“METODO SCRUM APLICADO AL SISTIEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN”

Wilmer de Jesús de la Hoz González
Miguel Ángel Méndez Chávez

La Gestión de Seguridad de la Información desde su aparición se ha convertido en el pilar que sostiene y garantiza la confidencialidad, integridad y disponibilidad de cada uno de los activos de las empresas, de aquí su gran importancia y necesidad en una organización. Cabe anotar que este concepto es utilizado por las diferentes normas y metodologías que incurren en el mercado hoy en día, pero en particular en este trabajo se **desarrollará la aplicación del método SCRUM en el SGSI**. El método SCRUM se compone de buenas prácticas que permiten su adaptabilidad en este tipo de proyecto y por medio del trabajo en equipo y guidado por un líder se logra obtener los objetivos propuestos.

POLITECNICO GRANCOLOMBIANO
METODO SCRUM- SGSI
TESIS DE GRADO
25/04/2016

METODO SCRUM APLICADO AL SISTIEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TRABAJO DE GRADO

PARTICIPANTES

DE LA HOZ GONZALEZ WILMER DE JESUS

MENDEZ CHAVEZ MIGUEL ANGEL

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

METODO SCRUM APLICADO AL SISTIEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TRABAJO DE GRADO

PARTICIPANTES

DE LA HOZ GONZALEZ WILMER DE JESUS

MENDEZ CHAVEZ MIGUEL ANGEL

Asesor

PIEDRAHITA SOLORZANO GIOVANNY ANDRES

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2016

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firmas de los jurados

Bogotá, 02 de Mayo de 2016

AGRADECIMIENTOS

En primer lugar agradezco a DIOS por haberme permitido la oportunidad de continuar con mis proyectos de vida, por la salud y la vida concedida para seguir adelante.

Deseo agradecer a todos los docentes que nos brindaron sus conocimientos, experiencias y que nos guiaron durante el desarrollo de esta especialización, y que motivaron la línea de investigación y aplicación de los estudios y en especial por la seguridad de la información, que día a día se enfrenta a nuevos avances y por ende debo mantenerme actualizado para superar los retos que se presenten a diario.

Quiero también agradecer a mi esposa Nelly Muñoz por ese apoyo incondicional y la motivación continua, a nuestra hija Kelly Michelle Bendición de Dios en nuestro hogar , a mis padres Alcides De La Hoz, Gloria Gonzalez, a mis hermanos Alcides, Kellis, Gisseth, Yair por estar presente en este camino de formación que me permitirá seguir creciendo profesionalmente y como persona.

Wilmer de Jesús De La Hoz González

Quiero agradecer a todos mis maestros ya que ellos me enseñaron durante el desarrollo de esta especialización, ese valorar por los estudios y en especial por la seguridad, a tener claro que debo superarme cada día.

Quiero también agradecer a mis padres Miguel Méndez y Jaqueline Chávez porque ellos estuvieron en los días más difíciles de mi vida como estudiante, por otra parte agradezco enormemente a mi esposa Sandra Díaz y mi hijo Salomón Méndez, por estar en esos momentos difíciles y de constante estudio día tras día.

También agradezco a mi principal motor y combustible, que no tiene precio ni comparación, ese es Dios, por darme la salud que tengo, por tener la voluntad y las ganas necesarias para analizar y pensar de la mejor manera y además un cuerpo sano y una mente de bien.

Estoy seguro que mis metas planteadas darán fruto en el futuro y por ende me debo esforzar cada día para ser mejor y en todo lugar, sin olvidar el respeto que engrandece a la persona.

Miguel Ángel Méndez Chávez

INDICE GENERAL

INDICE DE FIGURAS

INTRODUCCION

En los últimos años las empresas, organizaciones, universidades y demás entes han aprovechado los grandes avances que nos ofrece la tecnología y en algunos casos han experimentado los riesgos que esta trae consigo sin estar preparados para su mitigación y corrección del mismo.

Para ello, han surgido normas, estándares y metodologías que datan desde hace mucho tiempo que no eran del dominio público, debido a la preparación del recurso humano sobre las mismas para poder ser aplicado en las organizaciones.

A través del tiempo han surgido modificaciones en las normas, estándares en busca de las mejores prácticas para poder estar preparados ante los riesgos que se encuentra expuesta una organización e implementar un sistema de gestión que permita llevar de manera organizada todos los procesos involucrados en las actividades propias de la empresa.

Si bien un sistema de gestión busca establecer mediante procesos optimizados, disciplina y con un enfoque de gestión involucrar todas las partes de la organización para que de forma integrada se puedan lograr los objetivos propuestos.

El sistema de gestión ha sido extendido a la seguridad de la información, para que de manera integrada se pueda lograr los pilares fundamentales de un SGSI (Sistema de Gestión de Seguridad de Información) que son Confidencialidad, Integridad, Disponibilidad.

Un SGSI requiere de responsabilidad, dedicación y compromiso ya que es integrado por varios componentes que no se pueden pasar por alto. La identificación y desarrollo de estos componentes son lo que a primera vista pueden generar una perspectiva compleja del SGSI que conlleva a una reacción negativa por parte de los directivos de una organización, o empezar a trabajar de forma inadecuada generando resultados adversos a los esperados.

Con la elaboración del presente proyecto, buscamos **aplicar la Metodología SCRUM al Sistema de Gestión de Seguridad de la Información (SGSI)** y así lograr la integración de sus componentes y la participación de toda una organización de forma práctica orientados a sus objetivos.

1. RESUMEN EJECUTIVO

El gran adelanto tecnológico ha traído consigo en las empresas, una serie de situaciones a nivel de la seguridad de la Información, la cual es sin duda una preocupación no solo de este siglo, sino también de lo que se prevé que traerá la globalización, por tal motivo en la actualidad son diferentes los mecanismos y sistemas implementados en cada uno de los activos basados en la información y en toda su infraestructura, al igual existen empresas que no cuentan ni poseen ningún tipo de experiencia en materia de seguridad de la información, es esta la razón principal para que este sea un tema que en la actualidad sea muy discutido y abarque la temática como punto de partida en nuestro proyecto.

Esta situación problema no solamente afecta a las empresas, sino a todas aquellas partes donde existe información y que podrían verse afectado en cualquier aspecto, área, proceso en general.

Por otra parte y anexado a lo anterior, debemos tener en cuenta que en los últimos años la existencia de estándares, procesos, buenas prácticas y en especial las metodologías ágiles han irrumpido con fuerza en el mundo comercial o empresarial, relacionándolos directamente con los sistemas informáticos de cada una, como una forma nueva de quitar lo planteado por las metodologías convencionales, sin dejar a un lado que son muchas las organizaciones y entidades interesadas en la optimización de las mismas. El incurrir en esta nuevas prácticas hace que, aunque existen evidencias de los beneficios que pueden proporcionar, aún resulte difícil tomar las mejores decisiones de cual y como utilizar según las necesidades.

El presente proyecto se basa en el ***METODO SCRUM APLICADO AL SISTIEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*****,** garantizando una forma ágil de implementar el esquema de la seguridad de la información en las empresas. De igual forma se proponen un marco de trabajo para lograr la gestión de la seguridad, basándose en la aplicación de una metodología ágil de implementación y de buenas prácticas, esta metodología es la SCRUM.

El objeto de este proyecto que va de la mano con la evidencia de tesis de grado, es estudiar la evolución y técnicas utilizadas por metodologías ágiles, en concreto por la metodología SCRUM, para ser aplicada en la implementación de seguridad de la información, para ello se definió un marco de trabajo que integra los componentes del método SCRUM y los del SGSI.

Por lo anterior se presentan los resultados obtenidos como marco de referencia que permitan a las organizaciones iniciar el proceso de implementación de Seguridad de la Información, resaltándose el compromiso de trabajo en equipo.

Ilustración No 1 Componentes para el Marco de trabajo

La descripción detallada de cada uno de los componentes del marco de trabajo se encuentra definidos en el punto 5 Resultados y discusión.

Con la culminación de este proyecto se busca mejorar la competitividad de las empresas, sobre guardado y protección de su sistema de información, a través de un rápido y ágil método que le permita adaptarse a las actuales características del mercado social, económico y tecnológico.

2. JUSTIFICACIÓN

La seguridad de la información es uno de los mecanismos que hoy por hoy ha tomado fuerza dentro de las organizaciones debido a los avances tecnológicos que trae consigo riesgos que pueden afectar de manera directa e indirecta a la empresa.

Esta investigación busca mediante la aplicación de las teorías y los conceptos básicos de la planeación, estimación, organización, coordinación, dirección, aspectos legales, actores relevantes, situación problema, cadenas causales, flujo grama, valoración de viabilidad, gobernabilidad, pertinencia, plan de trabajo y entre otros, aplicar la metodología SCRUM para minimizar los riesgos en la realización del proyecto de un Sistema de Gestión de Seguridad de la Información.

A través del análisis de la metodología SCRUM se busca establecer los componentes necesarios que se puedan aplicar en todas las partes que integra un Sistema de Gestión de Seguridad de la Información.

Con la puesta en marcha de este proyecto y con una buena planificación del trabajo, se verán reflejados una serie de beneficios como son: Mayor competencia y desarrollo a nivel personal y profesional en un Sistema de Gestión de Seguridad de la Información, por medio de las buenas prácticas aplicadas de la metodología SCRUM, mejores prácticas, mayor conocimiento y solución de situaciones problemas que se puedan presentar a nivel de seguridad de la información.

