Color rojo: Corresponde a L0 y L1. Los procesos en este color, son los urgentes de mejorar.
- Color amarillo: Corresponde a L2 y L3. Los procesos son deseables de mejorar tan pronto como sea posible.
- Color verde: Corresponde a L4 y L5. Indica la evolución de los procesos, con base al mejoramiento continuo. [80]

Los valores obtenidos en cada apartado, serán tenidos en cuenta para establecer de forma orientativa, la madurez inicial de cada control de la seguridad, frente a las valoraciones CMM dados anteriormente (ver tabla 26).

Con respecto al campo llamado ***Nivel de cumplimiento,*** se trató de la misma manera como fue aplicado en el "***Análisis Diferencial ISO 27001",*** desarrollado al inicio de este estudio y el cual se puede observar en el mismo documento (ver archivo 1. Situación Actual.xls, pestaña Aclaraciones 1.9.1.1). Los criterios empleados para esta valoración son:

Valores asignados para el nivel de cumplimiento			Efectividad
Valor cuantitativo	*Valor cualitativo*	*Detalle*	
0	No existente	No existe certeza del estándar en la empresa.	0%
1	Inicial	Se han anexado normas a la medida de la compañía, pero presenta versatilidades.	10%
2	Repetible	La empresa tiene normas adaptadas, pero no tienen documentación al respecto.	50%
3	Definido	Existen normas acondicionadas a la organización, con la apropiada información registrada, pero no tienen medición.	90%
4	Administrado	Se miden de manera periódica los procesos de la entidad, y se realizan las mejoras necesarias.	95%
5	Optimizado	La entidad ha llevado a cabo todas las mejoras propuestas, cumpliendo así con las normas estándar y las buenas prácticas.	100%
6	No Aplica - N.A.		

Tabla 32. Criterios para evaluar el nivel de cumplimiento (Ver archivo 1. Situación actual.xls)

Las fuentes de información tomadas como base para llevar a cabo, el estado de madurez de la empresa se listan a continuación:

- Situación actual de la empresa.
- Verificación de los sistemas y comunicaciones.
- Análisis de la información recopilada durante este estudio.
- Reconocimiento de las áreas de: tecnología, redes, administración, R.H.

En este apartado se realiza la evaluación del SGSI, valorando el grado de madurez, de acuerdo a la ***"Estructura del estándar ISO/IEC 27001:2013"*** (ver apartado 1.4 Marco normativo ISO de referencia – 1.4.1 ISO/IEC 27001:2013), sección 4 a 10 con relación a lo que constituye el PDCA (Contexto de la organización, Liderazgo, Planificación, Apoyo, Funcionamiento, Evaluación de desempeño, Mejora) y con los controles del Anexo A (ISO/IEC 27002:2013, 14 dominios, 35 objetivos de control y 114 controles).

Permitiendo así, conocer en qué nivel se encuentra un control, aportando de esta manera, un valor a esta auditoría, con la cual se compruebe el cumplimiento actual de la organización frente a los requisitos, en otras palabras, verificar si ellos se cumplen o no.

La metodología se aplica de la misma forma, en las siguientes dos evaluaciones:

- 5.4 Evaluación de controles, madurez y nivel de cumplimiento de la organización frente a ISO/IEC 27001:2013.
- 5.5 Evaluación de controles, madurez y nivel de cumplimiento de la organización frente a ISO/IEC 27002:2013.

5.4 Evaluación de controles, madurez y nivel de cumplimiento de la organización frente a ISO/IEC 27001:2013 - V1.0

Los requisitos establecidos por la norma estándar ISO/IEC 27001:2013 a valorar, están distribuidas de la siguiente manera:

- Sección 4: Contexto de la organización. En este punto se hace hincapié en la *identificación de los problemas externos e internos* que engloban a la empresa. [78]

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

- Sección 5: Liderazgo. Se tiene que ajustar a *la relación y la responsabilidad que tiene la alta dirección* con respecto al Sistema de Gestión de Seguridad de la Información, por ejemplo: Garantizar que se *cumplan los objetivos* del SGSI, Garantizar la *disponibilidad de los recursos,* Garantizar los *roles y las responsabilidades.*

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

- Sección 6: Planeación. Esta sección está enfocada para *definir los objetivos de seguridad,* los cuales deben ser claros y deben contar con planes específicos para conseguirlos. Es *necesario presentar grandes cambios* durante el proceso de evaluación de riesgos: el proceso para llevar a cabo la evaluación de riesgos, el método utilizado para conseguir el objetivo a la hora de identificar los riesgos que se encuentran asociados, conocer el nivel de riesgo que se establece como base de la probabilidad de que suceda un riesgo, Se elimina el término propietario del activo y se establece el término propietario del riesgo.

  - 6.1 Acciones para tratar los riesgos y oportunidades.
  - 6.1.1 Consideraciones generales.
  - 6.1.2 Apreciación de riesgos de seguridad de la información.
  - 6.1.3 Tratamiento de los riesgos de seguridad de la información.
  - 6.2 Objetivos de Seguridad de la Información y planificación para su consecución.

- Sección 7: Soporte. Marca los requisitos de *soporte para establecer, implementar y mejorar* el Sistema de Gestión de Seguridad de la Información, según la norma ISO 27001:2013, en el que se incluye: recursos, personal competente, conciencia y comunicación de las partes interesadas. También abarca el proceso de *documentar, controlar, mantener y conservar la documentación,* correspondiente al Sistema de Gestión de Seguridad de la Información.

  - 7.1 Recursos.
  - 7.2 Competencias.
  - 7.3 Conciencia.
  - 7.4 Comunicación.
  - 7.5 Información documentada.
  - 7.5.1 Consideraciones generales.
  - 7.5.2 Creación y actualización.
  - 7.5.3 Control de la información documentada.

- Sección 8: Operación. Establece *todos los requisitos necesarios, para medir el funcionamiento* del Sistema de Gestión de Seguridad de la Información, las expectativas de la dirección y su realimentación, además de *cumplir con lo que establece la norma ISO 27001:2013.*
  Es necesario que las empresas tengan planificadas y controladas, tanto las operaciones como los requisitos de seguridad. Los *activos, las vulnerabilidades y las amenazas,* ya no son la base de la evaluación de riesgos. Solo es necesario para identificar los riesgos asociados con la *confidencialidad, integridad y disponibilidad.*

  - 8.1 Planificación y control operacional.
  - 8.2 Apreciación de los riesgos de seguridad de la información.
  - 8.3 Tratamiento de los riesgos de seguridad de información.

- Sección 9: Evaluación de desempeño. La *base de la identificación, medición de la eficiencia* y el desempeño del sistema de gestión, sigue siendo la auditoría interna, junto con las revisiones que se llevan a cabo en el sistema de gestión.

  - 9.1 Seguimiento, medición, análisis y evaluación.
  - 9.2 Auditoría interna.
  - 9.3 Revisión.

- Sección 10: Mejora. El principal elemento que se utiliza durante el *proceso de mejora, son las no conformidades que están identificadas*, las cuales tienen que contabilizarse y compararse con las acciones correctivas, para asegurarse de que no se repitan, de tal manera, las *acciones correctivas que se llevan a cabo sean efectivas.*

  - 10.1 No conformidad y acciones correctivas.
  - 10.2 Mejora continua.

El desarrollo de este apartado, se encuentra en el archivo adjunto a este documento llamado *5. Auditoría de Cumplimiento.xls,* pestaña *5.4 Evaluación ISO 27001.*

5.5 Evaluación de controles, madurez y nivel de cumplimiento de la organización frente a ISO/IEC 27002:2013 - V1.0

Para evaluar estos aspectos de la seguridad de la organización, se analizarán con sobre los 114 controles que constituye la norma mencionada, con una respectiva descripción / objetivo del control, los cuales pueden ser verificados en la siguiente imagen:

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
ISO27002.es PATROCINADO POR:
GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

Figura 18. Lista de los 114 controles - ISO/IEC 27002:2013. [11]

5.6 Informe de Auditoría

5.6.1 Alcance

El alcance del SGSI se ha determinado, como “Asistencia al proceso de Gestión de la Seguridad de la Información”.

Para lo cual, esta labor de auditoría se llevó a cabo en los siguientes ámbitos:

- *Sistemas* (entornos en Desarrollo, pruebas y producción, equipos de procesamiento de la información, uso y cuidado de los diferentes dispositivos empleados en la realización de sus labores, empleo de la información, reglas de mantenimiento de equipos, entre otros.).

- *Instalaciones de la organización* (seguridad dentro de la empresa, áreas de almacenamiento de información, equipos en general, sistemas con acceso restringido, etc.).

- *Infraestructura de hardware y software.*

- *Servicios de comunicación* (redes, servicios web, correo electrónico, etc.).

