MEMORIA TRABAJO FINAL
MASTER
RESUMEN EJECUTIVO

PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013

ROBIN J. SALCEDO B.
ISAGXXX
19 diciembre 2014
V1.0

ISAGXXX

RESUMEN EJECUTIVO
MEMORIA
TFM PLAN DE IMPLEMENTACIÓN DEL SGSI

Director Del Proyecto

Antonio Jose Segovia

MISTIC

UNIVERSIDAD OBERTA CATALUNYA

Información del Documento

Título del documento	Memoria del Trabajo Final del Master MISTIC
Aprobación	Comité Evaluador MISTIC
Documentos relacionados	• Políticas de Seguridad de la Información • Procedimientos de seguridad de la Información • Presentación del Proyecto • Estructura Organización del TFM MISTIC 2014
Lista de Distribución	Comité de Seguridad, **ISAGXXX**, Empleados internos.

REVISIÓN HISTÓRICA

Ver.	Tipo	Fecha	Revisión y Aprobación	Observaciones
1.0	Final	Nov 24 de 2014	Comité de Seguridad	

Agradezco a mis familiares, amigos y compañeros de trabajo que apoyaron de forma directa e indirecta en el desarrollo del plan de implementación del SGSI para ISAGXXX, para ISAGXX la gestión de seguridad de la información en un diferencial potencial en la gestión y operación del modelo de nuestro negocio.

Abstract (Resumen del Proyecto)

El trabajo final del master, describe los objetivos, el alcance, la expectativa del SGSI y la metodología asociada a la definición, planeación, identificación y creación del modelo de seguridad de la información para la organización **ISAGXXX**, basado en la norma ISO 27001:2013; iniciando desde el entendimiento de la organización desde la óptica de los procesos críticos de la operación de energía, ejecución del diagnóstico de seguridad de la información, identificación de las principales vulnerabilidades y amenazas, aplicando una metodología de gestión del riesgos para la gestión de riesgos de seguridad de la información, planeación de los planes de tratamiento de riesgos y generación del marco documental del sistema de gestión de seguridad de la información para **ISAGXXX**.

El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). De acuerdo a las siguientes fases del proyecto:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Definición de la situación actual y de los objetivos del SGSI.
- Análisis de Riesgos.
- Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.
- Identificación de amenazas, evaluación y clasificación de las mismas
- Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2005 en la organización.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Esquema Documental del sistema de gestión de seguridad de la información.
- Definición de Políticas, Procedimientos y guías de seguridad de la información.

Abstract

The final work of the master, describes the objectives, scope, the expectation of the ISMS and methodology associated with the definition, planning, identification and creation of model information security for **ISAGXXX** organization based on the ISO 27001: 2013 ; starting from the understanding of the organization from the perspective of critical processes of the operation of energy, implementation of diagnostic information security, identification of key vulnerabilities and threats applying a risk management methodology for risk management information security, planning of risk treatment plans and generation of document management system framework of information security for **ISAGXXX**.

The project involves setting the foundation for implementing an ISMS (Information security management system). According to the following project phases:

• normative documentation on best practices in information security.
• Definition of the current situation and the objectives of the ISMS.
• Risk Analysis.
    o Identification and valuation of corporate assets as a starting point to a risk analysis.
    o Identification of threats, evaluation and classification of the same
• Evaluation of the level of compliance with the ISO / IEC 27002: 2005 in the organization.
• Proposed projects face to achieve adequate safety management.
• Documentary Outline management system information security.
• Defining Policies, Procedures and guide information security.

TABLA DE CONTENIDO

1. INTRODUCCIÓN DEL PROYECTO 6

1.1 JUSTIFICACIÓN DEL PROYECTO 7
1.2 GLOSARIO DE TERMINOS 7
1.3 BENEFICIOS DEL PROYECTO 12

2. METODOLOGIA DEL PROYECTO 13

2.1 Entendimiento del Marco Normativo del Proyecto. 13
2.2 Fases del Proyecto 15

3. FASE 1: SITUACIÓN ACTUAL, CONTEXTO, OBJETIVOS Y ANALISIS DIFERENCIAL 17

3.1 DESCRIPCIÓN DE LA EMPRESA ISAGXXX 17
3.2 OBJETIVOS DEL PROYECTO 20
3.3 CONTEXTO DEL SGSI 21
3.4 ALCANCE DEL PROYECTO 24
3.5 GOBIERNO DEL SGSI 24
3.6 ANALISIS DIFEREMCIAL DE ISAGXXX 25

4 SISTEMA DE GESTIÓN DOCUMENTAL DEL SGSI 29

4.1 ESTRUCTURA ORGANIZACIONAL ISAGXXX 29
4.2 ESTRUCTURA DOCUMENTAL DEL SGSI 31
4.3 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN 31
4.4 PROCEDIMIENTOS DE SEGURIDAD 32

5 GESTIÓN DEL RIESGO 35

6 PROYECTOS PROPUESTOS DE SEGURIDAD DE LA INFORMACIÓN 36

7 AUDITORIA DE CUMPLIMIENTO 39

8 CONCLUSIONES DEL PROYECTO 40

9 ANEXOS 41

10 REFERENCIAS 42

1. INTRODUCCIÓN DEL PROYECTO

La información de ***ISAGXXX*** *se* constituye en uno de los activos de más valor para la compañía, por lo tanto, debe ser utilizada dentro de un adecuado entorno de seguridad, cualquiera que sea el medio en el que se encuentre (físico o lógico) y el ambiente tecnológico en que se procese.

ISAGXXX *es* consciente de que la seguridad de la información es principalmente un proceso administrativo, relacionado y dependiente de aspectos tecnológicos. Por esta razón, se establece un compromiso institucional mediante el desarrollo de un modelo de soporte para la gestión y la promoción de una cultura de seguridad, definiendo las responsabilidades por parte de su personal, clientes y usuarios, para la protección de la seguridad de sus activos de información.

Para ***ISAGXXX*** es una decisión gerencial y estratégica, implantar su Sistema de Gestión de Seguridad de la Información, el cual le permite brindar a sus funcionarios, clientes y socios de negocio, niveles apropiados de seguridad y protección de la información.

Las responsabilidades y el modelo de organización de la gestión de la seguridad de la información en ***ISAGXXX*** hacen parte de este Sistema de Gestión de Seguridad de la Información.

El objetivo principal de ***ISAGXXX*** para el procesamiento y almacenamiento de su información, es preservar niveles apropiados de seguridad y calidad de acuerdo con los siguientes criterios:

- **Disponibilidad:**

  Asegurar que los clientes, contratistas, proveedores y usuarios de los servicios de ***ISAGXXX*** puedan acceder a la información cuando lo requieran.

- **Confidencialidad:**

  Asegurar que la información pueda ser accedida únicamente por los clientes, contratistas, proveedores y usuarios de los servicios de ***ISAGXXX*** debidamente autorizados.

- **Integridad:**

  Asegurar que la información almacenada y/o procesada por ***ISAGXXX*** no sea alterada o modificada sin autorización.

- **Confiabilidad:**

  La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones. (Definición tomada de la circular externa 052 de 2007 expedida por la Superintendencia Financiera de Colombia)

- **Efectividad:**

La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente. (Definición tomada de la circular externa 052 de 2007 expedida por la Superintendencia Financiera de Colombia)

- **Eficiencia:**

  El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos. (Definición tomada de la circular externa 052 de 2007 expedida por la Superintendencia Financiera de Colombia)

El diseño, implantación y operación del Sistema de Gestión de Seguridad de la Información (SGSI) en ***ISAGXXX*** está directamente relacionado con las necesidades y objetivos del negocio, sus requerimientos de seguridad, el alcance definido por la Presidencia y la estructura propia de la compañía.

Para el desarrollo del Sistema de Gestión de Seguridad de la Información se han tenido en cuenta los requerimientos, controles y objetivos de control especificados en el estándar ISO/IEC 27001:2002013, así como las recomendaciones del estándar ISO/IEC 27002 antes conocido como ISO/IEC 17799:2005.

Este documento es confidencial y de propiedad de ***ISAGXXX*** La Dirección de Seguridad de la Información será responsable publicar las actualizaciones en la herramienta de documentación.

1.1 JUSTIFICACIÓN DEL PROYECTO

El presenta proyecto tiene como justificación principal, apoyar, optimizar y gestionar los procesos críticos de la operación de energía, gestión tecnológica y áreas transversales de la organización ISAGXX, con el fin de obtener beneficios a nivel de imagen reputacional, mejor relacionamiento con el mercado y los clientes, mejora continua de los riegos de seguridad de la información y establecer un retorno de inversión (ROI) para la organización, a través de la definición e implementación del SGSI en ISAGXXX.

1.2 GLOSARIO DE TERMINOS

- **Activo de Información:** Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa. La información, como activo corporativo, puede existir de muchas formas:

  - Impresa
  - Almacenada electrónicamente
  - Transmitida por medios electrónicos
  - Mostrada en videos
  - Suministrada en una conversación
  - Conocimiento de las personas

- **Alcance de la auditoría:** Extensión y límites de una auditoría.

- **Amenazas:** Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

- **Análisis de Riesgos:** Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

- **Audiovisuales:** Colección conformada por videos, disquetes, casetes, usb, microfichas, CD-ROM, discos duros y cintas.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.

- **Auditado:** Organización o Dependencia a la cual se le vá a realizar una auditoría.

- **Auditor:** Persona con la competencia para llevar a cabo una auditoría.

- **Auditor en seguridad de la información:** Persona con la competencia para efectuar auditorías internas de seguridad de la información
- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

- **Conclusiones de auditoría:** Resultado de una auditoría, proporcionada por el equipo auditor después de la consideración de los objetivos de la auditoría y de todos los hallazgos de auditoría.

- **Conformidad**: cumplimiento de un requisito.

- **Control:** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

- **Criterios de auditoría:** Conjunto de políticas, procedimientos o requisitos utilizados como una referencia frente a la cual se compara la evidencia de la auditoría.

- **Custodio:** Es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

- **Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.

- **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante nuestros clientes.

- **Efectividad:** Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

- **Eficacia:** Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

- **Eficiencia:** Relación entre el resultado alcanzado y los recursos utilizados.

- **Equipo auditor:** Uno o más auditores que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos.

- **Estimación del riesgo:** Proceso de asignación de valores a la probabilidad e impacto de un riesgo.

- **Evento de seguridad de la información:** Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política de seguridad de la información, falla en controles y contramedidas, o que implica una situación desconocida que puede ser pertinente a la seguridad de la información.

- **Evidencia de auditoría:** Registros, declaraciones de hechos o cualquier otra información que son relevantes para los criterios de auditoría y que son verificables. La evidencia de la auditoría puede ser cuantitativa o cualitativa.

- **Evitar el riesgo:** Decisión de la organización de no involucrarse en una situación de riesgo o tomar acciones para retirarse de dicha situación.

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

- **Hallazgo de auditoría:** Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de la auditoría.

- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

- **Impacto:** Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información**: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es

esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

- **Integridad:** La información de ISAGXXX debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la Empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas financieras.

- **La Dirección:** Es la encargada de combinar los recursos humanos y técnicos lo mejor posible para conseguir los objetivos de la empresa; está conformada por la presidencia y directivos, quienes se encargarán de desarrollar los planes a largo plazo de la empresa.

