ESTABLECIMIENTO DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN EN SFG BAJO LOS ESTÁNDARES DE LA NORMA ISO 27001: 2005

CAMILO AUGUSTO GARCIA GUEVARA

UNIVERSIDAD EAN
FACULTAD DE POSTGRADOS
ESPECIALIZACION EN GERENCIA DE TECNOLOGIA
BOGOTA
2012

ESTABLECIMIENTO DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN EN SFG BAJO LOS ESTÁNDARES DE LA NORMA ISO 27001: 2005

CAMILO AUGUSTO GARCIA GUEVARA

Informe final de investigación presentado como requisito parcial para optar por el Título de Especialista en Gerencia de Tecnología

Tutor: Carlos Humberto Olivella Zuleta
Ingeniero Industrial y Magíster en Administración

UNIVERSIDAD EAN
FACULTAD DE POSTGRADOS
ESPECIALIZACION EN GERENCIA DE TECNOLOGIA
BOGOTA
2012

PAGINA DE ACEPTACION

_____

Firma Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

_____

Ciudad y Fecha

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Se presentan en este trabajo el desarrollo de un marco conceptual y metodológico para la etapa de establecimiento de un sistema de gestión de seguridad de información bajo la perspectiva de las prácticas sugeridas por el estándar ISO 27001:2005 en una empresa de base tecnológica emergente. Se presenta a continuación el desarrollo de la metodología sugerida por la literatura y fuentes consultadas en cuanto a la determinación del alcance, identificación de activos, análisis y evaluación del riesgo y selección de controles y objetivos de control. Se resume este desarrollo con una declaración de aplicabilidad que muestra, en detalle, los objetivos y controles seleccionados.

Palabras clave: Información, Seguridad, Control, Organización, Riesgo, Activos, ISO 27001:2005

INTRODUCCIÓN

Solution Finders Group (en adelante SFG) es una empresa que apoya la toma de decisiones de fertilización en palma de aceite y suministra al palmicultor un conjunto de escenarios y alternativas de decisión para la compra de fertilizantes, que cumpla con todos los requerimientos nutricionales del cultivo y que de manera conjunta con los costos de aplicación represente la opción más económica, viable y efectiva para su plan de manejo de nutricional. El suministro de estas alternativas de decisión se logra a través de la aplicación de conocimientos técnicos, con bases científicas en materia de nutrición en palma de aceite y el uso de herramientas tecnológicas basadas en optimización matemática y sistemas de información que garantizan la viabilidad de las soluciones lar las cantidades óptimas de fertilizantes.

Para ejercer esta labor de manera segura, SFG debe preservar dos activos de información importantes: la información de sus clientes, sujeto de confidencialidad y también al soporte lógico y de gestión necesario como habilitador de las labores operativas, de tal modo que de la adecuada gestión de una y otra se garantice la prestación del servicio y directamente la continuidad del negocio. Ello sugiere entonces *la necesidad de establecer un sistema de seguridad de información que ponga de manifiesto un conjunto de políticas a ser ejecutadas al interior de SFG y que ofrezca las garantías necesarias para dicha preservación de información*.

El estándar ISO 27001:2005 propone un marco metodológico sólido para llevar a cabo la implementación de este tipo de sistemas de seguridad para cualquier organización, lo que sugiere un trabajo previo de identificación catalogación y aplicabilidad de los diferentes controles. Así mismo está estrechamente relacionado con otros marcos normativos, que propician el desarrollo de sistemas integrados de gestión.

JUSTIFICACIÓN

En general, como lo menciona la literatura [1] las empresas suelen comportarse de manera reactiva ante los aspectos de seguridad de información. Cada vez que se presenta un incidente, se establece un nuevo control. Sin embargo es raro encontrar un enfoque de planeación proactivo, que comience por el establecimiento y valoración de los activos de información y una tasación de su impacto en la empresa, para poder administrar los riesgos y su tratamiento.

De esta manera, con unas métricas orientadas a la permanente revisión y control de la seguridad de información, se facilita la labor de la gerencia tecnológica y se optimiza la implantación de las acciones correctivas y preventivas necesarias.

SFG, es una empresa de base tecnológica, expuesta a una gran cantidad de riesgos de información por su mismo quehacer misional. Es por ello que se plantea esta primera etapa de establecimiento del sistema de seguridad de información, bajo los estándares normativos de ISO 27001:2005, como un comienzo a los futuros procesos de implementación de un sistema integrado que soporte la preservación de los activos de información presentes en la organización.

OBJETIVOS

General

Implementar la fase de Establecimiento del sistema de seguridad de información en SFG bajo los estándares de la norma ISO 27001: 2005.

Específicos

- Enunciar el alcance del sistema de seguridad de información en SFG.
- Enunciar la Política de Seguridad de Información.
- Evaluar el riesgo mediante la metodología de seis pasos propuesta por la cláusula 4.2.1 del estándar.

CAPÍTULO 1. MARCO CONCEPTUAL Y METODOLÓGICO

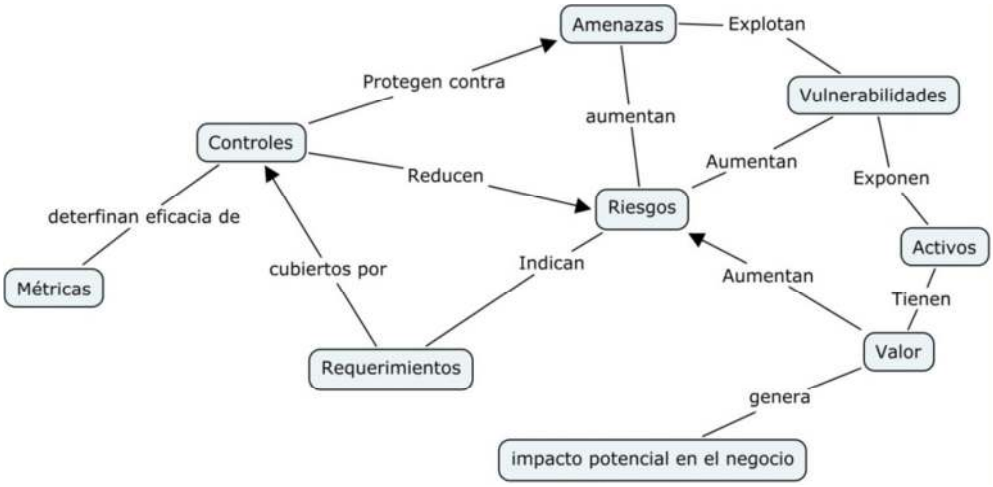

Figura 1: Mapa conceptual básico

1.1 Conceptos de Sistemas de Gestión de seguridad de Información

Los retos en la gestión de la información (que son enfrentados por toda organización con mayor o menor intensidad) pueden resumirse en tres conceptos clave que diferentes autores y el estándar (ISO, 2005) mismo proponen en sus definiciones:

- Disponibilidad: la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- Confidencialidad: la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.
- Integridad la propiedad de salvaguardar la exactitud e integridad de los activos.

La confidencialidad, integridad y disponibilidad de la información en la empresa son fundamentales para la competitividad de las organizaciones, que están entonces obligadas a implementar Sistemas de Gestión de Seguridad de Información que permitan asegurar que tienen identificados sus activos vitales de información, que han determinado de manera sistemática cuáles activos son los de riesgo y pueden con precisión instituir los controles pertinentes (Alexander, 2005a) para garantizar su continuidad y crecimiento.

Una reunión formal de las prácticas para la instauración de estos sistemas ha sido resultado del esfuerzo conjunto de diferentes entidades alrededor del mundo y algunas de ellas han encontrado inspiración y sustento en acuerdos multilaterales entre diferentes países, como por ejemplo las recomendaciones dadas por la OCDE, Organización para la Cooperación y el Desarrollo Económico, instituida en 1960 y con la participación actual de 30 países (estando Colombia en proceso de postulación reciente según Sergio Díaz-Granados ministro de Comercio, Industria y Turismo). Estas recomendaciones hacen énfasis en la

promoción de "*una cultura de seguridad entre todos los participantes como medio de proteger los sistemas y redes de información"*.(OCDE, 2002)

Resultado de este tipo de acuerdos, la problemática de la seguridad ha sido examinada a profundidad por entidades internacionales desde principios de 1990, con el ánimo de reunir una serie de métodos y buenas prácticas que permitan mitigar en parte los riesgos de ocurrencia de los incidentes que comprometen la seguridad de la información. Un breve resumen de estas iniciativas se muestra a continuación:

- A principios de 1990 – Departamento de comercio e industria del Reino Unido apoyó su desarrollo.
- 1995 – Por primera vez se adopta como norma inglesa (BSI).
- 1998 – Se lanzan los requisitos para su certificación.
- 1999 – Se emite una segunda edición de la norma.
- 2000 – Fue aprobada como la parte 1 de ISO 17799.
- 2002 – BS 7799-2 se publicó el 5 de septiembre: en esta revisión se adoptó el "modelo de proceso" con el fin de alinearla con ISO 9001 e ISO 14001.
- Hasta 2003, habían sido emitidos cerca de 500 certificados.
- A finales del 2004, cerca de 950 compañías se habían certificado en BS 7799-2.
- 15 de Octubre de 2005 – Se aprueba la Norma ISO 27001:2005 y en 2006 existen ya más de 2030 compañías certificadas a nivel mundial.
- AÑO 2007 - Se aprueba la ISO 27002 + la ISO 27004 (Indicadores y Cuadros de Mando).

1.2 Naturaleza Del SGSI ISO 27001:2005

El estándar ISO 27001:2005, es parte del sistema de gestión de la organización. Está basado en un enfoque de riesgos del negocio, para establecer, implantar, operar, monitorear, mantener y mejorar la seguridad de información. El sistema de gestión incluye, estructura organizacional, políticas, planeación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

Para implantar el modelo, la empresa debe determinar su alcance por lo que entonces la amplitud del modelo puede variar según la conveniencia de la empresa. Se puede aplicar a toda la firma o a algún proceso en particular, cubriendo los activos relevantes de información, sistemas, aplicaciones, servicios, redes y tecnologías usadas para procesar, almacenar y comunicar información.

El modelo propuesto por el estándar consiste de 134 mejores prácticas de seguridad (cubriendo 11 dominios o procesos) los cuales pueden ser adoptados por las organizaciones para construir su propia infraestructura de seguridad (ISO, 2005). Aun cuando una organización decida no buscar la certificación, el modelo propuesto por el estándar ayuda a las organizaciones a mantener la seguridad de la organización a través de la gestión continua e integrada de las políticas y procedimientos, capacitación de personal, selección e implementación de controles efectivos, la revisión de su eficacia y su mejora.

La fórmula que define la naturaleza de la norma, está fundamentada en el ciclo de Deming y además está alineada con las guías y principios de la OCDE ya mencionados. El ciclo Deming o PHVA por Planear,

Hacer, Verificar, Actuar, se refleja funcionalmente en la naturaleza de la norma, de acuerdo al proceso en la Figura 2: Ciclo de Deming.

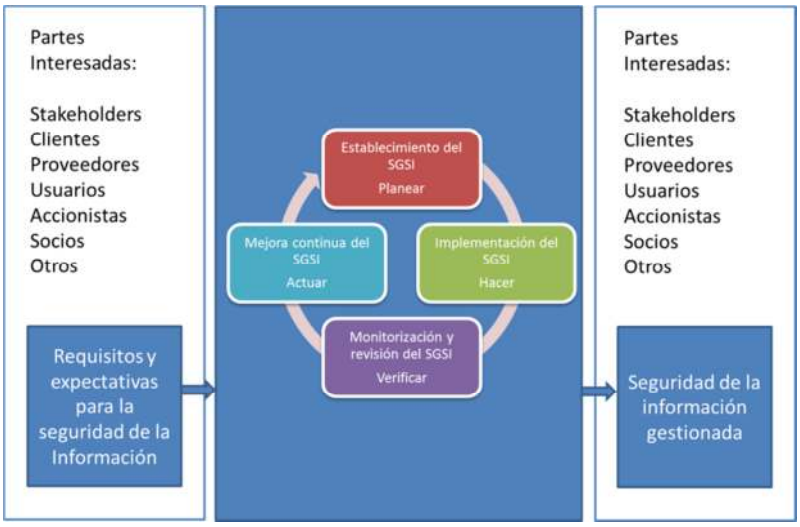

Figura 2: Ciclo de Deming

1.3 Enunciado de alcance

En la sección 4.2 (a) del estándar, se exige como punto de partida para establecer el SGSI que la empresa: "defina el alcance del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología" (ISO, 2005). Una vez determinado el alcance del modelo en la empresa, se debe proceder a identificar los distintos activos de información, los cuales se convierten en el eje principal del modelo.

En cualquiera de los casos, la determinación del alcance obedece a decisiones gerenciales de múltiples contextos, por lo cual en general se integran equipos multidisciplinarios para su elaboración (Kumar, 2012), (Alexander, 2005b)

1.3.1 Etapa Estratégica: Matriz para el despliegue de un SGSI

Como paso inicial a esta delimitación, se sugiere separar la elaboración del enunciado del alcance en dos etapas, una Estratégica y una Táctica. La etapa estratégica tiene como objetivo básico resolver la pregunta ¿cuál o cuáles procesos son los candidatos para implantar el modelo? Alexander (Alexander, 2007) propone una metodología de Matriz para el despliegue de un SGSI, en la cual se contrastan los procesos de negocio contra los factores críticos de éxito, como ayuda que permite focalizar a la organización en sus procesos vitales.

1.3.2 Etapa táctica: Metodología de las Elipses

La cláusula 4.2.1 del estándar, en relación con el alcance del modelo, refiere la siguiente obligación:

> "*Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance*". (ISO, 2005)

Alexander (Alexander, 2005b) propone la *Metodología de las Elipses* como herramienta de identificación de los componentes de cada proceso y las interfaces con otros procesos en la organización y con entidades externas a la empresa. Al finalizar con la aplicación del método de las elipses, la empresa estará lista para iniciar las tareas de análisis y evaluación del riesgo.

El método intenta visualizar con precisión inicialmente los distintos subprocesos que componen el alcance. Este listado de subprocesos se determina en una elipse central principal. El paso a seguir sugerido por el método es determinar con los usuarios y dueños de esos procesos, cuáles son los activos de información vitales en cada caso.

Después deben identificarse en una elipse intermedia las distintas interacciones que los subprocesos de la elipse central, tienen con otros procesos de la organización. Seguidamente, también se deben identificar con los dueños de esos procesos, los activos de información involucrados en las interacciones con la elipse central. Conviene adicionalmente dar una dirección de las interacciones, indicadas por fechas en este diagrama.