- *Tecnología.*

- *Administración.*

- *Recursos Humanos.*

5.6.2 Resumen Ejecutivo para la Dirección

Con el desarrollo del trabajo realizado, se han detectado diferentes hallazgos y posibles amenazas, por los riesgos no tratados sobre el SGSI (Sistema de Gestión de la Seguridad de la Información) de la entidad, incumpliendo así, con la mayoría de los controles establecidos, tanto en la norma ISO/IEC 27001 (describe cómo gestionar la seguridad de la información en una empresa, y puede ser implementada en cualquier tipo de entidad, con o sin fines de lucro, privada o pública, pequeña o grande) como en la ISO 27002 (norma que constituye los principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una compañía), de tal manera que su sistema no se encontraba en el estado de funcionamiento apropiado.

Sin embargo, con el estudio hecho anteriormente (valoración de: activos, amenazas y vulnerabilidades, análisis diferencial entre la situación inicial de la organización y las normas, identificación de amenazas, evaluación de riesgos, declaración de aplicabilidad, nivel de riesgo aceptable y riesgo residual), donde se destacan considerables falencias que revelaron los resultados obtenidos, a partir de ahí se expuso diversas propuestas en proyectos, se aplicó un tratamiento de riesgos, para ejecutar las correspondientes implementaciones de los controles, los cuales no generó una inversión considerable, ya que para el desarrollo de esta plan, fue suficiente llevarlo a cabo con el recurso humano, que la empresa tenía ya contratado, junto con la asistencia del *Instituto Nacional de Ciberseguridad de España (INCIBE)*, para proporcionar los talleres en el tema de *Capacitación al personal en seguridad de la información,* por la cual no se realizó ninguna remuneración (debido a que la AEPA – Asociación de Empresarios Profesionales de Alicante), a la que pertenece la compañía objeto de este estudio, contactó con INCIBE, la cual afirma: “Actualmente no está prevista la organización de más talleres, tan solo participamos en jornadas organizadas por terceros: asociaciones empresariales, colegios profesionales, etc." https://www.incibe.es/protege-tu-empresa/talleres-ciberseguridad-pymes). Y la compra de:

- *Software Belarc Advisor*: Se emplea para la planificación de actualización de hardware, estado de la ciberseguridad, auditorías de aseguramiento de información, gestión de activos TI, gestión de la configuración, construye un perfil detallado de software y hardware instalado, inventario de red, parches faltantes de Microsoft, estado de antivirus y criterios de seguridad. Toda esta información del PC, se mantiene privada en el mismo y no se envía a ningún servidor Web. **Tuvo un costo total de 1.592,49 euros.**

- *Firewall Perimetral:* Es una herramienta de software o hardware, que tiene como propósito brindar protección extra, a la red de computadoras, limitando los ataques a vulnerabilidades de equipos y servidores, los accesos no autorizados y la mayoría de los códigos maliciosos automatizados. En otras palabras, se encarga de filtrar las conexiones que ingresan, a la red interna de la organización, así como también las conexiones de red dirigidas hacia el exterior de la misma, evitando que usuarios de Internet, que no han sido autorizados para ingresar a la red de la empresa, puedan tener acceso a la misma o que miembros de la organización, accedan a servicios externos para los cuales no han sido

autorizados. **Su costo fue de 566,62 euros IVA incluido + portes de 3,99 euros, para un total de 570,61 euros.**

Con la colaboración, interés para que mejore la operatividad de la empresa, compromiso, conocimiento, experiencia de un buen equipo de personas de las diferentes áreas, con quienes se trabajó en este proceso, comenzando por la Alta Dirección, Sistemas, Tecnología, Servicios de Comunicación, Administración, Recursos Humanos, entre otros. Junto a la labor y el apoyo dado a la empresa, por parte del equipo auditor, se consiguió la mejora del sistema, además del alcance de un SGSI estable (cumplimiento de requisitos establecidos por la norma y la empresa considere, acorde a sus necesidades, además de la reglamentación estipulada por la misma), de acuerdo a las normas estándar mencionadas anteriormente.

Por lo cual, después de la implementación respecto a la madurez en cumplimiento y efectividad de la entidad, frente al estado inicial (análisis diferencial), se observó que el SGSI tuvo mejoras en varios aspectos, mostrando un progreso en las reglas de las normas ISO 27001 e ISO 27002, quedando así el sistema en el estado que se busca, encontrándose actualmente en condiciones aceptables (cumplimiento con los requisitos de las normas), después de mitigar los riesgos que estaba presentando la empresa (al no tratarlos a tiempo), evitando pérdidas financiera exorbitantes a la compañía y permitiendo la continuidad del negocio.

5.6.3 Entrega de soportes en digital de los estudios realizados

- ArteagaPalaciosAndrea_TFM_SGSI.pdf (Memoria del TFM - Informe)

- 1. Situación Actual.xls
  - Organización de los roles.
  - Análisis Diferencial ISO 27002.
  - Análisis Diferencial ISO 27001.
  - Criterios Análisis Diferencial.

- 1. Cronograma del TFM.mpp (Ms. Project)

- 2. Sistema de Gestión Documental.xls
  - Gestión de Indicadores.

- 3. Análisis de Riesgos.xls
  - Valoración de activos.
  - Escala de valoraciones-Activos.
  - Identificación de Amenazas.
  - Valoración de Amenazas.
  - Valores Amenazas y Vulnerabilidades.
  - Valoración de Vulnerabilidades.
  - Evaluación de riesgos.
  - Declaración de Aplicabilidad (DdA).
  - Nivel de riesgo aceptable.
  - Tratamiento de riesgos.
  - Riesgo residual.

- 4. Propuesta de proyectos.xls
  - Sugerencias en la propuesta de proyectos.
  - Estimación en recursos, dedicación y costos de los proyectos propuestos.

- 4. Cronograma de tiempos para los proyectos recomendados.mpp

- 5. Auditoría de cumplimiento.xls
  - Evaluación de controles, madurez y nivel de cumplimiento de la organización, frente a ISO/IEC 27001:2013.
  - Evaluación de controles, madurez y nivel de cumplimiento de la organización, frente a ISO/IEC 27002:2013.
  - Valores y criterios aplicados.
  - Resultados Norma ISO 27001.
  - Gráficos con base a los resultados, obtenidos con la norma ISO/IEC 27001:2013.
  - Resultados Norma ISO 27001.
  - Gráficos con base a los resultados, obtenidos con la norma ISO/IEC 27002:2013.

6. Presentación de Resultados y Entrega de Informes

Una vez realizada la auditoría sobre la situación actual de la organización, con respecto a los controles planteados en las normas, ISO/IEC 27001:2013 e ISO/IEC 27002:2013, se encontraron las siguientes desviaciones de *No Conformidades – NC (Mayor y Menor),* también se dan a conocer las *Observaciones* y *Oportunidad de Mejora* correspondientes a ellas. De no atenderse pronto tales NC se pueden convertir en incidencias considerables para la empresa.

6.1 Resultados de los estudios entre la organización y la norma ISO 27001

Después del análisis realizado antes (Auditoría), la cantidad total encontrada de *No Conformidades (Mayor y Menor)* para este caso, y con base a los resultados obtenidos, cabe señalar que la evaluación de controles de la organización, frente a la norma ISO 27001, fueron hallados 10 No Conformidades Mayor, las cuales deben ser tratadas con alta prioridad y 15 No Conformidades Menor, donde se tienen que dar el tratamiento pertinente, para evitar perjuicios a la entidad.

A continuación se dará el detalle de las No Conformidades resultantes, con sus respectivos controles y cantidades totales por dominio:

Control	Dominio	No Conformidad		Controles incumplidos	Total
		Mayor	Menor		
4	Contexto de la organización	0	2	4.1 y 4.4	2
5	Liderazgo	1	3	5.1, 5.2 y 5.3	3
6	Planificación	1	3	6.1.1, 6.1.2, 6.1.3 y 6.2	4
7	Apoyo	3	3	7.1, 7.2, 7.3, 7.4, 7.5.1, 7.5.2 y 7.5.3	7
8	Funcionamiento	3	0	8.1, 8.2 y 8.3	3
9	Evaluación de desempeño	2	1	9.1, 9.2 y 9.3	3
10	Mejora	0	2	10.1 y 10.2	2
Total		**10**	**15**		**24**

Tabla 33. No Conformidad (Mayor y Menor) por dominio (apartados 4 a 10), con base a la norma ISO 27001

De acuerdo a estos resultados, se listarán los controles sobre el total de No Conformidad Mayor, en forma descendente:

- 7. Apoyo: Tres NC Mayor.
- 8. Funcionamiento: Tres NC Mayor.
- 9. Evaluación de desempeño: Dos NC Mayor.
- 5. Liderazgo: Una NC Mayor.

- 6. Planificación: Una NC Mayor.
- 4. Contexto de la organización: Cero NC Mayor.
- 10. Mejora: Cero NC Mayor.

En consecuencia se reconocen los controles, por los que se deben empezar a tratar: Apoyo, Funcionamiento, Evaluación de desempeño, Liderazgo y Planificación. (Ver archivo 5. Auditoría de cumplimiento.xls, pestañas Resultados y Gráficos).