- **No conformidad:** El no cumplimiento de un requisito especificado. También puede denominarse no conformidad real.

- **No conformidad mayor:** El no cumplimiento de un requisito debido a la falta frecuente o deliberada de cumplimiento de un requisito documentado en el sistema, incumplimiento de requisitos legales o reglamentarios, múltiples no conformidades menores dentro del mismo requisito de la Norma o la falta deliberada en corregir No Conformidades.
- **No conformidad menor:** El no cumplimiento de un requisito sin que exista una amenaza relevante o significativa para el Sistema de Gestión de Calidad o cuando sea una instancia aislada de incumplimiento.

- **No conformidad potencial:** Evento en el cual no hubo No Conformidad, pero en caso de repetirse pudiera serlo, por la existencia de un riesgo. Una acción preventiva pudiera ser tomada para evitar su ocurrencia.

- **Observación:** Apartado del informe de auditoría en el que el auditor deja constancia de las oportunidades de mejora, de los riesgos para la calidad o de cualquier otro detalle que haya observado y le parece relevante registrar.

- **Observador:** Integrante del equipo auditor que se encuentra en proceso de entrenamiento y su objetivo es adquirir competencia mediante la observación. Algunas veces apoya al equipo auditor tomando notas de los hallazgos de la auditoría en las listas de chequeo.

- **Plan de auditoría:** Descripción de las actividades en el sitio y arreglos para una auditoría.

- **Probabilidad:** Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Proceso:** conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.

- **Programa de auditoría:** Conjunto de una o más auditorías planificadas para un período de tiempo específico y dirigido hacia un propósito específico.

- **Propietario de la Información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de

información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

- **Reducción del riesgo:** Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

- **Responsabilidades:** Compromisos u obligaciones del personal o grupo de trabajo.

- **Riesgo:** Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la información en los activos de una empresa.

- **Riesgo Inherente:** Es aquel riesgo que por su naturaleza no se puede separar de la situación donde se presenta. Es propio de las actividades que conlleva el proceso relacionado.

- **Riesgo Residual:** Nivel restante de riesgo después de su tratamiento.

- **Riesgo en la seguridad de la información:** Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

- **Seguridad de la información:** preservación de la integridad, la confidencialidad, y la disponibilidad de la información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. *(Fuente: NTC-ISO/IEC 27001:2005).*

- **S.G.S.I:** Sistema de Gestión de Seguridad de la Información.

- **Transferencia del riesgo:** Compartir con otra de las partes la pérdida (consecuencias negativas) de un riesgo.

- **Tratamiento de la Información:** Desarrollo de las siguientes actividades sobre la información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.

- **Tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.

- **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

- **Valoración del riesgo:** Proceso global de análisis y evaluación del riesgo.

- **Vulnerabilidades:** Debilidad de un activo de información frente a una amenaza.

1.3 BENEFICIOS DEL PROYECTO

A continuación se enumeran algunos de los beneficios en la implantación de un SGSI para **ISAGXXX:**

- Fomentar la aplicación de mejores prácticas de seguridad de la información.
- Robustecer la confiabilidad de los servicios ofrecidos a los clientes de ISAGXXX.
- Ganar confianza en el sector como una empresa comprometida con la seguridad de la información

2. METODOLOGIA DEL PROYECTO

2.1 Entendimiento del Marco Normativo del Proyecto.

De acuerdo a la distribución de controles, requisitos y mejores prácticas para la implementación de un sistema de gestión basado en las normatividades ISO 27001, se describen a continuación los controles que aplican para cada norma.

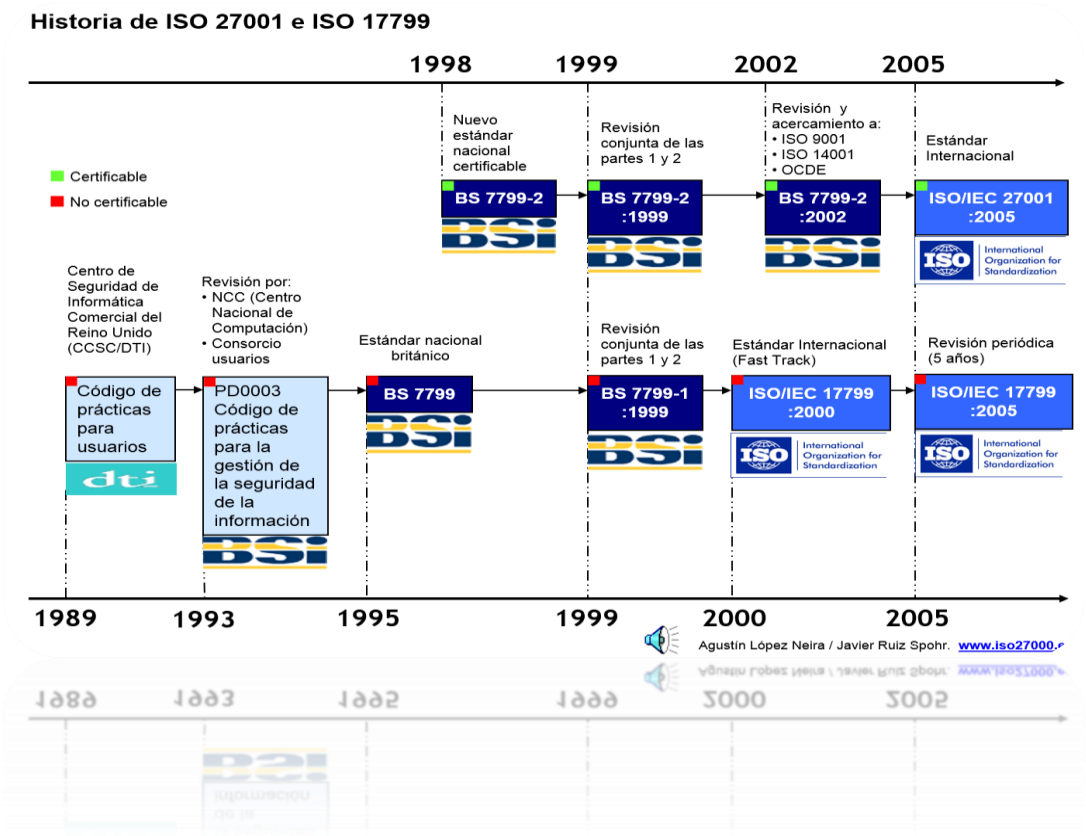


Figura 1. Evolucion de la ISO 27001

Controles ISO/IEC ISO 27001:2013

A cada entrevistado se presentó el alcance de cada uno de los dominios de seguridad ISO 27001. En resumen se explicaron:

- **Política de seguridad**: Documento en el cual se estipulan las políticas con respecto a la seguridad de la información de la organización ISAGXXX.

- **Organización de la seguridad**: Estructura del departamento de seguridad que le permita gestionar la seguridad de la información dentro de la organización: Roles, compromisos, autorizaciones, acuerdos, manejo con terceros, entre otros.

- **Gestión de activos**: Procedimientos para la identificación de los activos de información y los requerimientos de estos en cuanto a confidencialidad, integridad y disponibilidad.

- **Seguridad del Recurso Humano**: Procedimientos para asegurar que empleados, contratistas y terceros entienden sus responsabilidades y son idóneos para los roles a desempeñar minimizando los riesgos relacionados con personal.

- **Seguridad Física y del entorno**: Procedimientos y controles para prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la organización y a su información.

- **Gestión de comunicaciones y operaciones**: Procedimientos y controles para garantizar la correcta y segura operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica)

- **Control de acceso**: Procedimientos y controles para garantizar que el acceso a los activos de información este restringido a personal autorizado.

- **Adquisición, desarrollo y mantenimiento de sistemas de información**: Procedimientos y controles para asegurar la inclusión de los controles de seguridad en los nuevos sistemas de información (infraestructura, aplicaciones, servicios, etc.) o por cambios a los mismos.

- **Gestión de incidentes de seguridad**: Procedimientos y controles que buscan que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados de tal manera que se tome una acción correctiva adecuada y en el momento indicado.

- **Gestión de la continuidad del negocio**: Procedimientos y controles enfocados en reaccionar en contra de interrupciones de la función del negocio y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y por otro lado, asegurar que se recuperen a tiempo.

- **Cumplimiento**: Procedimientos y controles que buscan prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

2.2 Fases del Proyecto

A continuación se presenta las fases, actividades y la planeación del proyecto TFM, focalizado a la implementación del SGSI a la organización ISAGXXX.

- **Fase 1: Situación actual: Contextualización, objetivos y análisis diferencial**

Introducción al Proyecto. Enfoque y selección de la empresa que será objeto de estudio. Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto la ISO/IEC 27001+ISO/IEC 27002

- **Fase 2: Sistema de Gestión Documental**

Elaboración de la Política de Seguridad. Declaración de aplicabilidad y Documentación del SGSI

- **Fase 3: Análisis de riesgos**

Elaboración de una metodología de análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

- **Fase 4: Propuesta de Proyectos**

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

- **Fase 5: Auditoría de Cumplimiento de la ISO/IEC 27002:2013**

Evaluación de controles, madurez y nivel de cumplimiento de la organización con relación a la madurez en la implementación de controles de seguridad del SGSI, de acuerdo a las fases previas de definición, planeación del SGSI. La auditoría de cumplimiento es realizada como una auditoria interna de seguimiento al SGSI, en un periodo de tiempo de 3 meses, una vez definido e implantado alrededor de 50% de los controles de seguridad, sugeridos por el SGSI.

- **Fase 6: Presentación de Resultados y entrega de Informes**

A continuación se describen los entregables del proyecto de implementación del SGSI para la organización ISAGXXX.

- Informe Análisis Diferencial
- Modelo del SGSI mediante el esquema Documental ISO/IEC 27001
- Informes de Gestión de Riesgos (Gestión de Activos, Análisis y evaluación de riesgos, anexos).
- Plan de Tratamiento de riesgos (Iniciativas de Seguridad, Planeación de proyectos de seguridad de la información, roadmap de proyectos específicos, PESI, anexos).
- Procedimientos, instructivos, guías del SGSI.
- Auditoría de Cumplimiento
- Presentación de resultados del proyecto SGSI. (Presentación, resumen ejecutivo, conclusiones y lecciones aprendidas del proyecto).

3. FASE 1: SITUACIÓN ACTUAL, CONTEXTO, OBJETIVOS Y ANALISIS DIFERENCIAL

3.1 DESCRIPCIÓN DE LA EMPRESA ISAGXXX

El presente proyecto busca desarrollar el plan de implementación de la Norma ISO 27001:2013 para la organización **ISAGXXX**; en **ISAGXXX** construimos proyectos de generación, producción y comercialización de energía con el propósito de satisfacer las necesidades de nuestros clientes y crear valor empresarial. Trabajamos para ser líderes en generación y transacciones de energía en Colombia, aliados de la productividad de nuestros clientes y reconocidos por los negocios de energía en mercados internacionales.