Finalmente, mediante el uso de una elipse externa, se identifican aquellas organizaciones exteriores a la empresa que tienen cierto tipo de interacción con los subprocesos identificados en la elipse central. Nuevamente debe darse sobre estas interacciones un sentido y dirección. En este punto también se deben identificar los distintos tipos de activos de información, con miras a averiguar el tipo de relación que existe o debiera implementarse así como los contratos existentes y los grados de acuerdo necesarios.

Un ejemplo de la metodología desarrollada se muestra en la Figura 3: Desarrollo de la Metodología de las elipses **(Alexander, 2005b)**

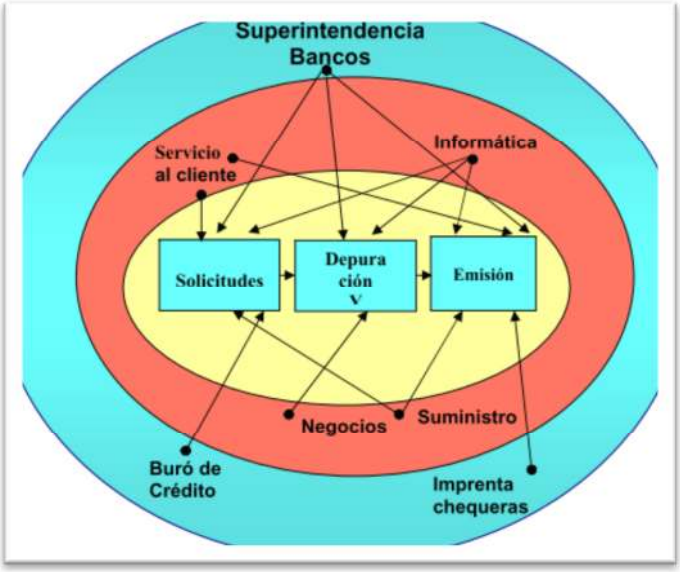

Figura 3: Desarrollo de la Metodología de las elipses (Alexander, 2005b)

1.4 La política de seguridad de información

Una política es una regla general que se ha establecido en una organización para limitar la discrecionalidad de los subordinados (Simon, 1957). En el ámbito de los sistemas de información, la política se ha definido en un contexto de planificación y control para establecer límites de conducta aceptable, limitar las decisiones, y estándares(Davis & Olson, 1985). Las políticas son especialmente importantes para los sistemas de seguridad de la información, ya que proporcionan los fundamentos para un programa de seguridad global y crear una plataforma para implementar prácticas seguras en una organización (von Solms & von Solms, 2004). El objetivo de la política es proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requerimientos del negocio y de las leyes y reglamentos pertinentes (ISO, 2005). Dentro del ámbito de la formulación de la política de seguridad de la información deben referirse los aspectos relevantes de integridad, disponibilidad y confidencialidad de los datos electrónicos generados y transmitidos entre sistemas de información y es la condición previa para la aplicación de medidas de mitigación de riesgo.

De acuerdo con Hone y Eloff (Höne & Eloff, 2002),'' Sin duda, la singular más importante de los controles es la política de seguridad de la información''. Otros investigadores afirman que el desarrollo de una política de seguridad de la información es el primer paso hacia la preparación de una organización contra los ataques procedentes de fuentes internas y externas (Whitman, Townsend, & Aalberts, 2000).

En general, existe un consenso sobre los elementos que deben incorporarse al enunciado de la Política de Seguridad Información. Recopilado de varias fuentes estos elementos se enumeran a continuación:

1.4.1 Necesidad y el alcance de la Seguridad de la Información

Esta es una breve declaración introductoria haciendo hincapié en la dependencia de la organización en la información y por lo tanto, la seguridad de la información (Office of Information Technology, 2003). Esta afirmación introductoria también proporciona el fondo de por qué la política es necesaria en la organización, teniendo en cuenta el entorno específico de la organización particular.

1.4.2 Objetivos de Seguridad de la Información

Los objetivos de seguridad de la información en una organización deben ser descritos brevemente para informar al lector sobre el objetivo específico de gestión de seguridad de la información en la organización. Estos objetivos deben estar claramente vinculados a la estrategia de la organización general de la empresa, las metas y los objetivos y la naturaleza del negocio (Office of Information Technology, 2003).

1.4.3 Definición de Seguridad de la Información

Una política de seguridad de la información generalmente está dirigida a un público diverso para el que la seguridad de la información puede ser un concepto extraño y nuevo. Por tanto, es crucial que la política contenga una definición breve y comprensible de seguridad de la información para asegurar una comprensión uniforme del concepto en toda la organización (Knapp, Franklin Morris, Marshall, & Byrd, 2009).

1.4.4 Compromiso de la Dirección de Seguridad de la Información

La declaración de compromiso es la declaración de singular más importante en una política de seguridad de la información. Sin esta declaración, los intentos de actividades por el personal de seguridad de la información no serán efectivos y la iniciativa no será tomada en serio en toda la organización (Höne & Eloff, 2002). La declaración de compromiso de la dirección puede forzar a los empleados a prestar atención a la seguridad de la información y demuestra la intención de la administración de hacer un éxito de la misma en la organización (Jarmon, 2002).

1.4.5 Aprobación de la Política de Seguridad de la Información (Firma)

La firma de aprobación también puede ser vista como la firma que avala la iniciativa y típicamente debe ser la de más alto rango directivo posible en la organización. Esta firma debe mostrarse en un lugar destacado como una señal más del compromiso de la alta gerencia de seguridad de la información.

1.4.6 Propósito u objetivo de la Política de Seguridad de la Información

El propósito u objetivo de la política de seguridad de la información no se debe confundir con las declaraciones introductorias sobre la necesidad de seguridad de la información en una organización. Estas declaraciones describirán las razones para el desarrollo de una política de seguridad de la información y, posiblemente, estarán vinculadas a las cuestiones de cumplimiento legal. Los principales objetivos de la política en sí es lo que se describe en esta sección.

1.4.7 Principios de Seguridad de la Información

Los principios de seguridad de la información describen las normas generales relacionadas con la seguridad de la información dentro de una organización. Estos principios tratan de explicar a los usuarios cuáles son los comportamientos correctos e incorrectos en la organización con respecto a diversos temas y conceptos. Algunos de estos principios estarán estrechamente vinculados a la cultura de una organización o con los requisitos reglamentarios que rigen la industria en la que la organización está funcionando. Otros, sin embargo, son aplicables a todas las organizaciones y se pueden encontrar en cualquier política de seguridad de la información, tales como la protección contra virus y la sensibilización de los usuarios y la educación.

Los principios, sin embargo, también cambian con el tiempo en función de los avances tecnológicos y los cambios. Una política de seguridad de la información escrita hace 20 años por lo general no hace referencia a cualquier forma de seguridad de la información electrónica, pero probablemente hará referencia detallada a la seguridad de la información física. Por tanto, es crucial que todo esta parte de la política se revisará periódicamente para su aplicabilidad.

1.4.8 Funciones y responsabilidades

Este es uno de los componentes más importantes de la política de seguridad de la información, ya que esta parte le dice al lector exactamente lo que se espera de él en términos de seguridad de la información en la organización.

Las funciones y responsabilidades deben cubrir todos los aspectos de seguridad de la información, así como las responsabilidades individuales de todos los partidos que utilizan recursos de la organización de la información (Office of Information Technology, 2003).

1.4.9 Violaciones a la Política de seguridad de información y medidas disciplinarias

La declaración sobre violaciones a la política de seguridad de información es una declaración muy poderosa, ya que asegura que las medidas disciplinarias se pueden tomar en contra de un usuario si la se adhiere a la política. Es muy importante que ésta declaración esté directamente relacionada con la política general de disciplina y comportamiento de la organización.

1.4.10 Seguimiento y revisión

Esta declaración se refiere a la necesidad de vigilar con frecuencia y revisar la vigencia y eficacia de la seguridad de la información con los controles implementados dentro de la organización. Sin esta declaración no hay una continuidad obligada para la mejora de la seguridad de la información puesta en práctica en la organización.

1.4.11 Declaración del Usuario y Reconocimiento

Esto no es un elemento común que se encuentre en una política de seguridad de la información, y suele presentarse como un apéndice o un documento separado. Es, sin embargo, un elemento muy útil, ya que normalmente se redacta como una versión abreviada de la política de seguridad de la información y está dirigida por completo a los usuarios de la organización. Los usuarios son entonces más propensos a leer toda la sección y tener una mejor comprensión de lo que se espera de ellos.

Con la firma de una declaración de usuario antes de poder acceder a la información electrónica, el usuario reconoce su responsabilidad con respecto a la seguridad de la información. La declaración de usuario y el reconocimiento también debe ser leído y firmado de nuevo sobre una base anual por todos los usuarios a fin de recordarles sus responsabilidades individuales en la protección de los activos de información dentro de la organización (Höne & Eloff, 2002).

1.4.12 Referencias cruzadas

La política de seguridad de la información nunca debe ser escrita en forma aislada y tendrá que ser apoyada por otras políticas, normas, procedimientos y procesos. A estos documentos aplicables se debe hacer referencia en la política para asegurar que el lector obtenga una imagen completa de todos los controles de seguridad de la información y las medidas utilizadas en la organización. A menudo, las organizaciones también están obligadas a poner en práctica ciertos controles y medidas según lo determinado por la legislación del país y los reglamentos. Entonces también es necesario hacer referencia a ellos en la política.

1.5 Análisis y evaluación del Riesgo

A los activos de información, se les debe efectuar un análisis y evaluación del riesgo e identificar los controles del anexo A del estándar, que tendrán que implementarse para mitigar el riesgo. Es importante en este punto clarificar qué es un activo de información en el contexto del ISO 27001:2005.

Según el ISO 17799:2005, (Código de Práctica para la Gestión de Seguridad de Información) un activo de información es: "*algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger.*" (ISO, 2005)

Los activos de información, son clasificados por el ISO 17799:2005 en las siguientes categorías:

- Activos de información (datos, manuales de usuario, etc.)
- Documentos de papel (contratos)
- Activos de software (aplicación, software de sistemas, etc.)
- Activos físicos (computadoras, medios magnéticos, etc.)
- Personal (clientes, personal)
- Imagen de la compañía y reputación)
- Servicios (comunicaciones, etc.)

Una vez identificados todos los activos de información comprendidos en el alcance, se procede a la fase de Establecimiento el SGSI, siguiendo las pautas del estándar ISO 27001:2005 en su sección 4.2.1 (ISO, 2005). En esencia lo que este exige es efectuar de manera sistemática un análisis y evaluación del riesgo de los activos identificados para determinar cuáles son aquellos que deben ser protegidos para mitigar su riesgo, así como definir también cual es el riesgo residual (el riesgo con el cual la empresa está decidida a convivir).

El método de evaluación de riesgo, acorde con el estándar y las buenas prácticas de negocio, puede resumirse mediante el proceso mostrado en la Figura 4: Metodología para el análisis y Evaluación del Riesgo **(Alexander, 2005a)**

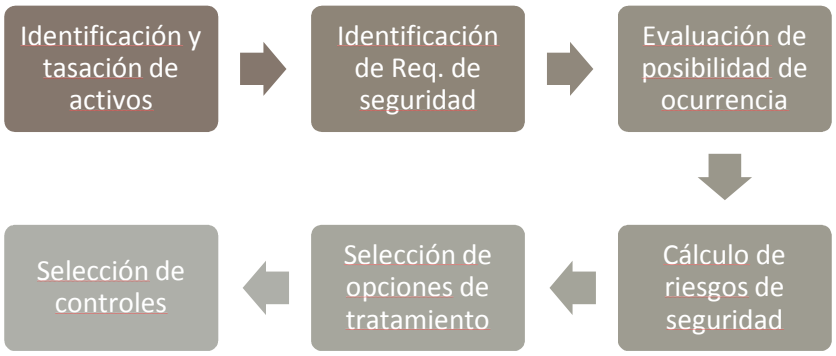

Figura 4: Metodología para el análisis y Evaluación del Riesgo (Alexander, 2005a)

En este punto debe hacerse una juiciosa selección de controles para reducir los riesgos a un nivel aceptable evaluado dentro del alcance del SGSI considerado. El modelo propone que estos controles sean seleccionados a partir del anexo A del ISO 27001:2005(ISO, 2005). El estándar presenta 11 cláusulas, 39 objetivos de control y 133 controles específicos. La selección de los controles debe ser sustentada por los resultados de la evaluación del riesgo y las vulnerabilidades asociadas a amenazas indican donde puede ser requerida una mayor protección y que forma debe tener. Especialmente para propósitos de certificación, las relaciones con la evaluación del riesgo deben ser documentadas para justificar la selección de los controles, incluyendo los procesos que han sido delegados en servicios tercerizados.

1.5.1 Identificación de amenazas y vulnerabilidades

Los activos de información están sujetos a diferentes formas de amenazas, que a su vez pueden causar incidentes que están en posibilidad de generar daño a la organización y a sus activos. Se define

amenaza como “la indicación de un potencial evento no deseado” (Christopher J. Alberts, 2003) y en general la literatura (Alexander, 2007) propone la siguiente clasificación:

- Amenazas naturales
- Amenazas a instalaciones (fuego, explosión, caída de energía, etc.)
- Amenazas humanas
- Amenazas tecnológicas
- Amenazas operacionales (crisis financieras, pérdida de proveedores, etc.)
- Amenazas sociales

Ahora bien, para que una amenaza cause daño a algún activo tendría que explotar una o más *vulnerabilidades* del sistema, aplicaciones o servicios usados por la organización a efectos de poder ser exitosa en su intención de hacer daño.

Por cada amenaza, para medir la posibilidad de su ocurrencia, se recomienda utilizar una escala de Likert (Alexander, 2007), que valore el riesgo de ocurrencia de cada una desde un nivel 1 o “Muy bajo” hasta 5 o “Muy alto”. De tal manera que podrán integrarse no solo datos históricos sino criterios del tomador de decisiones basado en su experiencia o tendencia organizacional.

El término *vulnerabilidad* usado anteriormente, se usa para definir debilidades de seguridad asociadas a los activos de la organización. La literatura, las define como: “debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas” (Christopher J. Alberts, 2003).

De manera similar a las amenazas, las vulnerabilidades también pueden ser clasificadas como:

- Seguridad de los recursos humanos
- Control de acceso
- Seguridad física y ambiental
- Gestión de operaciones y comunicación
- Mantenimiento, desarrollo y adquisición de sistemas de información.

Sugiere la literatura que las amenazas y vulnerabilidades debe presentarse juntas para poder causar incidentes que puedan dañar los activos. Por esta razón es necesario entender la relación entre ámbas, como una relación de causalidad y probabilidad de ocurrencia, como lo sugiere la Figura 5: Relación causa-efecto entre elementos de análisis de riesgo.