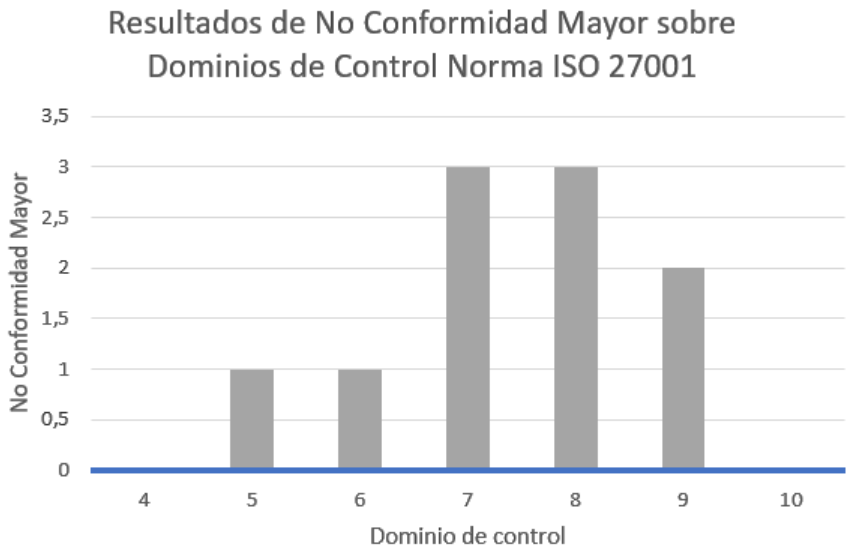


Gráfico 1. Resultados encontrados de No Conformidad Mayor con respecto a la norma estándar ISO/IEC 27001:2013

Ahora se listarán los controles sobre el total de No Conformidad Menor, en forma descendente:

- 5. Liderazgo: Tres NC Menor.
- 6. Planificación: Tres NC Menor.
- 7. Apoyo: Tres NC Menor.
- 4. Contexto en la organización: Dos NC Menor.
- 10. Mejora: Dos NC Menor.
- 9. Evaluación de desempeño: Una NC Menor.
- 8. Funcionamiento: Cero NC Menor.

En resumen, los controles que requieren de atención por NC Menor son: Liderazgo, Planificación, Apoyo, Contexto en la organización, Mejora y Evaluación de desempeño.

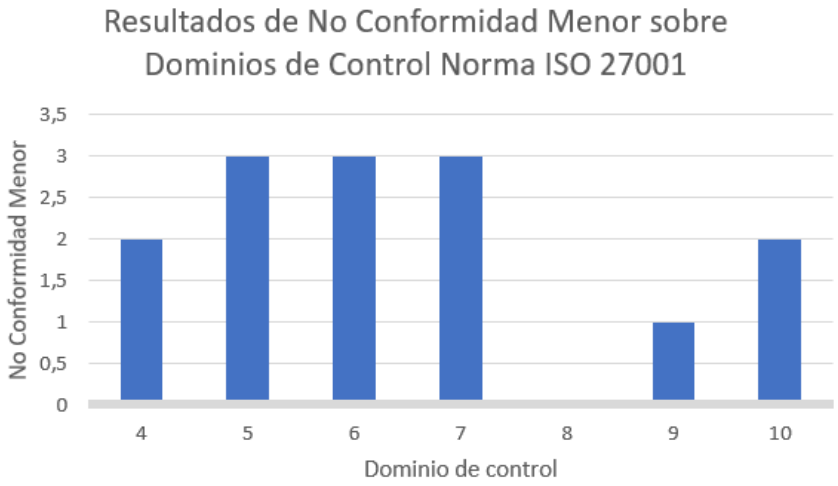


Gráfico 2. Resultados encontrados de No Conformidad Menor con respecto a la norma estándar ISO/IEC 27001:2013

Con relación a tales resultados, se tiene que los controles incumplidos por parte de la organización, frente a la norma estándar ISO 27001, son:

- 4.1 Comprensión de la organización y su contexto.
- 4.4 Sistema de Gestión de la Seguridad de la Información.
- 5.1 Liderazgo y compromiso.
- 5.2 Política.
- 5.3 Roles, responsabilidades y autoridades en la organización.
- 6.1.1 Consideraciones generales.
- 6.1.2 Apreciación de riesgos de seguridad de la información.
- 6.1.3 Tratamiento de los riesgos de seguridad de la información.
- 6.2 Objetivos de Seguridad de la Información y planificación para su consecución.
- 7.1 Recursos.
- 7.2 Competencia.
- 7.3 Concienciación.
- 7.4 Comunicación.
- 7.5.1 Consideraciones generales.
- 7.5.2 Creación y actualización.
- 7.5.3 Control de la información documentada.
- 8.1 Planificación y control operacional.
- 8.2 Apreciación de los riesgos de seguridad de la información.
- 8.3 Tratamiento de los riesgos de seguridad de información.
- 9.1 Seguimiento, medición, análisis y evaluación.
- 9.2 Auditoría interna.
- 9.3 Revisión por la Alta Dirección.
- 10.1 No conformidad y acciones correctivas.
- 10.2 Mejora continua.

Otra de las desviaciones a mencionar sobre el estudio realizado, se dio la *Observación* para atenuar, sobre los controles requeridos por ello y de los cuales, se describirán a continuación:

Control	Descripción	Desviación – Observación
4.2	Comprensión de las necesidades y expectativas de las partes interesadas.	No se tiene documentación, donde se encuentren acuerdos o compromisos.
7.3	Concienciación.	La persona contratada por la empresa debe tomar conciencia de: - La Contribución a la eficiencia del Sistema de Gestión de Seguridad de la Información (SGSI). - La política de seguridad de la información. - Las repercusiones de las no conformidades, con respecto a los requisitos del SGSI. - Los beneficios de una mejora del desempeño de la seguridad de la información.
7.4	Comunicación.	La organización debe estipular las necesidades de las comunicaciones, tanto internas como externas, concernientes al SGSI, que incluyan: - Quién debe comunicar. - Contenido de la comunicación. - Procesos para tener comunicación. - A quién comunicar. -En qué momento ha de hacerse la comunicación.
7.5.3	Control de la información documentada.	Para el control de dicha información documentada, la empresa debería tratar de llevar a cabo las siguientes actividades: - Control de cambios. - Retención y disposición. - Distribución, recuperación, acceso y uso. - Almacenamiento y preservación.
8.1	Planificación y control operacional.	La organización debería permanecer la información documentada en la medida solicitada, para que así, tener confianza en que los procesos se han ejecutado, de acuerdo a lo planeado.
8.2	Apreciación de los riesgos de seguridad de la información.	- Tener en cuenta los aspectos de la apreciación de los riesgos, reportando a los responsables de seguridad, para que registren las incidencias en sus seguimientos periódicos. - La compañía no debería centrarse solamente en los riesgos hallados, sino también tratar a fondo, en el análisis de riesgos, ya que éste resulta ser la base para cumplir con el objetivo de mejora continua, y en caso de presentarse una dificultad en la operación, corregirlo e implementar las acciones primordiales para evitar futuras amenazas.
8.3	Tratamiento de los riesgos de seguridad de información.	Se debe conservar documentado, los resultados del plan de tratamiento de riesgos.

9.2	Auditoría interna	Con la ejecución de la auditoría interna, se aporta información, con la cual se avala que el SGSI: - Es conforme con: los requisitos de la misma empresa para su SGSI y los requisitos de la norma estándar. - Está implementado y permanece funcionando de manera eficiente.
9.3	Revisión por la Alta Dirección.	- La norma ISO 27001:2013 establece períodos flexibles, para ejecutar esta actividad, pero no debe ser anualmente por requisito, sino de acuerdo a la planificación y requisitos de la seguridad de la información de cada empresa. - Esta revisión debe estar basado en tres partes esenciales: Revisión de la política de seguridad de la información; Revisión de los objetivos de seguridad de la información; Documentación y registro de los resultados obtenidos.
10.1	No conformidad y acciones correctivas.	La empresa debe conservar la información documentada, como evidencia de: - Los resultados de cualquier acción correctiva. - La naturaleza de las no conformidades y cualquier acción tomada en seguida.

Tabla 34. Observaciones dadas como otra de las desviaciones frente a la norma estándar ISO/IEC 27001:2013 (Ver archivo 5. Auditoría de cumplimiento)

De la misma forma, se estimó *Oportunidad de mejora* para el siguiente caso:

Control	Descripción	Oportunidad de mejora
4.3	Determinación del alcance del SGSI.	Realizar seguimiento y actualización.

