PROPUESTA DE IMPLEMENTACION DE SGSI BASADO EN LA NORMA ISO 27000-1:2013 PARA LA FIRMA DE ABOGADOS ASESORIAS Y CONSULTORIAS JURIDICAS S.A.S

CRISTIAN EDUARDO GARCIA SANCHEZ
(cristian.garcias@campusucc.edu.co)
NICOLAS ESTEBAN FORERO GONZALES
(nicolas.forerog@campusucc.edu.co)
MARÍA FERNANDA BOJACÁ BONILLA
(maria.bojacab@campusucc.edu.co)

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2021

PROPUESTA DE IMPLEMENTACION DE SGSI BASADO EN LA NORMA ISO 27000-1:2013 PARA LA FIRMA DE ABOGADOS ASESORIAS Y CONSULTORIAS JURIDICAS S.A.S

CRISTIAN EDUARDO GARCIA SANCHEZ
(cristian.garcias@campusucc.edu.co)
NICOLAS ESTEBAN FORERO GONZALES
(nicolas.forerog@campusucc.edu.co)
MARÍA FERNANDA BOJACÁ BONILLA
(maria.bojacab@campusucc.edu.co)

INFORME DE SEMINARIO DE GESTION DE PROYECTOS DE TECNOLOGIA
PGTI PARA OPTAR AL TITULO DE: INGENIERÍA ELECTRÓNICA

Yovanny L. Vela Sáenz
Ingeniero de Sistemas con Énfasis en Telecomunicaciones
Director de TI

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍA
INGENIERIA ELECTRÓNICA
BOGOTÁ
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogota (25, 07, 2021) (25-07-2021)

En primeria instancia agradecemos a nuestros formadores por todos los conocimientos que nos han compartido, a nuestras familias, compañeros, nuestros amigos y a Dios.

Por el apoyo suministrado hacia nosotros para cumplir nuestras metas y continuar llegando lejos en lo que nos propongamos.

AGRADECIMIENTOS

Gracias a nuestra universidad, por habernos permitido formarnos, gracias a todas las personas que fueron participantes de este proceso, ya sea de manera directa o indirecta, fueron ustedes los responsables de realizar un pequeño aporte, que el día de hoy se vería reflejado en la culminación de nuestro paso por la universidad. Gracias a nuestros padres.

CONTENIDO

Contenido

1. LISTA DE TABLAS

Pág

2. LISTA DE GRAFICAS

Pág

3. LISTA DE FIGURAS

Pág

4. GLOSARIO

FUGA DE INFORMACIÓN: Se denomina fuga de información al incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma.

RIESGOS: Es la vulnerabilidad o amenaza a que ocurra un evento y sus efectos sean negativos y que alguien o algo puedan verse afectados por él.

AMENAZAS: Es el peligro inminente, que surge, de un hecho o acontecimiento que aún no ha sucedido, pero que de concretarse aquello que se dijo que iba a ocurrir, dicha circunstancia o hecho perjudicará a una o varias personas en particular.

VULNERABILIDADES: puede definirse como la capacidad disminuida de una persona o un grupo de personas para anticiparse, hacer frente y resistir a los efectos de un peligro natural o causado por la actividad humana, y para recuperarse de los mismos.

SEGURIDAD: Se trata de un conjunto de técnicas y procedimientos que tienen como resultado eliminar o disminuir el riesgo de que se produzcan accidentes.

5. RESUMEN

Asesorías y consultorías Jurídicas S.A.S es una firma de abogados que se dedica principalmente a llevar casos legales de propiedad horizontal, se encarga de realizar y presentar demandas ante los juzgados y así mismo a representar a sus clientes, adicional toma casos enfocados al derecho civil, no solo asesorando a sus clientes sino también dando solución a sus peticiones. Se busca realizar una propuesta para ajustar los procesos y de esta manera garantizar la seguridad de estos en el área de tecnologías de la información de la organización por medio del establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO 27001:2013. El proyecto busca contemplar las tareas que se necesitan para el análisis y tratamiento de los riesgos haciendo uso de las fases de la metodología PHVA que incluye Planificar, hacer, verificar y actuar, en coordinación con los objeticos, estrategias y políticas de la organización.

La planeación conlleva la identificación del problema, los objetivos, la factibilidad operativa, técnica, legal y económica que implica el proyecto. Así mismo ver que limitaciones tendría poder realizar el proyecto. Para hacer un enfoque sistemático en el que se establezca, implemente, una operación que se pueda revisar y monitorear para mantener y mejorar la seguridad de la información, para lograr los objetivos comerciales y de servicio.