Figura 5: Relación causa-efecto entre elementos de análisis de riesgo

Adicionalmente, deberán establecerse como vulnerabilidades aquellos controles ya existentes en el sistema, pero cuya eficacia no puede establecerse o ha demostrado ser de un nivel inferior al esperado, evidenciado en recurrencia de problemas o aparición de nuevos hallazgos relacionados.

1.5.2 Riesgo Residual

Los riesgos no pueden eliminarse por completo pese a las medidas que tomen las organizaciones. Sin embargo, de acuerdo a las estrategias comentadas en la sección anterior pueden disminuir la ocurrencia de aquellos riesgos que pueden ser más críticos a unos niveles *aceptables*. Este riesgo que permanece después de haber implementado las medidas se conoce como residual y la organización tomará la decisión de convivir él.

1.6 Opciones para el tratamiento del riesgo

Cuando los riesgos han sido identificados y evaluados, la próxima tarea para la organización es identificar y evaluar la acción más apropiada de cómo tratar los riesgos. La decisión debe ser tomada basada en los activos involucrados y sus impactos en el negocio. Adicionalmente debe considerarse el nivel de riesgo remanente que ha sido identificado siguiendo la selección de la metodología apropiada de evaluación. El estándar ISO 27001:2005, requiere que la organización en relación al tratamiento del riesgo siga cuatro posibles acciones:

- Aplicación de apropiados controles para reducir los riesgos. Los controles tienen que ser identificados en el anexo A. Si los controles no pueden ser hallados en el anexo A, la firma puede crearlos y documentarlos.
- Aceptar objetivamente los riesgos partiendo del supuesto que satisfacen la política de la organización y su criterio para la aceptación del riesgo.
- Evitar los riesgos.
- Transferir el riesgo asociado a otras partes.

1.6.1 Selección de objetivos de control y controles

Para reducir el riesgo evaluado dentro del alcance del SGSI estudiado, se deben identificar y seleccionar justificadamente los controles de seguridad apropiados. Estos controles deben ser seleccionados del anexo A del ISO 27001:2005 (ISO, 2005). Este estándar presenta 11 cláusulas, 39 objetivos de control y 133 controles específicos.

Es muy importante hacer una mayor claridad y entendimiento sobre el rol del ISO 17799:2005 (Carlson, 2001). La organización puede utilizar el ISO 17799:2005 como guía para la implementación de los controles, pero deben ser escogidos del ISO 27001:2005. La selección de los controles debe ser sustentada por los resultados de la evaluación del riesgo y las vulnerabilidades y sus amenazas asociadas indican donde la protección pudiera ser requerida y que forma debe tener.

Especialmente para propósitos de certificación, las relaciones con la evaluación del riesgo deben ser documentadas para justificar la selección de los controles y cuando se seleccionen controles para la implementación, un número de factores deben ser considerados, incluyendo:

- Uso de controles

- Transparencia del usuario
- Ayuda otorgada a los usuarios para desempeñar su función
- Relativa fuerza de los controles
- Tipos de funciones desempeñadas.

1.7 Declaración de aplicabilidad

La declaración de aplicabilidad es un requisito exigido por la cláusula 4.2.1(j) (ISO, 2005) y que incluye todos los objetivos de control y controles escogidos del Anexo A conjuntamente con una explicación breve de las razones para su selección. Así mismo deben incluirse los controles existentes y por último detallar la exclusión de cualquier objetivo de control con la respectiva explicación.

CAPÍTULO 2. ESTADO DEL ARTE

El Estado del Arte presentado en este trabajo presenta en primera instancia a continuación algunas experiencias documentadas sobre las actividades principales abarcadas en la etapa de establecimiento de un sistema de Gestión de Seguridad de Información. No se presentan por secciones, ya que la mayoría de los trabajos documentados ofrecen un cubrimiento general sobre todos los aspectos de implementación de los Sistemas de Gestión de seguridad de información relacionados. Por otra parte y en segunda instancia se muestra un resumen contextual de la iniciativa empresarial SFG, aspectos relevantes de su planeación y su esquema de actuación por procesos.

2.1 Casos de Estudio

2.1.1 Análisis y Evaluación del Riesgo de Información: Un Caso en la Banca. Aplicación del ISO 27001:2005

En este documento, se presenta un caso exploratorio en la Banca Latinoamericana, en el que se detalla la definición del alcance mediante la metodología de las elipses para un proceso particular de la entidad en cuanto a la gestión de cuentas corrientes. Un aspecto vital a resaltar de este proceso, es que se conformó un grupo multidisciplinario, compuesto por los dueños de los subprocesos que conformaban el proceso escogido en el alcance. También en el grupo se incluyó a los clientes vitales y proveedores internos del proceso y posterior a la identificación de los activos de información, se incluyeron en el grupo a los dueños de los activos de información (Alexander, 2005b).

2.1.2 Implementación del Primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, Certificado bajo la Norma ISO27001:2005

En este artículo se presenta un resumen de la metodología general de implementación del modelo de gestión se seguridad de información y su certificación para un proveedor de servicios de telecomunicaciones. Aunque da un amplio espectro sobre la totalidad de la metodología empleada para alcanzar este logro, se hace un énfasis particular en las tareas llevadas a cabo para el análisis y evaluación del riesgo, siendo este un esfuerzo multidisciplinario y bajo un enfoque cualitativo puesto que se pudo abarcar todos los activos con mayor facilidad. Una de las conclusiones particulares que este trabajo arrojó, se refiere a las personas como el eslabón más débil de la cadena recomendando por tanto dentro del análisis y evaluación del riesgo del SGSI dar el énfasis necesario para considerar este tipo de amenazas (Pincay, 2005).

2.1.3 Implementación de un sistema de gestión de seguridad de la información (SGSI) en la Comunidad Nuestra Señora De Gracia, alineado tecnológicamente con la norma Iso 27001

En este trabajo se hace énfasis en la metodología de análisis de gap, que permite comparar los procesos actuales que tiene una organización con los lineamientos de cumplimiento de la norma ISO/IEC 27001 y establecer en qué áreas o procesos se debe priorizar y enfocar el esfuerzo para permitir incrementar la

seguridad de la información. (Puede encontrarse material adicional en: http://www.gapanalisis.com/) (Díaz, Collazos, & Cortez, n.d.).

2.1.4 Instituciones peruanas deben implementar La Norma ISO 27000

50 organismos del Estado deben prepararse no solo para llegar al cumplimiento de la norma, sino para certificarse, según estipula la resolución ministerial publicada el 14 de julio de 2011. El plazo vence en diciembre del 2012. En la actualidad, solo alrededor de 25% de organizaciones que operan en Perú han implementado la norma, destacando de este grupo que el mayor porcentaje lo comprenden organizaciones que reportan sus estados financieros al extranjero (Presidencia del Consejo de Ministros, 2011).

2.1.5 Implantación del SGSI de Sonda Uruguay

Sonda es la principal empresa latinoamericana de Servicios TI e Integración de sistemas, con unos ingresos reportados a 2008 de U$ 671 millones y una planta de empleados superior a 10000 personas, con presencia en 9 países, con 20 oficinas comerciales y más de 500 centros de servicio. Dentro de las experiencias documentadas con las que se cuenta en este caso, se resalta el hecho de que la oficina de gestión de proyectos corporativa apoyó en todo momento el proceso de certificación, integrando al proceso los mecanismos de control de proyecto dados por las metodologías PMP con las que contaba previamente la organización (Delmonte, 2009).

2.2 Contexto Empresarial de SFG

2.2.1 Historia y desarrollo de Negocio

Solution Finders Group (en adelante SFG) cuyo nombre significa “Buscadores de soluciones” es una empresa de base tecnológica que presta servicios de optimización de fertilizantes en palma de aceite, mediante la aplicación de conocimientos técnicos y el uso de herramientas tecnológicas basadas en modelos matemáticos. Se constituyó en el año 2010 y desde sus inicios ha implementado con éxito programas de optimización de fertilizantes en empresas palmeras de diversas zonas del país. Adicionalmente, cuenta con el apoyo del Gobierno Nacional y la Universidad Externado de Colombia a través del Fondo Emprender, luego de participar y ganar en la Convocatoria Nacional No. 10 en la cual fue seleccionada entre 1.431 proyectos. Adicionalmente, formó parte del grupo de 10 ganadores del Concurso Destapa Futuro patrocinado por la Fundación Bavaria, en el año 2011 en la cual se presentaron 8.400 proyectos a nivel nacional[1].

2.2.2 Organigrama Funcional

[1] El Fondo Emprender y el Programa Destapa Futuro apoyan y financian iniciativas empresariales que contemplan en sus propuestas de negocio un componente de innovación y base tecnológica, generan impacto social y aportan al desarrollo sostenible de Colombia.

Figura 6: Organigrama funcional, elaboración propia a partir del esquema de un organigrama funcional por cargos.

2.2.3 Descripción de cargos

A continuación se describen los roles organizacionales con una definición clara de funciones que permitan alcanzar los resultados esperados y responsabilidades asignadas a cada cargo, referenciar la toma de decisiones y delimitar la responsabilidad de cada integrante de SFG.

2.2.3.1 Gerente general

Es el representante legal de la empresa, encargado principalmente de dirigir y representar a SFG en todos los aspectos legales, jurídicos, comerciales y demás que se requiera para desarrollar su objeto social. Su objetivo principal es el de crear valor en base a los servicios ofrecidos por la organización. Dentro de sus funciones se encuentran principalmente:

- Definir los requerimientos de desarrollo de las herramientas tecnológicas con las cuales la empresa presta sus servicios y llevar a cabo los protocolos de validación de los mismos.
- Revisar y aprobar los contratos por todo concepto y monto, la facturación, los pagos de nómina y a proveedores, el Balance General y los Estados de Resultados.
- Gestionar los recursos financieros de la compañía, los programas de capacitación y demás funciones relacionadas con el personal como nombramientos, asignación de salarios y promociones.
- Coordinar el plan estratégico de mercadeo en las zonas palmicultoras para garantizar la venta de los servicios, así mismo llevar a cabo las actividades de marketing relacional, precio, distribución, comunicación, promoción y servicio.
- Liderar el proceso de planeación estratégica determinando los factores críticos de éxito, establecer los objetivos y metas específicas de la empresa.

Conocimientos requeridos: en fertilización en palma de aceite, aplicación de modelos matemáticos en la toma de decisiones, gestión financiera y contable, obligaciones legales aplicables a la gestión de la empresa.

Habilidades: Liderazgo activo para movilizar la organización hacia los objetivos, organizado, con autodisciplina, altos valores morales y éticos, habilidades administrativas y capacidad de desarrollo.

2.2.3.2 Ingeniero de Desarrollo

Las funciones de este cargo son desarrollar y mantener el sistema de modelos matemáticos e infraestructura lógica del producto, que de manera detallada se describen a continuación:

- Definir, validar, realizar y verificar las entregas de nuevos desarrollos y mantenimiento de los sistemas de información asociados al producto.
- Administrar y custodiar las bases de datos asociadas al producto.
- Realizar sistemas de contingencia para la plataforma tecnológica, así mismo implementar sistemas preventivos y correctivos para la plataforma.
- Mantener en forma operativa la plataforma de servidores.
- Documentar las implementaciones desarrolladas en los sistemas.
- Atender requerimientos de usuarios de soporte.
- Apoyar técnicamente a la gerencia en los temas consultados respecto a su ámbito de competencia.
- Controlar el desempeño efectivo de los proveedores contratados y los productos adquiridos a terceros.
- Participación en los equipos de trabajo designados por la empresa.

Requisitos básicos: Experto en herramientas de formulación y resolución de modelos matemáticos y en el uso del lenguaje GAMS., en desarrollo de software orientado a bases de datos en lenguaje VB.NET. Conocimientos generales en el uso y administración de BD en SQL Server. Con destreza para manejar Sistemas Operativos, Internet, Intranet, y diseñar programas preventivos y correctivos entorno a problemas de los equipos en el desarrollo de sistemas para soporte a la decisión basados en programación matemática.

2.2.3.3 Asesor Contable

Persona encargada de mantener actualizada a la empresa sobre las normas contables y tributarias para darles cabal cumplimiento, revisar los Balances y Estados de Resultados de la compañía junto con la documentación soporte, y elaborar las declaraciones de impuestos a que tenga lugar la empresa.

Requisitos básicos: Contador Público con tarjeta Profesional, Certificado de antecedentes disciplinarios al día y experiencia mínima de 3 años.

2.2.3.4 Asistente administrativo y contable

Es la persona encargada de coordinar y llevar a cabo la gestión administrativa y operativa de la empresa, del manejo de la relación con los diferentes proveedores, gestión de compras, control administrativo y disciplinario del personal. Las funciones detalladas de este cargo son:

Atención de llamadas, solicitudes, quejas, reclamos, coordinación de viajes y reuniones (reserva de tiquetes y hospedaje), elaboración de contratos comerciales con clientes y proveedores y seguimiento posterior; compras de papelería, útiles de oficina, útiles de aseo y cafetería, coordinación de mantenimiento de equipos, archivo y correspondencia. Recepción y registro de cuentas por pagar, elaboración y envío de facturas a clientes, liquidación de nómina y aportes parafiscales, legalización de gastos de viaje, cobro y seguimiento de cartera, pago de servicios públicos, manejo de caja menor. Reclutamiento, filtro de hojas de vida, aplicación de pruebas, psicotécnicas o de conocimiento, verificación de referencias, contratación (elaboración de contrato, apertura de hoja de vida del empleado, inducción general sobre la empresa, afiliaciones a EPS, ARP, cajas de compensación, pensiones y cesantías, apertura de cuentas de nómina).

Requisitos básicos: Conocimiento y destreza para manejar programas del Sistema Office: Word, Excel, PowerPoint; así como para el manejo de Internet - intranet, entre otros, requeridos para la elaboración y presentación de informes y documentos internos y/o externos propios de su gestión; conocimientos legales directamente relacionados con los procesos de contratación, administración y desarrollo de Personal

2.2.3.5 Agrónomo investigador

Es la persona encargada de realizar las visitas de campo para hacer las evaluaciones de los programas de fertilización establecidos por la empresa, mediante verificación visual tipo auditoría, sobre la ejecución de los planes de aplicación de fertilizantes con el propósito de evaluar si se está cumpliendo con lo pactado e identificar desviaciones entre el presupuesto y lo real.

Dentro de sus funciones también está mantener actualizada a la organización sobre mejores prácticas agronómicas aplicadas a la fertilización, información de nuevas actividades que realizan los palmicultores en cuanto a la nutrición vegetal, las posibles competencias, la resistencia al cambio y contribuir en el diseño de nuevas soluciones para los palmeros adecuados a cada zona o palmero. Adicionalmente se encargará de los informes y análisis de *benchmarking* entre palmeros y entre zonas.

Requisitos: ingeniero agrónomo o carreras afines preferiblemente con experiencia en campo y perfil comercial.