Tabla 35. Oportunidad de mejora estimada, como desviación con respecto a la norma ISO 27001

Después de las respectivas implementaciones, los resultados obtenidos en la evaluación de *Madurez,* tanto en la situación inicial de la organización (ver archivo 1. Situación Actual, hoja Análisis Diferencial ISO 27001) como en el estudio de la auditoría (ver archivo 5. Auditoría de cumplimiento, pestaña 5.4 Evaluación ISO 27001), el cual fue llevado a cabo, para estimar la madurez en ambas situaciones, sobre la seguridad en lo referente a los dominios de control, en este caso, los apartados 4 a 10 evaluados, para determinar el cumplimiento sobre estos controles, de acuerdo a lo que estipula la norma ISO/IEC 27001:

- 4.1 Comprensión de la organización y su contexto.
- 4.4 Sistema de Gestión de la Seguridad de la Información.
- 5.1 Liderazgo y compromiso.
- 5.2 Política.

- 5.3 Roles, responsabilidades y autoridades en la organización.
- 6.1.1 Consideraciones generales.
- 6.1.2 Apreciación de riesgos de seguridad de la información.
- 6.1.3 Tratamiento de los riesgos de seguridad de la información.
- 6.2 Objetivos de Seguridad de la Información y planificación para su consecución.
- 7.1 Recursos.
- 7.2 Competencia.
- 7.3 Concienciación.
- 7.4 Comunicación.
- 7.5.1 Consideraciones generales.
- 7.5.2 Creación y actualización.
- 7.5.3 Control de la información documentada.
- 8.1 Planificación y control operacional.
- 8.2 Apreciación de los riesgos de seguridad de la información.
- 8.3 Tratamiento de los riesgos de seguridad de información.
- 9.1 Seguimiento, medición, análisis y evaluación.
- 9.2 Auditoría interna.
- 9.3 Revisión por la Alta Dirección.
- 10.1 No conformidad y acciones correctivas.
- 10.2 Mejora continua.

NIVEL DE CUMPLIMIENTO		
Control	**Estado Inicial**	**Estado Final**
4.1 Comprensión de la organización y su contexto.	2	3
4.2 Comprensión de las necesidades y expectativas de las partes interesadas.	2	3
4.3 Determinación del alcance del SGSI.	2	4
4.4 Sistema de Gestión de la Seguridad de la Información.	2	3
5.1 Liderazgo y compromiso.	2	3
5.2 Política.	2	4
5.3 Roles, responsabilidades y autoridades en la organización.	1	4
6.1.1 Consideraciones generales.	0	3
6.1.2 Apreciación de riesgos de seguridad de la información.	1	4
6.1.3 Tratamiento de los riesgos de la seguridad de la información.	1	3
6.2 Objetivos de seguridad de la información y la planificación para su consecución.	1	4
7.1 Recursos.	1	4
7.2 Competencia.	1	4
7.3 Concienciación.	2	3
7.4 Comunicación.	0	4
7.5.1 Consideraciones generales.	2	3
7.5.2 Creación y actualización.	2	3
7.5.3 Control de la información documentada.	0	3
8.1 Planificación y control operacional.	0	4
8.2 Apreciación de los riesgos de seguridad de la información.	0	3
8.3 Tratamiento de los riesgos de seguridad de la información.	1	3
9.1 Seguimiento, medición, análisis y evaluación	2	3
9.2 Auditoría interna.	0	3
9.3 Revisión por la dirección.	0	3
10.1 No conformidad y acciones correctivas.	1	3
10.2 Mejora continua.	1	3

Tabla 36. Comparación de Madurez en Nivel de Cumplimiento, frente a la norma ISO 27001:2013

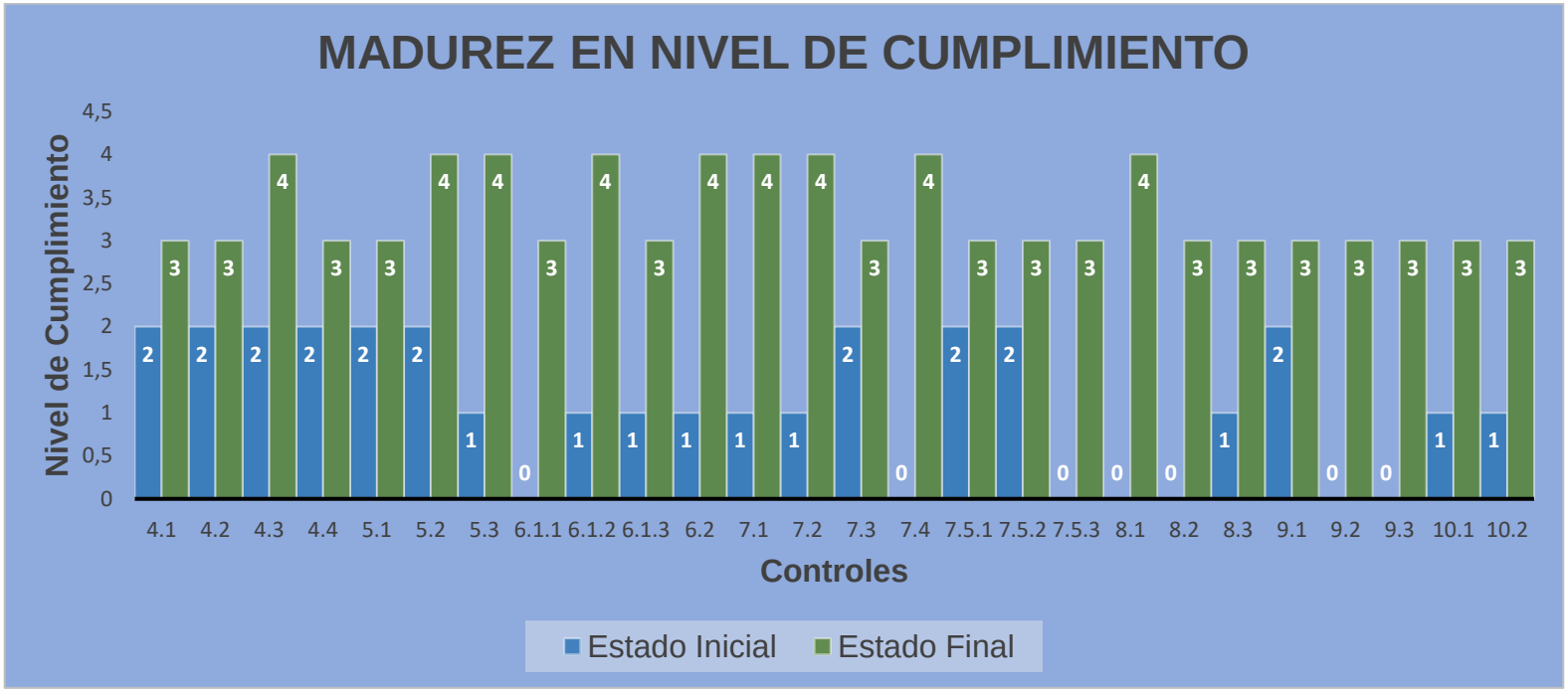


Gráfico 3. Comparación de madurez en el nivel de cumplimiento, entre los resultados obtenidos del análisis diferencial y auditoría, con respecto a la norma ISO 27001:2013

EFECTIVIDAD		
Control	**Inicial**	**Final**
4.1	50%	90%
4.2	50%	90%
4.3	50%	95%
4.4	50%	90%
5.1	50%	90%
5.2	50%	95%
5.3	10%	95%
6.1.1	0%	90%
6.1.2	10%	95%
6.1.3	10%	90%
6.2	10%	95%
7.1	10%	95%
7.2	10%	95%
7.3	50%	90%
7.4	10%	95%
7.5.1	50%	90%
7.5.2	50%	90%
7.5.3	0%	90%
8.1	0%	95%
8.2	0%	90%
8.3	10%	90%
9.1	50%	90%
9.2	0%	90%
9.3	0%	90%
10.1	10%	90%
10.2	10%	90%

Tabla 36. Comparación de Madurez en Efectividad, frente a la norma ISO 27001:2013