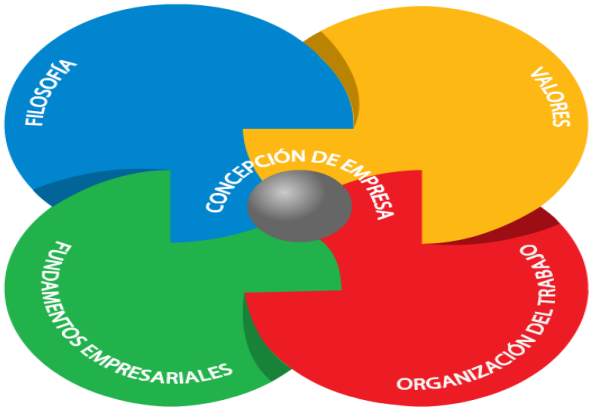
El desarrollo integral de los trabajadores y la responsabilidad empresarial son la base de la creación conjunta de valor para nuestros accionistas y la sociedad. Desarrollamos nuestra gestión con ética, enfoque en el cliente, sentido económico y responsabilidad social y ambiental. Somos una empresa de servicios públicos mixta, de carácter comercial y de orden nacional.

Poseemos y operamos cinco (5) centrales de generación; **86,43%** de nuestra capacidad es hidráulica, en cuatro (4) centrales, y **13,57%** es térmica, en una termoeléctrica, lo que nos brinda flexibilidad operacional en condiciones hidrológicas adversas.

Gestión de la Organización ISAGXXX

Es la concepción básica que orienta la gestión empresarial de la organización. Describe la filosofía, los valores y propósitos empresariales y la forma de hacer el trabajo para mejorar la productividad y competitividad.

A continuación se describen el modelo de gestión organizacional para **ISAGXXX**.



Misión DE ISAGXXX.

ISAGXXX desarrolla la capacidad de generación, produce y comercializa energía con el propósito de satisfacer las necesidades de sus clientes y crear valor empresarial. La gestión se desarrolla con ética, enfoque al cliente, sentido económico y responsabilidad social y ambiental.

Propósito superior

- Generamos energía inteligente y prosperidad para la sociedad.
- Generamos energía eficiente que contribuya a la mitigación del cambio climático, manteniendo la competitividad de la empresa en la industria, utilizando redes colaborativas y prácticas coherentes con el desarrollo humano sostenible y generando valor compartido con los grupos de interés.

Valores

Actitudes que definen la forma de actuar de la Organización y la forma en que quiere ser percibida por el entorno.

Ética: valor fundamental. Para **ISAGXXX** la ética es hacer las cosas correctamente y de buena fe; ser coherente entre lo que se piensa, se dice y se hace; y privilegiar el bien común sobre el particular, contribuyendo a la sostenibilidad de la sociedad y del medio en que ésta se desarrolla.

Los valores con los que la organización se relaciona con el entorno son:

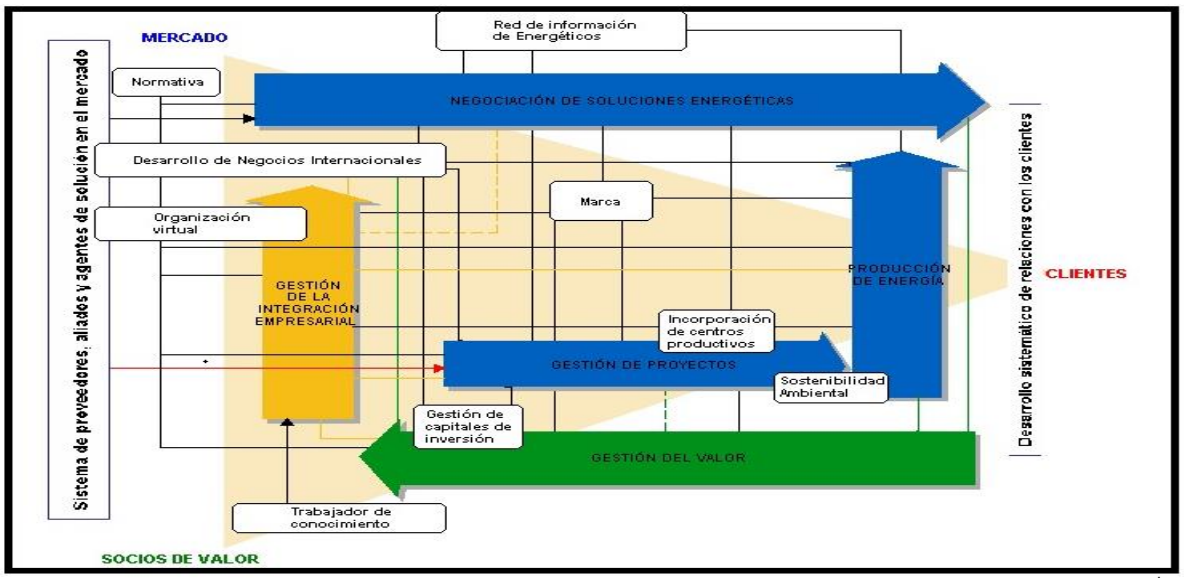
- Responsabilidad social y ambiental
- Enfoque al cliente
- Sentido económico

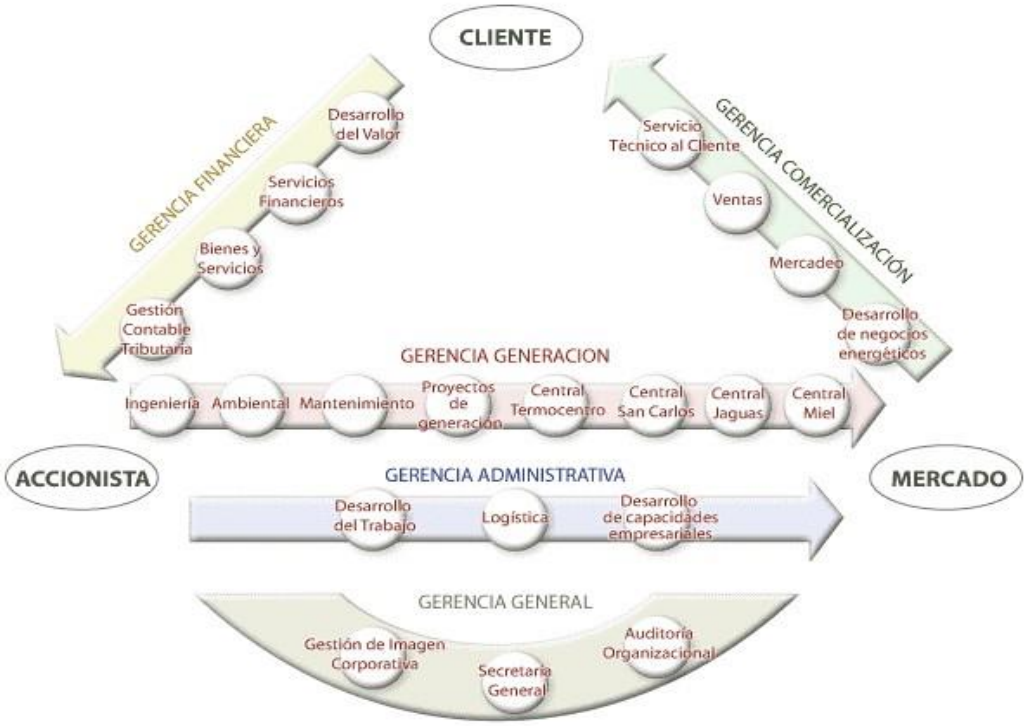
Los valores que se proyectan en la relación con las demás personas y para el crecimiento individual son:

- Respeto a las personas
- Trabajo en equipo
- Autocontrol
- Disposición al cambio
- Humildad

Mapa Orgánico de Procesos de la organización ISAGXXX.

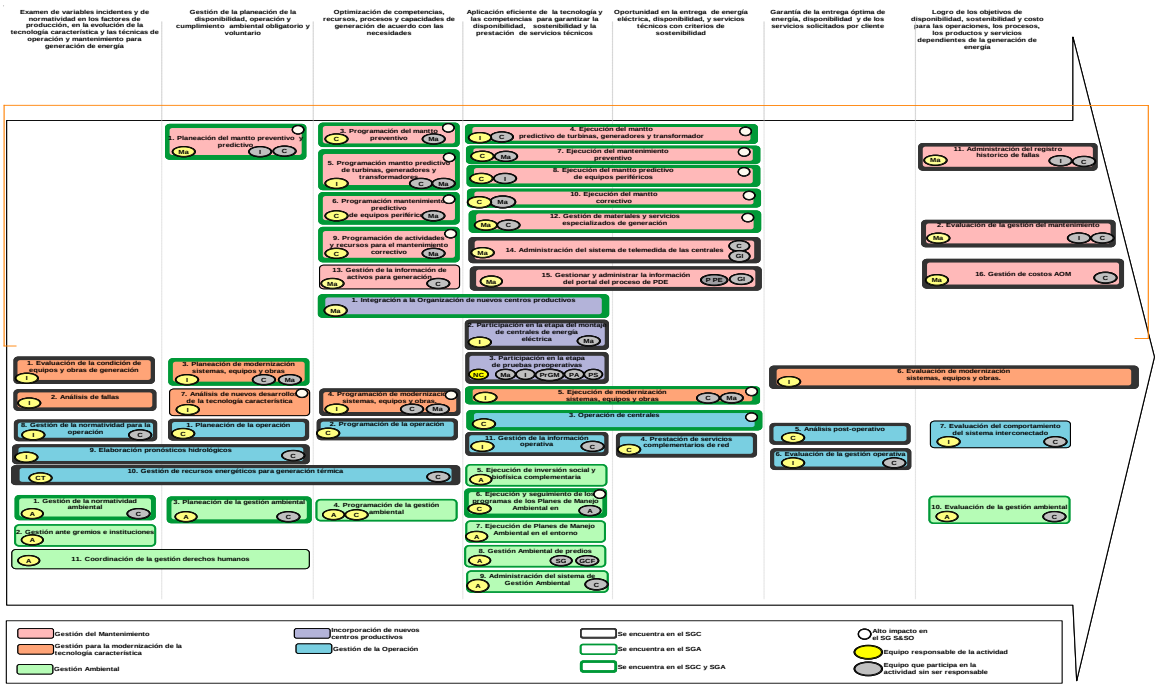
A continuación se describe el diagrama de proceso de la organización:





ISAGXXX, está compuesta por alrededor de más de 300 empleados, 5 gerencias estratégicas [Gerencia financiera, gerencia de comercialización, gerencia de generación, gerencia general y la gerencia administrativa]; en las anteriores graficas se explica la estructura organizacional, los procesos transversales, procesos críticos y los procesos de apoyo de la organización.

A continuación se describen los componentes, actividades y equipos responsables para los procesos de la gestión de generación, producción y comercialización de energía.



3.2 OBJETIVOS DEL PROYECTO

El Sistema de Gestión de Seguridad de la Información de ***ISAGXXX*** está orientado a la definición de todos los aspectos necesarios para establecer, operar, mantener y dirigir un sistema efectivo para el tratamiento seguro de la información perteneciente a la compañía.