2.2.3.6 Analistas / usuarios consultores

Son los encargados de llevar a cabo los procesos del programa de manejo integrado de la fertilización PMIF, realizar los cargues y análisis de datos de los palmeros, generar los escenarios de evaluación y los informes requeridos en cada una de las etapas de prestación de los servicios.

Requisitos: no requiere una profesión o experiencia específicas. Sin embargo, debe ser una persona con conocimiento y habilidad para el manejo de sistemas, especialmente Excel, tener habilidad numérica, creatividad, iniciativa, capacidad de aprendizaje, alto nivel de detalle y aptitud para cumplir normas, procedimientos y políticas de la empresa con precisión y eficacia.

2.2.4 Descripción de Servicios

Los servicios ofrecidos por SFG están dirigidos a soportar las decisiones del cliente relacionadas con la fertilización del cultivo de la palma de aceite, con el propósito de suministrar alternativas para optimizar recursos y buscar oportunidades de mejora en todo el proceso de determinación del programa de fertilización del palmicultor. Se trata de una asesoría integral especializada en fertilización y optimización al servicio del palmicultor.

El servicio principal ofrecido (que se describirá más ampliamente en este mismo apartado) tiene que ver con el soporte a las decisiones para la compra de fertilizantes. Como soporte tecnológico para la prestación de este servicio, se desarrolló el programa de manejo integrado de fertilización – PMIF, haciendo uso intensivo de tecnologías de formulación y resolución de modelos matemáticos de optimización . Entre estas últimas se cuenta la integración del lenguaje de modelación GAMS (General Algebraic Modeling System) con las diferentes tecnologías informáticas de apoyo para asegurar la factibilidad y optimalidad de las soluciones ofrecidas, mostrándose como una herramienta versátil, de fácil uso, óptimo desempeño, multiplataforma y con una gran cantidad de material de entrenamiento y soporte disponible. Para facilitar estas labores, el sistema cuenta con los mecanismos necesarios para el manejo de datos de entrada y salida, mecanismos de validación, cálculo y clasificación de la información.

Adicionalmente, además del programa PMIF que es gestionado, actualizado y mejorado directamente por personal capacitado de SFG, de tal manera que el tiempo y esfuerzo requeridos por parte del palmero sean mínimos, se ha definido un portafolio de servicios que se prestarán según las necesidades de cada cliente, con fin de manejar y negociar con el cliente la prestación de uno o varios servicios de manera agrupada o independiente. La descripción detallada de los servicios se muestra a continuación:

2.2.4.1 Soporte a las decisiones para la compra de fertilizantes

Consiste en suministrar al cliente un conjunto de escenarios y alternativas de decisión, con el fin de garantizar que las decisiones de compra de fertilizantes dentro del conjunto de fuentes comerciales aceptadas y aprobadas por el cliente, cumplan con las necesidades de fertilización de su cultivo de palma de aceite al menor costo posible, de manera conjunta con sus costos y necesidades de aplicación, según las condiciones dadas.

2.2.4.2 Actualización y seguimiento programa de fertilización

Se trata de actualizar los escenarios de evaluación de fuentes fertilizantes, según el cronograma de compras establecido para el año de vigencia del programa de fertilización, con el fin de incorporar los cambios, ajustes o nuevas cotizaciones de fuentes que se presenten para que el cliente pueda disponer de escenarios de decisión actualizados. El número total de actualizaciones al año dependerá del programa de compras de fertilizantes establecido por el cliente.

2.2.4.3 Diseño programa de fertilización

Consiste en diseñar y elaborar el programa de fertilización de la plantación para determinar las cantidades de nutrientes que requiere el cultivo a partir de la información suministrada por la plantación y teniendo en cuenta los siguientes aspectos: edad de la palma, material de siembra, análisis foliar actual, producción esperada de racimos de fruta fresca –RFF, requerimientos de extracción por cosecha,

ajustes por eficiencia agronómica, descuentos y/o aportes por aplicación de tusa, compost u otro producto orgánico, ajustes por siembras de cobertura si se requiere.

Para la elaboración de este programa se toman como referencia las mejores prácticas que se conozcan en fertilización en palma de aceite, se realiza un análisis integral de los 12 elementos esenciales requeridos por la palma y se analizan las relaciones entre nutrientes. Adicionalmente, si la plantación cuenta con análisis de suelos y un programa de nivelación edáfica, los resultados se analizan de manera integral con los resultados de los análisis foliares para buscar el balance adecuado de todos los elementos del sistema.

Este servicio aplica cuando el palmicultor no cuenta con las herramientas adecuadas para definir un programa de fertilización actual.

2.2.4.4 Identificación de oportunidades de mejora

Consiste en evaluar el programa de fertilización que se maneja actualmente en la plantación, con el fin de identificar oportunidades de mejora de acuerdo a la experiencia y conocimiento adquiridos por SFG, así como a la consulta permanente de publicaciones y artículos especializados.

2.2.5 Procesos operativos nucleares

Por su naturaleza de base tecnológica y para poder brindar las mejores prácticas aplicables en los servicios ofrecidos, cualquiera de estos es desplegado haciendo uso de los mismos procesos nucleares ajustados a cada uno de los casos. El resumen y descripción ampliada de estos procesos se muestra en las secciones siguientes.

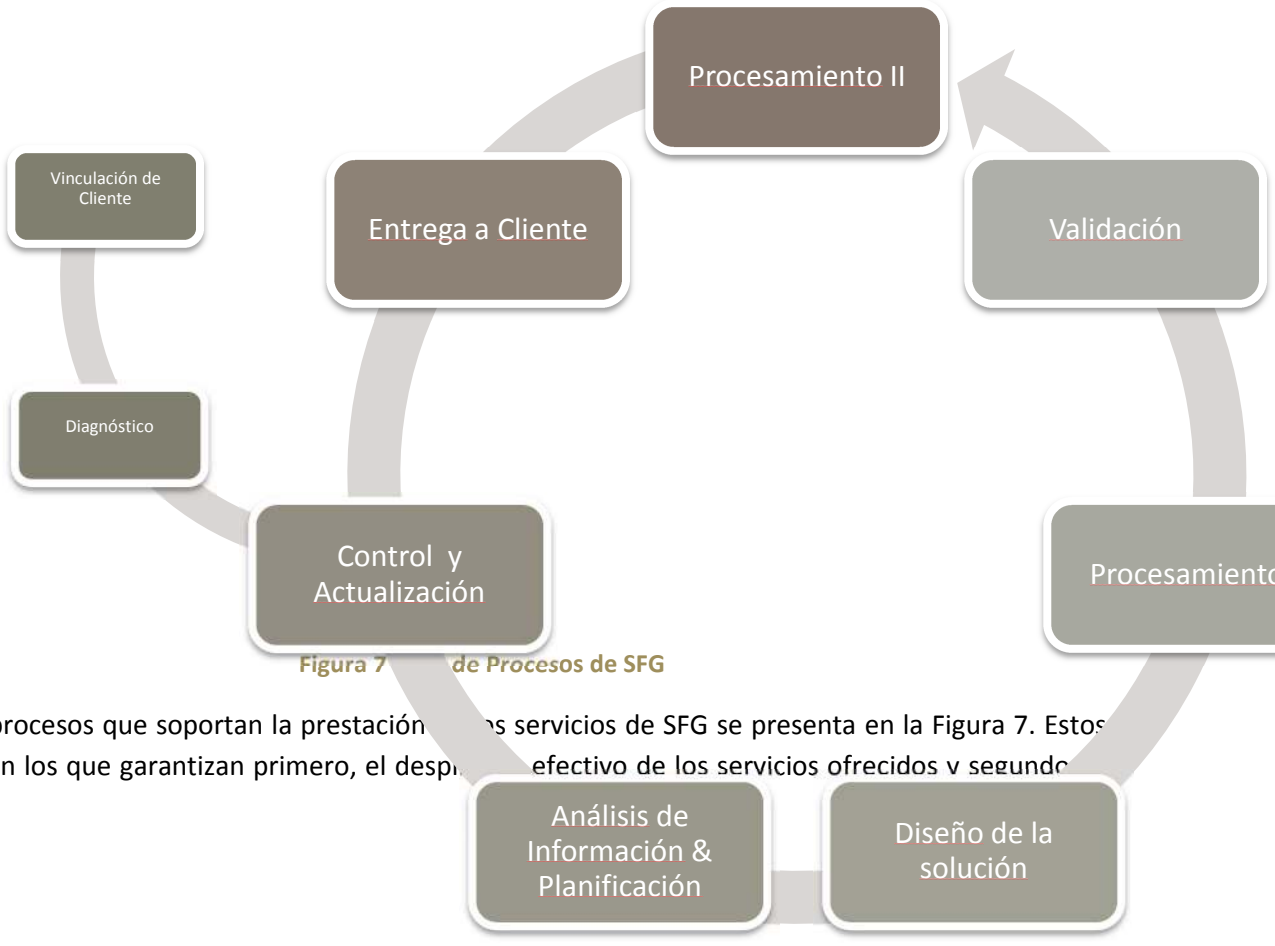

Figura 7 de Procesos de SFG

El ciclo de procesos que soportan la prestación s servicios de SFG se presenta en la Figura 7. Estos procesos son los que garantizan primero, el desp efectivo de los servicios ofrecidos y segundo

posibilidad de generar ingresos operativos. La mayoría de estos procesos tienen que ver con información protegida tanto del cliente como de la organización por lo que, en general, cualquier intervención se sujeta a cláusulas de confidencialidad y respeto de derechos de autor.

A continuación se hace una descripción general de estos procesos.

2.2.5.1 Vinculación del Cliente

La visita al cliente es la herramienta más eficaz y con la que se da inicio al proceso de venta del servicio, se trata de crear preferencia de compra con los palmicultores, de convencerlos y de llevarlos a la utilización del servicio. Para que este inicio sea exitoso se requiere un proceso efectivo que consiste en llevar a cabo los siguientes pasos:

- Realizar la prospección y clasificación de los clientes que se van a visitar para entrar en contacto con ellos mediante correo o vía telefónica, con el fin de evaluar un primer nivel de interés.
- Realizar una aproximación previa con de la empresa para identificar el tamaño de la plantación, a qué grupo pertenecen, quien participa en la decisión de compra. En este momento y con esta información se deben fijar los objetivos previos a la visita.
- Presentación y demostración del servicio ofrecido por SFG que permite describir el servicio, cuáles son sus características, ventajas beneficios y valor agregado que genera para las plantaciones el uso de esta tecnología.
- Recopilar la información que permita hacer una propuesta integral al cliente.

En estos puntos, se debe contar con una gran credibilidad y capacidad para captar el interés de los palmicultores, lograr una interacción que suponga una relación interactiva, generar interés y el sentimiento de necesidad por parte de los clientes.

Realizado el contacto del cliente y una vez aceptada la oferta mercantil enviada por SFG a través de la emisión de una orden de compra y el correspondiente pago de la primera cuota de prestación del servicio, se hace la vinculación del cliente, se definen las personas designadas para gestionar y acordar las actividades correspondientes al servicio y se establecen los canales de comunicación entre la plantación y SFG.

2.2.5.2 Diagnóstico

El objetivo es estudiar extensamente las necesidades del cliente para diseñar una solución que cumpla con sus especificaciones; se trata de conocer detalladamente al cliente, sus necesidades y expectativas, para buscar la solución adecuada a partir de las capacidades de los productos y servicios disponibles.

En esta etapa se visita la plantación, se recopila y analiza toda la información que alimenta el programa de fertilización con el fin de evaluar, entre otros, los siguientes aspectos:

- Cómo se establecen las metas de producción.
- Cómo se determinan las necesidades de nutrición.
- Cómo se seleccionan las fuentes fertilizantes.
- Qué modos de aplicación de fertilizantes se utilizan.

- Cuáles son los costos, recursos y restricciones de cada modo de aplicación.
- Qué criterios se utilizan para definir la época de aplicación de fertilizantes.
- Qué procesos de evaluación y seguimiento se utilizan para controlar el programa de fertilización.

A partir de esta información, se analizan y comparan las prácticas empleadas actualmente por la plantación con las mejores prácticas manejadas por expertos o encontradas en publicaciones especializadas en fertilización y se elabora un informe de oportunidades de mejora.

2.2.5.3 Análisis de Información y Planificación

En este punto, el objetivo es asegurar que la información que alimentará el programa de fertilización PMIF esté bien definida y depurada. Igualmente, se establece un cronograma de trabajo con el cliente, se precisan las restricciones para selección y aplicación de fertilizantes y se definen los informes y escenarios requeridos por la plantación.

2.2.5.4 Diseño de la Solución

El diseño de la solución comprende el establecimiento de las reglas de negocio que el cliente desea incorporar dentro de un conjunto de posibles escenarios delimitados y prediseñados de acuerdo a lo definido en el apartado de Tecnología Utilizada. En concordancia a estos conceptos se generan los requisitos de información necesarios para el procesamiento de la solución óptima.

En este diseño se incluyen además de los escenarios y los mecanismos de levantamiento de información necesaria para el diseño de los informes que el cliente requiere, los entregables a partir de la adaptación de los informes que están en posibilidad de ser generados automáticamente.

2.2.5.5 Procesamiento I

Durante esta etapa se lleva a cabo el montaje inicial de las bases de datos de producción para el cliente y así mismo la adaptación de la plataforma de modelos específica. Dado esto, se hará el proceso de optimización matemática de los escenarios definidos y la generación primaria de informes genéricos.

Los diferentes ajustes que se lleven a cabo sobre los datos en la operación se registran en un documento de memorias de cálculo en donde se muestran los diferentes procedimientos, bien sea de ajuste o de generación de datos. Por otro lado, se hace una calibración de los modelos, donde se comprueba que se estén respetando las restricciones, y que la naturaleza de los resultados está de acuerdo a lo definido de manera genérica en el diseño lógico del servicio.

2.2.5.6 Validación

Con los resultados del proceso anterior y con la participación del cliente se ejecuta un protocolo de validación en el cual se manifiesta la conformidad de la solución y así mismo se llevan a cabo los comentarios y ajustes finales sobre los informes para su entrega definitiva.

Esta etapa se resume en comparar y validar los escenarios propuestos por SFG a través de las herramientas de optimización vs. los resultados del programa de fertilización que maneja actualmente la plantación y se verifican los siguientes elementos:

- Datos de productividad entregados y/o generados.
- Datos de costeo entregados y/o generados
- Costeo paso a paso de los resultados.
- Muestreo de verificación de cumplimiento de restricciones.

2.2.5.7 Procesamiento II

A partir de los procesos de validación descritos, resumidos en el informe de validación, se llevan a cabo los ajustes que sean necesarios según los resultados de comparar y validar los escenarios y se ajustan los informes genéricos a su versión final entregable. El ajuste del modelo, en caso de ser necesario, genera una versión 2 del mismo que se almacena en el servidor de base de datos para su futura referencia.