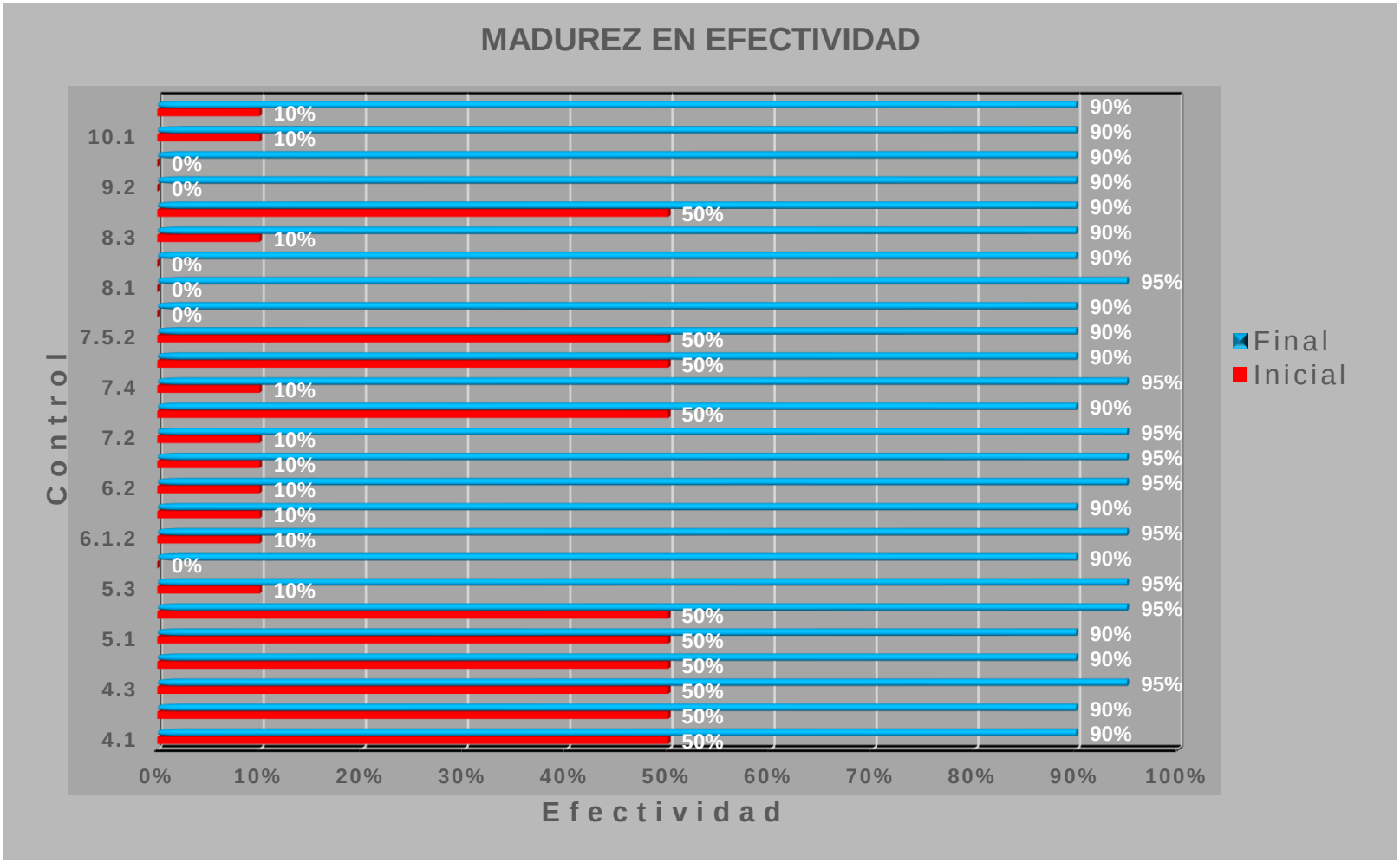


Gráfico 4. Comparación de Madurez en Efectividad, con respecto a la norma ISO 27001:2013

Como se observa en los anteriores resultados, en lo que respecta a las desviaciones (No Conformidad, Observación y Oportunidad de mejora), la madurez en el nivel de cumplimiento de los controles y la efectividad de los mismos, frente al Estado Inicial y el Estado Final, ha variado considerablemente a favor del mejoramiento en la organización.

Los resultados presentados brindan una perspectiva global, sobre el estado actual de seguridad, en la gestión de la información con respecto a la norma ISO/IEC 27001:2013. Además el estado final de la empresa, está alineado con sus objetivos, metas y estrategias determinadas por la entidad.

El hecho de haber llevado a cabo la implementación de los controles, ha permitido que la compañía pueda:

- Obtener el cumplimiento en sus objetivos definidos.
- Haber tratado a tiempo, las insuficiencias encontradas, aplicando los correctivos pertinentes y mitigando, los riesgos a los que estaba expuesta la organización, antes de que se salieran de su cauce.
- Estar en un nivel aceptable, frente a la situación inicial que presentaba.
- Tener en este momento, un buen funcionamiento en el sistema de gestión y el cual, debe seguirse haciendo seguimiento, para mantener un nivel estable.
- Reconocer el equipo de trabajo comprometido y dispuesto, ayudar en la mejora de sus diferentes labores desempeñados, en los cargos que se encuentran desempeñando.

Gráfico 5. Síntesis de los resultados en cantidad de controles no cumplidos, con base a la norma ISO 27001

La siguiente tabla, contiene los valores del gráfico anterior, los cuales representan los resultados obtenidos de la auditoría:

Dominio	Valor cualitativo	Cantidad de controles incumplidos
4. Contexto de la organización	Repetible	4
5. Liderazgo	Repetible	2
	Inicial	1
6. Planificación	No existente	1
	Inicial	3
7. Apoyo	Inicial	2
	Repetible	3
	No existente	2
8. Funcionamiento	No existente	2
	Inicial	1
9. Evaluación de desempeño	Repetible	1
	No existente	2
10. Mejora	Inicial	2

Tabla 37. Valores que representan el estado de madurez (CMM)

6.2 Resultados de los estudios entre la organización y la norma ISO 27002

Una de las desviaciones obtenidas en la Auditoría, fue de *No Conformidades (Mayor y Menor)*, tales resultados atañen a la evaluación de controles, frente a la norma ISO 27002, se encontraron 80 No Conformidades Mayor y 34 No Conformidades Menor.

Control	Dominio	No Conformidad		Controles incumplidos
		Mayor	Menor	
5	Políticas de seguridad.	2	0	N.C.Ma.: A.5.1.1, A.5.1.2
6	Aspectos organizativos de la seguridad de la información.	6	1	N.C.Ma.: A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4, A.6.2.1, A.6.2.2 N.C.Me.: A.6.1.5
7	Seguridad ligada a los recursos humanos.	6	0	N.C.Ma.: A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1
8	Gestión de activos.	10	0	N.C.Ma.: A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1,A.8.3.2, A.8.3.3
9	Control de accesos.	10	4	N.C.Ma.: A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.4 N.C.Me.: A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.5
10	Cifrado.	0	2	N.C.Me.: A.10.1.1, A.10.1.2
11	Seguridad física y ambiental.	10	5	N.C.Ma.: A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.2, A.11.2.7, A.11.2.8 N.C.Me: A.11.2.3, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.9
12	Seguridad en la operativa.	9	5	N.C.Ma.: A.12.2.1,A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.5.1, A.12.6.1, A.12.6.2, A.12.7.1 N.C.Me: A.12.1.1, A.12.1.2, A.12.1.3, A.12.1.4, A.12.3.1
13	Seguridad en las telecomunicaciones.	6	1	N.C.Ma.: A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4 N.C.Me.: A.13.1.3

14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	10	2	N.C.Ma.: A.14.1.1, A.14.1.2, A.14.1.3 A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A,14,3,1 N.C.Me.: A.14.2.8, A.14.2.9
15	Relaciones con suministradores.	1	4	N.C.Ma.: A.15.2.2 N.C.Me.: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1
16	Gestión de incidentes en la seguridad de la información.	1	6	N.C.Ma.: A.16.1.1 N.C.Me.: A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	1	3	N.C.Ma.: A.17.2.1 N.C.Me.: A.17.1.1, A.17.1.2, A.17.1.3
18	Cumplimiento.	8	0	N.C.Ma: A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5, A.18.2.1, A.18.2.2, A.18.2.3

Tabla 38. Resultados de No Conformidades halladas en la organización , con respecto a la norma ISO 27002:2013

Debido a que la cantidad de controles en este caso es muy amplio (114), lo cual puede hacer que se vuelva muy complejo su presentación gráfica, debido a ello se ha llevado a cabo un resumen, agrupándolos por dominios, brindando un informe ameno, en donde se darán resultados concisos. Sin embargo, para la confirmación y ampliación de la información, se puede consultar en los siguientes archivos:

- 1. Situación Actual.xls, hoja Análisis Diferencial ISO 27002, donde se plantea el escenario inicial de la organización, antes de realizar el estudio presentado en este documento.

- 5. Auditoría de Cumplimiento.xls, hoja 5.5 Evaluación ISO 27002, en el que se halla un análisis conciso, referente a la evaluación de controles, madurez y nivel de cumplimiento de la organización, tomando como base la norma ISO 27002.