Este documento describe los objetivos, metas, y responsabilidades relacionadas con el Sistema de Gestión de Seguridad de la Información de ***ISAGXXX*** y tiene como objetivo presentar y poner en vigencia las Políticas de Seguridad de la Información, los Procedimientos de Gestión del Sistema, y demás requerimientos del SGSI, a todos los funcionarios, contratistas y proveedores que deban utilizar los recursos y sistemas de información de ***ISAGXXX*** relacionados con el alcance definido.

ISAGXXX se reserva el derecho de alterar o modificar partes de este Manual, a fin de atender los requerimientos de su Sistema de Gestión de Seguridad de la Información, cuando sea necesario.

Los principales objetivos de seguridad propuestos en ***ISAGXXX*** *son*:

- Proteger la confidencialidad, integridad, disponibilidad, eficiencia, efectividad y confiabilidad de la información de la compañía y de cualquiera de sus clientes y socios de negocio.
- Establecer controles para minimizar los riesgos significativos y de alto impacto para el negocio, como el robo o fuga de información, accesos no autorizados, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial, la alteración o modificación de la misma, y en general la continuidad de las operaciones y la reputación de ***ISAGXXX***
- Establecer claramente al interior de la compañía los roles y responsabilidades en términos de Seguridad de la Información.
- Desarrollar y mantener una cultura en Seguridad de la Información orientada a la identificación y análisis de riesgos, a través de la sensibilización y de los funcionarios y contratistas de ***ISAGXXX***
- Promover el cumplimiento de las leyes y normas colombianas vigentes, las regulaciones internacionales y locales relacionadas con los servicios que presta la compañía y la adopción de buenas prácticas y estándares de seguridad como ISO/IEC 17799 e ISO/IEC 27001:2013.
- Registrar y revisar los problemas, fallas, eventos e incidentes de seguridad reportados e identificar las lecciones aprendidas para utilizarlas como fuente de mejora continua en los procesos de seguridad.
- Apoyar la definición, implantación y pruebas del plan de continuidad del negocio.

3.3 CONTEXTO DEL SGSI

El Mapa de Procesos que ha sido definido bajo el modelo de gestión planteado en el marco del proyecto SGSI para ISAGXXX donde los requisitos para el Sistema de Gestión y Control Integral se expresan a través de elementos y subelementos, que indican debes lo que es obligatorio cumplir.

Sin embargo, no establecen la manera de hacerlo. Cada proceso, en sus diferentes niveles, dará cumplimiento a los requisitos (“debes”) según su objetivo y alcance dentro de la organización, en conjunto con las disposiciones legales que le sean aplicables. Cabe anotar que cuando alguno de los requisitos establecidos en este marco no apliquen por la naturaleza de la organización, de sus procesos o por decisión de la Alta Dirección, la justificación de la no aplicabilidad del o los requisito(s) se debe documentar y comunicar.

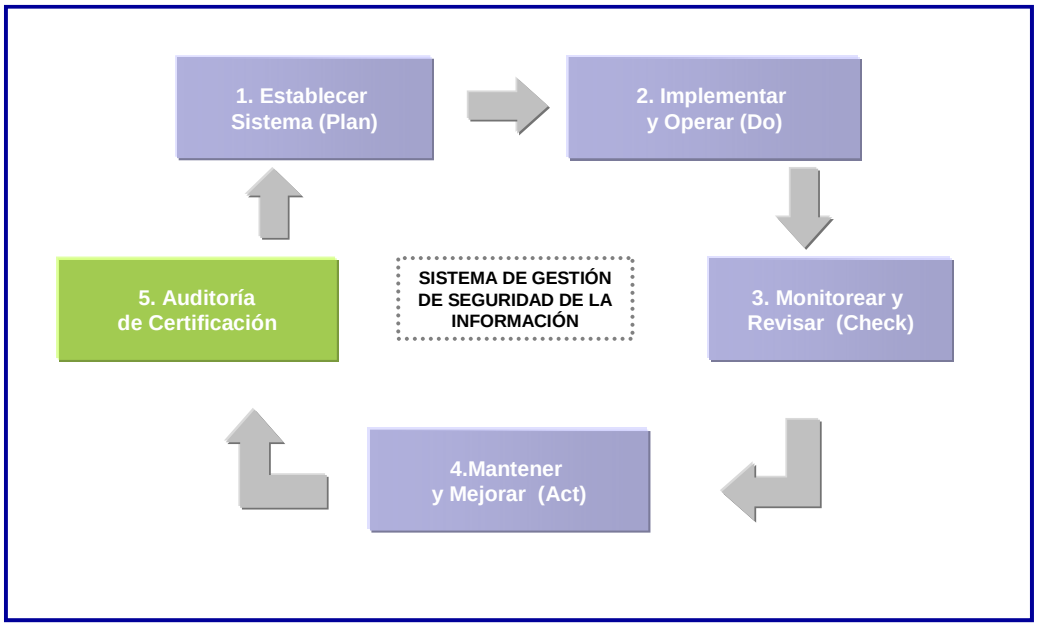


Figura 2. Visión esquemática del Marco de requisitos del SGSI

La orientación de este marco de requisitos promueve la adopción de un enfoque integral basado en procesos. Consiste en determinar, gestionar y controlar de manera eficaz una serie de actividades relacionadas entre sí. Una ventaja que proporciona este enfoque es el control continuo sobre los vínculos entre los procesos individuales que forman parte de un sistema conformado por procesos, así como sobre su combinación e interacción.

En ese sentido, se ha tomado la decisión de gestionar, bajo el marco del elemento de información y conocimiento, la aplicación de los requisitos establecidos en la Norma NTC-ISO/IEC 27001:2013 asociada a los Sistema de Gestión de Seguridad de la Información como parte del Sistema de Gestión integral de ISAGXXX, buscando la determinación de los activos críticos, sus riesgos y las medidas adecuadas para la mitigación de los mismos.

Así, el proyecto se divide en cinco (5) etapas:

1. **Establecer el SGSI (*Plan*)**

Esta etapa es fundamentalmente para la definición de la estructura del SGSI, validación de alcances, elaboración de la documentación especificada en la sección[1] del estándar ISO/IEC 27001:2013.

2. **Implantación y Operación del SGSI (*Do*)**

Esta etapa básicamente la ejecuta ISAG**XXX** bajo la coordinación de ROBIN SALCEDO y el equipo directivo del proyecto TFM MISTIC. Durante ésta se desarrollan los controles que integran la declaración de aplicabilidad (SoA: *Statement of Applicability*), asimismo, se lleva a cabo la ejecución del programa de concientización de los usuarios y el equipo de administración, y se inicia la operación del Sistema de Gestión de Seguridad de la Información.

3. **Monitoreo y Revisión del Sistema de Gestión de Seguridad de la Información (*Check*)**

Esta etapa la ejecuta **ISAGXXX** en coordinación con **ROBIN SALCEDO**. Durante esta etapa se realizan una serie de revisiones y auditorías al SGSI para detectar las áreas de oportunidad en la eficiencia de implantación de controles de seguridad, y determinar el grado de apego del SGSI a los objetivos de negocio de **ISAGXXX**. Después de estas revisiones, **ROBIN SALCEDO** en conjunto con **ISAGXXX** trabajará para cerrar las brechas detectadas.

4. **Mantenimiento y Mejora (*Act*)**

Esta etapa la coordina **ROBIN SALCEDO** y la ejecuta ISAGXXX. Mientras la empresa lleva a cabo las correcciones necesarias, **ROBIN SALCEDO** asesora la ejecución de éstas, con base en las observaciones de la Etapa 3.

[1] **1 requerimientos de documentación.** El SGSI debe incluir:
- a) Documento del SGSI incluyendo política y objetivos;
- b) Alcance del SGSI;
- c) Controles y procedimientos que soportan al SGSI;
- d) Metodología de evaluación de riesgos;
- e) Reporte de la evaluación de riesgos;
- f) Plan de tratamiento de riesgos;
- g) Procedimientos documentados necesarios para asegurar una efectiva planeación, operación y control de los procesos de seguridad de la información y la descripción de cómo medir la efectividad de los controles requeridos por el estándar;
- h) Declaración de Aplicabilidad.

5. **Auditoría de Certificación**

Un auditor de una Entidad Certificadora autorizada realiza una revisión para detectar el grado de apego a la norma ISO/IEC 27001:2013. Basado en el dictamen de ésta, ROBIN SALCEDO coordinará y apoyará a la empresa en la ejecución de las actividades necesarias para cerrar las brechas detectadas.

Exclusiones:

- NO es parte del alcance de esta fase la ejecución de un "Plan de Continuidad del Negocio" ni de un "Plan de Recuperación ante Desastres" (BCP y DRP respectivamente por sus siglas en inglés).

Con base en el Marco de referencia para implantación del estándar descrito en la sección anterior y en la situación actual de ISAG**XXX** en torno a la seguridad, las acciones a realizar durante el proyecto son las siguientes:

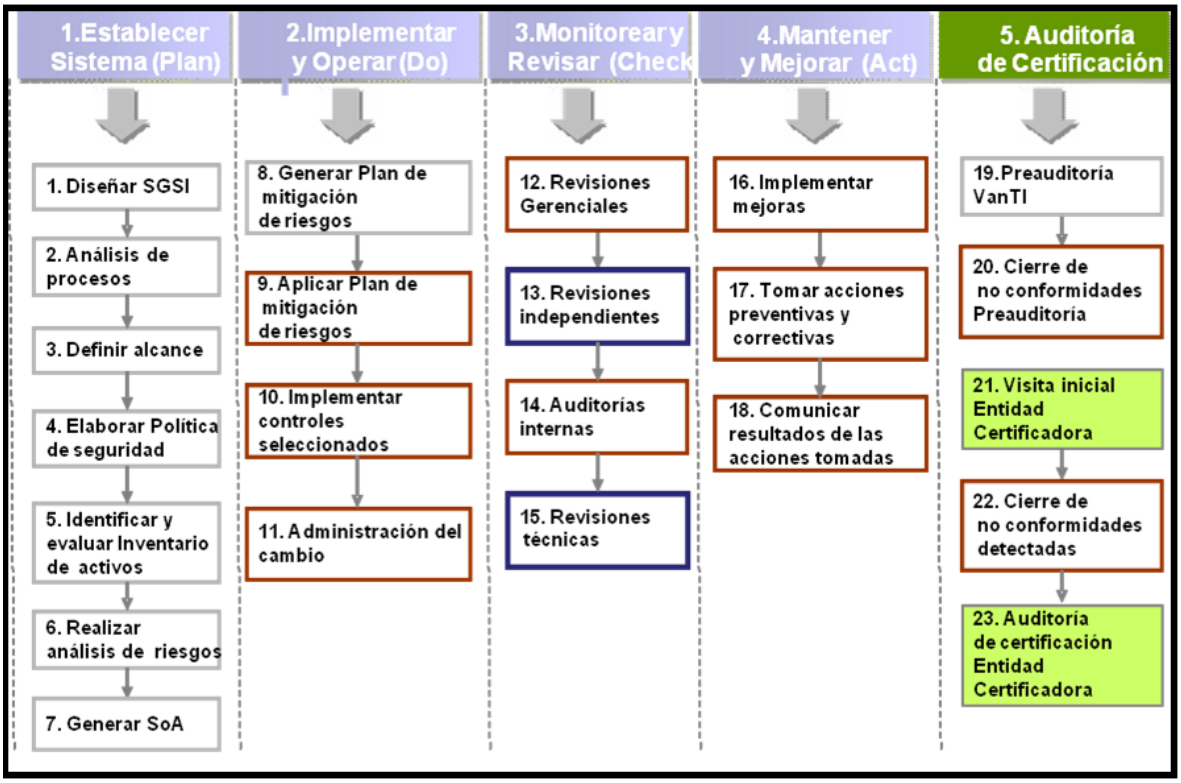


Figura 3. Actividades del Plan de Implementación del SGSI.