2.2.5.8 Entrega a Cliente

La etapa de entrega a cliente incluye los detalles finales para completar el ciclo de servicio obteniendo del cliente la aceptación de las entregas finales. Adicionalmente debe llevarse a cabo una sesión de lecciones aprendidas para registrar la información relacionada con las áreas que deben mejorarse y las prácticas recomendadas.

Este proceso incluye finalizar todas las actividades definidas para cerrar formalmente el servicio. Se registra la existencia a conformidad de todos los productos entregables, e investiga y documenta las razones por las cuales se realizaron ciertas acciones si el servicio se da por finalizado antes de completarlo y adicionalmente se contrasta el impacto previsto de la ejecución con el impacto real. Igualmente, se realizan las actualizaciones de los documentos generales y se archiva la totalidad de la documentación de acuerdo con las directrices de documentación.

Finalmente, se lleva a cabo la Encuesta de Cierre, de acuerdo al formato establecido para ello y se dispone y analiza de acuerdo a los mecanismos de servicio al cliente establecidos.

2.2.5.9 Control y Actualización

La etapa de control corresponde a incluir la información de operación real del cliente dentro de los modelos de control disponibles, con una temporalidad acordada con el cliente. Esta información incluye los datos de aplicación de los que se tenga evidencia, así como las inclusiones de elementos diferentes dentro de los planes futuros.

Los modelos de control sugerirán los ajustes necesarios para conservar políticas óptimas, sin embargo, si el costeo de las operaciones llevadas a cabo por el cliente difieren en una cantidad apreciable con respecto al modelo propuesto, deberá llevarse a cabo el procedimiento de servicio completo para la entrega de informes.

CAPÍTULO 3. PROCESO METODOLÓGICO

3.1 Determinación del alcance del modelo

En la sección 4.2(a) del estándar, se exige como punto de partida para establecer el SGSI que la empresa: "defina el alcance del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología." (ISO, 2005)

Una vez determinado el alcance del modelo en la empresa, se debe proceder a identificar los distintos activos de información, los cuales se convierten en el eje principal del modelo.

Se debe recalcar la participación de todos los miembros del equipo de SFG en la conformación de los diversos procesos y la estructuración de la documentación llevada a cabo en esta etapa. Siendo una empresa de base tecnológica, la relación con respecto al manejo y seguridad de la información resultaba un requisito prioritario de servicio y mejora.

Metodológicamente, la definición del alcance obedece a dos etapas: la primera es la estratégica y la otra táctica, que obedece a criterios netamente técnicos.

3.1.1 Etapa estratégica

Estos procesos vienen dados por la interacción entre los procesos nucleares y los diferentes servicios ofrecidos, mencionados en la sección 2.2.5. Dada la orientación de base tecnológica y procesos de SFG se modifica la metodología original propuesta por Alexander (Alexander, 2007) proponiendo un listado alternativo de servicios, más que de procesos de negocio o áreas funcionales.

3.1.1.1 Factores Claves de Éxito

Se entienden los factores clave de éxito como: "aquellas características organizacionales de quien depende el éxito o fracaso de la empresa" (Alexander, 2007). De acuerdo al quehacer de la organización y gracias a que ya se han estudiado desde diferentes ópticas aún desde los procesos de planeación estratégica, los factores claves corresponden a los siguientes:

- Tiempo de Entrega
- Talento Humano competente
- Nuevos servicios
- Satisfacción del cliente
- Reserva sobre la información
- Nivel de Gastos Administrativos
- Generación de nuevo conocimiento
- Estandarización de procedimientos

3.1.1.2 Matriz para el despliegue

El propósito de la matriz es identificar aquellos servicios de la organización que mayor impacto tienen en los factores clave de éxito. Estos servicios de mayor impacto son los candidatos para la implantación del modelo.

Tabla 1: Matriz para el despliegue

	Factores Clave de éxito							
Servicios	Tiempo de Entrega	Talento humano competente	Nuevos servicios	Satisfacción del cliente	Reserva de información	Nivel de Gastos	Nuevo conocimiento	Estandarización
Soporte a las decisiones para compra de fertilizantes	**X**	**X**		**X**	**X**		**X**	**X**
Actualización y seguimiento programa de fertilización		**X**	**X**			**X**		
Diseño programa de fertilización	**X**	**X**			**X**			**X**
Identificación de oportunidades de mejora		**X**	**X**	**X**		**X**	**X**	

Dados estos resultados se delimita el alcance específicamente sobre el servicio 2.2.4.1 *Soporte a las decisiones para la compra de fertilizantes*, dado que dentro de los servicios ofrecidos es el más regular, el que mayor interacción tiene con el cliente y el que tiene una serie de formatos, procedimientos y apoyos estandarizados para su despliegue en diferentes clientes.

3.1.2 Etapa Táctica

La descripción completa de los procesos de ejecución del servicio *Soporte a las decisiones para la compra de fertilizantes* corresponde al siguiente diagrama:

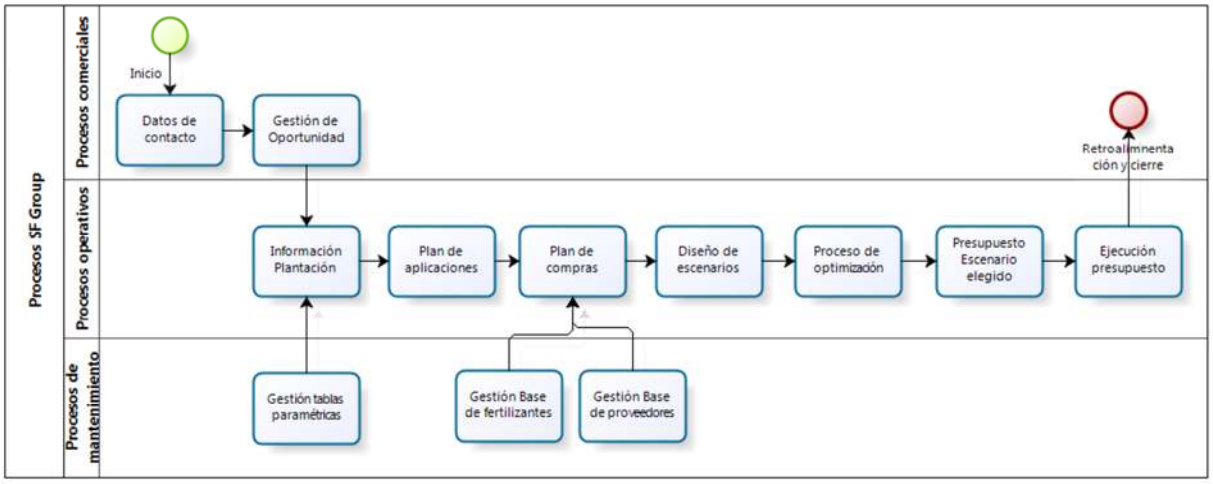

Figura 8: Diagrama de Procesos servicio de Soporte a las decisiones para la compra de fertilizantes

3.1.2.1 Aplicación Metodología de las Elipses

Dado el diagrama detallado de la sección inmediatamente anterior, se reagrupan los procesos operativos y mediante la metodología de las elipses se encuentran en primera instancia sus relaciones con respecto a los procesos de mantenimiento, comerciales y de apoyo dentro de la misma organización. Adicionalmente, se muestran en el diagrama siguiente las interrelaciones con entidades externas a SFG, donde las flechas indican la direccionalidad que tiene el flujo de información.

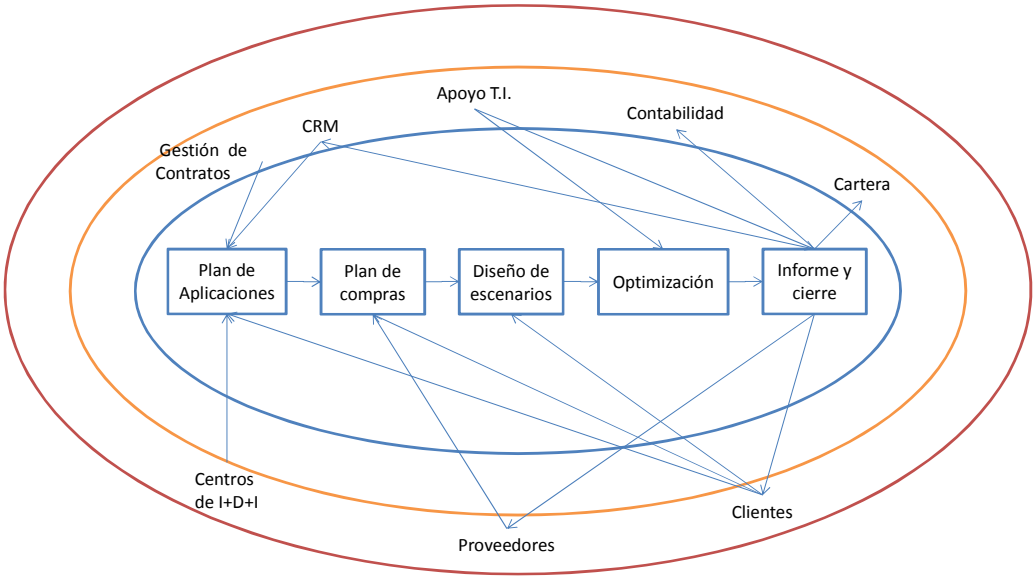

Figura 9: Diagrama de elipses del proceso

En general y como se detallará en secciones posteriores, cada uno de los flujos mostrados está relacionado con una serie de documentos, cuyo uso y características principales se muestran en la sección 3.2.1

3.2 Análisis y evaluación del Riesgo

La metodología a usar en esta etapa y sus actividades, se explicaron en la sección 1.5, comenzando por una descripción de los activos de información identificados de acuerdo a los componentes presentes y sus interacciones mostrados en el diagrama de elipses. Estos activos, de acuerdo a (ISO, 2005), pueden ser de diversa índole y puede ser usado de diferente forma.

3.2.1 Identificación detallada de activos de información

El resumen de los activos, su descripción y características generales se muestran a continuación. Se hacen comentarios y descripciones adicionales de acuerdo a las características de cada uno y las precauciones en su gestión y manejo en el momento presente y se divide la información de acuerdo a si es un activo de registro (información o soporte lógico registrada en cualquier medio) o un elemento físico (como puede ser el hardware y sus tecnologías asociadas de soporte y mantenimiento).

Tabla 2: Inventario de activos de información - Registro

Activo	Descripción	Tipo	Almacenamiento	Identificación	Comentarios
Buenas prácticas de fertilización	Corresponde a una reunión extensa de información de diversa índole que comprende principalmente tablas de estándares, descripciones y exclusiones de manejo de productos de fertilización en diferentes regiones y especies.	Electrónico	Carpeta Compartida	N/A	N/A
Contratos de Servicio	Son la colección de contratos de servicio firmados con los diferentes clientes, en los que se especifican obligaciones de las partes, cantidad y forma de pago y claúsulas generales sobre derechos de autor.	Físico	Archivo	Número	Manejado solo por una persona, se ha establecido un estándar con modificaciones mínimas.
Acuerdos de confidencialidad y niveles de servicio	Son los acuerdos que acompañan al contrato, en los cuales se detalla el grado de servicio, tiempos de respuesta compromisorios y la confidencialidad y uso de la información disponible para las partes.	Físico	Archivo	Número	Manejado solo por una persona, se ha establecido un estándar con modificaciones mínimas.
Información de registro de lotes*	Corresponde a la información mínima de registro de los lotes de producción del cliente, incluyendo algunas características de ubicación, económicas y agronómicas. Se complementa normalmente con la georeferenciación de la plantación para fines complementarios.	Electrónico	Carpeta Compartida	Nombre de archivo	Se hace uso de una serie de archivos estándar, ubicados en carpetas de acuerdo al cliente y temporada.
Resultados de análisis de plantación*	Es la información agronómica y nutricional ligada a los lotes registrados, la envía directamente el cliente, proveniente de sus análisis periódicos en el formato en el cuál su proveedor hace la entrega.	Electrónico	Carpeta Compartida	Nombre de archivo	Se hace uso de una serie de archivos estándar, ubicados en carpetas de acuerdo al cliente y temporada.
Información histórica de fertilización	Corresponde a las políticas, modos y cantidades de productos de fertilización aplicados en períodos anteriores a los lotes registrados. Su uso tiene dos fines: hacer calibración de niveles de eficiencia de los potenciales productos a ser recomendados y por otro lado poder medir previamente ahorros de las propuestas técnicas llevadas a cabo.	Electrónico	Carpeta Compartida	N/A	El formato de los archivos varía, dado que son formatos del cliente con diferente grado de información y estandarización.
Niveles de producción históricos	Corresponde a la medida de la producción en unidades estándar por lote. Su análisis permite comprobar la incidencia de niveles faltantes en las aplicaciones de fertilización o la evaluación de condiciones exógenas no controlables mediante la planificación detallada de la fertilización y el manejo de cultivos.	Electrónico	Carpeta Compartida	N/A	El formato de los archivos varía, dado que son formatos del cliente con diferente grado de información y estandarización.
Niveles de holgura aceptables*	Esta información proviene de una primera interacción con el cliente y detalla cuánto está dispuesto el cliente a ceder en la precisión de los planes presentados con respecto a las buenas prácticas documentadas. Esta holgura normalmente reporta beneficios económicos y logísticos que se contrastan con diversas pérdidas de productividad y calidad del producto. Así mismo pueden reflejar condiciones específicas del terreno que le permiten asimilar con mayor o menor dificultad elementos particulares del plan de fertilización.	Electrónico	Carpeta Compartida	Nombre de archivo	Se hace uso de una serie de archivos estándar, ubicados en carpetas de acuerdo al cliente y temporada.

Niveles periódicos meta de fertilización*	Este elemento, dado por el cliente, permite proponer una serie de requerimientos nutricionales variables adicionales, de acuerdo a los niveles esperados de producción, contrastados con los niveles históricos alcanzados.	Electrónico	Carpeta Compartida	Nombre de archivo	Se hace uso de una serie de archivos estándar, ubicados en carpetas de acuerdo al cliente y temporada.
Base de datos de proveedores*	Esta base, administrada y conocida únicamente por el equipo de trabajo, contiene los datos de los principales proveedores de productos fertilizantes de las zonas de geográficas de trabajo. Contiene adicionalmente los nombres de los contactos comerciales por zona y las condiciones generales mercantiles ofrecidas.	Electrónico	Base de datos	Nombre de archivo	N/A
Base de datos de fuentes fertilizantes*	Esta base, relacionada con la de proveedores, contiene las características técnicas detalladas del producto, evidenciadas en las fichas técnicas y los registros ante las autoridades sanitarias y agrarias de cada país.	Electrónico	Base de datos	Nombre de archivo	N/A
Facturas de servicio	Representan la evidencia de aceptación de la entrega de informes de servicio y se contrastan con los diferentes contratos comerciales.	Físico	Archivo	Número	Manejado solo por una persona, se ha establecido un estándar con modificaciones mínimas.
Modelos matemáticos de optimización*	Corresponden a la principal herramienta desarrollada para la prestación del servicio. Es una serie de expresiones contenidas en software específico de modelación y optimización matemática que obedecen a modelos conceptuales desarrollados específicamente para esta tarea.	Electrónico	Archivo	Versión	Modificado por solo una persona. Adicionalmente está acompañado de un manual técnico y un manual de implementación.
Informes de cierre*	Son los documentos que resumen cada orden de servicio y sus principales incidencias. Entre aspectos destacados contienen la memoria técnica y los informes detallados de planes de fertilización recomendados para cada cliente/temporada,	Físico/ electrónico	Archivo	Número / Fecha	Contiene una serie de formatos estándar e información ajustada para cada cliente.