Todo esto se podrá llevar a cabo gracias a la capacidad en el manejo temático y analítico aprendido durante el desarrollo de la cátedra del módulo de Opción de Grado y de cada una de las que conforman este proceso desarrollado en el Politécnico Gran Colombiano.

Por último se desarrollará el proyecto obteniendo un mayor entendimiento en la realización de este, y así poder realizarnos como Especialista en la Seguridad de la Información.

3. MARCO TEÓRICO

En este marco teórico encontraremos palabras claves que se encuentran definidas de acuerdo a la idea central y otras que son propias del material consultado.

La definición de cada una de ellas, nos darán una claridad sobre el tema tratado y el uso de las mismas durante el desarrollo del proyecto.

- ✓ **Sistema de Gestión:** "*Un sistema de gestión es un conjunto de reglas y principios relacionados entre sí de forma ordenada, para contribuir a la gestión de procesos generales o específicos de una organización*". [2]

- ✓ **Ciclo Deming o PHVA:** Planear, Hacer, Verificar y Actuar. Este ciclo es la base aplicada en las normas ISO. [14]

- ✓ **Información:** "*Conjunto de dato organizado, procesado, almacenado"*. [9]

- ✓ **Seguridad Informática:** "*La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad".* [13]

- ✓ **Seguridad de la información:** *"Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad"*. [7]

- ✓ **SGSI - Sistema de Gestión de Seguridad de la Información:** *"Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información"*. [7]

- ✓ **Confidencialidad:** *"Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados"*. [7]

- ✓ **Integridad:** *"Propiedad de salvaguardar la exactitud y el estado completo de los activos".* [7]

- ✓ **Disponibilidad:** *"Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada"*. [7]

- ✓ **Análisis de Riesgos:** *"Uso sistemático de la información para identificar las fuentes y estimas riesgos"*. [7]

- ✓ **Vulnerabilidad:** Es una debilidad asociada a un software, hardware, procedimientos o error humano que permite a un atacante aprovecharla para causar daño. [8]

- ✓ **Amenaza:** Es el peligro potencial a la información, hardware, software, proceso el cual se encuentra expuesto. [8]

- ✓ **Gestión de Riesgo:** *"Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo"*. [7]

- ✓ **Gestión de activos de información:** Es el uso de un proceso sistemático para identificar y clasificar los activos de información de la organización. De su correcta clasificación depende la integración con la gestión de riesgos. [3]

- ✓ **Gestión de recursos financieros:** Es el proceso mediante el cual se establecen las directrices para llevar a cabo la distribución de los recursos financieros destinados a la inversión por medio de una correcta planificación a corto, mediano y largo plazo. [3]

- ✓ **Gestión de recursos humano:** Es el proceso mediante el cual se establecen las directrices sobre el recurso humano para su vinculación, capacitación, sensibilización y seguimiento de las actividades. [7]

- ✓ **NTC–ISO/IEC 27001:** "*Norma técnica colombiana que establece los requisitos para el modelo de Sistema de Gestión de Seguridad de la Información"*. [7]

- ✓ **COBIT:** *"Es un marco de trabajo que ofrece un conjunto de buenas prácticas por medio principios orientados a las áreas de TI que les permita tomar un rol estratégico dentro de las organizaciones"*. [10]

- ✓ **ITIL:** "*Es un marco de mejores prácticas para la Gestión de Servicios de TI, el cual cuenta con puntos en común para Seguridad de la Información enmarcado el proceso denominado Gestión de la Seguridad."* [10]

- ✓ **NIST 800-100:** "*Es un documento guía que enfocado a la implementación de Seguridad de la Información y cómo lograr el apoyo de la dirección partiendo de la comprensión de que es seguridad de la información".* [10]

- ✓ **Defensa en Profundidad:** "*Es un concepto de seguridad que surge de la estrategia militar que permite establecer un grupo o capas de controles para proteger la información".* [10]

- ✓ **ISM3 o O-ISM3 (Open Information Security Management Maturity Model):** "*Es un modelo de trabajo que permite la creación de un SGSI. Este modelo pretende alcanzar el nivel de seguridad con un riesgo aceptable*

para garantizar los objetivos del negocio. Ofrece un conjunto de herramientas para la seguridad por medio de las buenas prácticas como ITIL, COBIT, TOGAF, ISO27001". [10]

- ✓ **NTC–ISO/IEC 27005:** "*Norma técnica colombiana que establece directrices para gestión de riesgos en seguridad de la información".* [8]
- ✓ **NTC–ISO/IEC 31000:** "*Norma técnica colombiana que estable un marco de gestión y administración de riesgos en general*".[11]
- ✓ **MAGERIT:** "*Es una metodología de gestión de riesgos para la administración pública española*". [11]
- ✓ **OCTAVE:** *"Es una metodología de gestión de riesgos que cuenta con diferentes versiones adecuadas al tamaño de una organización".* [11]
- ✓ **NIST 800-30:** "*Es una metodología de gestión de riesgos de seguridad de la información*". [11]
- ✓ **SCRUM:** Es un proceso donde se aplican las buenas prácticas para el trabajo colaborativo y en equipo, que permite obtener mejores resultados de un proyecto. [1]
- ✓ **SCRUM MASTER:** Persona conocedora de un proceso y su liderazgo debe estar al servicio del Equipo Scrum (Scrum Team). [1]
- ✓ **EQUIPO SCRUM (SCRUM TEAM):** Equipo de trabajo que es auto organizado y multifuncional para llevar a cabo la planificación del Sprint (Sprint Planning). [1]
- ✓ **PLANIFICACION DEL SPRINT (SPRINT PLANNIG):** Corresponde a la reunión de planificación de las actividades a realizar durante el Sprint.
- ✓ **LISTA DE PRODUCTO (PRODUCT BACKLOG):** Es donde se establecen los requerimientos de un proyecto de manera ordenada y priorizada. [1]
- ✓ **SPRINT:** Corresponde al periodo o bloque de tiempo (time-box) en el cual se debe desarrollar el trabajo. [1]
- ✓ **SCRUM DIARIO (SCRUM DAILY):** Corresponde a una reunión de corto tiempo de cada día del sprint para revisar el estado de un proyecto. [1]
- ✓ **REVISION DEL SPRINT (SPRINT REVIEW):** Es una reunión que tiene como objetivo verificar lo ejecutado del sprint planning. [1]

- ✓ **RETROSPECTIVA DE SPRINT (SPRINT RETROSPECTIVE):** Es una reunion llevada a cabo posterior al Sprint Review, con el objetivo de analizar las mejoras a implementar antes de continuar con el siguiente Sprint. [1]

- ✓ **DUEÑO DEL PRODUCTO (PRODUCT OWNER):** Representa al cliente, y es el encargado de negociar, con el Scrum Master, con el equipo y como facilitador, y establece la prioridad del trabajo a realizar. [1]

4. METODOLOGÍA

Para poder abordar la elaboración del proyecto que busca atender la **COMPLEJIDAD EN LAS EMPRESAS PARA IMPLEMENTAR SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, se realizará un análisis de cada uno de los componentes establecidos en un SGSI, el cual varía de acuerdo a la norma, estándar, metodologías, buenas prácticas que giran alrededor de la seguridad de la información como se pudo describir en el marco teórico y para el presente proyecto, nos basamos en la norma ISO 27001, y por ser de la familia ISO – ICONTEC, las empresas implementan dentro de sus procesos el Sistema de Gestión de la Calidad y en este orden de idea, existen algunos procesos de esta norma que son aprovechados en la implementación del SGSI.

Para las organizaciones que no son del sector financiero (transportadores de valores, bancos, entre otras), se puede generar una percepción equivoca a nivel directivo y extendida dentro de la organización, creando una visión incorrecta sobre seguridad de la información, dado a cada uno de los factores involucrados en el SGSI.

Para lo anterior, se requiere una comprensión de cada una las herramientas existentes que buscan apoyar a las organizaciones en definir las directrices que conlleven al diseño e implementación del SGSI y que este a su vez permita la adecuada operación, seguimiento, mantenimiento y mejora continua del mismo.

Como herramienta para dar solución a la complejidad que mencionamos, hemos identificado la existencia de la **METODOLOGIA SCRUM**, que ha sido tomada como marco de referencia en la elaboración de distintos tipos de proyectos.

Con la Metodología SCRUM, buscamos identificar cada uno de sus actores, fases, roles que nos permita su aplicación a cada uno de los componentes del SGSI previamente identificado, y por medio de los resultados obtenidos en cada fase, se logre la integración de los mismos para obtener una correcta visión, diseño, implementación, operación, seguimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

Un SGSI requiere del compromiso, responsabilidad, conciencia de toda una organización, por ende, la Metodología SCRUM se basa en el trabajo en equipo y permite la entrega de parcial de los resultados en cada uno de ellos, garantizando así la correcta comprensión de las actividades, tareas asignadas a cada equipo. Al ser un trabajo en equipo, se aprovecharía al máximo la participación de cada integrante, generando un ambiente de colaboración y apoyo, donde son tenidas en cuenta cada opinión, generando en cada individuo el sentido de pertenencia e importancia dentro de los procesos de la organización, reflejándose en la cultura organizacional para la gestión del cambio.