3.4 ALCANCE DEL PROYECTO

Definición e Implementación del SGSI basado en la Gestión de la Seguridad de la Información que soportan las actividades de los procesos de generación de energía y gestión tecnológica de los activos críticos para la organización ***ISAGXXX****X; incluyendo los procesos de gestión de mantenimiento, sistemas transaccionales o tecnológicos, teleprocesos, TI y nuevos proyectos de modernización.*

DECLARACIÓN DEL COMPROMISO ISAGXXX

Con el fin de establecer y manifestar su compromiso con el Sistema de Gestión de Seguridad de la Información, la Presidencia de ***ISAGXXX*** ha asignado los recursos necesarios para la implantación, operación, mantenimiento y mejora de todos los elementos que componen este Sistema. Así mismo, se compromete a ser un ejemplo en el cumplimiento de las políticas y demás responsabilidades definidas en el sistema.

XXXXXXXXXXXX
Presidente **ISAGXXX** S.A.

VIGENCIA DEL SGSI ISAGXXX

Todas las reglas contenidas en el presente documento y responsabilidades que de éstas se desprenden toman vigencia a partir del 24 de noviembre de 2014, fecha en la cual ***ISAGXXX*** hace oficial la aplicación de su Sistema de Gestión de Seguridad de la Información.

3.5 GOBIERNO DEL SGSI

Todas las actuaciones del Equipo de Dirección de la empresa ISAGXXX, conformado por el Director, y Líder del SGSI, así como las de todos los colaboradores del Instituto y del CITT, están enmarcadas en las disposiciones del Código de Buen Gobierno y el Código de Ética de la empresa.

Uno de los compromisos adquiridos por el equipo de dirección, es la implementación del sistema de gestión de seguridad de la información, con el fin de obtener los siguientes beneficios:

- Aspecto organizacional: Compromiso: el registro de las actividades permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización, en todos sus niveles y probar la diligencia razonable de sus administradores.
- Aspecto legal: Conformidad con requisitos legales: el registro permite demostrar que la organización observa todas las leyes y normativas aplicables al alcance.
- Aspecto funcional: Gestión de los riesgos: obtención de un mejor conocimiento de los sistemas de información, sus debilidades y los medios de protección. Garantiza también una mejor disponibilidad de los materiales y datos.
- Aspecto comercial: Credibilidad y confianza: los socios, los accionistas y los clientes se tranquilizan al constatar la importancia que la organización concede a

la protección de la información. Una certificación también puede brindar una diferenciación sobre la competencia y en el mercado.

- Aspecto financiero: Reducción de los costos vinculados a los incidentes.
- Aspecto humano: Mejora la sensibilización del personal hacia la seguridad y a sus responsabilidades en la organización.

3.6 ANALISIS DIFEREMCIAL DE ISAGXXX

Análisis Diferencial ISO 27001:2013

El análisis diferencial fue basado en la norma ISO 27001:2013, esta nueva versión a diferencia de su antecesora la norma ISO 27001:2005 incluye una cláusula independiente donde se específica la importancia de las partes interesadas y sus requerimientos deben estar debidamente identificados. Los conceptos de "documentos" y "registros", se combinan dentro del término información documentada; este nuevo concepto elimina el requisito del antiguo estándar acerca de tener procedimientos documentados para control de documentos, auditoría interna, acciones correctivas y acciones preventivas. Otro de los cambios sobresalientes corresponde a la evaluación y tratamiento de riesgos, pues brinda mayor libertad en la forma en que se identifican los riesgos, cambiando el concepto de propietario de los activos por el término "dueño del riesgo", llevando la responsabilidad a un nivel más alto.

Los objetivos, seguimiento y medición toman mayor importancia, con cláusulas separadas y reglas concretas. Es necesario contar con objetivos claros, diseñar un programa de seguridad para el logro de los objetivos, definir métricas y definir quién debe analizar y evaluarlos resultados.

El detalle de la evaluación de diagnóstico de **ISAGXXX** en la norma ISO 27001:2013 se encuentra en el anexo A de este documento. La figura 6. **ISAGXXX ISO 27001:2013** describe de manera gráfica el resultado respecto al estado actual de los diferentes dominios establecidos en la norma y por otro lado la tabla cuatro (4) muestra la calificación que se obtuvo por dominio para cada uno de los requerimientos de gestión identificados en el la norma ISO 27001.

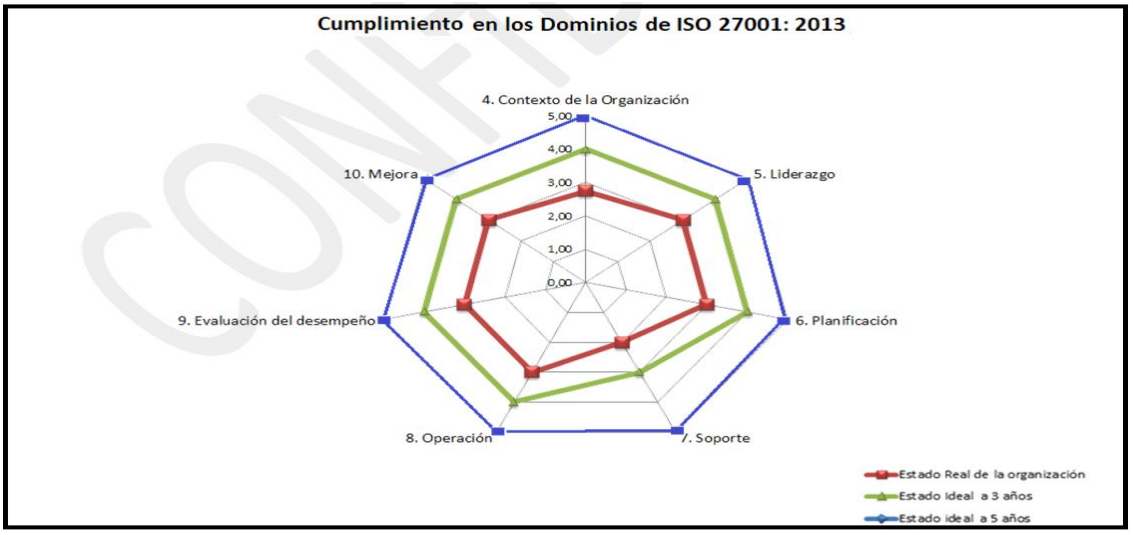


Figura 4. ISAGXXX ISO 27001:2013

PUNTAJE – DOMINIO		
DOMINIO	**Porcentaje**	**Calificación**
4. Contexto de la Organización	2,75	Repetible
5. Liderazgo	3,00	Repetible
6. Planificación	3,00	Definido
7. Soporte	2,00	Repetible
8. Operación	3,00	Definido
9. Evaluación del desempeño	3,00	Definido
10. Mejora	3,00	Repetible
PROMEDIO	***2,82***	***Repetible***

La situación actual del diagnóstico de seguridad de la información asociado a los requerimientos del estándar ISO 27001:2013 **[2,82 - Estado de madurez comprendido, de acuerdo a lo establecido en el estándar COBIT 4,1, entre el nivel de madurez Repetible y Definido**], indica que **ISAGXXX** está trabajando en estrategias para fortalecer la seguridad de la información en la entidad, las cuales deben ser afinadas para lograr un nivel de madurez mayor. En este documento no se especifica un valor proyectado específico, este valor debe ser resultado de las decisiones internas y las estrategias planteadas por los responsables directos de la implementación del proyecto de seguridad de la información en **ISAGXXX**.

Análisis Diferencial de ISAGXXX vs requerimientos de seguridad informática de las normas ISO 27002: 2013

El Diagnostico de seguridad informática (GAP análisis) fue basado en la norma ISO 27002:2013. Dentro de los cambios que vale la pena resaltar, están los controles para el uso de dispositivos móviles y teletrabajo.

El detalle de la evaluación de diagnóstico de **ISAGXXX** en la norma ISO 27002 se encuentra en el anexo B de este documento. La figura 7. **ISAGXXX ISO 27002:2013** muestra de manera gráfica el resultado de cómo se encuentran actualmente los diferentes dominios establecidos en la norma ISO 27001:2013 y la siguiente tabla describe la calificación que se obtuvo por dominio.

A continuación mediante la siguiente gráfica, los niveles de madureces actuales para cada uno de los dominios correlacionados entre la norma ISO 27002:2013, adicionalmente la presentación mediante una escala de color [Rojo, Verde, Azul] para los niveles actuales, niveles deseados a tres años y los niveles recomendados de forma ideal para un plan de acción a largo plazo de 5 años para la organización ISAGXXX.

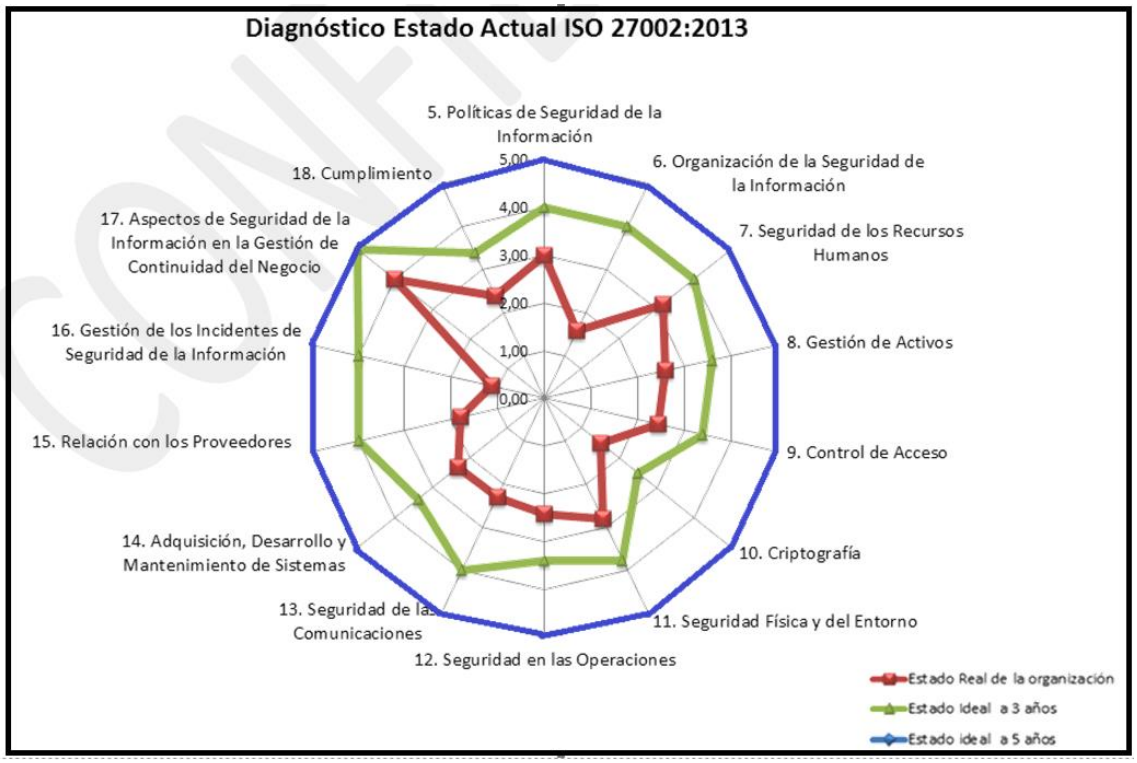


Figura 5. ISAGXXX ISO 27002:2013

A continuación se describen los niveles de madurez actuales ponderados para los dominios, controles y requerimientos de seguridad informática comunes para las normas ISO 27002.