Tabla 3: Inventario de activos de información – Elementos Físicos

Activo	Descripción	Tipo	Almacenamiento	Identificación	Comentarios
Equipo de Cómputo	El equipo de cómputo que se encuentra a disposición del personal que lleva a cabo todos los procesos	Físico	N/A	Serial	Se mantiene un registro comprobado de las licencias autorizadas de hardware y software disponibles para cada equipo.
Equipo remoto de hosting	Servicio tercerizado en el que se encuentra la información disponible tanto a nivel de web pública como en un futuro la web privada para alojar los servicios de información a clientes registrados.	Virtual	N/A	Contrato	Se mantienen una serie de informes de nivel de servicio para fines de monitoreo.
Servidor de Procesamiento*	Es el servidor principal encargado de las tareas de optimización. Contiene el software de optimización y el software de apoyo y gestión de peticiones de optimización, y la gestión general de las bases de datos para este fin.	Físico	N/A	Serial	Se mantiene un registro comprobado de las licencias autorizadas de hardware y software disponibles para cada equipo.
Copias de respaldo	Copias de los archivos imprescindibles para la restitución del servicio, contiene tanto el software necesario como las capas de datos vigentes.	Físico	Archivo	Número / Fecha	N/A

De estos activos identificados se centrará el análisis en aquellos activos vitales, enmarcados dentro de los procesos nucleares por su escasa posibilidad de recuperación rápida y por la especificidad de su procedimentación y uso. Estos activos han sido marcados con * en la Tabla 2: Inventario de activos de información.

3.2.2 Tasación de activos y clasificación

En esta etapa, se lleva a cabo un análisis de los activos identificados como vitales en el proceso anterior. Para poder identificar la protección apropiada a los activos, es necesario tasar su valor en términos de la importancia a la gestión comercial, o dadas ciertas oportunidades determinar su valor potencial. En este caso, como se mencionó anteriormente, estos activos tienen en común la dificultad de poder ser reemplazados y el hecho de ser imprescindible su uso dentro del proceso nuclear de la organización.

En el caso de los activos de información del servicio de Soporte a las decisiones para la compra de fertilizantes, se tasó su impacto en relación a su confidencialidad, integridad y disponibilidad (ver la sección 1.1 Conceptos de Sistemas de Gestión de seguridad de Información). Se manejó una escala de Likert, en dónde el valor 1 significa "muy poco" y 5 "muy alto" con respecto a la pregunta ¿Cómo una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?

Tabla 4: Tasación de activos de información

Activos	Confidencialidad	Integridad	Disponibilidad	Total
Información de registro de lotes	4	5	5	4.67
Resultados de análisis de plantación	2	5	5	4.00
Niveles de holgura aceptables	1	5	5	3.67
Niveles periódicos meta de fertilización	3	5	5	4.33
Base de datos de proveedores	4	5	5	4.67
Base de datos de fuentes fertilizantes	3	5	5	4.33
Modelos matemáticos de optimización	5	5	5	5.00
Informes de cierre	5	5	3	4.33
Servidor de Procesamiento	1	5	5	3.67

En la cláusula 4.2.1 (d) (ISO, 2005) el ISO 27001:2005 exige que la empresa no solo realice la tasación, sino que también identifique a los propietarios, dado el carácter operativo de la totalidad de activos tasados, el propietario es el área técnica en cabeza del ingeniero de desarrollo.

3.2.3 Identificación de amenazas y vulnerabilidades

De acuerdo a las diferentes definiciones y aproximaciones conceptuales dadas en la sección 1.5.1 Identificación de amenazas y vulnerabilidades, el siguiente paso corresponde a la identificación de las diferentes amenazas y vulnerabilidades para después efectuar el proceso de cálculo de riesgo.

El proceso de cálculo, relaciona la tasación del activo dada por el paso metodológico anterior con la posibilidad de ocurrencia de las amenazas y de explotación de las vulnerabilidades, lo cual brinda una aproximación al criterio de valor en riesgo por uno y otro concepto y cuya suma ofrecerá un criterio para que los activos sean ordenados de acuerdo a su factor de exposición al riesgo.

Tabla 5: Resumen de amenazas y vulnerabilidades

Activos	Tasación	Amenazas	Vulnerabilidades
Información de registro de lotes	4.67	Alteración	Acceso no autorizado
		Pérdida	Deficiencia Respaldo
		Ignorancia de cambios	Deficiencia procedimental
Resultados de análisis de plantación	4.00	Ilegibilidad	Deficiencia formatos
		Codificación errónea	Deficiencia formatos
		Metodología incompleta	Deficiencia procedimental
		Unidades de medida erróneas	Deficiencia formatos
Niveles de holgura aceptables	3.67	Incomprensión del procedimiento	Falta entrenamiento
		Metodología incompleta	Deficiencia procedimental
Niveles periódicos meta de fertilización	4.33	Incomprensión del procedimiento	Falta entrenamiento
		Metodología incompleta	Deficiencia procedimental
Base de datos de proveedores	4.67	Pérdida	Deficiencia Respaldo
		No Integridad relacional	Estructuración deficiente
		Duplicidad	Falta entrenamiento
		Desactualización	Personal Deficiente
Base de datos de fuentes fertilizantes	4.33	Datos incompletos	Falta entrenamiento
		Unidades de medida erróneas	Falta entrenamiento
		Duplicidad	Falta entrenamiento
		No Integridad relacional	Estructuración deficiente
Modelos matemáticos de optimización	5.00	Infactibilidad Matemática	Estructuración deficiente
		Tiempo de solución alto	Codificación ineficiente
		Omisión de reglas	Estructuración deficiente
		Plagio	Acceso no autorizado
Informes de cierre	4.33	Plagio	Política de confidencialidad
		Alteración	Falta de seguridad
		Pérdida	Deficiencia envío
		Retraso en entrega	Deficiencia envío
Servidor de Procesamiento	3.67	Fallos Técnicos	Respaldo y continuidad
		Caída de infraestructura	Respaldo y continuidad
		Agotamiento de recursos	Requerimientos inadecuados
		Virus, Hacking	Seguridad electrónica

3.2.4 Evaluación del riesgo

Dado el listado de amenazas y vulnerabilidades de la sección anterior, es necesario calcular la posibilidad de su ocurrencia conjunta y causar un riesgo. El riesgo, estimado sobre la tasación del activo como base de cálculo permite encontrar unos rangos o niveles de riesgo aceptables, caso en el cuál puede omitirse una acción de mitigación. En el caso contrario, los demás riesgos están estar sujetos a tratamiento y proceso de toma de decisiones posterior. El resumen de Medición de riesgo para las amenazas y vulnerabilidades de los distintos activos seleccionados se muestra en la Tabla 6: Cálculo del riesgo.

Tabla 6: Cálculo del riesgo

Activos	Tasación	Amenazas	Probabilidad	Total	Vulnerabilidades	Probabilidad	Total	Riesgo sobre activo
Información de registro de lotes	4.67	Alteración	4%	0.19	Acceso no autorizado	90%	0.17	3.53
		Pérdida	10%	0.47	Deficiencia Respaldo	90%	0.42	
		Ignorancia de cambios	90%	4.20	Deficiencia procedimental	70%	2.94	

Resultados de análisis de plantación	4	Ilegibilidad	60%	2.80	Deficiencia formatos	40%	1.12	6.30
		Codificación errónea	90%	4.20	Deficiencia formatos	40%	1.68	
		Metodología incompleta	90%	4.20	Deficiencia procedimental	70%	2.94	
		Unidades de medida erróneas	30%	1.40	Deficiencia formatos	40%	0.56	
Niveles de holgura aceptables	3.67	Incomprensión del procedimiento	90%	4.20	Falta entrenamiento	20%	0.84	1.17
		Metodología incompleta	10%	0.47	Deficiencia procedimental	70%	0.33	
Niveles periódicos meta de fertilización	4.33	Incomprensión del procedimiento	90%	4.20	Falta entrenamiento	20%	0.84	1.17
		Metodología incompleta	10%	0.47	Deficiencia procedimental	70%	0.33	
Base de datos de proveedores	4.67	Pérdida	30%	1.40	Deficiencia Respaldo	90%	1.26	4.44
		No Integridad relacional	60%	2.80	Estructuración deficiente	70%	1.96	
		Duplicidad	10%	0.47	Falta entrenamiento	20%	0.09	
		Desactualización	80%	3.74	Personal Deficiente	30%	1.12	
Base de datos de fuentes fertilizantes	4.33	Datos incompletos	70%	3.27	Falta entrenamiento	20%	0.65	3.27
		Unidades de medida erróneas	50%	2.34	Falta entrenamiento	20%	0.47	
		Duplicidad	90%	4.20	Falta entrenamiento	20%	0.84	
		No Integridad relacional	40%	1.87	Estructuración deficiente	70%	1.31	
Modelos matemáticos de optimización	5	Infactibilidad	70%	3.27	Estructuración deficiente	70%	2.29	7.19
		Tiempo de solución alto	80%	3.74	Codificación ineficiente	40%	1.49	
		Omisión de reglas	40%	1.87	Estructuración deficiente	70%	1.31	
		Plagio	50%	2.34	Acceso no autorizado	90%	2.10	
Informes de cierre	4.33	Plagio	30%	1.40	Política de confidencialidad	20%	0.28	2.90
		Alteración	60%	2.80	Falta de seguridad	80%	2.24	
		Pérdida	10%	0.47	Deficiencia envío	20%	0.09	
		Retraso en entrega	30%	1.40	Deficiencia envío	20%	0.28	
Servidor de Procesamiento	3.67	Fallos Técnicos	20%	0.93	Respaldo y continuidad	20%	0.19	2.90
		Caída de infraestructura	30%	1.40	Respaldo y continuidad	20%	0.28	
		Agotamiento de recursos	20%	0.93	Requerimientos inadecuados	50%	0.47	
		Virus, Hacking	60%	2.80	Seguridad electrónica	70%	1.96	

Dada esta información, pueden establecerse dos clasificaciones de priorización, una orientada al tratamiento de amenazas/vulnerabilidades individuales y otra que contemple una clasificación de riesgo por activo. Estos dos resúmenes y priorización se muestran enseguida, en las la Tabla 7: Priorización de Amenazas/Vulnerabilidades y Tabla 8: Priorización de activos.

Tabla 7: Priorización de Amenazas/Vulnerabilidades

Amenazas	Vulnerabilidades	Probabilidad	Total	Prioridad
Ignorancia de cambios	Deficiencia procedimental	0.7	2.9421	1
Metodología incompleta	Deficiencia procedimental	0.7	2.9421	2
Infactibilidad Matemática	Estructuración deficiente	0.7	2.2883	3
Alteración	Falta de seguridad	0.8	2.2416	4
Plagio	Acceso no autorizado	0.9	2.1015	5
No Integridad relacional	Estructuración deficiente	0.7	1.9614	6
Virus, Hacking	Seguridad electrónica	0.7	1.9614	7
Codificación errónea	Deficiencia formatos	0.4	1.6812	8
Tiempo de solución alto	Codificación ineficiente	0.4	1.4944	9
No Integridad relacional	Estructuración deficiente	0.7	1.3076	10
Omisión de reglas	Estructuración deficiente	0.7	1.3076	11
Pérdida	Deficiencia Respaldo	0.9	1.2609	12
Ilegibilidad	Deficiencia formatos	0.4	1.1208	13
Desactualización	Personal Deficiente	0.3	1.1208	14
Incomprensión del procedimiento	Falta entrenamiento	0.2	0.8406	15
Incomprensión del procedimiento	Falta entrenamiento	0.2	0.8406	16
Duplicidad	Falta entrenamiento	0.2	0.8406	17
Datos incompletos	Falta entrenamiento	0.2	0.6538	18
Unidades de medida erróneas	Deficiencia formatos	0.4	0.5604	19
Unidades de medida erróneas	Falta entrenamiento	0.2	0.467	20
Agotamiento de recursos	Requerimientos inadecuados	0.5	0.467	21
Pérdida	Deficiencia Respaldo	0.9	0.4203	22
Metodología incompleta	Deficiencia procedimental	0.7	0.3269	23
Metodología incompleta	Deficiencia procedimental	0.7	0.3269	24
Plagio	Política de confidencialidad	0.2	0.2802	25
Retraso en entrega	Deficiencia envío	0.2	0.2802	26
Caída de infraestructura	Respaldo y continuidad	0.2	0.2802	27
Fallos Técnicos	Respaldo y continuidad	0.2	0.1868	28
Alteración	Acceso no autorizado	0.9	0.16812	29
Duplicidad	Falta entrenamiento	0.2	0.0934	30
Pérdida	Deficiencia envío	0.2	0.0934	31

Tabla 8: Priorización de activos

Activo	Medida de riesgo	Prioridad
Modelos matemáticos de optimización*	7.19	1
Resultados de análisis de plantación*	6.3	2
Base de datos de proveedores*	4.44	3
Información de registro de lotes*	3.53	4
Base de datos de fuentes fertilizantes*	3.27	5
Informes de cierre	2.9	6
Servidor de Procesamiento	2.9	7
Niveles de holgura aceptables	1.17	8
Niveles periódicos meta de fertilización	1.17	9

Una conclusión parcial a este punto es que la metodología sugiere un interesante frente de trabajo en cuanto al manejo de los aspectos procedimentales de la operación y su correcta aplicación a los datos e información. Así mismo y para efectos del alcance de esta primera aproximación se complementará el análisis para los riesgos relacionados con los 5 primeros activos priorizados en la Tabla 8: Priorización de activos dada su naturaleza, como se expondrá en la sección 3.2.6 Opciones de tratamiento de Riesgo.

Así mismo, y dada su estrecha relación se aplican los controles de mitigación a los activos Modelos matemáticos de optimización (en prioridad 1) y Servidor de Procesamiento (prioridad 7), dado que aunque este último *no es imprescindible* para la generación de las soluciones para los clientes, si representan una herramienta de productividad para esta labor.

Aún con estas exclusiones y aceptación de riesgo y dado que existen amenazas y vulnerabilidades comunes a varios activos/servicios, lo natural es que al implementar medidas de mitigación para algunos se puede disminuir la exposición al riesgo de los restantes.

3.2.5 Política y objetivos de seguridad

Los aspectos contemplados en las anteriores secciones, dan los elementos necesarios para hacer una primera redacción de la Política y los objetivos de seguridad, de conformidad con la cláusula 4.2.1 (b) :

> "b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:
>
> > 1) incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información;
> >
> > 2) tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;

3) esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI;

4) establezca el criterio con el que se evaluará el riesgo (ver 4.2.1c);

5) haya sido aprobada por la gerencia." (ISO, 2005)

3.2.5.1 Política de seguridad

Para SFG son de vital importancia los sistemas de información y la tecnología de optimización matemática, permitiendo con estos elementos brindar a sus clientes el más adecuado soporte en sus procesos de decisión en fertilización a un costo mínimo y demás valores agregados.

Asegurar estos resultados requiere esfuerzos importantes en diseño, desarrollo y mantenimiento, procesos que deben llevarse a cabo de manera confiable y segura. La administración del riesgo tecnológico y procedimental ligada a estos procesos se da en niveles proporcionales a la gestión mediante políticas, controles y mecanismos de aseguramiento de calidad de los sistemas de generación de información. Para tal efecto, SFG fundamenta sus esfuerzos en un sistema integrado de gestión orientado a cumplir con los estándares ISO9001:2008 e ISO27001:2005 y con todos los requisitos de información emitidos por las autoridades colombianas y ecuatorianas.

Los colaboradores actúan con sentido de corresponsabilidad y mejora respecto a los criterios de confidencialidad, integridad y disponibilidad de los procesos, tecnologías y datos, así como en el adecuado uso tanto de información protegida del cliente externo, como de los mecanismos dispuestos por SFG para el desempeño de las labores, protegidos por registro de derechos de autor.

3.2.5.2 Objetivos de Seguridad de Información

- Contar con un sistema ágil de gestión de seguridad de información, con la finalidad de mitigar los riesgos tecnológicos y procedimentales.
- Fortalecer una cultura de autocontrol, formación autónoma y corresponsabilidad en el manejo de la seguridad y calidad de la información, desde la perspectiva de la confidencialidad, la integridad y la disponibilidad de la información.
- Llevar a cabo un regular plan de auditorías para garantizar la validez y aplicabilidad de los controles, así como la pertinencia y actualidad de los procedimientos y políticas necesarios para su adecuada implementación.

3.2.6 Opciones de tratamiento de Riesgo

Dada la clasificación de los activos en la Tabla 8: Priorización de activos, se procede a evaluar las posibilidades de tratamiento de riesgo para cada uno, también de acuerdo al tipo de amenazas y vulnerabilidades presentes. Así mismo se muestran aquellos activos excluidos del análisis en esta primera instancia, dada su calificación de riesgo y la naturaleza de su uso y exposición.

Así mismo, pese a ser una práctica aceptable, la *transferencia de riesgo* para los casos catalogados hasta este punto no es posible, debido a dos consideraciones: la primera es que encontrar esquemas de data center con las aplicaciones necesarias para la prestación del servicio supera en mucho el costo del mantenimiento local y el costo de disminución de riesgo y segunda, dada que una de las labores

principales tiene que ver con el desarrollo de nuevas técnicas e investigación de nuevas metodologías, un esquema de data center remoto entorpece este proceso, por lo que se prefiere la creación de pequeños y temporales laboratorios de desarrollo de aplicaciones en un esquema controlado local.

Tabla 9: Estrategias para tratamiento de riesgo

Activos	Amenazas	Vulnerabilidades	Tipo estrategia
Modelos matemáticos de optimización	Infactibilidad	Estructuración deficiente	Reducción
	Tiempo de solución alto	Codificación ineficiente	Reducción
	Omisión de reglas	Estructuración deficiente	Reducción
	Plagio	Acceso no autorizado	Evitar
Servidor de Procesamiento	Fallos Técnicos	Respaldo y continuidad	Transferencia
	Caída de infraestructura	Respaldo y continuidad	Reducción
	Agotamiento de recursos	Requerimientos inadecuados	Aceptación
	Virus, Hacking	Seguridad electrónica	Reducción
Resultados de análisis de plantación	Ilegibilidad	Deficiencia formatos	Reducción
	Codificación errónea	Deficiencia formatos	Reducción
	Metodología incompleta	Deficiencia procedimental	Reducción
	Unidades de medida erróneas	Deficiencia formatos	Reducción
Base de datos de proveedores	Pérdida	Deficiencia Respaldo	Reducción
	No Integridad relacional	Estructuración deficiente	Reducción
	Duplicidad	Falta entrenamiento	Reducción
	Desactualización	Personal Deficiente	Reducción
Información de registro de lotes	Alteración	Acceso no autorizado	Reducción
	Pérdida	Deficiencia Respaldo	Reducción
	Ignorancia de cambios	Deficiencia procedimental	Reducción
Base de datos de fuentes fertilizantes	Datos incompletos	Falta entrenamiento	Reducción
	Unidades de medida erróneas	Falta entrenamiento	Reducción
	Duplicidad	Falta entrenamiento	Reducción
	No Integridad relacional	Estructuración deficiente	Reducción

Tabla 10: Activos excluidos (Aceptación de Riesgo)

Activos	Amenazas	Vulnerabilidades	Tipo estrategia	Justificación
Informes de cierre	Plagio	Política de confidencialidad	Aceptación	Los informes de cierre, pese a que son confidenciales no

	Alteración	Falta de seguridad	Aceptación	contienen directamente la información original protegida. Adicionalmente su backup, recuperación y registro puede darse fácilmente con políticas simples.
	Pérdida	Deficiencia envoi	Aceptación	
	Retraso en entrega	Deficiencia envoi	Aceptación	
Niveles de holgura aceptables	Incomprensión del procedimiento	Falta entrenamiento	Aceptación	Los niveles de holgura pese a que son un insumo que puede generar cambios importantes en la generación del servicio, pueden establecerse fácilmente a partir de buenas prácticas. Adicionalmente la cantidad de información es pequeña y puede dejarse evidencia mediante actas de inicio.
	Metodología incompleta	Deficiencia procedimental	Aceptación	
Niveles periódicos meta de fertilización	Incomprensión del procedimiento	Falta entrenamiento	Aceptación	Estos niveles pueden recuperarse de cualquiera de los informes técnicos, adicionalmente hay evidencia de ellos en las actas de reunión.
	Metodología incomplete	Deficiencia procedimental	Aceptación	

3.2.7 Selección de controles y objetivos de control

De acuerdo a las enumeraciones anteriores, deben decidirse los objetivos de control y los controles para el tratamiento de riesgo. Como ya se mencionó en el apartado 1.6.1 Selección de objetivos de control y controles, la elección de estos elementos debe efectuarse tomando en cuenta el criterio establecido para la aceptación de los riesgos, así como los requerimientos legales, reguladores y contractuales. Estas son exigencias puntuales de la norma en su cláusula 4.2.1 (g):

> "*Seleccionar objetivos de control y controles para el tratamiento de riesgos Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos (ver 4.2.1(c)), así como los requerimientos legales, reguladores y contractuales.*
>
> *Se deben seleccionar los objetivos de control y los controles del Anexo A como parte de este proceso conforme sea apropiado para cubrir estos requerimientos.*
>
> *Los objetivos de control y controles listados en el Anexo A no son exhaustivos y también se pueden seleccionar objetivos de control y controles adicionales.*" (ISO, 2005)

De tal modo, se presentan a continuación los objetivos y controles para el alcance delimitado:

3.2.7.1 Controles Generales para el ámbito del servicio

Estos controles son considerados como de obligatoria instauración de acuerdo a la práctica internacional. Así mismo, la implementación de estos controles, cubrirán los riesgos generales trasversales a todos los servicios y activos catalogados.

- A.5.1.1 Documentar política de seguridad de información
- A.6.1.3 Asignación de responsabilidades de la seguridad de la información
- A.8.2.2 Capacitación y educación en seguridad de la información
- A.12.2 Procesamiento correcto en las aplicaciones.
- A.12.6 Gestión de vulnerabilidad técnica
- A.14 Gestión de la continuidad comercial
- A.13.2 Gestión de incidentes y mejoras en la seguridad de la información

3.2.7.2 Objetivos y controles específicos para el ámbito del servicio

Los objetivos y controles adicionales cuya implementación se encontró apropiada de manera preliminar para las diferentes exposiciones a riesgo se muestran a continuación, pero serán ajustados de acuerdo a controles relacionados, complementarios, o repetidos. La nomenclatura de los controles recomendados y los objetivos pueden encontrarse en el Anexo A de la norma.

Tabla 11: Controles específicos preliminares

Activo	Controles
Modelos matemáticos de optimización*	A.6.1.5, A.9.1.3, A.9.1.5, A.9.2.4, A.10.1.4, A.10.4.1, A.10.5, A.10.6, A.11.7, A.12.2, A.12.4, A.12.5, A.15
Resultados de análisis de plantación*	A.6.2.2, A.6.2.3, A.10.1.1, A.10.5, A.10.6, A.10.8, A.11.2, A.11.3
Base de datos de proveedores*	A.10.1.3, A.10.5, A.10.6, A.11.2, A.11.3
Información de registro de lotes*	A.6.2.2, A.6.2.3, A.10.1.1, A.10.5, A.10.6, A.10.8, A.11.2, A.11.3
Base de datos de fuentes fertilizantes*	A.10.1.3, A.10.5, A.10.6, A.11.2, A.11.3

3.2.8 Declaración de Aplicabilidad

La declaración de aplicabilidad, tal como lo exige el ISO 27001:2005 en la cláusula 4.2.1(4)(j), es un registro resumido y práctico de los últimos controles establecidos (ISO, 2005). Su uso es apropiado para mantener un registro de los últimos controles instaurados en el SGSI. A continuación, en la Tabla 12: Declaración de aplicabilidad se muestra el resumen de los objetivos y controles instaurados en la primera etapa del presente estudio.

Tabla 12: Declaración de aplicabilidad

Objetivos de control	Controles	Aplicabilidad (Si/no)	Control / Justificación
A.5.1 Política de Seguridad de Información. **Objetivo: Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.**	A.5.1.1 Documentar política de seguridad de información	SI	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
	A.5.1.2 Revisión de la política de seguridad de la información	SI	Control La política de seguridad de la información debe ser revisada regularmente a intervalos

			planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A.6.1 Organización interna. **Objetivo: Manejar la seguridad de la información dentro de la organización.**	A.6.1.1 Compromiso de la gerencia con la seguridad de la información	SI	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
	A.6.1.2 Coordinación de la seguridad de información	SI	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
	A.6.1.3 Asignación de responsabilidades de la seguridad de la información	SI	Control Se deben definir claramente las responsabilidades de la seguridad de la información.
	A.6.1.4 Proceso de autorización para los medios de procesamiento de información	NO	El proceso de desarrollo vigente tiene inicio y aprobación de cambios dado por la gerencia en primera instancia.
	A.6.1.5 Acuerdos de confidencialidad	SI	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
	A.6.1.6 Contacto con autoridades	NO	Existen los reportes y procedimientos para los mismos dados por la normativa tributaria vigente.
	A.6.1.7 Contacto con grupos de interés especial	NO	No en primera instancia. Se busca a cambio canalizar estas labores sobre una función centralizada de vigilancia tecnológica
	A.6.1.8 Revisión independiente de la seguridad de la información	NO	No en primera instancia, se debe buscar formalizar el sistema de auditoría interno previo a auditoría de tercera parte. Certificación no es un objetivo de corto/mediano plazo.
A.6.2 Entidades externas **Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.**	A.6.2.1 Identificación de riesgos relacionados con entidades externas	NO	No hay acceso permitido vigente a entidades externas. Existe proyecto web, sin embargo la información consultada en este mecanismo será pre procesada y no on-line.
	A.6.2.2 Tratamiento de la seguridad cuando se trabaja con clientes	SI	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
	A.6.2.3 Tratamiento de la seguridad en contratos con terceras personas	NO	La organización recibe insumos más no brinda accesos para su procesamiento.
A.8.2 Seguridad de los Recursos Humanos, durante el empleo **Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los**	A.8.2.1 Gestión de responsabilidades	SI	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
	A.8.2.2 Capacitación y educación en seguridad de la información	SI	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado

riesgos de error humano.			conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
	A.8.2.3 Proceso disciplinario	SI	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.9.1 Áreas seguras **Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.**	A.9.1.1 Perímetro de seguridad física	NO	No hay visita de clientes a instalaciones, salvo por circunstancias excepcionales planeadas con suficiente antelación.
	A.9.1.2 Controles de entrada físicos	NO	No hay visita de clientes a instalaciones, salvo por circunstancias excepcionales planeadas con suficiente antelación.
	A.9.1.3 Seguridad de oficinas, habitaciones y medios	SI	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
	A.9.1.4 Protección contra amenazas externas y ambientales	NO	No en primera instancia por lo reducido de la planta de personal e infraestructura física. Se remite a respaldo de información
	A.9.1.5 Trabajo en áreas seguras	SI	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
	A.9.1.6 Áreas de acceso público, entrega y carga	NO	No hay visita de clientes a instalaciones, salvo por circunstancias excepcionales planeadas con suficiente antelación.
A.9.2 Seguridad del equipo **Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización**	A.9.2.1 Ubicación y protección del equipo	SI	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
	A.9.2.2 Servicios públicos	SI	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
	A.9.2.3 Seguridad en el cableado	SI	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
	A.9.2.4 Mantenimiento de equipo	SI	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
	A.9.2.5 Seguridad del equipo fuera-del- local	NO	No aplica, por la metodología de trabajo y repositorios locales de la información
	A.9.2.6 Eliminación seguro o re-uso del equipo	NO	No aplica, por la metodología de trabajo y repositorios locales de la información
	A.9.2.7 Traslado de Propiedad	SI	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.
A.10.1 Procedimientos y responsabilidades operacionales **Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información**	A.10.1.1 Procedimientos de operación documentados	SI	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
	A.10.1.2 Gestión de cambio	SI	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
	A.10.1.3 Segregación de deberes	SI	Control Se deben segregar los deberes y áreas de

			responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
	A.10.1.4 Separación de los medios de desarrollo y operacionales	SI	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.4 Protección contra software malicioso y código móvil **Objetivo: Proteger la integridad del software y la información.**	A.10.4.1 Controles contra software malicioso	SI	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
	A.10.4.2 Controles contra códigos móviles	NO	No está autorizado el uso.
A.10.5 Respaldo (back-up) **Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.**	A.10.5.1 Back-up o respaldo de la información	SI	Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 Gestión de seguridad de redes **Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.**	A.10.6.1 Controles de red	SI	Control Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
	A.10.6.2 Seguridad de los servicios de red	SI	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.8 Intercambio de información **Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.**	A.10.8.1 Procedimientos y políticas de información y software	SI	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
	A.10.8.2 Acuerdos de intercambio	SI	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
	A.10.8.3 Medios físicos en tránsito	NO	No aplica, este tipo de tránsito de medios electrónicos mediante uso de dispositivos físicos no se permite.
	A.10.8.4 Mensajes electrónicos	SI	Control Se debe proteger adecuadamente los mensajes electrónicos.
	A.10.8.5 Sistemas de información comercial	SI	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.11.2 Gestión del acceso del usuario **Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no- autorizado a los sistemas de información.**	A.11.2.1 Inscripción del usuario	SI	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
	A.11.2.2 Gestión de	SI	Control

	privilegios		Se debe restringir y controlar la asignación y uso de los privilegios.
	A.11.2.3 Gestión de la clave del usuario	SI	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
	A.11.2.4 Revisión de los derechos de acceso del usuario	SI	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario **Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.**	A.11.3.1 Uso de clave	SI	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
	A.11.3.2 Equipo de usuario desatendido	SI	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
	A.11.3.3 Política de pantalla y escritorio limpio	SI	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.7 Computación móvil y tele-trabajo **Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.**	A.11.7.1 Computación móvil y comunicaciones	SI	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
	A.11.7.2 Tele-trabajo	SI	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12.2 Procesamiento correcto en las aplicaciones **Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.**	A.12.2.1 Validación de data de Insumo	SI	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
	A.12.2.2 Control de procesamiento interno	SI	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.
	A.12.2.3 Integridad del mensaje	SI	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
	A.12.2.4 Validación de data de output	SI	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.4 Seguridad de los archivos del sistema **Objetivo: Garantizar la seguridad de los archivos del sistema**	A.12.4.1 Control de software operacional	SI	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
	A.12.4.2 Protección de la data de prueba del sistema	SI	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
	A.12.4.3 Control de acceso al código fuente del programa	SI	Control Se debe restringir el acceso al código fuente del programa.

A.12.5 Seguridad en los procesos de desarrollo y soporte **Objetivo: Mantener la seguridad del software e información del sistema de aplicación**	A.12.5.1 Procedimientos de control de cambio	SI	Control La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
	A.12.5.2 Revisión técnica de las aplicaciones después de cambios en el sistema operativo	SI	Control Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
	A.12.5.3 Restricciones sobre los cambios en los paquetes de software	SI	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
	A.12.5.4 Filtración de información	SI	Control Se deben evitar las oportunidades de filtraciones en la información.
	A.12.5.5 Desarrollo de outsourced software	NO	No aplica, se ha restringido estrictamente el desarrollo del software nuclear a desarrollos in house.
A.12.6 Gestión de vulnerabilidad técnica **Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.**	A.12.6.1 Control de vulnerabilidades técnicas	SI	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información **Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.**	A.13.2.1 Responsabilidades y procedimientos	SI	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
	A.13.2.2 Aprendizaje de los incidentes en la seguridad de la información	SI	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
	A.13.2.3 Recolección de evidencia	SI	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial **Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.**	A.14.1.1 Incluir seguridad de la información en el proceso de gestión de continuidad comercial	SI	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
	A.14.1.2 Continuidad comercial y evaluación del riesgo	SI	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
	A.14.1.3 Desarrollar e implementar planes de continuidad incluyendo	SI	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información

	seguridad de la información		en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
	A.14.1.4 Marco referencial para la planeación de la continuidad comercial	SI	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
	A.14.1.5 Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	SI	Control Los planes de continuidad comercial se deb probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
A.15.1 Cumplimiento con requerimientos legales **Objetivo: Evitar violaciones de cualquier ley, obligación reguladora contractual y de cualquier requerimiento de seguridad**	A.15.1.1 Identificación de legislación aplicable	SI	Control Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
	A.15.1.2 Derechos propiedad de intelectual (IPR)	SI	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
	A.15.1.3 Protección los registros Organizacionales	SI	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
	A.15.1.4 Protección de data y privacidad de información personal	SI	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
	A.15.1.5 Prevención de mal uso de medios de procesamiento de información	SI	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
	A.15.1.6 Regulación de controles Criptográficos	SI	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico **Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.**	A.15.2.1 Cumplimiento con las políticas y estándares de seguridad	SI	Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
	A.15.2.2 Chequeo de cumplimiento Técnico	SI	Control Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.

CAPÍTULO 4. RECOMENDACIONES, MEJORAS Y CONCLUSIONES

4.1 Recomendaciones y Mejoras

4.1.1 Pasos siguientes en la implementación

La metodología sugerida por la literatura sugiere la identificación de necesidades de documentación y la instauración de los planes de trabajo específicos para las áreas funcionales de la empresa o procesos relacionados (Kumar, 2012). El desarrollo de estas actividades cumple además con una buena práctica documentada permanentemente en la literatura correspondiente a tratar este tipo de iniciativas como proyectos, con procesos de gerencia autónoma y con sus correspondientes medidas de aseguramiento de calidad (Alexander, 2007).

4.1.2 Sistemas integrados de gestión: Aseguramiento de Calidad

El desarrollo del trabajo sugiere una necesidad grande de integración entre diferentes marcos normativos y de gestión, como complemento a los esfuerzos en seguridad de información. Dentro de estas relaciones, vale la pena destacar una gran oportunidad con respecto a los esquemas de mejora continua propuestos en particular por la familia de normas ISO 9000 en aspectos relevantes como los controles A.10.1 Procedimientos y responsabilidades operacionales y A.13.2.2 Aprendizaje de los incidentes en la seguridad de la información, que para este caso particular tienen una estrecha relación con los esquemas de aseguramiento de calidad en productos y servicios, fundamental en los requisitos expresados por ISO 9001:2008.

Adicionalmente a este punto se encuentra una estrecha relación entre los diferentes esquemas de responsabilidad, compromiso y revisión por la dirección, puntos en los cuáles los insumos de información brindados por este trabajo encuentran objetivos comunes e integrados para tener un concepto fuerte y completo del término calidad y servicio.

4.1.3 Sistemas integrados de gestión: Seguridad y Salud ocupacional

Adicionalmente a lo anterior se presentan oportunidades de integración y complementariedad con respecto a normas técnicas y buenas prácticas en las áreas de seguridad y salud ocupacional, ya que para esta industria en particular dichos riesgos están circunscritos a los ámbitos de trabajo electrónico, teletrabajo y relacionados. Es así como por ejemplo los controles A.9.1.5 Trabajo en áreas seguras y A.9.2 Seguridad del equipo son un buen insumo para el comienzo de actividades en estas áreas de mejora y prevención.

4.2 Conclusiones

Al aplicar la metodología completa de establecimiento de un sistema de gestión de seguridad de información para esta organización en particular se encontraron, finalmente, 22 objetivos de control y 66 controles relacionados para su cumplimiento. Este número contrastado contra la literatura consultada puede parecer alto, sin embargo, siendo este un caso específico de una organización de base tecnológica, de rápido desarrollo y muy dependiente de los medios tecnológicos y de información es un

número proporcionado a la cantidad de procesos de información en los cuáles esta organización incurre todos los días y que dieron origen a los riesgos catalogados en primera instancia.

La metodología de cálculo de riesgo y priorización sugirió, muy consistentemente con el tipo de industria y servicios ya comentados, que gran parte de los riesgos tienen que ver con la formación técnica de los colaboradores con respecto a la gestión de la calidad y la preservación de la información. Es importante destacar este hecho, ya que aunque se trata de un servicio muy intensivo en situaciones de desarrollo y creación de tecnología, no pueden estos procesos estar por fuera de al menos un marco regulatorio central para las labores de diseño e implementación.

Adicionalmente, este trabajo propone un paso inicial para la gerencia de continuidad del negocio, entendiendo esta como un concepto amplio, en el cual los procesos vitales, identificados mediante esta primera aproximación puedan contar con los respaldos suficientes en caso de falla, para continuar siendo un proveedor de servicios confiable.

LITERATURA CONSULTADA

Alexander, A. G. (2005a). Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001:2005. *Information Security*, (511), 1-6.

Alexander, A. G. (2005b). Análisis y Evaluación del Riesgo de Información : Un Caso en la Banca Aplicación del ISO 27001 : 2005.

Alexander, A. G. (2007). *Diseño de un sistema de Gestión de Seguridad de Información* (1st ed., p. 176). Bogotá: Alfaomega Colombiana S.A.

Carlson, T. (2001). *Information Security Management : Understanding ISO 17799* (p. 22). Retrieved from http://www.netbotz.com/library/ISO_17799.pdf

Christopher J. Alberts, A. J. D. (2003). *Managing Information Security Risks: The Octave Approach* (1st ed., p. 471). Addison-Wesley Professional.

Davis, G. B., & Olson, M. H. (1985). *Management Information Systems: Conceptual Foundations, Structure and Development*. (McGraw-Hill, Ed.) (Vol. 2., p. 693). McGraw-Hill. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.45.12&rep=rep1&type=pdf

Delmonte, P. (2009). *Implantación del SGSI de Sonda Uruguay*. Montevideo.

Díaz, A. F., Collazos, G. I., & Cortez, H. (n.d.). Implementacion de un sistema de gestión de seguridad de la información (sgsi) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma iso 27001.

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security*, *21*(5), 402-409. doi:10.1016/S0167-4048(02)00504-7

ISO. (2005). ESTANDAR INTERNACIONAL ISO / IEC 27001, *2005*, 41.

Jarmon, D. (2002). *A Preparation Guide to Information Security Policies* (p. 17). Retrieved from http://www.sans.org/reading_room/whitepapers/policyissues/preparation-guide-information-security-policies_503

Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508. Elsevier Ltd. doi:10.1016/j.cose.2009.07.001

Kumar, V. P. (2012). ISMS Implementation Guide. *The Journal of infectious diseases*, *205*(9), NP. doi:10.1093/infdis/jis093

OCDE. (2002). Directrices de la ocde para la seguridad de sistemas y redes de información, 1-12.

Office of Information Technology. (2003). Information security guideline for NSW Government [electronic resource]. (N. S. W. O. of I. Technology, Ed.). Sydney, N.S.W. :: Office of Information Technology. Retrieved from http://www.oit.nsw.gov.au/pdf/4.4.18.IS-pt3.pdf

Pincay, F. (2005). Implementación del Primer Sistema de Gestión de Seguridad de la Información , en el Ecuador , Certificado bajo la Norma.

Presidencia del Consejo de Ministros. (2011). Resolución Ministerial 197, 49-50.

Simon, H. A. (1957). *Administrative behavior: a study of decision-making processes in administrative organization*. Macmillan.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2000). *Information Security Management*. (G. Dhillon, Ed.). IGI Global. doi:10.4018/978-1-878289-78-0

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security*, *23*(4), 275-279. doi:10.1016/j.cose.2004.01.013

ANEXO I: LICENCIA DE USO

LICENCIA DE USO – AUTORIZACIÓN DE LOS AUTORES

Actuando en nombre propio identificado (s) de la siguiente forma:

Nombre Completo Camilo Augusto García Guevara.

Tipo de documento de identidad: C.C. ☒ T.I. ☐ C.E. ☐ Número: 3'212453

Nombre Completo _____

Tipo de documento de identidad: C.C. ☐ T.I. ☐ C.E. ☐ Número: _____

Nombre Completo _____

Tipo de documento de identidad: C.C. ☐ T.I. ☐ C.E. ☐ Número: _____

Nombre Completo _____

Tipo de documento de identidad: C.C. ☐ T.I. ☐ C.E. ☐ Número: _____

El (Los) suscrito(s) en calidad de autor (es) del trabajo de tesis, monografía o trabajo de grado, documento de investigación, denominado:

Establecimiento del Sistema de Seguridad de la Información en SFG bajo los estándares de la norma ISO 27001: 2005

Dejo (dejamos) constancia que la obra contiene información confidencial, secreta o similar: SI ☐ NO ☒
(Si marqué (marcamos) SI, en un documento adjunto explicaremos tal condición, para que la Universidad EAN mantenga restricción de acceso sobre la obra).

Por medio del presente escrito autorizo (autorizamos) a la Universidad EAN, a los usuarios de la Biblioteca de la Universidad EAN y a los usuarios de bases de datos y sitios webs con los cuales la Institución tenga convenio, a ejercer las siguientes atribuciones sobre la obra anteriormente mencionada:

A. Conservación de los ejemplares en la Biblioteca de la Universidad EAN.
B. Comunicación pública de la obra por cualquier medio, incluyendo Internet
C. Reproducción bajo cualquier formato que se conozca actualmente o que se conozca en el futuro
D. Que los ejemplares sean consultados en medio electrónico
E. Inclusión en bases de datos o redes o sitios web con los cuales la Universidad EAN tenga convenio con las mismas facultades y limitaciones que se expresan en este documento
F. Distribución y consulta de la obra a las entidades con las cuales la Universidad EAN tenga convenio

Con el debido respeto de los derechos patrimoniales y morales de la obra, la presente licencia se otorga a título gratuito, de conformidad con la normatividad vigente en la materia y teniendo en cuenta que la Universidad EAN busca difundir y promover la formación académica, la enseñanza y el espíritu investigativo y emprendedor.

Manifiesto (manifestamos) que la obra objeto de la presente autorización es original, el (los) suscritos es (son) el (los) autor (es) exclusivo (s), fue producto de mi (nuestro) ingenio y esfuerzo personal y la realizó (zamos) sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de exclusiva autoría y tengo (tenemos) la titularidad sobre la misma. En vista de lo expuesto, asumo (asumimos) la total responsabilidad sobre la elaboración, presentación y contenidos de la obra, eximiendo de cualquier responsabilidad a la Universidad EAN por estos aspectos.

En constancia suscribimos el presente documento en la ciudad de Bogotá D.C.,

NOMBRE COMPLETO: Camilo Angelo Cañon
FIRMA: _____
DOCUMENTO DE IDENTIDAD: 3212452
FACULTAD: Postgrados
PROGRAMA ACADÉMICO: Maestría de Ecología

NOMBRE COMPLETO: _____
FIRMA: _____
DOCUMENTO DE IDENTIDAD: _____
FACULTAD: _____
PROGRAMA ACADÉMICO: _____

NOMBRE COMPLETO: _____
FIRMA: _____
DOCUMENTO DE IDENTIDAD: _____
FACULTAD: _____
PROGRAMA ACADÉMICO: _____

NOMBRE COMPLETO: _____
FIRMA: _____
DOCUMENTO DE IDENTIDAD: _____
FACULTAD: _____
PROGRAMA ACADÉMICO: _____

Fecha de firma: 25/7/2012