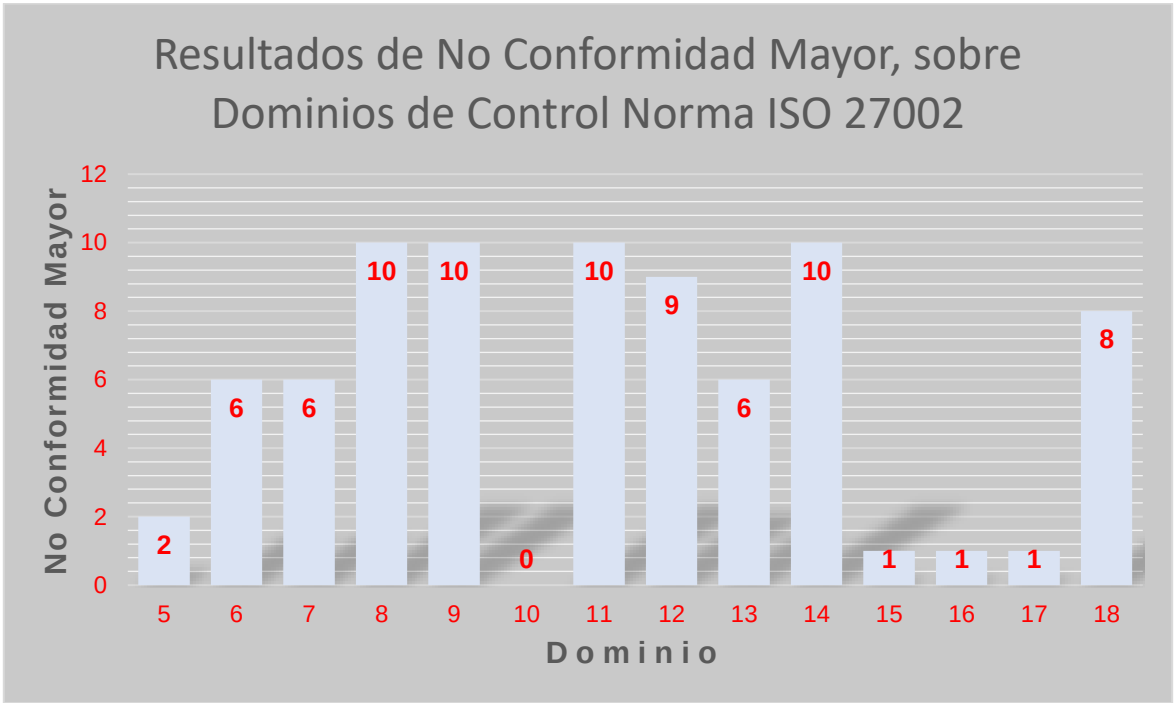


Gráfico 6. Resultados obtenidos de la Evaluación de Controles, tratados sobre norma ISO 27002

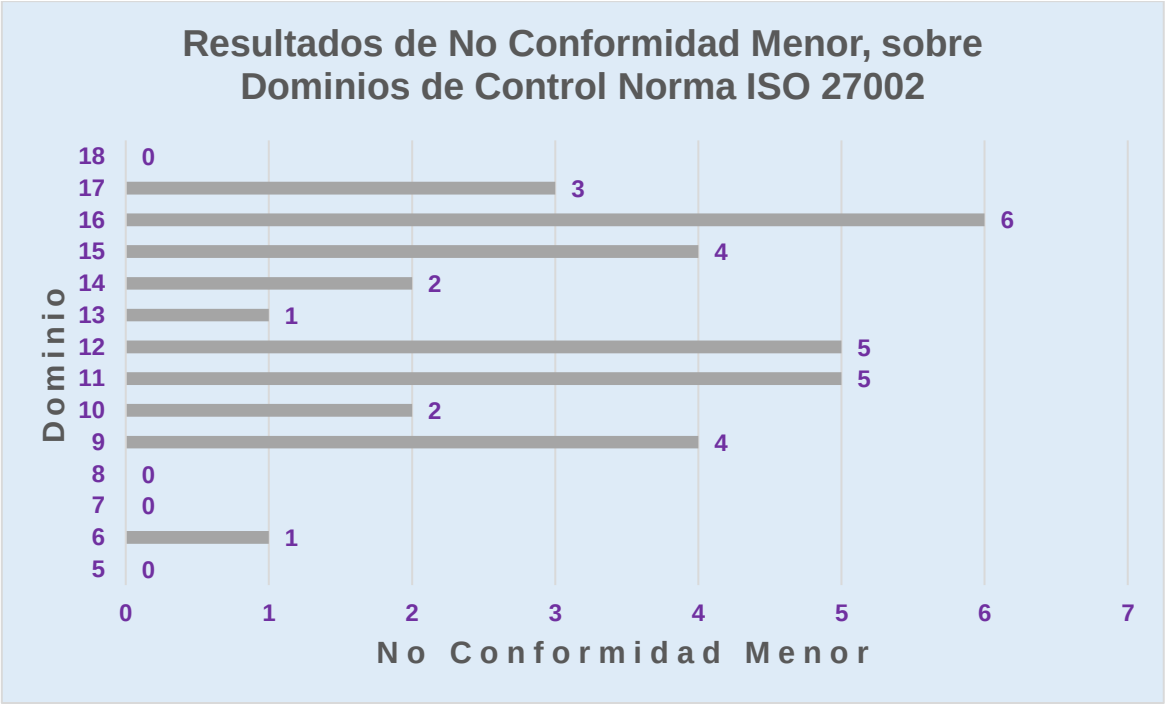


Gráfico 7. Resultados obtenidos de la Evaluación de Controles, tomando como base la norma ISO 27002

En los parámetros presentados en las gráficas, se puede observar prontamente, la cuantía de No Conformidades Mayor es alta en un solo dominio, tales son los casos de los dominios 8, 9, 11, 12, 14 y 18, seguidos por 6, 7 y 13. Lo cual está dando a conocer alertas, de los riesgos que se están generando y se deben atender de manera inmediata, así evitar que tales peligros se conviertan en amenazas reales.

Otra de las desviaciones a nombrar en este apartado, es la *Observación* para atenuar, sobre los controles requeridos por ello y de los cuales, se dará detalle a continuación:

Control	Descripción	Desviación – Observación
A.6.1.1	Asignación de responsabilidades para la seguridad de la información.	Cada activo de información existente en la organización, debe tener un dueño responsable de su seguridad. La información que la compañía use, para el cumplimiento de sus objetivos de negocio, debe tener asignado un dueño, quién la utiliza en su área y es responsable de usarlo correctamente.
A.6.1.2	Segregación de tareas.	Se deben separar las tareas, para minimizar las probabilidades de cambios no autorizada o no intencional, con respecto a la información de la empresa, o el uso inapropiado de los activos de la entidad.
A.6.1.3	Contacto con las autoridades.	Apoyo en la solución de conflictos, en lo que respecta a la seguridad de la información en la organización.

A.6.1.4	Contacto con grupos de interés especial.	Es conveniente disponer de contactos apropiados, con grupos de interés especial, foros y asociaciones profesionales, especialistas en el tema de la seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Durante la planeación y ejecución de proyectos de la entidad, además de contar con el apoyo de las partes interesadas, debe intervenir el área encargada de la seguridad de la información, como generador de recomendaciones, en el tema de evaluación de los riesgos con tales proyectos.
A.6.2.1	Política de uso de dispositivos para movilidad.	Se debe tener una política y medidas de seguridad de soporte, para administrar los riesgos originados por el uso de dispositivos para movilidad.
A.6.2.2	Teletrabajo.	Proteger la información a la que se tiene acceso, es procesada o almacenada en lugares, en los que se desarrolla teletrabajo. Tal información debería estar encriptada y disponer del software requerido, para salvaguardar este activo de los ataques que se puedan dar.
A.7.1.1	Investigación de antecedentes.	Con este proceso, se quiere mitigar los riesgos concernientes al uso de la información.
A.7.1.2	Términos y condiciones de contratación.	En los acuerdos contractuales tanto con empleados como contratistas, se deben determinar sus responsabilidades y de la misma organización, frente a la seguridad de la información.

Tabla 39. Observaciones dadas como otra de las desviaciones frente a la norma estándar ISO/IEC 27001:2013

Esta desviación también se debe tratar, ya que por ser solamente observaciones, no quiere decir se deba prestar menos importancia, aunque en el momento no resultan ser relevantes, es aconsejable aplicar un proceso de mejora a cada uno, antes de que se conviertan en No Conformidades.

Siguiendo con la temática de la evaluación, se prosigue a indicar los resultados concernientes a la madurez en el nivel de cumplimiento, en relación al estado inicial de la empresa (antes de este estudio) y el estado final (después de las implementaciones), con la respectiva tabla de valores, recopilados durante la auditoría que se realizó anteriormente, para que de esta forma se pueda tener claridad con el gráfico estadístico:

NIVEL DE CUMPLIMIENTO		
Dominio	**Estado Inicial**	**Estado Final**
5	0	3
6	0	3
	1	
7	0	3
8	0	4
		3
9	0	4
	2	3
	1	
10	1	3
11	0	4
	2	3
	1	
12	0	4
	2	3
	1	
13	0	4
	2	3
14	0	4
	1	3
15	0	3
	1	
16	0	4
	1	3
17	0	3
	1	
18	0	4
		3

Tabla 40. Resultados de la comparación de Madurez, en Nivel de Cumplimiento, con base a la ISO 27002.