4.1 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

Como primera medida antes de entrar a lleno con todo lo concerniente con un sistema de gestión de seguridad de la información, debemos tener muy claro que el concepto de seguridad de la información, el cual es definido como *"Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad"*. [7]

Estos principios se describen de la siguiente manera:

- ✓ **Confidencialidad:** *"Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados"*. [7]

- ✓ **Integridad:** *"Propiedad de salvaguardar la exactitud y el estado completo de los activos".* [7]

- ✓ **Disponibilidad:** *"Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada"*. [7]

Siguiendo con la definición de un Sistema de Gestión de la Seguridad de la Información(SGSI), este es traducido por sus siglas en inglés (Information Security Management System), como el conjunto o serie de actividades de gestión que por alguna u otra medida, deben realizarse mediante procesos sistemáticos, documentados y conocidos por la parte donde se está desarrollando, teniendo en cuenta que representa uno de los principios básicos para el control, mejora y desarrollo de cada uno de los procesos que conforman la seguridad de la información y la preservación de los tres pilares fundamentales mencionados anteriormente.

Teniendo en cuenta las necesidades que se evidencian la falta de un modelo o guía para la gestión de la seguridad en la información en las empresas que no pertenecen al sector financiero y de seguridad, debemos tener muy claro que el verdadero propósito de un sistema de gestión de la seguridad de la información no es solo garantizar la seguridad, que nunca podrá ser definida en una forma precisa y estandarizada en todos los casos, sino garantizar y facilitar que todos los posibles riesgos que se puedan presentar a nivel de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma, ya sea documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a cada uno de los cambios que se produzcan.

4.1.1 BENEFICIOS DE LA IMPLEMENTACIÓN DE UN SGSI

Teniendo en cuenta la misión y visión de la empresa en que se está desarrollando el SGSI, se define una arquitectura de gestión de la seguridad por medio de la cual se identifica y valora los riesgos, con el objetivo de implementar medidas, procesos y demás procedimientos que ayuden en su apropiado control y una mejora continua.

Un SGSI aporta los siguientes beneficios a una organización:

- ✓ Análisis de riesgos, identificación de las amenazas, vulnerabilidades e impactos sobre los activos de información.
- ✓ Minimiza los riesgos en materia de confidencialidad, integridad y disponibilidad.
- ✓ Mejora continua de la seguridad de la información, por medio de la supervisión, revisión y eficacia de los procesos implantados, como también las acciones correctivas y preventivas que conllevan a la madurez del SGSI.
- ✓ Aporta un valor añadido y/o diferencial a la compañía.
- ✓ Exterioriza una clara vocación por el cumplimiento de la normativa sobre protección de datos.
- ✓ Certifica una especial solvencia técnica en materia de seguridad de la información.
- ✓ Uso apropiado de los recursos financieros por medio de planes de inversión a corto, mediano y largo plazo.

4.1.2 JUSTIFICACIÓN DE LA IMPLEMENTACIÓN DE UN SGSI

Al igual que cada uno de los procesos, la información, el personal y los sistemas que hacen parte del uso de ellas, son definidos dentro de los activos que representan un pilar muy importante dentro de una empresa y en general, teniendo en cuenta la confidencialidad, integridad y disponibilidad de información, obliga y representa cada uno de los elementos esenciales para mantener los niveles de competitividad en el mercado, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr las metas u objetivos propios de la organización y asegurar beneficios.
Las empresas se ven en la necesidad de implementar un SGSI modelado por una metodología, debido a que con el desarrollo tecnológico sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que pueden generar traumatismo e inestabilidad en la organización.

4.1.3 COMPONENTES PRINCIPALES DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN –SGSI

Existen varios modelos que permiten la implementar seguridad de la información, de los cuales podemos mencionar:

ISO 27000: Se basa en el ciclo PHVA (Planear, Hacer, Verificar, Actuar)

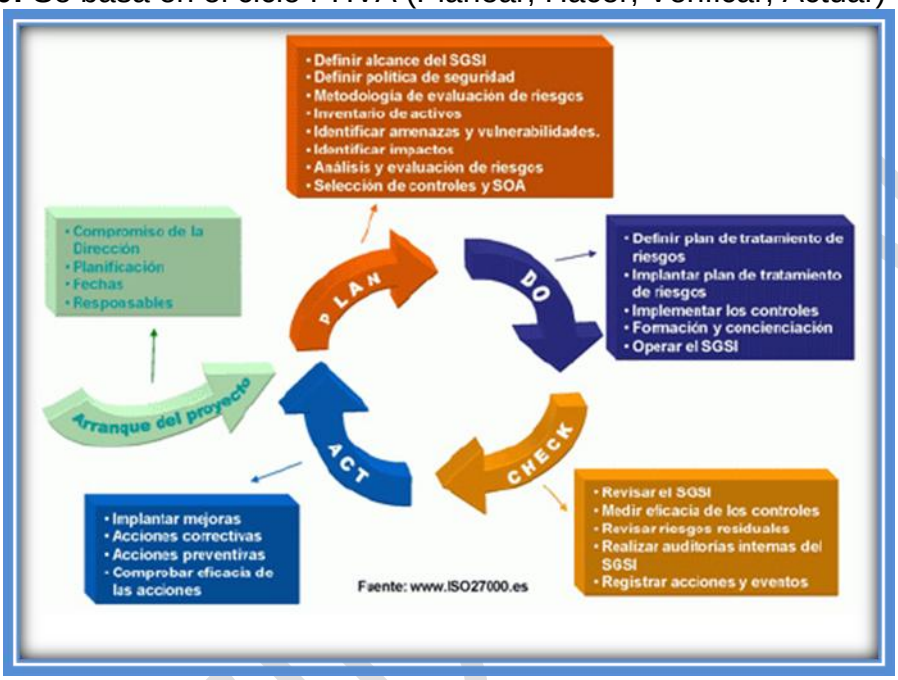

Ilustración No 2 Fuente: http://www.iso27000.es

COBIT: Establece 5 principios que mantienen interacción con diferentes marcos de trabajo, estándares que brindan las buenas prácticas en beneficio de la organización.

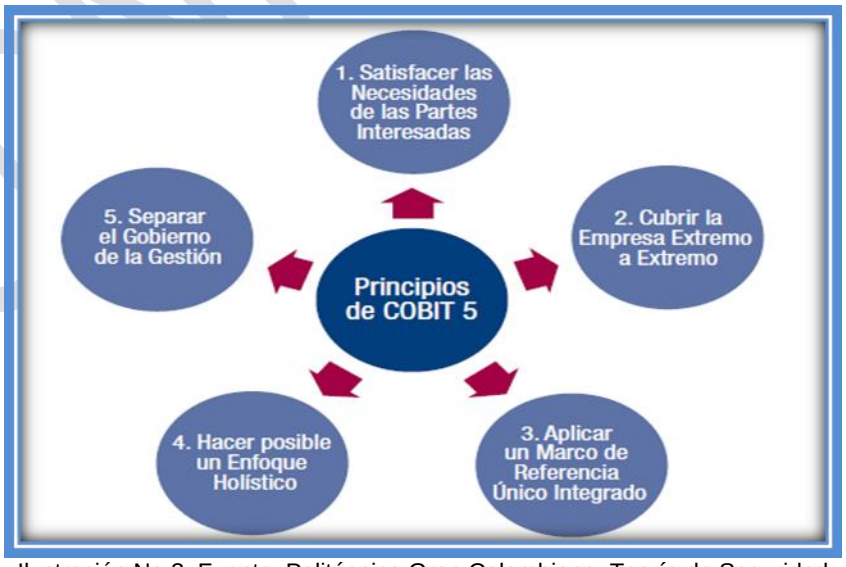

Ilustración No 3 Fuente: Politécnico Gran Colombiano: Teoría de Seguridad

ITIL: Marco de trabajo que establece las mejores prácticas para la gestión de servicios de TI, pero posee algo en común que es la Gestión de Seguridad.

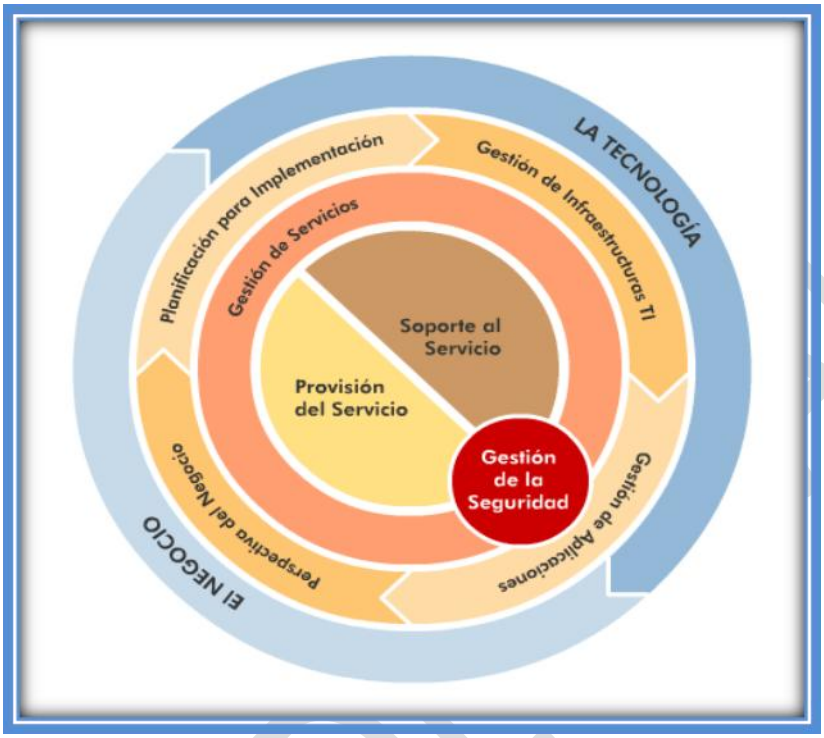

Ilustración No 4 Fuente: Politécnico Gran Colombiano: Teoría de Seguridad

ISM3 (Open Information Security Management Maturity Model): Es un modelo de seguridad moderno que se basa de estándares, guías como Togaf, ITIL, Cobit, ISO 27001.