PUNTAJE - DOMINIO		
DOMINIO	**Porcentaje**	**Calificación**
5. Políticas de Seguridad de la Información	3,00	Definido
6. Organización de la Seguridad de la Información	1,57	Inicial
7. Seguridad de los Recursos Humanos	3,17	Definido
8. Gestión de Activos	2,60	Repetible
9. Control de Acceso	2,43	Repetible
10. Criptografía	1,50	Inicial
11. Seguridad Física y del Entorno	2,80	Repetible
12. Seguridad en las Operaciones	2,43	Repetible

13. Seguridad de las Comunicaciones	2,29	Repetible
14. Adquisición, Desarrollo y Mantenimiento de Sistemas .	2,31	Repetible
15. Relación con los Proveedores	1,80	Inicial
16. Gestión de los Incidentes de Seguridad de la Información	1,14	Inicial
17. Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio	4,00	Gestionado
18. Cumplimiento	2,38	Repetible
PROMEDIO	***2,39***	***Repetible***

La situación actual del diagnóstico de seguridad de la información asociado a los requerimientos del estándar ISO 27002:2013 **[2,39 - Estado de madurez comprendido, de acuerdo a lo establecido en el estándar COBIT, entre el nivel de madurez Repetible y Definido**], indica que **ISAGXXX** está trabajando en estrategias para fortalecer la seguridad de la información en la entidad, las cuales deben fortalecerse para lograr un nivel de madurez mayor. En este documento se especifica un valor proyectado específico para cada uno de los aspectos que comprende la norma, se encuentra detallado en cada uno de los conceptos emitidos por el grupo consultor y con base en este valor se realizará el Roadmap a tener en cuenta por el personal de **ISAGXXX** encargado de realizar en forma directa la implementación del proyecto de seguridad de la información en **ISAGXXX**.

Para más detalles del diagnóstico o análisis diferencial actual de la organización **ISAGXXX**, por favor remítase a los siguientes anexos.

Metodología y Descripción del Proceso
Ver Anexos: Fase1 Situación Actual

- Matriz Análisis Diferencial ISO 27001:2013
- Matriz Análisis Diferencial ISO 27002:2013
- Declaración de Aplicabilidad

4 SISTEMA DE GESTIÓN DOCUMENTAL DEL SGSI

4.1 ESTRUCTURA ORGANIZACIONAL ISAGXXX

La estructura organizacional de la Seguridad de la Información de ***ISAGXXX*** *corresponde* al esquema definido y aprobado por la Presidencia, en donde se identifican las dependencias funcionales y estratégicas en términos de Seguridad de la Información para la compañía.

Para el caso específico de recursos humanos relacionados con la operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información de ***ISAGXXX,*** *la* Organización de la Seguridad de la Información se estructura en 3 (tres) niveles de jerarquía:

a) Nivel Gerencial:

Es el grupo encargado de definir la estrategia de seguridad y continuidad de la información para la compañía, definir y aprobar las políticas de seguridad de la información, elaborar y presentar los proyectos de seguridad, establecer las prioridades para su desarrollo, y revisar la implantación y la efectividad de las medidas adoptadas.

Este grupo lo compone un comité de seguridad en el que participa la Alta Dirección de la compañía, de manera que las decisiones y proyectos que se definan cuenten con su aval y sean acordes a los objetivos estratégicos del negocio.

La Alta Dirección demostrará su compromiso a través de:

- La revisión y aprobación de las Políticas de seguridad de la información.
- La promoción activa de una cultura de seguridad dentro de la compañía.
- Facilitar la divulgación de este manual a todos los funcionarios de la compañía.
- El aseguramiento de los recursos adecuados para implantar y mantener las Políticas y el Sistema de Gestión de seguridad de la información.

b) Nivel Técnico-Operativo de Seguridad:

Son grupos que tienen responsabilidades específicas dentro del Sistema de Gestión de Seguridad de la Información, principalmente en lo relacionado con la implementación y desarrollo del modelo de seguridad definido. Los principales integrantes de este grupo corresponden a los funcionarios del área de seguridad de la información de **ISAGXXX**

c) Nivel Usuarios Finales:

Son los usuarios de la información y por tal razón son los responsables de cumplir el modelo, políticas y definiciones establecidas para la compañía.

A continuación se presenta el organigrama de la nueva estructura organizacional el cual está orientado a cumplir con los requisitos esenciales de funcionamiento y operación en términos de seguridad de la información.

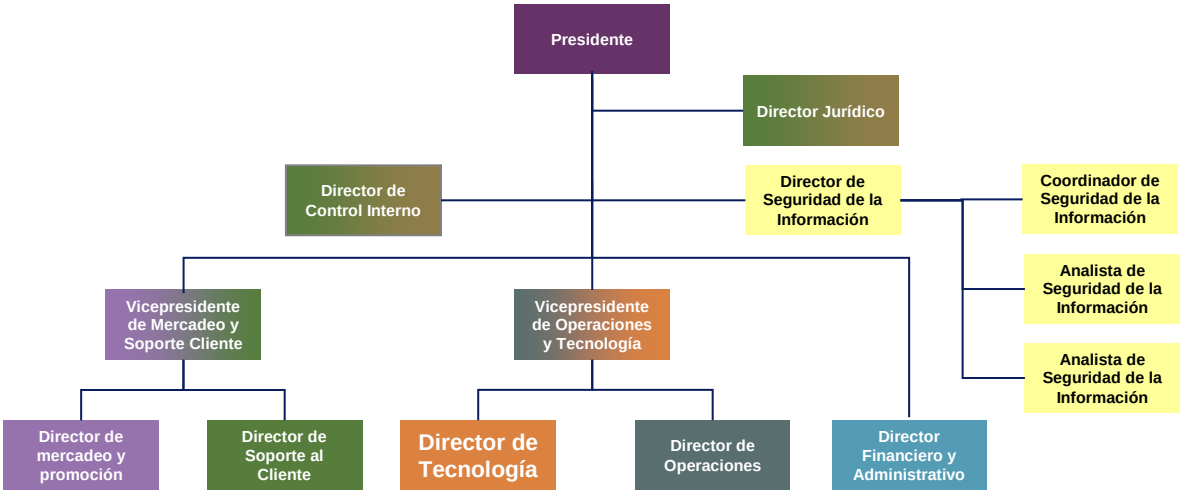


Figura 6. Estructura Organizacional

Comité de Seguridad de ISAGXX:

El Comité de Seguridad de ***ISAGXXX*** está conformado por los directores de todas las áreas de la compañía, el presidente y los vicepresidentes. Éste comité es el responsable de la centralización de todas las acciones relacionadas con la Seguridad de la información y Continuidad del negocio, y para todos los efectos se reúne de manera periódica, mínimo cada dos (2) meses o cuando se presenten situaciones que así lo requieran. [ISO/IEC 27001, A6.1.2].

El Comité está conformado actualmente por los siguientes cargos:

- Presidente
- Vicepresidente de Operaciones y Tecnología
- Director de Seguridad de la Información
- Director de Soporte al Cliente
- Director de Operaciones
- Director de Tecnología
- Director Administrativo y Financiero
- Director de Control Interno
- Director Jurídico
- Director de Mercadeo

4.2 ESTRUCTURA DOCUMENTAL DEL SGSI

A continuación se describe la estructura documental definido para el modelo del SGSI de la organización ISAGXXX.

Figura 7. Modelo del SGSI.

4.3 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

ISAGXXXX basa la administración de Seguridad de los Activos de Información en las políticas generales contenidas en el directorio de políticas y por lo tanto estos documentos hacen parte de la normativa que regula la administración de la Seguridad de sus activos. Con su divulgación se busca que toda comunidad de funcionarios, contratistas, terceros y directivos conozcan ese marco normativo y de forma individual y colectiva brinden su apoyo para que la Empresa administre, utilice y disponga de información con niveles adecuados de seguridad.

Estos documentos permiten establecer las políticas sobre las cuales se debe direccionar el desarrollo de la seguridad de información para ISAGXXX y los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información en la Empresa

ISAGXXX ha definido la política institucional y una serie de políticas específicas de seguridad de la información las cuales hacen parte del SGSI y se encuentran en documentos anexos a este manual, los cuales se encuentran en la herramienta de documentación de la compañía.

Metodología y Descripción del Proceso
Ver Anexos: Fase2_SistemaGestiónDocumental

- Manual del SGSI **ISAGXXX** v1.0
- SGSI-POL-1_1 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas
- SGSI-POL-1_1 Política de Control de Acceso
- SGSI-POL-1_1 Política de Cumplimiento
- SGSI-POL-1_1 Política de Gestión de Activos
- SGSI-POL-1_1 Política de Gestión de Continuidad
- SGSI-POL-1_1 Política de Gestión de Incidentes
- SGSI-POL-1_1 Política de Gestión de Operaciones y Comunicaciones
- SGSI-POL-1_1 Política de Organización de la Seguridad de la Información
- SGSI-POL-1_1 Política de Seguridad Física
- SGSI-POL-1_1 Política de Seguridad Recursos Humanos
- SGSI-POL-1_1 Políticas Generales de Seguridad de la Información

4.4 PROCEDIMIENTOS DE SEGURIDAD

Un **Procedimiento de seguridad** es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los Procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización. Se describe **cómo** se implementan, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, atendiendo a sus formas de ejecución, periodicidad, personal participante y medios**.**

Se sustenta sobre la base de los recursos disponibles y, en dependencia de los niveles de seguridad alcanzados se elaborará un Programa de Seguridad Informática, que incluya las acciones a realizar por etapas para lograr niveles superiores.

Verificar si el sistema de gestión de seguridad de la información opera de acuerdo con los planes, procedimientos, registros y controles establecidos y es conforme con los requisitos de la norma ISO 27001:2006 y es eficaz para satisfacer los requisitos relacionados con seguridad de la información.

Describir las actividades requeridas para llevar a cabo una auditoría interna del Sistema de Gestión de Seguridad de la información - SGSI del Centro de Información Técnica y Tecnológica, con el fin de determinar si los objetivos de control definidos, los controles implementados, los procesos establecidos y procedimientos definidos, cumplen los requerimientos de la norma NTC-ISO/IEC 27001 y acatan las políticas, lineamientos y directrices, emitidos por la organización.