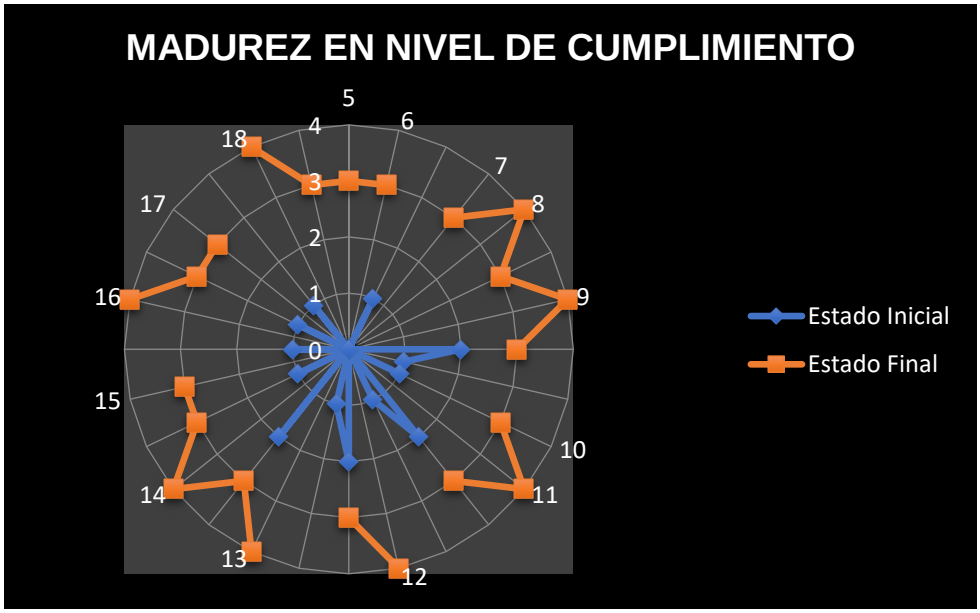


Gráfico 8. Gráfico comparativo de madurez en nivel de cumplimiento, de acuerdo al estado inicial y final de la empresa, sobre la norma ISO 27002.

EFECTIVIDAD		
Dominio	**Efectividad Inicial**	**Efectividad Final**
5	0%	90%
6	0%	90%
	10%	
7	0%	90%
8	0%	95%
		90%
9	0%	95%
	50%	90%
	10%	
10	10%	90%
	50%	
11	0%	90%
	10%	95%
12	0%	90%
	10%	95%
	50%	
13	0%	90%
	50%	95%
14	0%	90%
	10%	95%
15	0%	90%
	10%	95%
16	0%	90%
	10%	95%
17	0%	90%
	10%	
18	0%	90%
		95%

Tabla 41. Resultados de la comparación de Madurez, en Efectividad, con base a la ISO 27002.

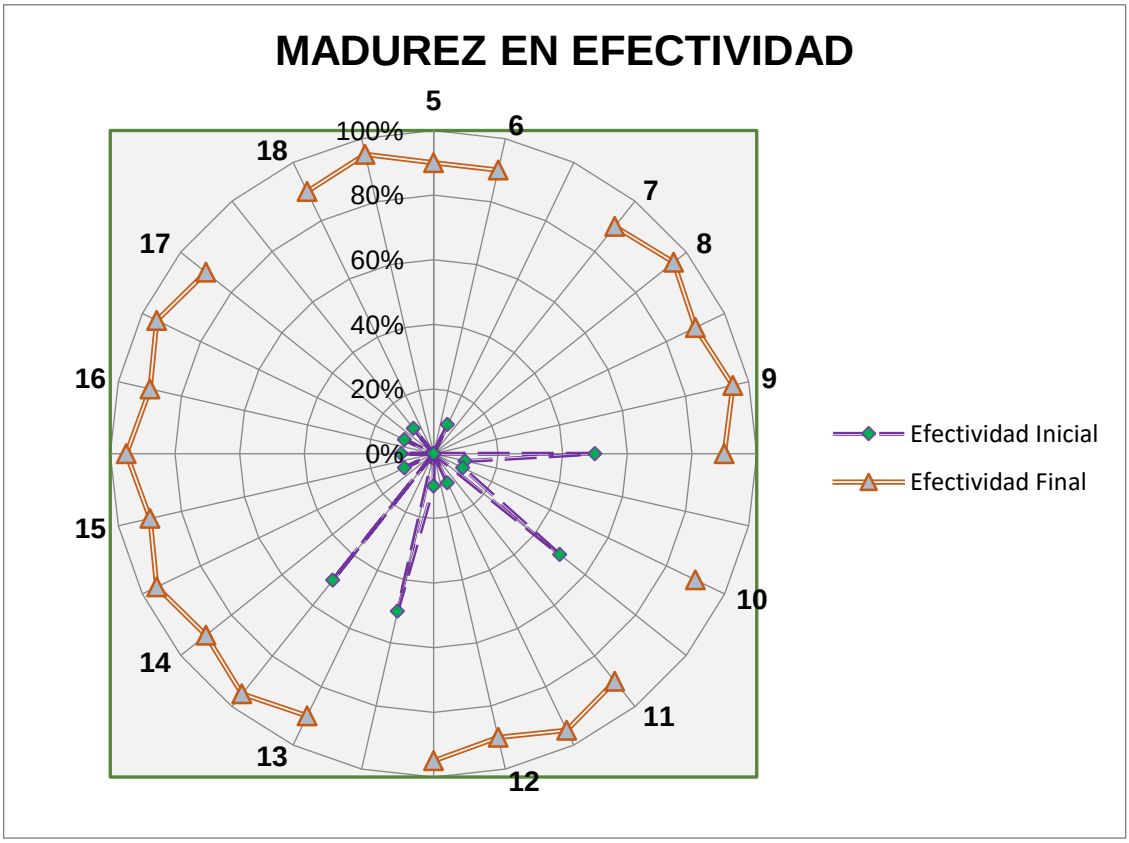


Gráfico 9. Gráfico comparativo de madurez en efectividad, de acuerdo al estado inicial y final de la empresa, sobre la norma ISO 27002.

Se sintetizaron los resultados de las evaluaciones de controles (No Conformidad Mayor, No Conformidad Menor, Observación y Oportunidad de mejora), obtenidos por dominios, al igual que los estados de madurez (Nivel de Cumplimiento y Efectividad), sobre la situación inicial de la entidad (es decir, antes de comenzar este estudio) y CMM después de la implantación de los proyectos propuestos, a manera comparativa en el segundo aspecto mencionado.

Con lo cual se puede verificar que dicho trabajo, con relación a la norma ISO/IEC 27002:2013 (guía de buenas prácticas con los objetivos y controles recomendados, para la seguridad de la información), presenta una evolución y mejora de madurez en su SGSI.

Donde para la entidad, el nivel de cumplimiento ecuánime fue el calificado por, *Proceso Definido (L3),* con una efectividad del 90% y por ello, la mayoría de los salvaguardas quedaron en este nivel, aunque se dieron casos en lo que se logró superar este valor objetivo, quedando en *Gestionado y medible (L4)* con el 95% de su efectividad. Por ello emergió el compromiso por parte de la organización, de continuar con las medidas requeridas de mejora continua, con el propósito de llegar al nivel *Optimizado (L5 – 100%)* y así conseguir la certificación.

Gráfico 10. Síntesis de los resultados de controles que no se cumplen por dominio, con base a la norma ISO 27002

Lo anterior indica que por un dominio, tiene un estado de madurez determinado por una cantidad representativa, la cual señala el valor de salvaguardas que no se cumplen.

6.3 Conclusiones generales sobre el cumplimiento de requisitos - SGSI

La empresa necesitó implementar una gran cantidad de controles y mejorar la efectividad, sobre aquellos que se encontraron en estados como, *No existente, Inicial y Repetible o Reproducible,* lo cual dio a conocer un mal funcionamiento en el sistema, con respecto a lo estipulado por las normas ISO 27001 (la cual engloba, los requisitos necesarios para la implementación de un SGSI) e ISO 27002 (se trata de una guía sobre las buenas prácticas, con los dominios, objetivos y controles recomendados, para la Seguridad de la Información).

De acuerdo a los resultados obtenidos, con los cuales se puede abstraer el estado donde está perjudicando al sistema, muestra exactamente donde se encuentran tales hallazgos, y las vulnerabilidades más fuertes de la organización, como se dan a conocer los datos registrados en ***gráficos 5 y 6***. Razón por la cual se hizo el estudio requerido, sobre las normas ISO 27001 e ISO 27002, arrojando información que demuestra, las grandes falencias se encuentran por el mayor incumplimiento, en la evaluación realizada sobre la segunda norma y en la primera norma, existe un nivel regular de cumplimiento; las cuales se listan a continuación, teniendo en cuenta que los controles se han agrupado por dominios (grupos generales):

- Según la norma ISO 27002:
  - El dominio 8 (Gestión de activos), presenta 10 controles en estado de No Existen.
  - El dominio 9 (Control de accesos) -> 10 controles que No Existen.
  - El dominio 11 (Seguridad física y ambiental) -> 10 controles
  - Dominio 12 -> 9 controles No Existen.
  - Dominio 14 -> 9 controles No Existen.
  - Dominio 18 -> 6 controles No Existen.
  - Dominio 6 (Aspectos organizativos de la Seguridad de la Información -> 6 controles No Existen.
  - Dominio 13 (Seguridad en las telecomunicaciones) -> 6 controles No Existen.