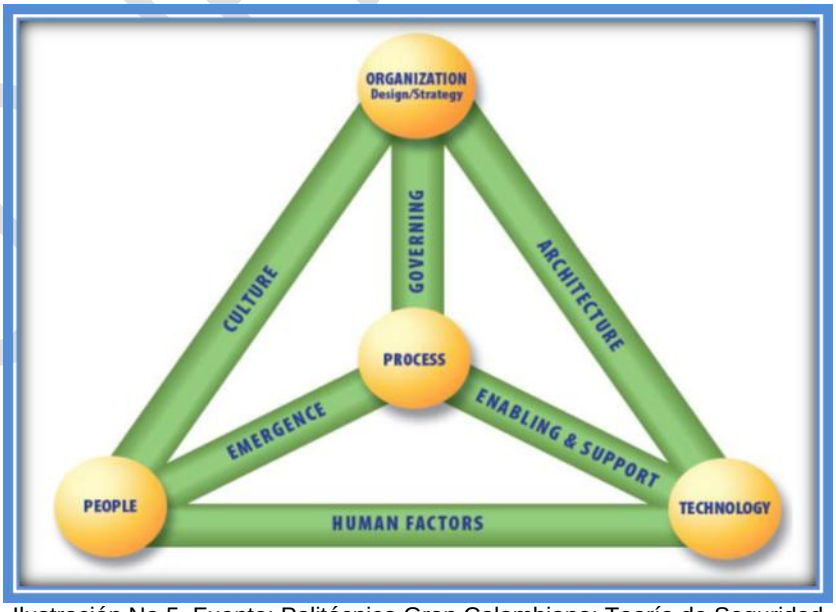

Ilustración No 5 Fuente: Politécnico Gran Colombiano: Teoría de Seguridad

De manera general se pueden definir los siguientes componentes sobre seguridad:

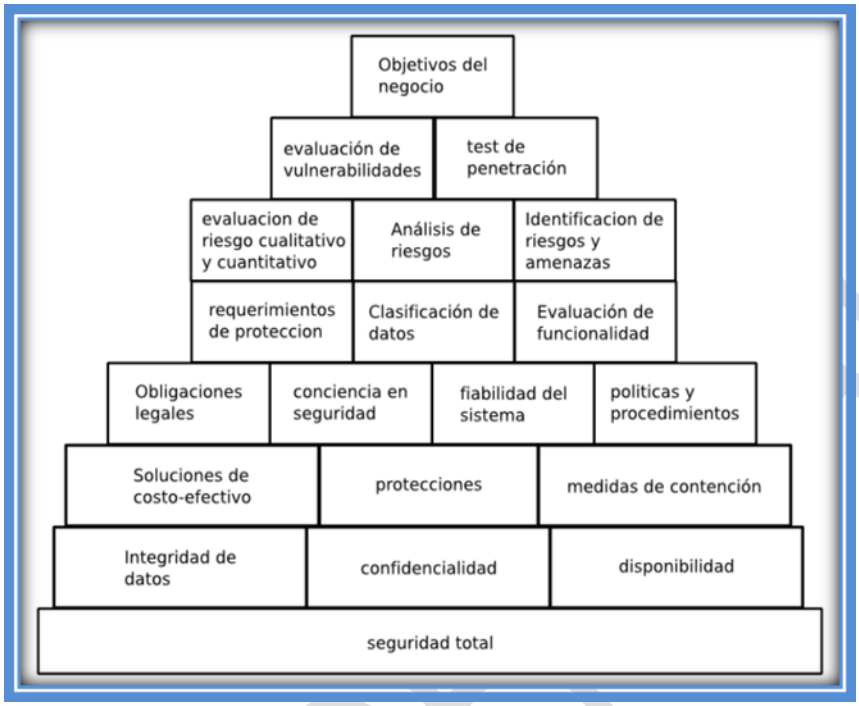

Ilustración No 6 Fuente: Politécnico Gran Colombiano: Teoría de Seguridad

Tomando de referencia la norma ISO 27001 como uno de los estándares utilizados para implementar seguridad de la información, podemos mencionar la siguiente estructura:

- ✓ **Alcance del SGSI**: se define como el contorno de la organización que queda sometido, incluyendo una identidad clara de las áreas, relaciones y términos que existen entre ellas.

- ✓ **Política y objetivos de seguridad**: representa el documento o contenido que establece el compromiso de todas aquellas personas que conforman la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- ✓ **Estándares, Procedimientos, y Guías que soportan el SGSI**: son aquellos mecanismos que regulan el buen funcionamiento del SGSI que se está implementando.

- ✓ **Metodología de Evaluación de riesgos**: representa cada una de las descripciones con respecto a la metodología a implementar, es decir relacionar las dos a nivel de análisis de amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información.

- ✓ **Informe de evaluación de riesgos**: no es más que el estudio consecuente de aplicar la metodología adquirida para la evaluación con respecto los activos de información de la organización.

- ✓ **Plan de tratamiento de riesgos**: es el documento por medio del cual se identifica las acciones del personal de la dirección, teniendo en cuenta los recursos, sus responsabilidades y preferencias para gestionar los riesgos en la seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos.

- ✓ **Registros**: Documentos que proporcionan evidencias de todo lo que se está desarrollando en conformidad con los requisitos y del buen funcionamiento del SGSI.

- ✓ **Declaración de aplicabilidad**: No es más que el contenido que abarca los objetivos y controles contemplados dentro del SGSI, basado en los resultados de los procesos y tratamientos de riesgos, justificando inclusiones y exclusiones.

- ✓ **Control de la documentación**: Este componente representa cada uno de los documentos generados y que hacen parte del sistema SGSI, los cuales deben establecer, documentar, implementar y mantener un procedimiento que defina las acciones de gestión necesarias.

4.1.4 CUADRO COMPARATIVO ENTRE METODOLOGÍAS DE GESTION DE RIESGOS

METODOLOGIA	ISO/IEC 27005	MAGERIT	MEHARI	OCTAVE
CONCEPTO	Definido como un estándar internacional que se ocupa de la gestión de riesgos, por medio de esta determinamos las directrices en los sistemas de seguridad	Considerada como una metodología de carácter público y por medio de la cual se basa en la gestión y análisis de riesgos.	Desarrollada por un club francés para CISO, por medio de la cual facilita un método de evaluación y gestión de riegos.	Metodología basada en la gestión y análisis de riegos, definiendo evaluación y planificación en seguridad.
CARACTERÍSTICAS	-Conjunto de directrices en el análisis de riesgos. -Apoya el análisis y gestión en un SGSI. -Afirma los conceptos propios de la norma ISO/IEC 27001:2005.	-Concientizar a los responsables de que existen riesgos. -ofrecer un método sistemático. -ayuda a describir y planificar.	-Aplica herramientas para la gestión de riesgos. -Permite un análisis individual. -Integración obligatoria de la norma ISO 27000.	-Construye perfiles con las amenazas. -Identifica la infraestructura de la vulnerabilidad. -Desarrolla planes y estrategias de seguridad de acuerdo a las necesidades.
ANÁLISIS DEL RIESGO	-Alcance -Normativas de referencias -Términos -Estructura -Antecedentes -Visión -Evaluar -Tratar -Aceptar -Comunicar el riesgo -Monitorizar	-Identificar activos -Identificar amenazas -Determinar las salvaguardas con que se cuenta -estimar el impacto .Estimar el riesgo	-Establecer el contexto -Tipología y lista de los activos -Daños potenciales -Análisis de las amenazas -Elementos de reducción de riesgos	-Visión organizativa, construcción de los activos -Visión tecnológica, identificar vulnerabilidades -Desarrollo de estrategias, planes de seguridad -Análisis y evaluación
APLICACIÓN	Puede ser aplicada en cualquier organización pública o sociedades mercantiles,	Puede ser aplicada en el gobierno, organismos, compañías grandes, PYME, compañías	Puede ser empleada en el gobierno, organismos, compañías grandes, PYME,	Puede ser aplicada en PYME pequeñas y medianas empresas.

	ONGS, agencias púbicas o gestores de SGSI.	comerciales y no, además en privadas.	pequeña y mediana empresa, salud, comercial, educación.	
VENTAJAS	-Permite identificar las necesidades de la empresa -Ayuda a crear el SGSI -Aborda los riesgos de manera eficaz y oportuna -Integra todas las actividades de la gestión de seguridad	-Se hace fácil su comprensión -Tiene en cuenta los tres pilares de la gestión de seguridad -Comprende el análisis y gestión de riesgos -Soporta herramientas	-Evalúa y simula los niveles de riesgos -Soporta herramientas comerciales -Usa un modelo de análisis de riesgos -Metodología en la gestión de riesgos	-Es compatible con otras metodologías -Involucra todas las áreas en el proceso -Considerada una de las más completas, por involucrar una serie de actividades claves de la gestión
DESVENTAJAS	-No recomienda una metodología concreta -Depende de una serie de factores dentro del SGSI	-No toma en cuenta en no repudio -No realiza análisis de vulnerabilidades -Estima los impactos en la gestión de riesgos	-Solo tiene en cuenta los pilares de la agestión como principios -Los controles no lo realiza dentro del análisis de riesgos	-Aplicable solo en PYME pequeñas y medianas. -No tiene compatibilidad con otros estándares

Cuadro No 1 Comparación entre metodologías de gestión de riesgos

Uno de los componentes de un SGSI es Gestión de Riesgos, por el cual se debe crear un SCRUM para llevar acabo la selección de la metodología de gestión de riesgos a implementar.