Para la puesta en práctica del Sistema de Gestión de Seguridad de la Información, se han definido una serie de procedimientos y formatos los cuales están ubicados en la herramienta de documentación de la compañía.

REVISIÓN POR LA DIRECCIÓN.

Asegurar una adecuada planeación y corrección de las desviaciones en el cumplimiento de los objetivos, estableciendo los requisitos mínimos, los responsables y los mecanismos para realizar la Revisión por la Dirección de los procesos y macro procesos del Sistema de Gestión de Seguridad de la Información de ISAGXXX.

El Sistema de Gestión de Seguridad de la Información de ISAGXXX contempla una evaluación periódica, sistemática y estructurada del SGSI de ISAGXXX a cargo de la Alta Dirección que permite asegurar una adecuada planeación y la corrección de las desviaciones en el cumplimiento de los objetivos y como tal, incluye la toma de decisiones sobre acciones necesarias, que dentro de un marco de conveniencia razonable para la organización, promueva el mejoramiento de productos, procesos y capacidades organizacionales que permitan alcanzar resultados de eficiencia, eficacia y efectividad.

Este procedimiento hace parte del Sistema de Gestión de Seguridad de la Información de ISAGXXX; es aplicable a todos los funcionarios responsables por el seguimiento y evaluación del SGSI, de la organización y a los Representantes de la Dirección.

Metodología y Descripción del Proceso
Ver Anexos: Fase2_SistemaGestiónDocumental

- Proc_Revision del SGSI por la Dirección ISGXXX v1.0

ROLES Y RESPONSABLES DEL SGSI

El Sistema de Gestión de Seguridad de la Información de ISAGXXX define los diferentes roles y funciones de los diferentes participantes del SGSI en ISAGXXX, estos roles están alineados y cumplen con la funciones necesarias para poder llevar a satisfacción el desarrollo y ejecución del SGSI basado en la norma ISO 27001:2005.
Entre estas definiciones de roles y responsabilidades se podrán identificar alguno de los siguientes items:

- Quien es el responsable de la ejecución de cada hito
- Quien toma las decisiones, solo o conjuntamente con otros
- Quien gestiona los recursos y controla el progreso del trabajo
- Quien debe ser informado
- Quien debe ser consultado
- Quien debe participar
- Quien debe dar apoyo o dotar de infraestructura al equipo
- Quien asegura la calidad de los resultados

Metodología y Descripción del Proceso
Ver Anexos: Fase2_SistemaGestiónDocumental

- Proc_Roles y responsabilidades SGSI ISAGXXX v1.0

METRICAS DEL SGSI

Los indicadores reflejarán cuáles fueron las consecuencias de acciones tomadas en el pasado en el marco de una organización. El objetivo principal es que los indicadores sienten las bases para acciones a tomar en el presente y en el futuro.

Es importante que los indicadores reflejen los datos veraces y fiables, ya que el análisis de la situación, de otra manera, no será correcto. Por otra parte, si los indicadores son ambiguos, la interpretación será complicada.

Se implementarán indicadores de gestión para mantener monitorizado y actualizado del SGSI, los cuales permitirán controlar el funcionamiento de las medidas de seguridad implementadas, eficacia y eficiencia.

Metodología y Descripción del Proceso
Ver Anexos: Fase2_SistemaGestiónDocumental

- Proc_Metricas e Indicadores SGSI ISAGXXX v1.0

AUDITORIAS DEL SGSI

Verificar si el sistema de gestión de seguridad de la información opera de acuerdo con los planes, procedimientos, registros y controles establecidos y es conforme con los requisitos de la norma ISO 27001:2006 y es eficaz para satisfacer los requisitos relacionados con seguridad de la información.

Describir las actividades requeridas para llevar a cabo una auditoría interna del Sistema de Gestión de Seguridad de la información - SGSI del Centro de Información Técnica y Tecnológica, con el fin de determinar si los objetivos de control definidos, los controles implementados, los procesos establecidos y procedimientos definidos, cumplen los requerimientos de la norma NTC-ISO/IEC 27001 y acatan las políticas, lineamientos y directrices, emitidos por la organización.

Metodología y Descripción del Proceso
Ver Anexos: Fase2_SistemaGestiónDocumental

- Proc_Procedimiento Auditoria_interna v1.0

5 GESTIÓN DEL RIESGO

El objetivo de este proceso es identificar y analizar los riesgos a los cuales están expuestos los activos de información, para identificar y seleccionar los controles apropiados de seguridad. La evaluación está basada en la valoración de los activos, en los requerimientos de seguridad propios del negocio y en los controles existentes.

La metodología empleada para la valoración de riesgo en la presente Consultoría de Seguridad, está alineada con el ejercicio anterior de riesgos desarrollada por ISAGXXX, teniendo en cuenta los lineamientos y buenas prácticas recomendadas en las normas ISO 27001 e ISO 27005 para la gestión y tratamiento del riesgo.

La figura 8 ilustra el flujo de actividades asociadas al proceso de análisis y valoración de riesgos como fuente principal de datos en la identificación de opciones de tratamiento y gestión del riesgo.

Figura 8. Metodología de análisis de riesgos.

El análisis se desarrolla a partir de la definición del alcance del proyecto (revisión y actualización del análisis de riesgo en el marco de la revisión del SGSI de ISAGXXX), y el levantamiento de información para entendimiento de cada uno de los procesos críticos involucrados del negocio. La definición del contexto de la Organización se realiza inicialmente a través de consulta de la información en el sistema de documentación de calidad de ISAGXXX, lo cual permite tener un mejor entendimiento del flujo de los procesos, entradas y salidas, así como las áreas de apoyo interno y externos que posibilitan la ejecución de las actividades. En la figura 2 se puede observar el mapa de procesos de ISAGXXX.

Posteriormente, se acuerdan y unifican los criterios de evaluación, de impacto y de aceptación de los riesgos, la lista de amenazas, vulnerabilidades, riesgos y controles, los cuales se encuentran alineados con la metodología de riesgos operativos de la Organización.

Una vez acordado los criterios básicos de estimación y valoración de riesgos y acotado el alcance del proyecto, se realiza el levantamiento de información para el análisis a través de entrevistas de trabajo (aprobadas por ISAGXXX), entendiendo los diferentes aspectos que conforman la operación del negocio de la organización, tanto en el aspecto tecnológico, como en los procesos e identificando las posibles amenazas que al materializarse comprometen la confidencialidad, integridad y disponibilidad de los recursos de información

En los informes de Evaluación de Riesgos periódicos se encuentran los resultados de este proceso así como la definición del nivel de riesgo aceptable.

El Comité de Seguridad realiza las evaluaciones periódicas del reporte entregado por la Dirección de Seguridad, para tomar las medidas y acciones que considere apropiadas, entre las cuales se encuentran la revisión de los niveles de riesgo esperados, el nivel de riesgo residual, las opciones de tratamiento, los planes de acción y los resultados obtenidos de actividades anteriores.

Para más detalles del proceso de identificación, clasificación y evaluación de activos de información asociados al proceso de generación de energía y a las actividades de gestión tecnológica de la organización **ISAGXXX**, por favor remítase a los siguientes anexos.

Metodología y Descripción Del Proceso
Ver Anexos: Fase3_Analisis de Riesgos

- Fase 3: gestión de Riesgos
- Matriz Gestión de Activos
- Matriz Gestión de Riesgos
- Declaración de Aplicabilidad
- Descripción de la metodología ISO 27005.
- Procedimiento Gestión de Riesgos.

6 PROYECTOS PROPUESTOS DE SEGURIDAD DE LA INFORMACIÓN

Para la puesta en práctica del Sistema de Gestión de Seguridad de la Información, se han definido una serie de proyectos, planes de acción o planes de tratamiento de los riesgos de seguridad de la información, los cuales están identificados en la siguiente carpeta del proyecto.

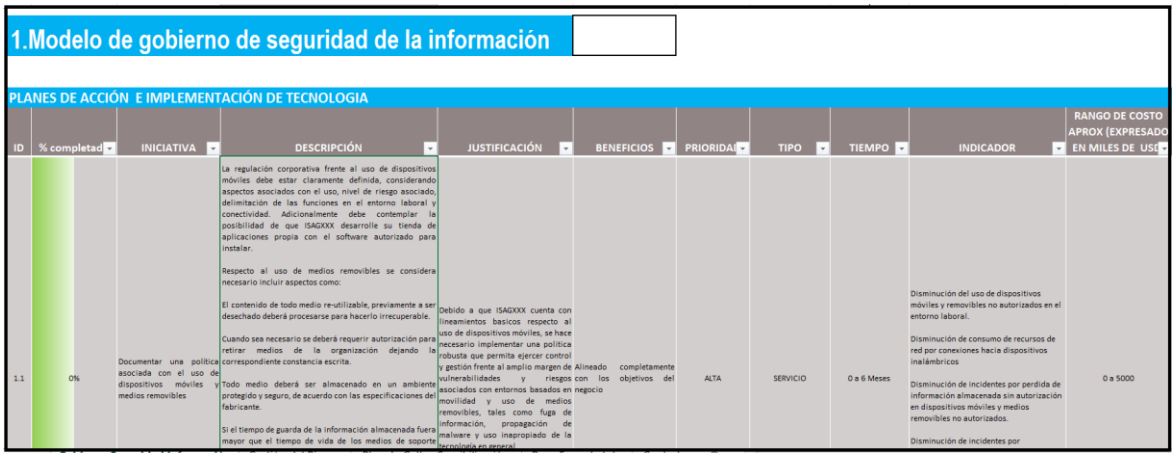
Teniendo en cuenta los hallazgos identificados, a continuación se presentan los controles que deben ser implementados, mantenidos y mejorados que permitirían mitigar los riesgos actualmente identificados y contribuirían al mejoramiento de los niveles de confidencialidad, integridad y disponibilidad de la información de ISAGXXX.

Los proyectos propuestos de seguridad informática, se agrupan de acuerdo a los siguientes criterios:

- Controles de seguridad evaluados en el diagnóstico de situación actual para la organización XM.
- Objetivos de control de seguridad.
- Dominios de seguridad informática de acuerdo a las normas y estándares ISO 27001, ISO 27002.
- Debilidades identificadas para controles con niveles de madurez muy bajos.
- Debilidades identificadas por la falta de controles de seguridad no identificados.
- Debilidades a nivel de gobierno corporativo en seguridad informática.
- Debilidades de seguridad que afectan el core del negocio y la gestión de los procesos de la organización XM.

A continuación se describen la propuesta de iniciativas de seguridad informática, presentada en 7 grupos, las cuales permiten desarrollar los planes de acción del roadmap de seguridad informática para los procesos transaccionales y el proceso del sistema de tiempo real.

A continuación se describen los atributos de algunos proyectos de seguridad, los cuales forman parte de las iniciativas de seguridad de la información para ISAGXXX.