Para ampliar la información, se recomienda ver el archivo en digital llamado 5. Auditoría de Cumplimiento, Evaluación ISO 27002.

- Según la norma ISO 27001:
  - Dominio 7 (Apoyo) -> 2 controles No Existen.
  - Dominio 8 (Funcionamiento) -> 2 controles No Existen.
  - Dominio 9 (Evaluación de desempeño) -> 2 controles No Existen.

Igual que el caso anterior, se sugiere ver el archivo en digital, denominado 5. Auditoría de Cumplimiento, Evaluación ISO 27001.

Una vez se conoció la situación actual de la organización, se recurrió a presentar los proyectos que ayudarían, con la implementación y cumplimiento de los salvaguardas, de acuerdo a lo establecido por las normas. Puesto que para los

dos casos, se encontraron falencias, pero como se conoció, el mayor nivel de incumplimiento está en los requisitos propuestos por la norma ISO 27002. Los cuales fueron los primeros en tratarse entre el equipo auditor y el personal correspondiente de la organización, quienes nos brindaron mucho apoyo y colaboración al conocer estos resultados, se concienciaron y comprometieron ayudar, para proteger el activo información de la empresa.

Con la labor realizada entre todos y el cumplimiento de las actividades, correspondientes a cada responsable de área (contando con la Alta Dirección, Sistemas, Tecnología, Recursos Humanos, entre otros), señaladas en el cronograma de trabajo, se alcanzó a cumplir con el propósito, dejar estable el SGSI.

Después de esto, la empresa se comprometió a realizar un seguimiento y monitoreo a su SGSI, con el fin de mejorarlo, mitigar cualquier riesgo que surja, conseguir la certificación y llevar a cabo la continuidad del negocio, con la seguridad de su información.

BIBLIOGRAFÍA

[1] Cruz, A., Daniel. Análisis de riesgos. Material docente de la UOC.

[2] Alonso, C., José María; Castillo, P., Sergio; García, A., Joaquín; Guzmán, S., Antonio; Herrera, J., Jordi; Laguna, D., Pedro; Martín, B., Guillermo; Robles, M., Sergi (2011). Vulnerabilidades de seguridad. Material docente de la UOC. Barcelona: Eureca Media, SL.

[3] García, A., Joaquín. Sistemas de detección de intrusos en red (2011). Material docente de la UOC. Barcelona: Eureca Media, SL.

WEBGRAFÍA

[1] https://advisera.com/27001academy/es/que-es-iso-27001/

[2] https://www.iso.org/standard/50297.html

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

[4] http://www.magazcitum.com.mx/?p=2397%C2%B7.XHxQoaCCE0M#.XHzyK6B7ncs

[5]

http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html

[6]
https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XH0JhqB7ncs

[7] https://exacato.wordpress.com/2015/01/28/la-gestion-del-riesgo/

[8] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNBoFdI19dg. [Último acceso: 28 Octubre 2017].

[9] https://administracionelectronica.gob.es/ctt/magerit#.WfS3WI_Wxdg

[10] https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

[11] http://www.iso27000.es/download/ControlesISO27002-2013.pdf

[12] https://www.uoc.edu/portal/es/arxiu/gestio-documental/que-es/index.html

[13]
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=2ahUKEwjpsrXg3vrgAhUGJBoKHUzsDF0QFjAJegQICRAC&url=https%3A%2F%2Fadministracionelectronica.gob.es%2Fpae_Home%2Fdam%2Fjcr%3Ac1e4cb3c-028a-4ae7-a2ff-54553a183749%2F91inciativas-legales.pdf&usg=AOvVaw2uJEPdoXkiAKa79tBFyw8i

[13] https://www.uoc.edu/portal/es/arxiu/gestio-documental/que-es/index.html

[14] https://ieeexplore.ieee.org/document/8010711

[15] https://link.springer.com/article/10.1057/rm.2012.9

[16] https://www.iso.org/standard/65694.html

[17] https://www.escuelaeuropeaexcelencia.com/2018/01/iso-310002018-estandar-renovado-simplificado-la-gestion-riesgos/

[18] https://www.iso.org/standard/43170.html

[19] https://www.nueva-iso-45001.com/

[20] https://iso45001.es/

[21] https://www.iso.org/standard/75281.html

[22] https://link.springer.com/chapter/10.1007/978-3-8348-9870-8_3

[23] https://www.ticportal.es/temas/sistema-gestion-documental/que-es-sistema-gestion-documental

[24] https://www.sogeti.es/politica-de-seguridad-de-la-informacion/

[25] https://www.pmg-ssi.com/2014/12/iso-27001-la-politica-de-seguridad-en-la-organizacion/

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

[27] https://dialnet.unirioja.es/descarga/articulo/4527565.pdf

[28] https://advisera.com/2_7001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/

[29] https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

[30] https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

[31] https://www.escuelaeuropeaexcelencia.com/2014/04/iso27001-auditoria-interna-sgsi/

[32] https://www.pmg-ssi.com/2013/11/iso-27001-auditorias-de-los-controles-del-sistema-de-seguridad/

[33] https://www.sothis.tech/que-indicadores-de-un-sgsi-pueden-ser-utiles-para-la-alta-direccion/

[34] http://ingertec.com/iso-27001-revision-por-la-direccion/

[35] http://sigud.udistrital.edu.co/vision/filesSIGUD/Gestion%20Integrada/Documentos/GI-GUI-004.pdf

[36] http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/.

[37] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WNBoFdI19dg.

[38] https://administracionelectronica.gob.es/ctt/magerit#.WfS3WI_Wxdg.

[39] https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. [Último acceso: 28 Octubre 2017].

[40] http://www.iso27000.es/glosario.html

[41] https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/12028/1/52437232.pdf

[42] https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

[43] http://www.corponor.gov.co/NORMATIVIDAD/NORMA%20TECNICA/Norma%20T%E9cnica%20NTC%205254.pdf

[44] https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[45] https://www.escuelaeuropeaexcelencia.com/2018/07/principales-cambios-en-iso-310002018-gestion-de-riesgos/

[46] https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

[47] https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

[48] https://www.pilar-tools.com/doc/magerit/v2/cat-es-v11.pdf

[49] https://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf

[50] https://www.pmg-ssi.com/2015/04/iso-27001-la-gestion-del-riesgo-en-un-sgsi/

[51] https://www.um.es/docencia/barzana/GESESI/GESESI-Metodo-MAGERIT.pdf

[52] https://ericmorana.wordpress.com/2012/10/29/niveles-de-riesgo-aceptable-versus-criterios-de-aceptacion-del-riesgo/

[53] https://www.iit.comillas.edu/pfc/resumenes/44a527e27a231.pdf

[54] https://es.scribd.com/doc/232787821/ISO27001-2013-Anexo-a-En-Tabla-Excel

[55] https://www.academia.edu/17629009/METODOLOGIA_DE_GESTION_DE_RIESGOS_por Gustavo_Ramos

[56] https://advisera.com/27001academy/es/documentation/procedimiento-para-control-de-documentos-y-registros/

[57] https://smarterworkspaces.kyocera.es/blog/los-6-principales-tipos-sistemas-informacion/

[58] https://www.tecnozero.com/firewall/

[59] https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

[60] https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

[61] https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[62] http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf

[63] http://www.ciifen.org/index.php?option=com_content&view=category&layout=blog&id=84&Itemid=336&lang=es

[64] https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

[65] http://www.iso27000.es/glosario.html

[66] https://www.pmg-ssi.com/2017/07/iso-27001-contexto-alcance-y-politica/

[67] https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

[68] https://www.escuelaeuropeaexcelencia.com/2015/11/iso-31000-terminos-definiciones/

[69] https://www.pmg-ssi.com/2018/05/auditorias-internas-iso-27001/

[70] http://ingertec.com/auditoria-interna-iso-27001/

[71] https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

[72] http://siga.unal.edu.co/images/informes-presentaciones/ISO_31000_Gestion_riesgo.pdf

[73] https://es.slideshare.net/JoseSzarfman/i-la-nueva-norma-iso-31000-2018-y-la-gestion-de-riesgos

[74] https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

[75] https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[76] https://www.globales.es/imagen/internet/Informaci%C3%B3n%20General%20CMMI.pdf

[77] https://cdn.www.gob.pe/uploads/document/file/205393/R._D._002-2018-VIVIENDA-OGEI.pdf

[78] https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/

[79] https://www.pmg-ssi.com/2016/01/iso-27001-version-2013-que-hay-despues-de-auditoria-certificacion/

[80] https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

[81] http://cv.uoc.edu/webapps/xwiki/wiki/matm1709/view/Main/An%C3%A1lisis+diferencial