Del cuadro comparativo, coincidimos que la metodología OCTAVE brinda las herramientas necesarias para llevar de una forma adecuada, organizada y controlada la gestión de riesgos, permitiendo crear las acciones necesarias para gestionar los incidentes de seguridad. Esta metodología cuenta con versiones que se adaptan al tamaño de organización sin perder el objetivo principal.

Por lo anterior colocamos a consideración el estudio de la metodología OCTAVE dentro del SCRUM – Gestión de Riesgos.

4.2 METODOLOGIA ESCRUM

4.2.1 ALGO DE HISTORIA SOBRE LA METODOLOGIA SCRUM

La metodología SCRUM creada en el año 1986 por Ken Schwaber y Jeff Sutherland, con el fin de crear un método ágil que permitiera el desarrollo de un proyecto donde se involucrara un equipo de trabajo y así lograr buenos resultados por cada fase y que conllevara a cumplir con los objetivos propuestos en el proyecto. [6.2.1]

A continuación se describen algunas empresas que han utilizado el método SCRUM:

SECTOR	EMPRESAS
Media y Telcos	BBC, BellSouth, British Telecom, DoubleYou, Motorola, Nokia, Palm,Qualcomm, Schibsted, Sony/Ericsson, Telefonica I+D, TeleAtlas, Verizon
Software, Hardware	Adobe, Autentia, Biko2, Central Desktop, Citrix, Gailén, IBM, Intel, Microfocus, Microsoft, Novell, OpenView Labs, Plain Concepts, Primavera, Proyectalis, Softhouse, Valtech, VersionOne.
Internet	Amazon, Google, mySpace, Yahoo
ERP	SAP
Banca e Inversión	Bank of America, Barclays Global Investors, Key Bank, Merrill Lynch
Sanidad y Salud	Patientkeeper, Philips Medical
Defensa y Aeroespacial	Boeing, General Dynamics, Lockheed Martin
Juegos	Blizzard, High Moon Studios, Crytek, Ubisoft, Electronic Arts
Otros	3M, Bose, GE, UOC, Ferrari

Cuadro No 2 Ejemplos de empresas que han aplicado el método SCRUM. [6.2.1b]

4.2.2 VISION GENERAL DE SCRUM

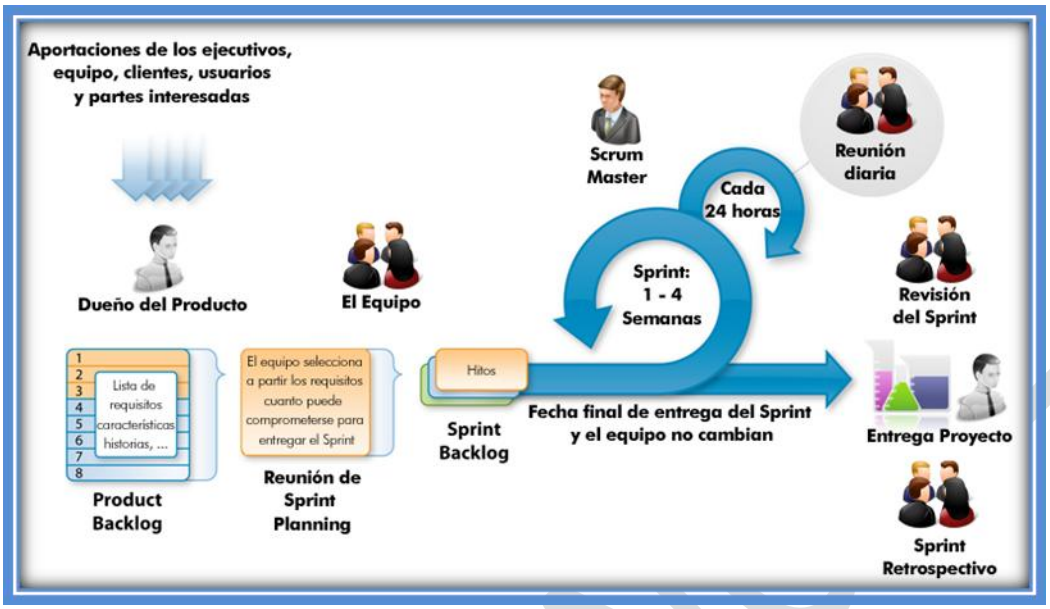

Ilustración No 7 Fuente: http://www.islavisual.com/articulos/desarrollo_web/diferencias-entre-scrum-y-xp.php

SCRUM es un marco de trabajo que se caracteriza por el trabajo en equipo para el desarrollo de proyectos, productos de manera iterativa e incremental.

La estructura SCRUM se basa en trabajos por ciclos llamados Sprint o Iteraciones que se limitan a un tiempo de 4 semanas y se realizan los sprints de forma secuencial.

Para el inicio de cada sprint, el equipo de trabajo elabora una lista de las actividades a realizar por los requerimientos del cliente o del producto, manteniendo el objetivo colectivo para la entrega final del sprint. Cabe recalcar que una vez definido el sprint no se puede adicionar nuevos elementos ya que se pierde el objetivo del mismo. Si se requiere realizar modificaciones se debe colocar en conocimiento al Scrum Master o Lider del Scrum para evaluar la adición del elemento junto al equipo de trabajo y programarse para un nuevo sprint.

El equipo debe reunirse diariamente por espacio muy corto solo para evaluar las actividades realizadas y su progreso con el fin de completar el trabajo sin contratiempos.

Cuando se ha finalizado el sprint, el equipo verifica la lista de requerimientos del producto con lo desarrollado y determinar el logro del objetivo propuesto.

Es importante realizar una retroalimentación al finalizar el ciclo, para así adoptar las mejoras continuas antes de comenzar con un nuevo sprint.

4.2.3 APLICACIÓN DE LA METODOLOGIA SCRUM

La metodología SCRUM es una herramienta que permite ser aplicada a diferentes tipos de proyectos, ya que se encuentra conformada por una estructura que conlleva a la sinergia de trabajo en equipo [1].

El trabajo en equipo en una organización genera entre sus colaboradores un sentido de pertenencia, debido a la participación que tienen dentro de un proyecto y donde sus conocimientos, experiencias, cualidades son aprovechadas al máximo para poder lograr los objetivos propuestos.

En el enfoque de los proyectos de Seguridad de la Información, la metodología SCRUM puede ser aplicada para lograr los pilares de un SGSI que son: Confidencialidad, Integridad y Disponibilidad.

Para su aplicación, se debe definir el Product Owner o Dueño del producto quien establecerá los lineamientos, características del producto solicitado. Tomando como ejemplo de producto o resultado a entregar sería Gestión de riesgos.

Al crear el SCRUM – GESTIÓN DE RIESGOS, se define la persona líder del SCRUM o SCRUM MASTER, quien será el encargado de guiar al Equipo de Trabajo o SCRUM TEAM, donde este grupo de colaboradores serán los responsables de planificar, establecer e implementar Gestión de Riesgos.

Para lo anterior, El SCRUM MASTER debe cumplir dentro sus funciones:

- ✓ Gestionar de manera efectiva la lista de producto o Product backlog.
- ✓ Ayudar al equipo a entender las necesidades con elementos claros.
- ✓ Facilitar y Gestionar las los eventos del SCRUM.
- ✓ Guiar al equipo para que sea auto organizado y multifuncional.
- ✓ Eliminar los impedimentos que se presenten en contra de la evolución y progreso del equipo.
- ✓ Motivar los cambios que permitan su crecimiento.

Adicional, el Equipo de trabajo o SCRUM TEAM deben ser:

- ✓ Auto organizados.
- ✓ Multifuncionales, donde se aproveche como equipo las habilidades de cada integrante.
- ✓ Equitativos con todos los miembros del equipo.
- ✓ Respetuosos y dar valor a los demás colaboradores

Cuando se ha establecido el SCRUM y definido el equipo de trabajo, cuenta con una serie de eventos que permitirán el desarrollo adecuado de las actividades planificadas.

Los eventos de Scrum se clasifican en:

- ✓ El sprint
- ✓ Reunión de planificación de Sprint o Sprint Planning Meeting.
- ✓ Scrum Diario o Daily Scrum.
- ✓ Revisión del Sprint o Review Sprint
- ✓ Retrospectiva de Sprint o Sprint Retrospective

Al consultar en [1], se identifica que cada uno de estos eventos permite desarrollar de manera adecuada y organizada un trabajo en equipo. Adicional, se cuenta con la participación del Product Owner y Scrum Master para el seguimiento del SCRUM, beneficiándose el equipo para poder aclarar las dudas e inquietudes que se presenten durante el Sprint.