1.Modelo de gobierno de seguridad de la información

PLANES DE ACCIÓN E IMPLEMENTACIÓN DE TECNOLOGIA

ID	% completad	INICIATIVA	DESCRIPCIÓN	JUSTIFICACIÓN	BENEFICIOS	PRIORIDAI	TIPO	TIEMPO	INDICADOR	RANGO DE COSTO APROX (EXPRESADO EN MILES DE USD
1.1	0%	Documentar una política asociada con el uso de dispositivos móviles y medios removibles	La regulación corporativa frente al uso de dispositivos móviles debe estar claramente definida, considerando aspectos asociados con el uso, nivel de riesgo asociado, delimitación de las funciones en el entorno laboral y conectividad. Adicionalmente debe contemplar la posibilidad de que ISAGXXX desarrolle su tienda de aplicaciones propia con el software autorizado para instalar. Respecto al uso de medios removibles se considera necesario incluir aspectos como: El contenido de todo medio re-utilizable, previamente a ser desechado deberá procesarse para hacerlo irrecuperable. Cuando sea necesario se deberá requerir autorización para retirar medios de la organización dejando la correspondiente constancia escrita. Todo medio deberá ser almacenado en un ambiente protegido y seguro, de acuerdo con las especificaciones del fabricante. Si el tiempo de guarda de la información almacenada fuera mayor que el tiempo de vida de los medios de soporte	Debido a que ISAGXXX cuenta con lineamientos basicos respecto al uso de dispositivos móviles, se hace necesario implementar una política robusta que permita ejercer control y gestión frente al amplio margen de vulnerabilidades y riesgos asociados con entornos basados en movilidad y uso de medios removibles, tales como fuga de información, propagación de malware y uso inapropiado de la tecnología en general.	Alineado completamente con los objetivos del negocio	ALTA	SERVICIO	0 a 6 Meses	Disminución del uso de dispositivos móviles y removibles no autorizados en el entorno laboral. Disminución de consumo de recursos de red por conexiones hacia dispositivos inalámbricos Disminución de incidentes por perdida de información almacenada sin autorización en dispositivos móviles y medios removibles no autorizados. Disminución de incidentes por	0 a 5000


1. Iniciativas Estratégicas del plan de seguridad Informática XM 2014-2019
• Aplicar los proyectos de Seguridad Informática identificados en el PESI teniendo en cuenta las actividades y planes de acción focalizados a las directrices de Gobierno, políticas, procedimientos, estándares, roles y responsabilidades necesarias para desarrollar el Plan de Seguridad Informática para XM
2. Iniciativas de Seguridad en Aplicaciones
• Implementar proyecto de Código Seguro, metodologías de desarrollo de Software Seguro, Análisis Estático de Código, criterios de aseguramiento en aplicaciones, pruebas de seguridad en aplicaciones WEB, tecnologías de cifrado en aplicaciones, gestión de la información en las aplicaciones e Iniciativas de Programa de Prevención y Fuga de Información
3. Iniciativas Programa de Prevención y Fuga de Información
• Desarrollar y Gestionar el programa de prevención y fuga de información para la organización, implementando tecnologías y soluciones de seguridad informática como DLP [Data Loss Preventions], fomentando la sensibilización, gestión y protección de los datos, privacidad de la información y soporte tecnológico de las soluciones tecnológicas para el Plan de Seguridad Informática para XM.
4. Iniciativas de Seguridad Informática para Dispositivos Móviles y Cloud Computing
• Implementar directrices de seguridad para integrar las tecnologías móviles a las estrategias de seguridad tecnológica que tiene actualmente XM, gestión de roles, usuarios y manejo de aplicaciones en el dispositivo móvil, aplicaciones de políticas de seguridad en dispositivos móviles, integración de dominio y directorio activo, gestión de identidad para soluciones móviles [IDM] y otras soluciones tecnológicas aplicables para la gestión de tecnologías móviles en la organización XM.
• Identificar procedimientos tecnológicos para el manejo de información en la NUBE, políticas de seguridad en la Nube, implementación de metodologías OWASP (Open Source Web Aplications Security Project) los cuales hacen parte del Plan de Seguridad Informática para XM.
5. Iniciativas de seguridad de infraestructura
• Identificar los temas relacionados con la arquitectura de red.
6. Monitoreo
• Fomentar el monitoreo activo de toda la infraestructura, (incluye terceros).
7. Seguridad física
• Fortalecer los aspectos que involucren la Seguridad física

Metodología y Descripción Del Proceso
Ver Anexos: Fase4_PropuestasProyectos

- Matriz Proyectos de Seguridad Propuestos v1.0
- Informe PTR Proyectos Propuestos Seguridad v1.1
- Matriz Gestión de Riesgos

7 AUDITORIA DE CUMPLIMIENTO

Para la puesta en práctica del Sistema de Gestión de Seguridad de la Información, se han definido el informe de la primera auditoria interna de seguimiento del SGSI, para determinar el nivel de avance en la implementación de proyectos, controles y planes de acción al corto plazo, en la gestión del SGSI.

Nota: para el desarrollo del TFM del master, se realiza una auditoria interna al SGSI de la organización ISAGXX, para evaluar el nivel de cumplimiento de los controles implementados en los planes de tratamiento de riesgos, iniciativas de seguridad de la información, hasta la fecha actual del proceso de implementación y validar le evolución de la madurez de la organización.

Metodología y Descripción del Proceso
Ver Anexos: Fase5_AuditoriaCumplimiento

- Informe de auditoría Interna SGSI **ISAGXXX** v1.0
- Auditoria de Cumplimiento ISO 27002 v1.0
- Auditoria de Cumplimiento ISO 27001 v1.0

8 CONCLUSIONES DEL PROYECTO

A continuación se describen las conclusiones del Proyecto.

- La cultura organizacional a nivel de seguridad de la información se ha incrementado en un 40%, debido a las actividades desarrolladas por el proyecto.

- Se llevaron a cabo campañas de sensibilización en la norma ISO 27001:2013 y los cambios con la ISO 27001:2005.

- El apoyo de la dirección es un factor clave en el gobierno del SGSI y en la madurez de la organización ISAGXX.

- Es necesario desarrollar una segunda auditoria interna al SGSI, para determinar el estado de los controles de seguridad que no fueron implementados en esta primer parte del proyecto.

- La gestión de riesgos, debe involucrar a todos los niveles de la organización y a la alta dirección de ISAGXXX.

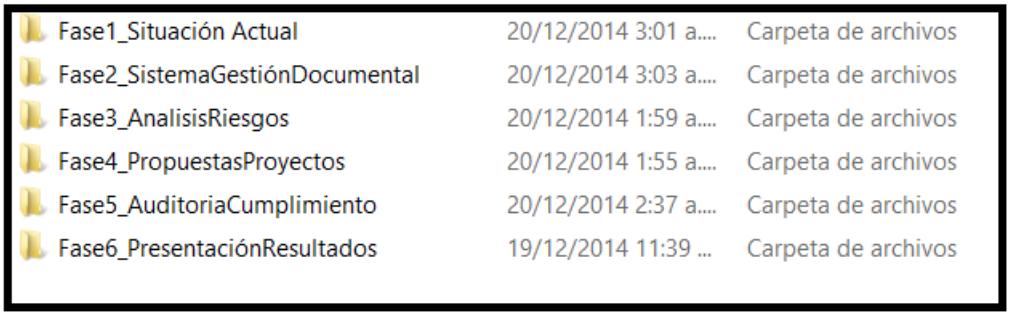
- Es necesario dimensionar un presupuesto más amplio para las estrategias de seguridad de la información en la organización ISAGXXX.

- Se deben incrementar las pruebas de seguridad de forma periódica en ISAGXXXX.

- Es necesario fortalecer el comité de seguridad de la información, para optimizar el gobierno del SGSI.

9 ANEXOS

Carpeta del Proyecto: Salcedo_rsalcedob_Fase_6_20-12-2014_12_15_57



- Manual del SGSI **ISAGXXX** v1.0
- SGSI-POL-1_1 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas
- SGSI-POL-1_1 Política de Control de Acceso
- SGSI-POL-1_1 Política de Cumplimiento
- SGSI-POL-1_1 Política de Gestión de Activos
- SGSI-POL-1_1 Política de Gestión de Continuidad
- SGSI-POL-1_1 Política de Gestión de Incidentes
- SGSI-POL-1_1 Política de Gestión de Operaciones y Comunicaciones
- SGSI-POL-1_1 Política de Organización de la Seguridad de la Información
- SGSI-POL-1_1 Política de Seguridad Física
- SGSI-POL-1_1 Política de Seguridad Recursos Humanos
- SGSI-POL-1_1 Políticas Generales de Seguridad de la Información
- Informe de auditoría Interna SGSI **ISAGXXX** v1.0
- Auditoria de Cumplimiento ISO 27002 v1.0
- Auditoria de Cumplimiento ISO 27001 v1.0
- Matriz Gestión de Activos
- Matriz Gestión de Riesgos
- Declaración de Aplicabilidad
- Descripción de la metodología ISO 27005.
- Procedimiento Gestión de Riesgos.
- Proc_Procedimiento Auditoria_interna v1.0
- Presentación Ejecutiva TFM SGSI v1.1
- Link de la Presentación TFM Master 2014 (Plataforma KNOVO).

10 REFERENCIAS

- International Standards Organization, ISO/IEC 27001: Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de la seguridad de la Información (SGSI) – Requisitos.
- International Standards Organization, ISO/IEC 27002: Tecnología de la Información – Técnicas de Seguridad – Código de práctica para la gestión de la seguridad de la información.
- International Standards Organization, ISO/IEC 27005: Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo en la seguridad de la información.
- ISACA: Gobierno de seguridad de la Información. CISM.
- ISC2: Information Security Governance. CISSP
- IT Governance Institute, COBIT 4.1: Control Objectives For Information And Related Technology
- International Organization for Standardisation, ISO/IEC GUIDE 73:2002: Information Technology – Risk Management Vocabulary – Guidelines for use in standards
- Computer Security Division of the National Institute of Standards and Technology, NIST 800-30: Risk Management Guide for Information Technology Systems
- Computer Security Division of the National Institute of Standards and Technology, NIST 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- Computer Security Division of the National Institute of Standards and Technology, NIST 800-34: Contingency Planning Guide For Information Technology Systems
- E-Commerce Security, Securing de Network Perimeter, Deloitte & Touche, Information Systems Audit and Control Foundation, ISACF

Referencias WEB

- Introducción al Sistema de Gestión de Seguridad de la Información - SGSI
- http://www.iso27000.es/sgsi.html
- Historia de la ISO 27000
- http://www.iso27000.es/iso27000.html
- Presentación de documentos y elaboración de presentaciones
- http://materials.cv.uoc.edu/cdocent/NR64BN4TZTOGMDE0V2D7.pdf?ajax=true
- Redacción de textos científicos
- http://materials.cv.uoc.edu/cdocent/_D_CBBU62JZTHQ9CQQGJ.pdf?ajax=true
- Sistema de Gestión de Seguridad de la Información
- http://www.iso27000.es/download/doc_sgsi_all.pdf
- ISO 27001 Normas y estándares
- http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Normas-y-estandares/ISO-27001/
- Guía de implementación del SGSI
- http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/61_leccin_26_auditoras_internas_del_sgsi.htmlg
- Organización interna del SGSI
- https://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html

- Implementación de un SGSI organizacional
- http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf