Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de final de máster

Elaboración de un plan de implementación de la Norma ISO/IEC 27001:2013 en una empresa prestadora de servicios de acueducto y alcantarillado.

Julieth Parra Casallas

Colombia, Mayo 2015

Tabla de contenido

Tabla de figuras

1 HISTORIA NORMAS ISO/IEC 27001: 2013 E ISO/IEC 27002:2014

1.1 NORMA ISO/IEC 27001:2013

La ISO 27001 es la norma que especifica los requisitos necesarios para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información.

Figura No. 1. Resumen historia ISO/IEC 27001:2013

Su origen fue:

- La BS 7799-1, publicada en 1995: serie de mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Incluía recomendaciones que no daban opción a ningún tipo de certificación ni establecía la forma de conseguirla.

- La BS 7799-2, en 1998 (segunda parte de la BS 7799-1): establecía los requisitos a cumplir para tener un Sistema de Gestión de Seguridad de la Información certificable.

  Ambas partes fueron revisadas en el año 1999 y en el año 2000 la Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799. En este momento la norma no experimentó grandes cambios. En el año 2001 fue revisada de acuerdo a la línea de las normas ISO.

- Nueva versión de la BS 7799 en el año 2002: incluyó la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.

- Estándar ISO 27001 en el año 2005: modificación de la ISO 17799.

- Estándar ISO 27002:2005 en el año 2007: surge de renombrar la ISO 17799

- Nueva versión de la ISO 27001:2007

- ISO 27001:2007/1M: 2009: Esta norma es conocida en Chile como NCh-ISO27001, en España como UNE-ISO/IEC 27001:2007, en Colombia como NTC-ISO-IEC 27001, en Venezuela como Fondo norma ISO/IEC 27001, en Argentina como IRAM-ISO IEC 27001, en México como NMX-I-041/02-NYCE y en Uruguay como UNIT-ISO/IEC 27001.

- Nueva versión de la ISO 27001 en el año 2013: trae cambios en la estructura, en la evaluación y tratamiento de los riesgos.

- Nueva versión de la ISO 27002 en el año 2014: Se actualiza de acuerdo con los cambios de la norma ISO 27001:2013

1.2 ESTRUCTURA ACTUAL NORMA ISO/IEC 27001:2013

La nueva ISO 27001 de desarrolla en base al anexo SL de ISO, el cual proporciona el formato y lineamientos bajo una misma estructura a cumplir por todos los documentos relacionados con los sistemas de gestión, lo que facilita la integración entres sistemas.

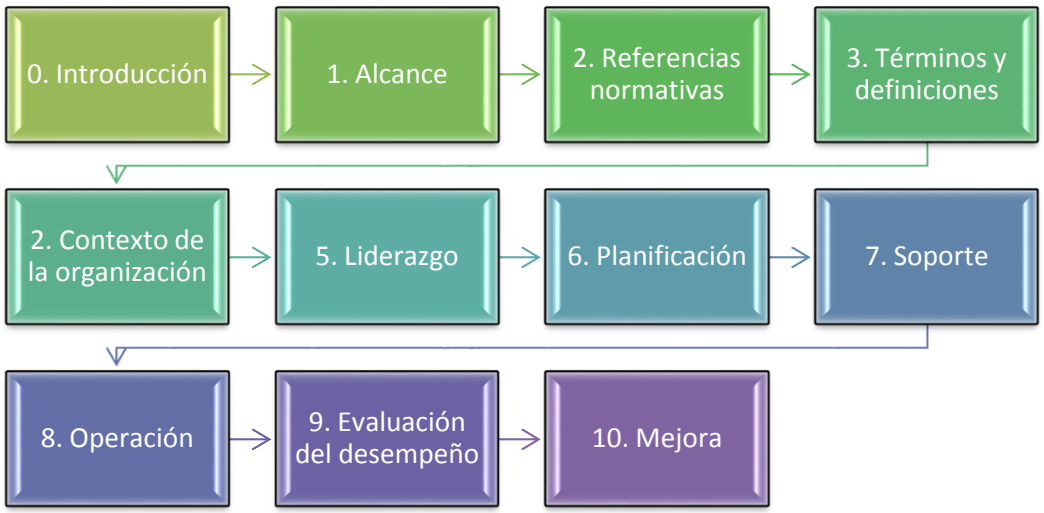

Figura No. 2. Estructura actual de la norma **ISO/IEC 27001:2013**

La norma ISO 27001:2013 incluye el Anexo A el cual corresponde al resumen de dominios y controles detallados en la norma ISO 27002:2014, los cuales se presentan a continuación:

- Políticas de seguridad
- Organización de la seguridad de la información
- Seguridad de los RRHH
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y ambiental
- Operaciones de seguridad
- Seguridad de las comunicaciones
- Sistemas de adquisición, desarrollo y mantenimiento
- Relación con proveedores
- Gestión de incidentes
- Seguridad de la información para la continuidad del negocio
- Cumplimiento

2 SITUACIÓN ACTUAL

2.1 INTRODUCCIÓN

El estado colombiano ha definido como estrategia para la implementación del Modelo de seguridad de información en las entidades públicas, la implementación de un Sistema de Seguridad de la Información sostenible basado en el ciclo PHVA.