De esta buena práctica, se aplica a los demás componentes del proyecto de Seguridad de la Información y el resultado de cada uno de los SCRUM definidos, es lo que conlleva al Sistema de Gestión de Seguridad de la Información.

5. RESULTADOS Y DISCUSIÓN

Como propuesta para la implementación de un Sistema de Gestión de Seguridad de la información – SGSI, hemos establecido como marco de trabajo el "Método SCRUM aplicado al Sistema de Gestión de Seguridad de la Información".

Una vez verificado y analizados cada uno de los componentes de los modelos del SGSI, SCRUM, hemos definido lo siguiente como marco de trabajo para lograr los resultados que conlleven a obtener los objetivos de implementar Seguridad de la Información en una organización.

Ilustración No 8 Resultado Marco de trabajo

5.1 SCRUM SGSI – GESTION ADMINISTRATIVA

La unión de los resultados esperados en cada sprint que componen el Scrum SGSI – Gestión Administrativa, son los que darán las pautas a seguir en cada uno de los SCRUMS y los respectivos sprints que proponemos.

- ✓ Sprint1 - Conceptualización en Seguridad de la información
- ✓ Sprint2 - Análisis actual en seguridad de la información.
- ✓ Sprint3 - Alcance y Límite del SGSI.
- ✓ Sprint4 - Política y Objetivo del SGSI.
- ✓ Sprint5 - Cumplimiento legal y normativo.
- ✓ Sprint6 - Lineamientos para la gestión de recursos.

Este SCRUM en el primero que se debe abordar, que en este se debe contar con la participación de la Dirección de la empresa y el equipo estaría conformado por las Gerencias de Planeación Corporativa, Gerencia Financiera, Jurídica y los demás integrantes de la junta directiva de la organización.

5.2 SCRUM SGSI – GESTION DE ACTIVOS.

La gestión de activos dentro de un SGSI juega un papel muy importante, dado que de ahí se identifican los activos de información que formarán parte del sistema de gestión. El SCRUM estaría comprendido por lo siguiente:

- ✓ Sprint1 - Identificación y Clasificación de Activos.
- ✓ Sprint2 - Valoración de activos.

Para este SCRUM se debe contar con el personal de activos fijos, jefes de área, colaboradores de las áreas que estén al frente del manejo de información, colaboradores del área de planeación corporativa. Si la organización ya cuenta con Gestión de Riesgos, el SCRUM – GESTION DE ACTIVOS y GESTION – DE RIESGOS, tienen un trabajo adelantado y su aporte es muy valioso para el SGSI.

5.3 SCRUM SGSI – GESTION DE RIESGOS.

La gestión de riesgos nos permitirá conocer las vulnerabilidades, amenazas y riesgos al cual se encuentra expuesto los activos de una organización y poder implementar las medidas necesarias para su mitigación. El SCRUM estaría comprendido por lo siguiente:

- ✓ Sprint1 - Análisis y Selección de la metodología de gestión de riesgos.
- ✓ Sprint2 - Identificación de riesgos.
- ✓ Sprint3 - Evaluación y valoración de riesgos.
- ✓ Sprint4 - Plan de tratamiento de riesgo.
- ✓ Sprint5 - Plan de gestión de incidentes.

Como se mencionó en 5.2, si la organización cuenta con Gestión de Riesgos, el desarrollo de este SCRUM se facilita y se puedo lograr realizar una correcta valoración de riesgos abarcando los activos que se identifiquen.

5.4 SCRUM SGSI – GESTION DE RECURSOS HUMANO.

El éxito de una organización para cumplir sus objetivos se debe al recurso humano que se encuentra vinculado a ella. Por ende la importancia y el valor que representa para una organización contar con el personal idóneo para el desarrollo de las actividades diarias y la cultura organizacional que garanticen la gestión del cambio. El SCRUM estaría comprendido por lo siguiente:

- ✓ Sprint1 - Plan de capacitación y sensibilización.
- ✓ Srpint2 - Cultura organizacional y gestión del cambio.
- ✓ Sprint3 - Evaluación de desempeño del recurso humano.

Este SCRUM se debe contar con el Jefe de Gestión Humana, colaboradores de salud ocupacional, profesional de capacitaciones, Gerente Financiero y participación del jefe de seguridad IT.

5.5 SCRUM SGSI – GESTION DE MEJORA CONTINUA.

Para que un SGSI logre la madurez esperada, es necesario que cada uno de sus procesos sean verificados, revisados, analizados y evaluados de forma periódica. Lo anterior permitirá identificar los puntos que deben ser mejorados aplicando las acciones correctivas y preventivas que den a lugar. El SCRUM estaría comprendido por lo siguiente:

- ✓ Sprint1 - Plan de auditoría.
- ✓ Sprint2 - Plan de Seguimiento de acciones correctivas y preventivas.
- ✓ Sprint3 - Formación de auditores internos en SGSI.

Este SCRUM se debe contar con el Jefe de seguridad IT, Jefe de control interno, Representante ante la dirección, grupo de auditores internos y demás profesionales que formen parte de la organización que apoye el SGSI.

5.6 DIAGRAMA DE GANTT

A continuación se propone el siguiente diagrama de Gantt para el desarrollo del SCRUM SGSI en una organización que cuente con un Sistema de Gestión implementado como en el caso de Sistema de Gestión de Calidad, Gestión de Riesgos.

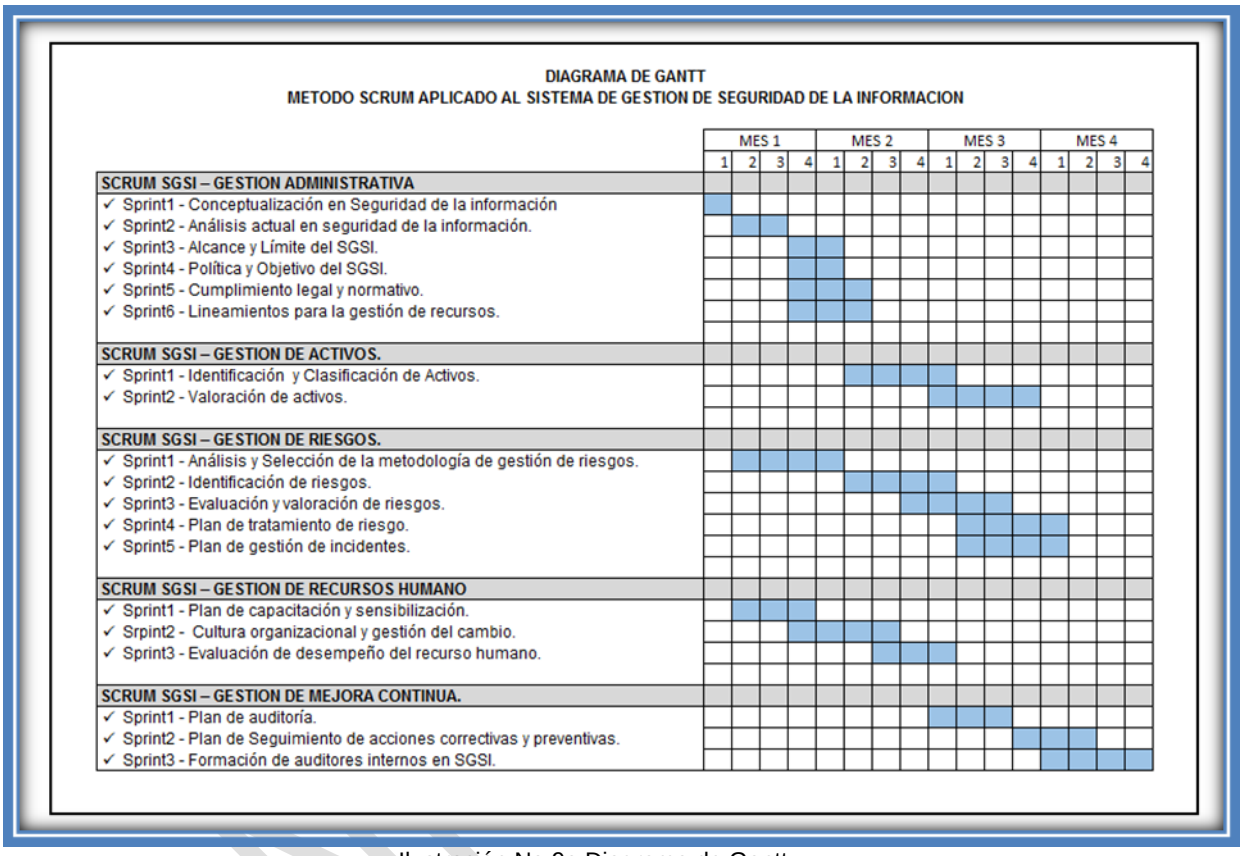

Ilustración No 9a Diagrama de Gantt

Cuando la organización cuenta con temas adelantados como documentación de procesos, identificación de activos, gestión de riesgos, esto conllevaría a que el proceso de establecimiento, implementación, operación, seguimiento, revisión y mejoramiento de SGSI sea llevado en un mejor tiempo.

Para que lo anterior pueda ser aplicado, se debe contar con el compromiso de la Dirección de la organización y de la dedicación, responsabilidad del personal que participa en cada una de estas fases. Otro factor que juega mucha importancia es la cultura organizacional para el trabajo en equipo, ya que por medio de la comprensión, respeto, orientación y la participación constante se puede lograr los objetivos de cada SCRUM.

Los SCRUM SGSI propuestos, se pueden ajustar de acuerdo a las necesidades de las organizaciones, ya que se pueden incluir los SPRINT necesarios para abarcar los temas importantes para una mejor comprensión del SGSI y sus componentes.

La ventaja de los SPRINT es que estos pueden ser de forma secuencial, y solo se puede continuar cuando el SPRINT anterior haya sido culminado. También se puede trabajar en SPRINT de forma paralela siempre y cuando los integrantes y los objetivos de los SPRINT sean diferentes y que a su vez sean las entradas para el siguiente SPRINT.

El dinamismo aplicado en los SPRINT dentro de un SCRUM permite obtener buenos resultados para alcanzar los objetivos propuestos a nivel de SCRUM y a nivel organizacional, de ahí la importancia de contar con el personal adecuado y una buena planificación para realizar el SPRINT.

Lo contrario en las organizaciones donde no exista una implementación de un Sistema de Gestión, los tiempos propuestos para el SCRUM SGSI varían, debido al tiempo invertido para que el recurso humano pueda recibir una capacitación, sensibilización sobre los Sistemas de Gestión, plan que no se encuentra dentro del alcance de este proyecto.

En el siguiente cuadro se expone un tiempo estimado para abordar la implementación de un SGSI sin la aplicación de la metodología SCRUM

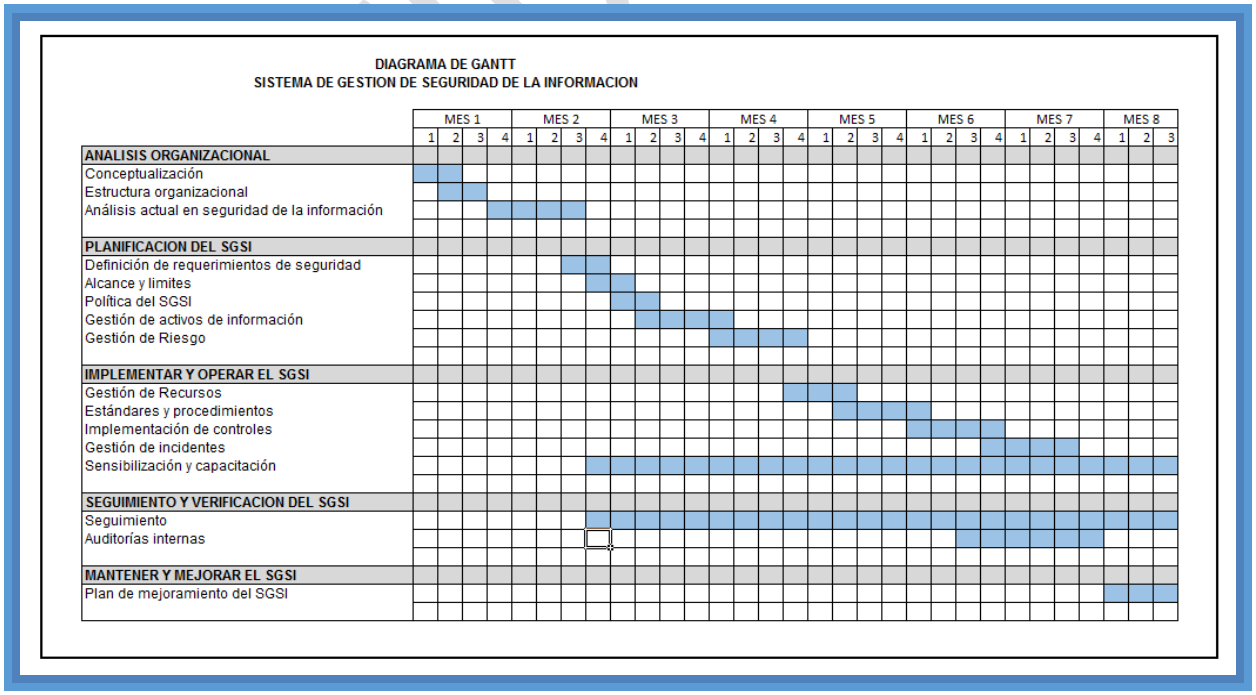

Ilustración No 9b Diagrama de Gantt

Para una organización como se mencionaba anteriormente, el tiempo para implementar un SGSI puede tardar meses, realizándolo etapa por etapa y de forma secuencial. A continuación se suministra un link que permite realizar el cálculo del tiempo estimado en meses bajo la norma ISO 27001

"http://advisera.com/27001academy/es/herramientas/calculador-gratuito-del-tiempo-de-implementacion-para-iso-27001-iso-22301/ [15] "

METODOLOGIA	ISO/IEC 27001	MAGERIT	MEHARI	OCTAVE	SCRUM
DESARROLLO	Presenta 13 procesos desarrollado en 4 bloques.	Presenta 6 elementos fundamentales en su desarrollo.	Dentro de sus procesos integra la norma ISO 27000.	Presenta 9 procesos desarrollados en etapas.	Presenta un desarrollo incremental con entregas frecuentes.
TIEMPO	Requiere tiempo y teniendo él cuenta su desarrollo y número de empleados. 12-24 Meses. Link simulador de tiempo: [15]	Requiere tiempo y según experiencias en su implementación y desarrollo este puede variar. 12-24 Meses.	Requiere tiempo y teniendo en cuenta la integración con otras normas su tiempo puede estar 12-24 Meses	Requiere tiempo y además existe como punto de partida un inventario. 18-24 Meses.	Requiere tiempo y su desarrollo depende de buen trabajo en equipo, ágil y de buenas prácticas, un ejemplo de su tiempo se evidencia en el proyecto.

Ilustración No 9c Cuadro comparativo en Desarrollo y Tiempo.

6. CONCLUSIONES

1. Aplicación de las mejores prácticas en cada una de las áreas y procesos que intervienen en los sistemas de información, siendo estos menos vulnerables y más protegidos ante posibles amenazas.

2. Implementación de nuevos procesos acorde a las funciones y necesidades de la empresa, relacionando cada una de las áreas y personal con los mismos objetivos.

3. A partir del método SCRUM los trabajos e implementaciones de sistemas de seguridad manejan un orden y un proceso de trabajo rápido y eficaz ante las diferentes situaciones.

4. A través del método SRCUM aplicado al sistema de gestión de seguridad de la empresa, se logró establecer u marco de trabajo para lograr obtener los resultados deseados.

5. Existen un mecanismo más detallado y ágil con respecto a la gestión de cada uno de los activos y riesgos de la empresa.

6. Mayor conocimiento y aplicabilidad por parte de cada una de las áreas y del personal encargado de los sistemas de seguridad de la información.

7. Mayor competitividad de la empresa con respecto al mercado laboral y con todo lo concerniente al trabajo ágil y seguro de los sistemas de información.

8. Manejos y control con respecto a los tres pilares más importante de la seguridad de la información: Confidencialidad, integridad y disponibilidad.

9. A pesar de crear unos roles durante el desarrollo de la metodología, siempre existe el trabajo en equipo y el buen rendimiento ágil y de buenas prácticas.

10. Dentro del desarrollo de la metodología SCRUM en los sistemas de seguridad de la información, se denoto la importancia de los resultados con que contara la empresa, evidenciados a través de actas y demás procesos que conllevan a una mejora continua.

7. BIBLIOGRAFÍA

1. SCRUM GUIDES – La Guía de Scrum: http://www.scrumguides.org/docs/scrumguide/v1/Scrum-Guide-ES.pdf.

2. Implementación SIG – Sistemas Integrados de Gestión: http://thinkandsell.com/servicios/consultoria/software-y-sistemas/sistemas-de-gestion-normalizados/

3. ISOTools Excellence - Blog especializado en Sistemas de Gestión de Seguridad de la Información: http://www.pmg-ssi.com/2015/07/que-es-sgsi/

4. QUAC - Asociación española para la calidad: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

5. [6.2.1a] CEREM BUSINESS SCHOOL – Nuevas metodologías para la gestión de proyectos: http://www.cerembs.co/blog/nuevas-metodologias-para-la-gestion-de-proyectos

6. [6.2.1b] PROYECTOS AGILES ORG - Historia de SCRUM: http://proyectosagiles.org/historia-de-scrum/

7. ICONTEC NTC-ISO/IEC 27001 – Norma técnica colombiana Sistema de Gestión de Seguridad de la Información

8. ICONTEC NTC-ISO/IEC 27005 – Norma técnica colombiana Sistema de Gestión de Riesgos en Seguridad de la Información.

9. Politécnico Gran Colombiano – Gestión de seguridad: Principios de la seguridad de la información.

10. Politécnico Gran Colombiano – Análisis de Riesgos: Análisis de Riesgos.

11. Politécnico Gran Colombiano – Teoría de Seguridad: Teoría de Seguridad.

12. http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

13. Gestión de riesgos en la seguridad informática - https://protejete.wordpress.com/gdr_principal/definicion_si/

14. Gerencie: http://www.gerencie.com/ciclo-phva.html

15. http://advisera.com/27001academy/es/herramientas/calculador-gratuito-del-tiempo-de-implementacion-para-iso-27001-iso-22301/

8. ANEXOS

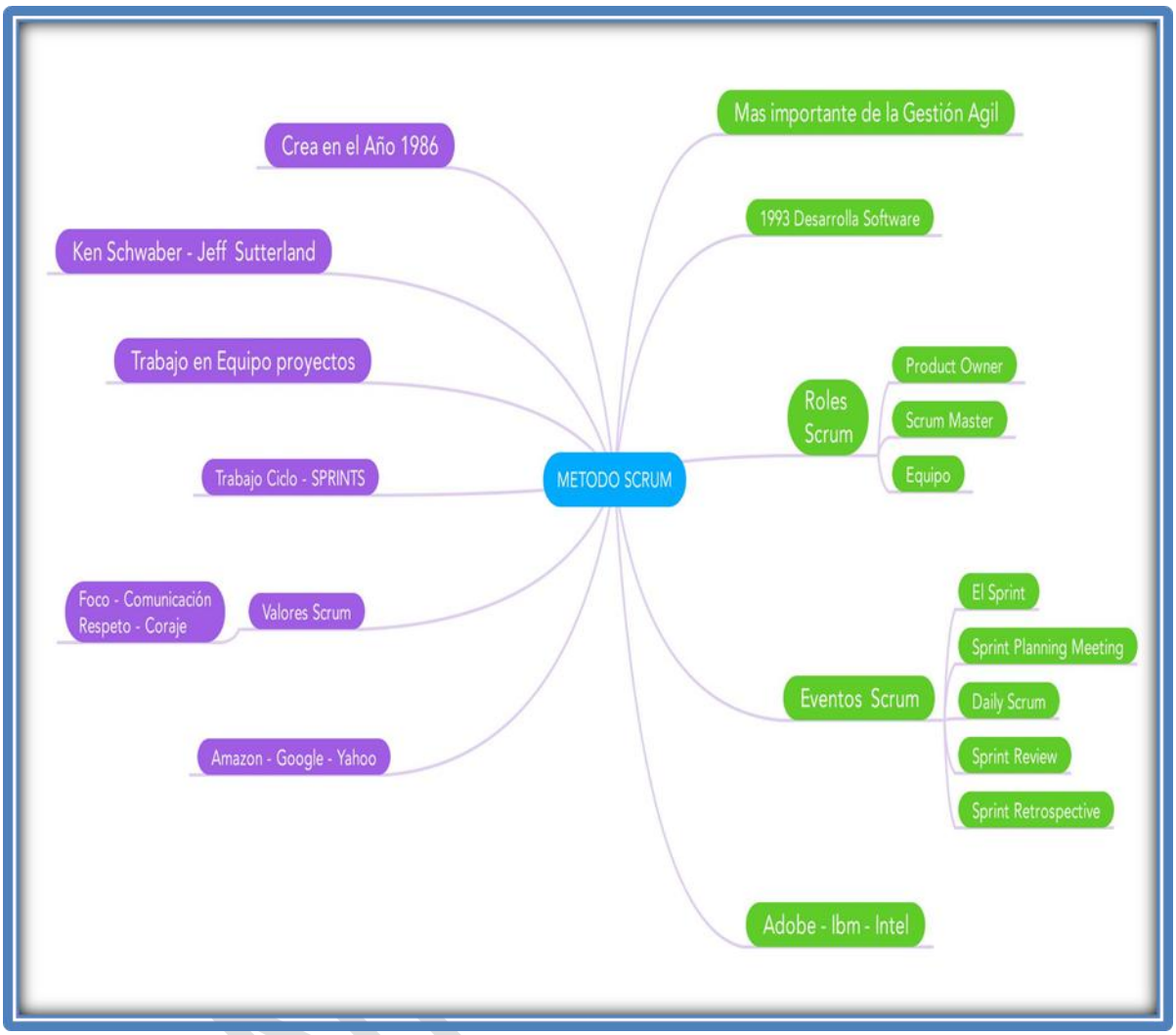

Ilustración No 10 Método SCRUM

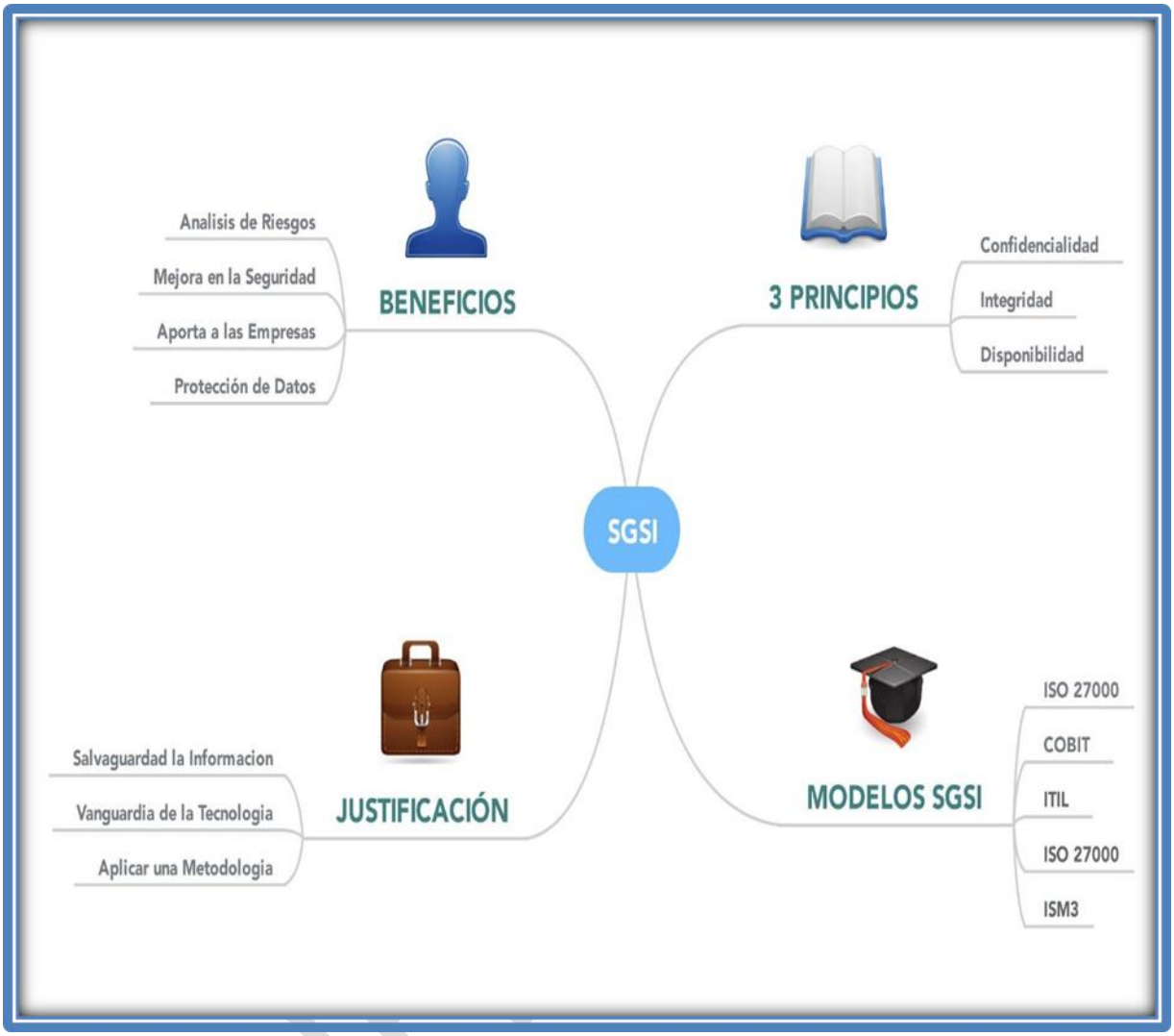

Ilustración No 11 SGSI

8.1 FORMATO LISTA DE PRODUCTO O PRODUCT BACKLOG

PRODUCT BACKLOG
Lista de Producto

Fecha elaboracion: _____
Fecha aprobación: _____
Versión Lista: _____

Producto
Objetivo

REQUERIMIENTOS

ID	Descripción	Estimación tiempo	Orden

_____
Dueño del Producto

Ilustración No 12 Lista de Producto

8.2 FORMATO REUNION DE PLANIFICACIÓN DEL SPRINT O SPRINT PLANNING MEETING

SPRINT PLANNING MEETING
Reunión de Planificación de Sprint

Fecha elaboracion: _____
SCRUM MASTER: _____

Producto
Objetivo

¿Qué puede entregarse en el Incremento resultante del Sprint que comienza?
¿Cómo se conseguirá hacer el trabajo necesario para entregar el Incremento?

_____
SCRUM MASTER

Ilustración No 13 Reunión de Planificación del Sprint

8.3 FORMATO SCRUM DIARIO O SCRUM DAILY

SCRUM DAILY
Scrum Diario

Fecha elaboracion: _____
SPRINT No: _____

Producto
Objetivo

¿Qué actividades se realizó desde la reunión anterior?
¿Qué actividades se realizarán hasta la próxima reunión?
¿Qué inconvenientes se han presentado y que se debe solucionar para poder continuar?

_____
SCRUM MASTER

Ilustración No 14 Scrum Diario

8.4 FORMATO REVISION DEL SPRINT O SPRINT REVIEW

SPRINT REVIEW
Revisión del Sprint

Fecha elaboracion: _____
PRODUCT OWNER _____
SCRUM MASTER _____

Producto
Objetivo

REQUERIMIENTOS

ID	Descripción	% de Cumplimiento	Observación del Equipo	Observación del Producto Owner

PRODUCT OWNER SCRUM MASTER

Ilustración No 15 Revisión del Sprint.