Por lo anterior en este documento se desarrollan las etapas más importantes que se deben tener en cuenta para la implementación de un Sistema de Gestión de Seguridad de la Información en una empresa.

Etapas:

- Fase 1: Definición de la situación actual
- Fase 2: Sistema de gestión documental del SGSI
- Fase 3: Análisis de riesgos
- Fase 4: Propuestas de proyectos
- Fase 5: Fase de auditoría y cumplimiento
- Fase 6: Presentación de resultados

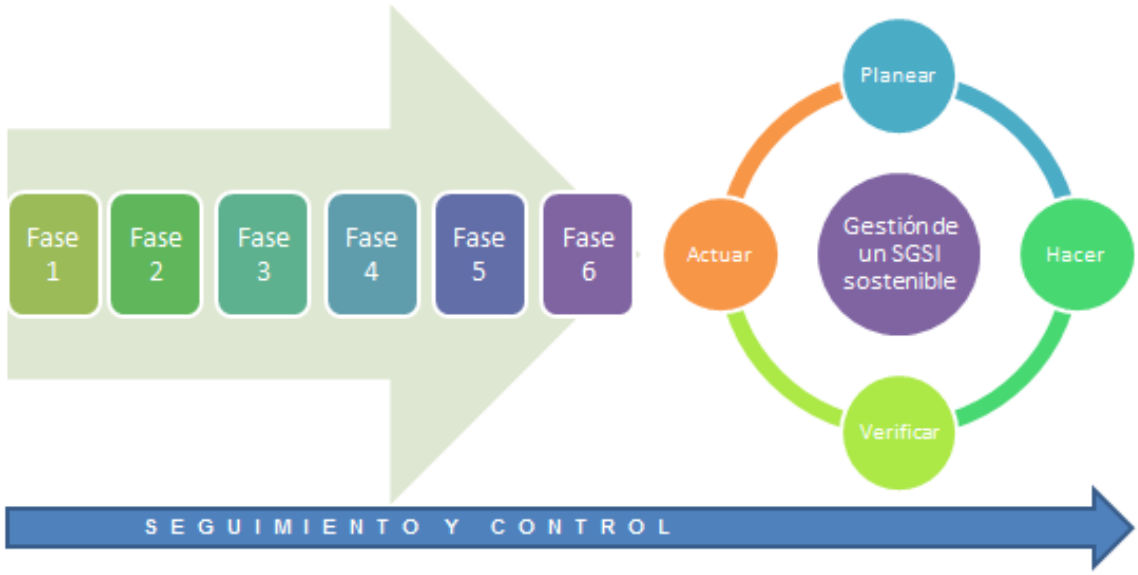

Figura No. 3. Fases de desarrollo del proyecto

2.2 Conociendo la ISO/IEC 27002

Para la implementación del SGSI en las entidades públicas se tomará como marco de referencia no solo la Norma ISO 27001:2013 sino la ISO 27002:2013, la cual está diseñada para uso por parte de las entidades, como referencia para la selección de controles dentro del proceso de implementación.

2.3 Contextualización

La empresa elegida para el desarrollo de las fases descritas a lo largo de este documento, es una empresa pública prestadora de los servicios de acueducto y alcantarillado sanitario y pluvial.

Cuenta aproximadamente con 1200 colaboradores, empleados y contratistas.

Visión:
Ser un modelo público sostenible en la gestión integral del agua, manejo residuos sólidos y en la prestación de servicios con calidad, transparencia, inclusión y equidad.

Misión:

Empresa pública, responsable con la gestión integral del agua y el saneamiento básico como elementos comunes de vida y derechos humanos fundamentales, generadora de bienestar, que contribuye a la sostenibilidad ambiental del territorio.

Valores Corporativos:

- Vocación del servicio.
- Transparencia.
- Respeto.
- Responsabilidad.
- Excelencia en la gestión.

Estructura organizacional:

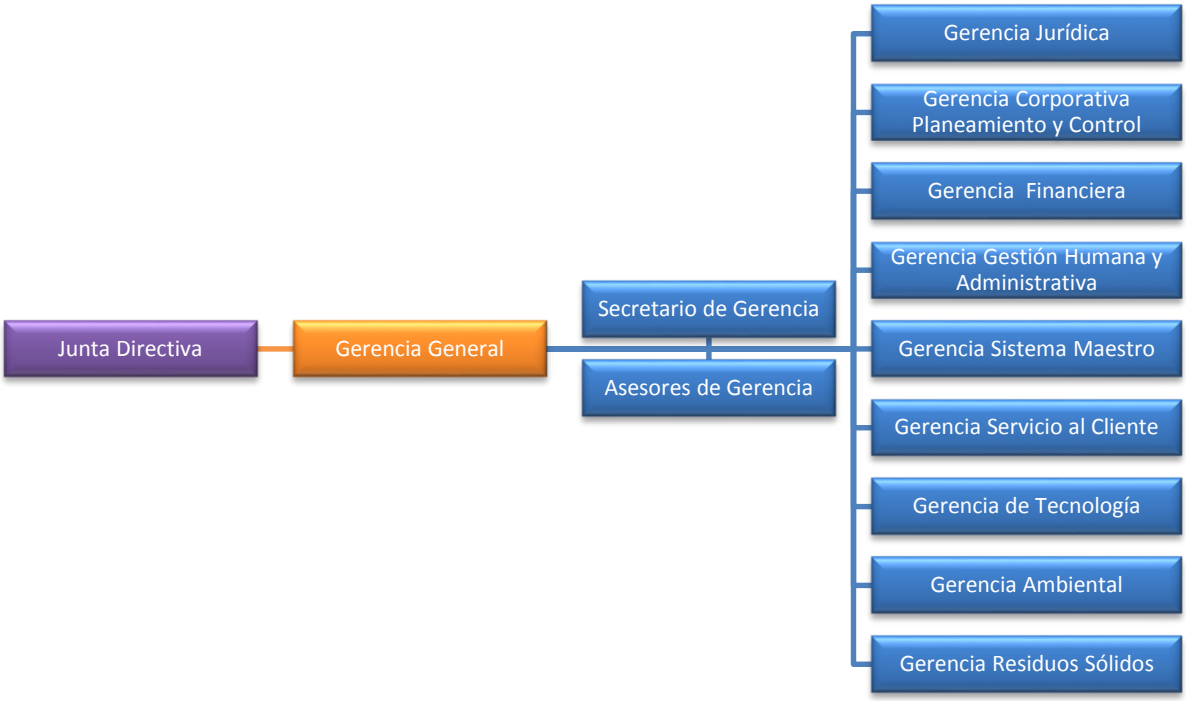

Figura No. 4. Organigrama de la entidad

Mapa de procesos

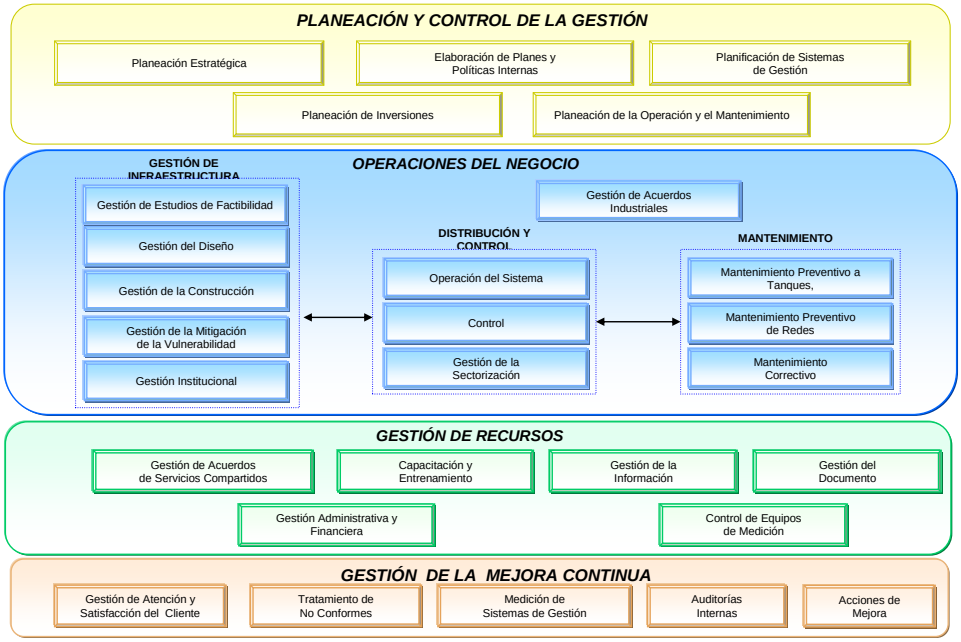

Figura No. 5. Mapa de procesos de la entidad

Diagrama de red sede principal

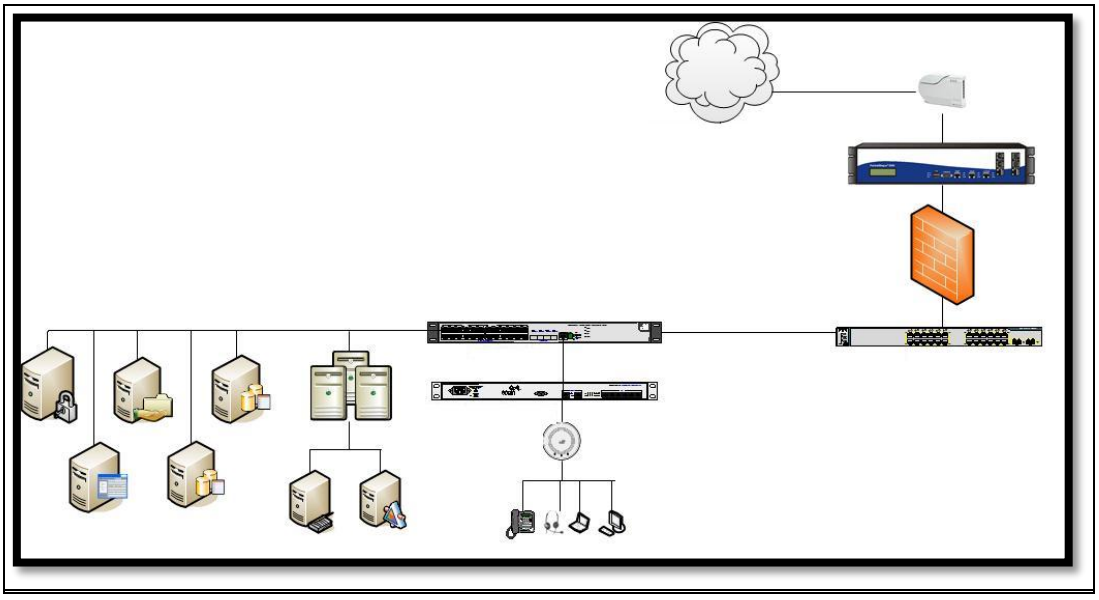

Figura No. 6. Diagrama de red de la entidad

Alcance:

Los criterios utilizados para la selección de los procesos del alcance fueron los siguientes:

Análisis del proceso y sus actividades, dando prioridad a la inclusión en el alcance, los procesos que están asociados directamente al servicio de acueducto y alcantarillado sanitario y pluvial; y no a aquellos que son soporte de éstos.

En el Anexo 1 – Alcance, se describen:

- Documento 1. Alcance: Contiene la definición detallada del alcance y el análisis realizado.
- Documento 2. Contexto
- Documento 3. Interfaces y Dependencias
- Documento 4. Partes interesadas

Compromisos legales contractuales

Ley 1273 de 2009	Ley general de delitos informáticos
Ley 594 de 2000	Ley general de archivo
Ley 257 de 1999	Comercio electrónico
Ley 1255 de 2008	Dicta las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 142 de 1994	Servicios públicos domiciliarios

2.4 OBJETIVOS DEL PLAN DIRECTOR

La empresa de servicios públicos como miembro del Estado colombiano, hace parte de las infraestructuras definidas como críticas y estratégicas del país, por lo que se hace necesario que ésta cuente con las medidas pertinentes que le permitan asegurar su adecuada operación, protegiendo su información y su relación con las demás entidades del estado.

De acuerdo con lo anterior y con el fin de desplegar esta iniciativa, se emitió la directiva No. DIR2014-18 del 19de junio de 2014 en la que se menciona:

"1.2. Alcance

La presente directiva define la política, controles de uso aceptable y las directrices en relación con la seguridad de la información en las instituciones y entidades del Sector Público.

Las políticas establecidas en la directiva y sus posteriores actualizaciones aplican a todos los recursos y activos de información de las instituciones y entidades que conforman el Sector Público, así como a los designados para su uso y custodia en el territorio nacional y fuera de él.

2.3 Generalidades

El Ministerio de las Tecnologías de la Información y las Comunicaciones en cumplimiento de la normativa emitida por el Gobierno Nacional apoya y acompaña a las instituciones y entidades que conforman el Sector Público en la implementación de un Sistema de Gestión de Seguridad de la Información formalizado, documentado, alineado con los objetivos estratégicos del Sector, enfocado a gestionar y reducir los riesgos a un nivel aceptable, mejorando en forma continua los procesos de seguridad de la información; valiéndose de un talento humano capacitado, competente, comprometido con la seguridad de la información y el uso aceptable de los activos de información, con tecnología apropiada que satisfaga las necesidades del Sector Público en términos de disponibilidad, confidencialidad e integridad."

2.5 ANÁLISIS DIFERENCIAL

Para realizar la evaluación del estado actual en seguridad de la información de la empresa prestadora de servicios públicos objeto de este estudio, se realizó un análisis de brechas "GAP" de las norma ISO 27001:2013 e ISO 27002:2013.

A continuación se muestran los resultados generales obtenidos:

Norma ISO 27001:2013 (Requisitos de la norma)

- Cumplimiento de un 35%

Figura No. 7. Gráfica de requisitos norma ISO 27001:2013

Anexo A de la norma ISO 27002:2013

- Cumplimiento de un 30%

Figura No. 8. Gráfica de "Anexo A" norma ISO 27001:2013

Se anexa archivo con el detalle del análisis realizado: Anexo 2 – Análisis GAP inicial.

2.6 RESULTADOS

A continuación se resumen los aspectos definidos durante esta primera fase:

- Alcance
  El alcance del SGSI para la empresa prestadora de servicios públicos cubre la información del macro-proceso DISTRIBUCIÓN Y CONTROL, el cual hace parte fundamental de la operación de la entidad.

- Objetivos del Plan Director
  El objetivo principal es dar cumplimiento con los requerimientos del Estado colombiano, que consiste en asegurar infraestructuras críticas del país, implementando un SGSI que permita brindar adecuada protección de los activos de información más importantes de para la operación de la entidad.

- Resultados del Análisis Diferencial
  El resultado del análisis de brechas realizado permite visualizar un panorama general del estado de los requerimientos de seguridad dentro de la entidad.

  A continuación se muestra un consolidado del análisis GAP de las normas ISO 27001:2013 e ISO 27002:2013:

- Requisitos de la norma ISO 27001:2013

Ítem	Aspectos Requeridos del SGSI	Cumplimiento
4	Contexto de la organización	50%
5	Liderazgo	74%
6	Planificación	0%
7	Soporte	70%
8	Operación	13%
9	Evaluación del desempeño	3%
10	Mejora	35%

Figura No. 9. Tabla de requerimientos norma ISO 27001:2013

- Anexo A de la norma 27002:2013

Ítem	Dominios	Cumplimiento
5	Política de seguridad	40%
6	Organización de la seguridad de la información	33%
7	Seguridad de los recursos humanos	41%
8	Gestión de activos	34%
9	Control de acceso	31%
10	Criptografía	28%
11	Seguridad física y del entorno	39%
12	Seguridad de las operaciones	24%
13	Seguridad de las comunicaciones	16%
14	Adquisición, desarrollo y mantenimiento de sistemas	31%
15	Relaciones con los proveedores	30%
16	Gestión de incidentes de seguridad	38%
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	14%
18	Cumplimiento	20%
TOTAL		30%

Figura No. 10. Tabla de "Anexo A" norma ISO 27001:2013

3 SISTEMA DE GESTIÓN DOCUMENTAL

3.1 INTRODUCCIÓN

La norma ISO 27001 se divide en dos partes, los referentes a los requisitos obligatorios que la entidad debe cumplir para soportar su SGSI y el "anexo

A", que corresponde al listado de dominios y controles que se deben usar como referencia para la selección de controles dentro del proceso de implementación del SGSI.

De acuerdo con lo anterior, a continuación se describirán en forma detallada el listado de documentos base que soportarán el SGSI de la empresa objeto de este estudio.

3.2 ESQUEMA DOCUMENTAL

Figura No. 11. Esquema documental

- Anexo 3 - Política de Seguridad
- Anexo 4 - Procedimiento de Auditorías Internas
- Anexo 5 - Gestión de Indicadores
- Anexo 6 - Procedimiento Revisión por Dirección
- Anexo 7 - Gestión de Roles y Responsabilidades

- Anexo 8 - Metodología de Análisis de Riesgos
- Anexo 9 - Declaración de Aplicabilidad

4 ANÁLISIS DE RIESGOS

4.1 INTRODUCCIÓN

La gestión de riesgos de seguridad de la información para cumplir con los requisitos de la norma ISO27001:2013 está basada en la norma ISO3100, la cual define el marco de trabajo para la gestión de riesgos, esta norma principalmente menciona tres aspectos generales que definen la gestión de riesgos: los principios, el marco de trabajo, y el proceso de gestión.

Los principios son los siguientes:

- Crear valor
- Parte integral de los procesos de la organización
- Parte del proceso de decisión
- Tiene en cuenta la incertidumbre de manera explicita
- Sistemática, estructurada y a tiempo.
- Basada en la mejor información disponible
- Ajustada a la organización
- Toma en cuenta factores humanos y culturales
- Transparente e inclusive
- Dinámica, iterativa y reactiva al cambio.
- Facilita la mejora continua y el desarrollo de la organización.

El marco de trabajo define el ciclo de mejora continua, los procesos y los niveles de reporte necesarios para que la información de riesgos llegue a los niveles adecuados se tomen las decisiones necesarias y que el proceso de riesgos se mejore y ajuste a las necesidades específicas y dinámicas de la organización.

4.2 INVENTARIO DE ACTIVOS Y VALORACIÓN DE ACTIVOS

En el archivo del Anexo 10 – Activos de información se adjunta la siguiente información:

- Inventario de activos
- Valoración de activos

4.3 DIMENSIONES DE SEGURIDAD Y TABLA DE RESUMEN DE VALORACIÓN

En el archivo del Anexo 10 – Activos de información se adjunta la siguiente información:

- Dimensiones de seguridad
- Tabla resumen de valoración

4.4 ANÁLISIS DE AMENAZAS – IMPACTO

La metodología de riesgos definida tiene las siguientes fases:

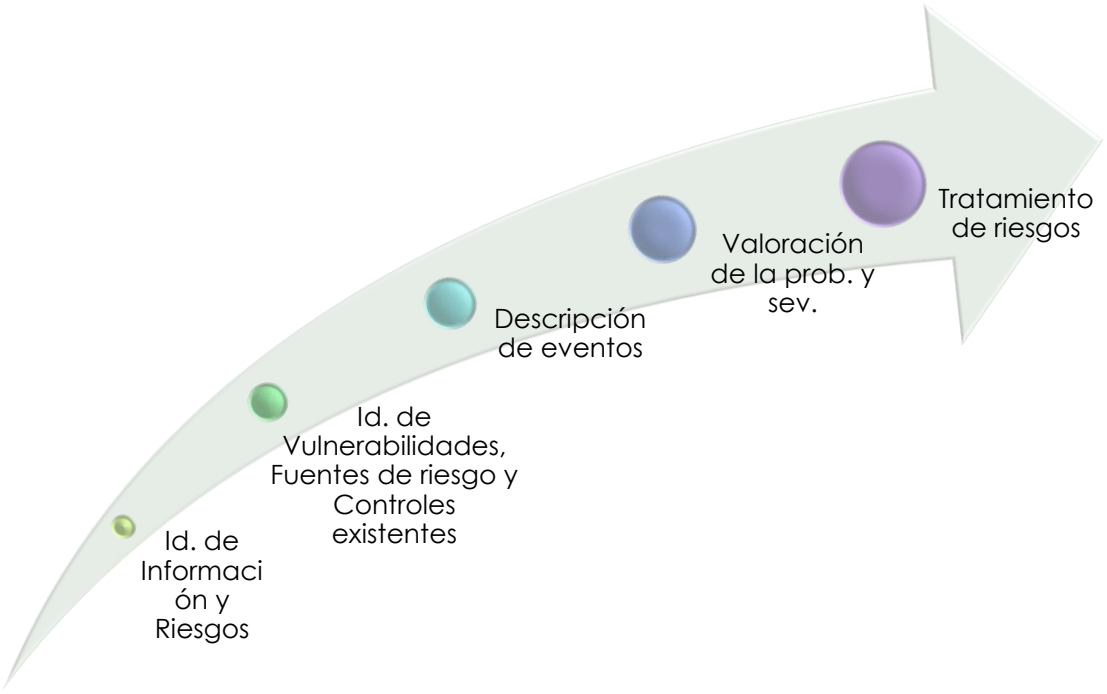

Figura No. 12. Esquema de gestión de riesgos

Fase 1: Identificación de información

En esta etapa se identifica la Información en el inventario del proceso alcance del SGSI que se definió por su valoración debe ir a la etapa de análisis de riesgos.

Fase 2: Identificación del riesgo de seguridad de la información

De la valoración dada al activo en confidencialidad, integridad y disponibilidad, se toman los valores más altos y se define un riesgo en cada una de ellas, el cual puede ser:

- Riesgo de pérdida de confidencialidad
- Riesgo de pérdida de disponibilidad
- Riesgo de pérdida de integridad

Fase 3: Identificación de vulnerabilidades

Se eligen cuáles son las vulnerabilidades que aplican para cada uno de los riesgos identificados de acuerdo con un escenario definido.

Fase 4: Identificación de la fuente del riesgo

Identificar las fuentes externos e internas que pueden explotar las vulnerabilidades ya identificadas que puedan materializar el componente de riesgo.

Fase 5: Identificación de controles existentes

Después de identificar las vulnerabilidades y fuentes de riesgo se procede a la etapa de identificación de controles existentes que se encuentran implementados y los planificados.

Fase 6: Identificación y descripción de eventos

En la etapa de identificación de eventos se describe el evento más probable por el cual se podría materializar el riesgo identificando las causas y consecuencias que produce.

Fase 7: Valoración de la probabilidad y severidad

Evaluar la posible afectación de cada uno de los riesgos sobre los Recursos Empresariales en términos de la probabilidad y la severidad de sus consecuencias.

Fase 8: Tratamiento de los riesgos de seguridad de la información

Una vez identificados y priorizados los riesgos de acuerdo a los criterios de evaluación del riesgo, la entidad debe tomar decisiones y actuar.

Fase 9: 2.8. Análisis cualitativo valoración de riesgo residual

Luego de concluir de implementar los tratamientos planteados, se vuelve a realizar una valoración de controles para valorar el riesgo residual.

Fase 10: Resultado final

En el archivo del Anexo 11 – Riesgos de seguridad de la información se adjunta la siguiente información en la que se consolida la ejecución de las fases de la 1 a la 9:

- Análisis amenazas
- Análisis vulnerabilidades
- Análisis de impacto

4.5 NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

En el archivo del Anexo 11 – Riesgos de seguridad de la información se adjunta la siguiente información:

- Resultado del análisis de riesgos
- Matriz de riesgos
- Matriz de riesgo residual

4.6 RESULTADOS

Activos:

Se identificaron 75 activos, en la siguiente gráfica se muestra el porcentaje de activos valorado por cada categoría:

Figura No. 13. Gráfica valoración de activos

Riesgos

En el archivo de riesgos del Anexo 11 – Riesgos de seguridad de la información se pueden ver las matrices de riesgo y de riesgo residual por cada uno de los efectos definidos dentro de la metodología: financiero, reputación, humano e información.

5 PROPUESTAS DE PROYECTOS

5.1 INTRODUCCIÓN

Una vez analizado y cuantificado los riesgos, así como el impacto que tiene en su plan de negocio el emprendedor debe analizar cuál es el nivel de oportunidad en caso de asumir el riesgo.

Para que el tratamiento de los riesgos sea efectivo, es necesario que el líder de seguridad de la información adopte determinadas medidas y acciones encaminadas a modificar, reducir o eliminar el riesgo. Del mismo modo, si se decide no adoptar ninguna medida contra el riesgo, puede tener importantes pérdidas.

El tratamiento del riesgo debe ser el más apropiado de acuerdo a su importancia y relevancia en la actividad de la empresa.

5.2 PROPUESTAS

De acuerdo con o definido en la metodología de riesgos, en el formato "Anexo 11 - Análisis de riesgos.xls", en la hoja "Riesgos_Información" en la sección de "Gestión de controles" se observan los planes de tratamiento propuestos para mitigar los riesgos identificados, así mismo en esa sección también se valoran y se muestra el estado del riesgo residual luego de su implementación.

Por otra parte en los formatos "Anexo 12 - Formato opciones de tratamiento.xls" y "Anexo 12 – Detalles planes de tratamiento" se muestra el detalle de los planes de tratamiento estado y número de acuerdo con el que el dueño del riesgo aprueba su tratamiento.

5.3 RESULTADOS

A continuación se muestran los mapas de calor del riesgo con controles existentes y el riesgo residual luego de la implementación de los planes propuestos:

Recurso financiero

Riesgo actual **Riesgo residual**

Figura No. 14. Diagramas de calor riesgo Recurso financiero.

Recurso reputación

Riesgo actual **Riesgo residual**

Figura No. 15. Diagramas de calor riesgo Recurso reputación.

Recurso Humano

Riesgo actual **Riesgo residual**

Figura No. 16. Diagramas de calor riesgo Recurso humano.

Recurso Información

Riesgo actual **Riesgo residual**

Figura No. 17. Diagramas de calor riesgo Recurso información.

6 AUDITORÍA DE CUMPLIMIENTO

6.1 INTRODUCCIÓN

La revisión de auditoría se realiza con el fin de evaluar el nivel de implementación de los controles y su efectividad para el SGSI.

A continuación se presenta un comparativo entre el diagnóstico inicial dado en el numeral dos de este documento.

Así mismo se recuerda que la escala de valoración utilizada es la siguiente:

Nivel de Implementación	% de Cumplimiento	Descripción
Gestionado	100%	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.
Medible	80%	Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.
Definido	60%	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.
Repetible	40%	Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.
Inicial	20%	Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.
Inexistente	0%	La organización no ha identificado una situación que debe ser tratada.

Figura No. 18. Escala de madurez COBIT.

6.2 METODOLOGÍA

La metodología utilizada para realizar esta revisión es a través de un análisis de brechas "GAP" final en el que se evaluará el nivel de madurez adquirido durante todo este ciclo.

6.3 EVALUACIÓN DE LA MADUREZ

En el "Anexo 14 – Análisis GAP final" se muestra la revisión realizada a los controles del "Anexo A" de la Norma ISO 27007:2013.

Los resultados del diagnóstico muestran que el nivel de cumplimiento promedio del SGSI con base a los requerimientos mínimos de la norma ISO/IEC 27001:2013 (numerales 4 al 10) es del 48%, lo que corresponde a un nivel "REPETIBLE" dentro de la escala de medición utilizada por la metodología de GAP.

6.4 PRESENTACIÓN DE RESULTADOS

A continuación se muestra el nivel de madurez adquirido durante la implementación respecto al GAP inicial

Ítem	Aspectos Requeridos del SGSI	Inicial	Final
4	Contexto de la organización	50%	60%
5	Liderazgo	74%	73%
6	Planificación	0%	56%
7	Soporte	70%	68%
8	Operación	13%	53%
9	Evaluación del desempeño	3%	33%
10	Mejora	35%	26%
Promedio Total		35%	53%

Figura No. 19. Porcentajes requisitos norma ISO 27001:2013.

Figura No. 20. Análisis de brecha "GAP" requisitos ISO 27001:2013.

Desde el punto de vista de los 14 dominios recomendados para implementación por parte de la norma ISO/IEC 27002, se encontró un nivel de madurez promedio del 55%, estado "REPETIBLE". El avance del nivel de madurez de cada dominio respecto al análisis GAP inicial:

Figura No. 21. Análisis de brecha "GAP" del "Anexo A" ISO 27001:2013.

6.5 RESULTADOS

La calificación obtenida de acuerdo a cada dominio del "Anexo A" de la norma ISO 27001:2013, nos permite evidenciar lo siguiente:

Cumplimiento controles	GAP Inicial	GAP Final	Nivel de Implementación
Política de seguridad	40%	80%	Medible
Organización de seguridad de información	33%	60%	Definido
Seguridad de los recursos humanos	41%	69%	Definido
Gestión de activos	34%	53%	Repetible
Control de acceso	31%	58%	Repetible
Criptografía	28%	50%	Repetible
Seguridad física y del entorno	39%	63%	Definido
Seguridad de las operaciones	24%	59%	Repetible
Seguridad de las comunicaciones	16%	40%	Repetible
Adquisición, desarrollo y mantenimiento de sistemas	31%	47%	Repetible

Cumplimiento controles	GAP Inicial	GAP Final	Nivel de Implementación
Relaciones con los proveedores	30%	52%	Repetible
Gestión de incidentes de seguridad	38%	37%	Inicial
Aspectos de seguridad de la información de la gestión de continuidad del negocio	14%	53%	Repetible
Cumplimiento	20%	50%	Repetible

Figura No. 22. Dominios "Anexo A" de la norma ISO 27001:2013.

6.6 AUDITORÍA

En el "Anexo 14 – análisis gap final y reporte auditoría" se muestra el resultado de las "No conformidades" y las "Observaciones" identificadas durante la medición

7 PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORMES

7.1 INTRODUCCIÓN

Luego de concluir toda la etapa de implementación desarrollada a lo largo del documento, por último queda hacer la presentación final de los resultados obtenidos, en la que se muestra el nivel de madurez obtenido y el estado de implementación de los controles definidos por los planes de tratamiento.

7.2 OBJETIVOS DE LA FASE

El objetivo de esta fase es hacer un balance del resultado de la implementación a través del cual de entregue:

- Inventario de activos de la entidad
- Resultado del análisis de riesgos realizado
- Diagrama de calor de riesgo inherente y residual
- Planes de tratamiento implementados
- "GAP" final de los controles de los "Requisitos" y el "Anexo A" de la norma ISO 27001:2013.

7.3 ENTREGABLES

En el "anexo 15 – Informe de Resultados" se muestra un resumen de lo descrito en el numeral anterior. Así mismo se encuentra la presentación realizada a la alta gerencia sobre el trabajo realizado.

8 DEFINICIONES

- **Alcance:** Ámbito de la organización que queda sometido al SGSI.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Aceptación del riesgo:** Decisión informada de asumir un riesgo concreto.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Auditor:** Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.
- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos.

- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- **Identificación de riesgos:** Proceso de encontrar, reconocer y describir riesgos.

- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Objetivo:** Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

- **Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Segregación de tareas:** Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **SGSI:** Sistema de Gestión de la Seguridad de la Información.

- **Tratamiento de riesgos:** Proceso de modificar el riesgo, mediante la implementación de controles.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

9 ANEXOS

9.1 ANEXO 1 – ALCANCE

9.2 ANEXO 2 – ANÁLISIS GAP INICIAL

9.3 ANEXO 3 – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

9.4 ANEXO 4 – PROCEDIMIENTO DE AUDITORÍAS INTERNAS

9.5 ANEXO 5 – GESTIÓN DE INDICADORES

9.6 ANEXO 6 – PROCEDIMIENTO REVISIÓN POR DIRECCIÓN

9.7 ANEXO 7 – GESTIÓN DE ROLES Y RESPONSABILIDADES

9.8 ANEXO 8 – METODOLOGÍA DE ANÁLISIS DE RIESGOS

9.9 ANEXO 9 – DECLARACIÓN DE APLICABILIDAD

9.10 ANEXO 10 – ACTIVOS DE INFORMACIÓN

9.11 ANEXO 11 – RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

9.12 ANEXO 12 – FORMATO OPCIONES DE TRATAMIENTO Y DETALLES

9.13 ANEXO 13 – PROCEDIMIENTO DE CONTROL DE DOCUMENTOS

9.14 ANEXO 14 – ANÁLISIS GAP FINAL Y REPORTE AUDITORÍA

9.15 ANEXO 15 – INFORME DE RESULTADOS

10 BIBLIOGRAFÍA Y REFERENCIAS ELECTRÓNICAS

[1] La NCh ISO 27001. Origen y evolución. Disponible en: http://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/.

[2] ISO 27001:2013. Nueva estructura. http://www.pmg-ssi.com/2013/11/iso-270012013-nueva-estructura/.

[3] ISO (International Standard Organization).“Published Document PD ISO/IEC guide 73. Risk Management – Vocabulary - Guidelines for use in standards”, 2002.

[4] ISO (International Standard Organization). “Estándar de Seguridad ISO/IEC 27005. Tecnología de la Información – Técnicas de seguridad – Gestión del Riesgo de seguridad de la información", 2008.

[5] ISO (International Standard Organization). “Estándar de Seguridad ISO/IEC 31000. Gestión del riesgo – Principiosdirectrices", 2011.

[6] Ministerio de administraciones públicas, "MAGERIT - Metodología de análisis y gestión de riesgos de los sistemas de información" – Método. Versión 2, España, 2006.

[7] ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación) NTC 5254 - Norma Técnica Colombiana. “Gestión de riesgo”, 2006.

[8] NIST (National Institute of Standards and Technology). “NIST SP 800-30. Guía de Gestión de riesgo para sistemas de tecnología de la Información – Recomendaciones del Instituto Nacional de Estándares y Tecnología”, 2002

11 CONTROL DE VERSIONES

Versión	Fecha	Comentarios	Por	Aprobado
1.0	06-03-2015		Julieth Parra Casallas	
2.0	27-03-2015		Julieth Parra Casallas	
3.0	24-04-2015		Julieth Parra Casallas	
4.0	15-05-2015		Julieth Parra Casallas	
5.0	29-05-2015		Julieth Parra Casallas	
6.0	10-06-2015		Julieth Parra Casallas	