El objetivo principal de SGSI es proteger la información y para ello se debe identificar los activos de información que deben ser protegidos. Se realiza la gestión de riesgos donde esta el inventario de los activos, la valoración, el análisis de amenaza y valoración de riesgos.

Para finalizar, se genera el análisis y recomendaciones para la implementación del SGSI en la organización Asesorías y consultorías Jurídicas S.A.S.

6. ABSTRACT

Legal Consulting and Consulting SAS is a law firm that is mainly dedicated to taking legal cases of horizontal property, it is in charge of making and filing lawsuits before the courts and also to represent its clients, additionally it takes cases focused on civil law, not only advising their clients but also giving solutions to their requests. It seeks to make a proposal to adjust the processes and in this way guarantee the security of these in the 12nál of information technology of the organization through the establishment 12náli Information Security Management System (ISMS) 12nálisis the ISO 27001: 2013 standard. The 12nálisi seeks to contemplate the tasks that are needed for the 12nálisis and treatment of risks making use of the phases of the PDCA methodology that include Planning, doing, checking and acting, in coordination with the objectives, strategies and policies of the organization.

The planning entails the identification of the 12nálisis, the objectives, the operational, technical, legal and economic feasibility that the 12nálisi implies. Also see what limitations it would have to be able to carry out the 12nálisi. To make a systematic approach that establishes, implements, an operation that can be reviewed and monitored to maintain and improve information security, to achieve business and service objectives.

The main objective of ISMS is to protect the information and for this the information assets that must be protected must be identified. Risk management is carried out where the asset inventory, valuation, threat 12nálisis and risk assessment are located.

Finally, the evaluation and recommendations for the implementation of the ISMS are generated.

PALABRAS CLAVE: PLANIFICAR, ANALIZAR, SERVICIO

7. INTRODUCCION

Asesorías y consultorías jurídicas es una firma de abogados que se encarga de tratar temas legales principalmente de propiedad horizontal, siguiendo casos con juzgados, demandas, entre otros. Adicional se especializa principalmente en derecho civil. Se encarga de llevar casos de sus clientes buscando siempre dar una solución, también se encarga del tema de cartera de los conjuntos residenciales de los que se encuentra a cargo en la parte jurídica.

Al ser una firma de abogados , esta cuenta con información muy personal y clasificada de cada uno de sus clientes por lo que es necesario que la organización implemente un control adecuado con el que actualmente no cuenta, para que garantice la confianza de resguardar la integridad y total seguridad de la información y que avale una disponibilidad y la exactitud en el tratamiento de la información, para brindar una protección que es necesaria en el manejo de los datos de clientes, empleados, socios comerciales y la sociedad en general.

Esta propuesta radica en tratar de dar solución a la falta de seguridad en el tratamiento de la información, buscando dar un control que sobreguarda la integridad, disponibilidad, confidencialidad de sus clientes, a través de la implementación de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001:2013, de esta manera proponer una posible solución que responda a los requerimientos de seguridad adecuados aplicando prácticas, valorando riesgos y los procedimientos de gestión utilizados en el modelo PHVA (planificar, hacer, verificar y actuar).

8. ALCANCE

Se pretende analizar los procesos relacionados a la seguridad de la información que se puedan implementar en Asesorías y consultorías Jurídicas S.A.S, para poder establecer un sistema de gestión de seguridad de la información, de forma que la compañía pueda cumplir con los estándares que integran los principios de SGSI.

La dirección de la empresa contará con una documentación necesaria para poder iniciar con el establecimiento del SGSI, especificando lo necesario para establecer, mantener y mejorar el sistema de gestión de seguridad de la información, utilizando como guía la norma ISO-IEC 27001:2013

Se podría establecer los siguiente:
-Informe de vulnerabilidades de la información en la entidad
-Informe de evaluación de posibles riesgos
-Documento de las políticas de seguridad donde se especifique los hallazgos encontrados
-Documentación de las recomendaciones, donde Asesorías y consultorías Jurídicas S.A.S pueda estar preparada para los procesos de evaluación, auditoria, certificación o acreditación correspondiente a la seguridad e integridad de los datos de la empresa

Limitaciones
-Disponibilidad de tiempo por parte de la organización en la implementación de todos requerimientos disponibles
-Veracidad e integridad de todos los datos de acción en los que se puedan hacer las implementaciones en la organización con respecto al tratamiento de datos de los usuarios.

9. OBJETIVOS

9.1 OBJETIVO GENERAL

Formular y evaluar las políticas que se propongan, los mínimos requerimientos de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013 para el área de tratamiento de datos en la empresa Asesorías y Consultorías Jurídicas S.A.S.

9.2 OBJETIVOS ESPECÍFICOS

Identificar las falencias en los procesos de mejora continua en el control y la planificación con la cantidad de cambios que se puedan generar a última hora y poder trabajar de manera ágil en base en el modelo scrum.

Diseñar las políticas, controles de los planes de mejoramiento que sean necesarios en la minimización y mitigación de la probabilidad de impactos y riesgos identificados en la seguridad de la información.

Evaluar la viabilidad de mejora de la empresa si decide implementar la propuesta de sistemas de gestión de seguridad de la información (SGSI).

10. PLANTEAMIENTO DEL PROBLEMA

10.1 DEFINICIÓN DEL PROBLEMA

Dentro de los compromisos y políticas de la empresa, está establecido el ofrecer confidencialidad en el manejo de la información de los clientes dentro y fuera de la compañía y el cumplimiento de estándares de calidad para poder brindar un buen servicio.

La firma de abogados Asesorías y Consultorías Jurídicas S.A.S está en busca de una forma de implementar un sistema de seguridad de la información en donde pueda evitar situaciones de riesgo tales como la fuga de información que genere peligro en la confidencialidad, la integridad, la disponibilidad en la compañía, la dificultad de administrar y gestionar la enorme cantidad de datos que maneja.

En base a la problemática generada en la empresa, es fundamental realizar un análisis de riesgo e identificar la seguridad con la que cuenta actualmente, ya que la información que maneja la empresa es un activo muy valioso, por este motivo es primordial el aseguramiento de la empresa, implementando el uso de herramientas que ayuden en la protección de la seguridad de la información ya que una vez que esta caiga en la manos equivocadas podrían causar daños en la imagen, credibilidad de la empresa y así mismo afectar enormemente a los clientes.

10.2 JUSTIFICACIÓN

La seguridad de la información es un componente que, hoy en día se ha vuelto una pieza clave en las organizaciones debido a los avances tecnológicos que vienen acompañados de riesgos internos y externos en las empresas.

La implementación de un sistema de gestión de seguridad de la información (SGSI), establecerá en la firma de abogados Asesorías y Consultorías Jurídicas S.A.S, los controles adecuados para el aseguramiento de información, confiablidad, disponibilidad, defendiendo toda la información que maneje la empresa, ya sea de esta misma o de sus clientes. En base a el cumplimiento de la norma ISO 27001:2013, en donde se encuentran todas las políticas, objetivos y controles que se deben llevar a cabo para lograr una excelente mejora en las diferentes áreas de la organización que manipulen información importante, ser más eficiente, segura, ágil y organizada a la hora de hacer uso de la información que disponga la empresa.

Por medio de la metodología scrum, se busca establecer una previa identificación de datos para lograr hacer una correcta integración de estos para conseguir una correcta visión, diseño, implementación, operación, seguimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

Es de suma importancia que la firma de abogados Asesorías y Consultorías Jurídicas S.A.S considere implementar la propuesta del sistema de gestión de seguridad de la información en base a el estudio del análisis de riesgo e identificación de la seguridad con la que cuenta actualmente la organización, ya que no cuenta con los controles de seguridad necesarios para evitar complicaciones de fugas de información en la organización.

11. MARCO TEÓRICO

En esta sección se encuentran palabras importantes para entender el proyecto que se llevara a cabo, con sus respectivas definiciones para obtener claridad en diferentes aspectos sobre el tema tratado.

- **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*".

- **Información:** "*Conjunto de dato organizado, procesado, almacenado*".

- **Seguridad de la información:** *"La Gestión de la Seguridad es una necesidad que adquiere un carácter estratégico para la protección de la información y aplica a todos los activos de información y tecnologías de soporte a través de la identificación de los riesgos corporativos analizándolos y estableciendo medidas adecuadas para su control".*

- **SGSI – Sistema de Gestión de Seguridad de la Información:** *"consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales"*.

- **Confidencialidad:** **"***Propiedad que determina que la información no se encuentre disponible ni sea expuesta a individuos, entidades o procesos no autorizados***".**

- **Disponibilidad:** ***"****Medio de garantizar que la información se accesible cuando sea necesaria y utilizable por solicitud de un ente autorizado"*

- **Integridad:" Esta** *propiedad garantiza la autenticidad de los datos en datos y de la información".*

- **Activo:** *"Es un recurso del sistema de la información, sumamente necesario ya que sin este afectaría en gran manera el funcionamiento de los procesos y objetivos de la organización".*

- **Riesgo:** *“El riesgo se encarga de considerar las probabilidades de que una amenaza se materialice sobre los activos de la organización, ocasionando efectos negativos o pérdidas”.*

- **Análisis de riesgo:** “*Uso metódico de la información para la identificación de las fuentes y estimación de riesgos”.*

- **Amenaza:** *“Es el peligro a el que se encuentra expuesto algún activo de la organización”.*

- **Vulnerabilidad:** *“Es una la probabilidad de que una amenaza se lleve a cabo sobre algún activo de la organización y pueda ser usado para generar algún daño”.*

- **Gestión de riesgo: “**Son las actividades para dirigir y controlar una organización con relación al riesgo que puede llegar a presentar**”.**

- **Gestión de activos de información:** *“Es usado para identificar y clasificar los activos de información en una organización”.*

- **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”.*

- **NIST 800-30:** “*Es una metodología de gestión de riesgos de seguridad de la información*”.
- **SCRUM:** Es una metodología donde se aplican las buenas prácticas para el trabajo colaborativo y en equipo, que permite obtener mejores resultados de un proyecto.

- **SCRUM MASTER:** Persona conocedora de un proceso y su liderazgo debe estar al servicio del Equipo Scrum (Scrum Team).

- **EQUIPO SCRUM (SCRUM TEAM):** Equipo de trabajo que es auto organizado y multifuncional para llevar a cabo la planificación del Sprint (Sprint Planning).

- **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.

- **SPRINT:** Corresponde al periodo o bloque de tiempo (time-box) en el cual se debe desarrollar el trabajo.

- **SCRUM DIARIO (SCRUM DAILY):** Corresponde a una reunión de corto tiempo de cada día del sprint para revisar el estado de un proyecto.

- **REVISION DEL SPRINT (SPRINT REVIEW):** Es una reunión que tiene como objetivo verificar lo ejecutado del sprint planning.

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

- **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.

- ***ISO 27001.*** Se conoce como una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

  La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2(«¿Qué es norma ISO 27001?», s. f.). La importancia y reconocimiento de la norma ISO 27001 en materia de seguridad de los sistemas de información permite establecer el estándar a aplicar, documentación y procedimientos a seguir de acuerdo con la evaluación de seguridad que se realice.

  Unas de las razones por la cuales de usa la ISO 27001 como guía, es que otorga beneficios como lo son:

- Reduce los riesgos riesgo que pueden producir pérdidas de información en las organizaciones. Por pérdidas también entendemos robos y corrupciones en la manipulación de esta.
- Se implementa una revisión continua de los riesgos a los que están expuestos los clientes. Además de esto, se realizan controles de manera periódica.

- Establece una metodología gracias a la cual se puede gestionar la seguridad de la información de forma clara y concisa.
- Establece medidas de seguridad para que los clientes puedan acceder a la información.
- Permite a las empresas continuar con la operación con normalidad en caso de que se produzca algún problema.
- El contar con un SGSI que ofrece la garantía a los clientes y socios de que la organización se preocupa por la confidencialidad y la seguridad de la información que maneja la empresa.

- **Sistema de gestión de seguridad de la información**

Un SGSI radica en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades que son administrados por una organización, en búsqueda de proteger sus activos de riesgo que puedan presentarse.

Para poder implementar un SGSI, se debe tener en cuenta el estándar ISO 27001:2013.

Ya que con esta norma se puede generar un enfoque sistemático para implementar, establecer, operar, monitorear, revisar, mantener, y mejorar la seguridad de la información de una organización y lograr cumplir los objetivos comerciales y de servicio de una manera más eficiente.

Los principios que se busca dar protección están definidos de la siguiente manera:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. Es necesario acceder a la información mediante autorización y control.

- **Integridad**: se debe mantener la exactitud y completitud de la información y sus métodos de proceso. Su objetivo es prevenir modificaciones no autorizadas de la información.

- **Disponibilidad**: Garantizar el acceso y la utilización de la información y los sistemas de tratamiento de esta, por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Su objetivo es prevenir interrupciones no autorizadas de los recursos informáticos.

Figura No 1. Principios SGSI

Fuente: https://lh5.googleusercontent.com/6Jo8b2Z8YV9OmWMcW3N9JvkP19vWRhOajtChbaNFCKgUUAUpjGsMx8Xek89BwPD9a3HUG00adiDEovkwNqwARPiQKml9891iYyaKU50rH2D-7aBjz6d3kuQ-d0Nwiw

- **Componentes principales de un sistema de gestión de la seguridad de la información**

Dentro de los componentes se encuentran diferentes formas de implementar la seguridad de la información entre ellas están:

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

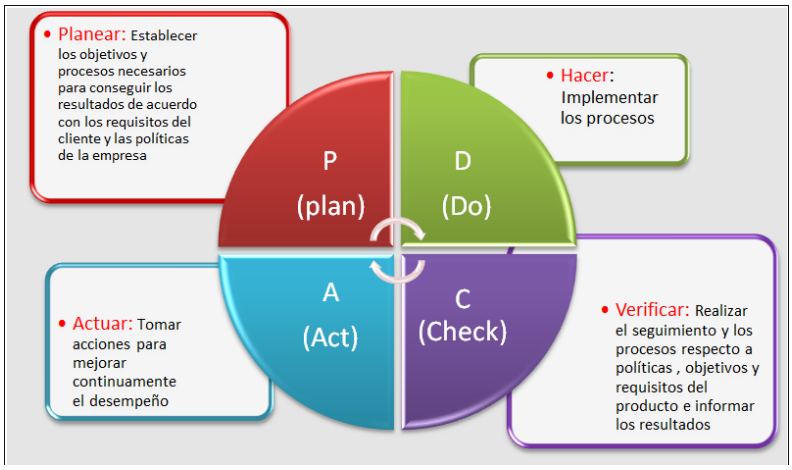


Figura No 2. Ciclo Deming
Fuente: https://comunidad.iebschool.com/universoagile/files/2014/11/Circulo-de-DEMING.png

- **Visión general de la metodología scrum**

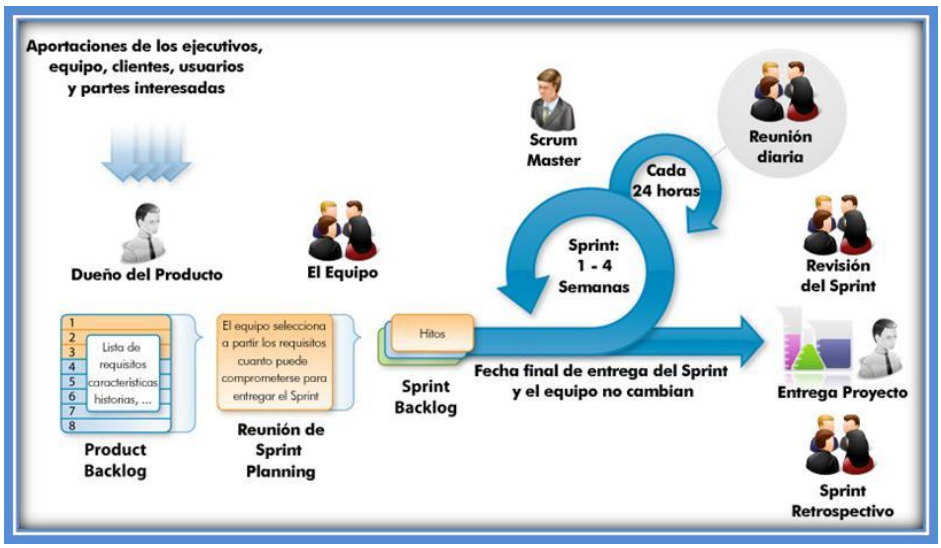


Figura No 3. Visión general de Scrum http://www.islavisual.com/articulos/desarrollo_web/diferencias-entre-scrum-y-xp.php

SCRUM hace referencia a un marco de trabajo donde su carácter se basa en el trabajo en equipo con el desarrollo de proyectos.

La estructura SCRUM se realiza en ciclos de trabajo llamados Sprint o iteraciones que están limitadas generalmente a 4 semanas y los sprints son secuenciales

Por cada inicio de un sprint, se elabora por equipo de trabajo, un listado de las actividades que se van a realizar seguir los requerimientos del cliente o del producto, manteniendo el objetivo colectivo para la entrega final del sprint. Recalcando que una vez iniciado un sprint no se le pueden adicionar nuevos elementos ya que

cambiaría el objetivo, si se desean realizar modificaciones se debe informar al scrum Máster o líder del scrum donde evaluaran la adición del elemento junto al equipo de trabajo para programar 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.

- **Aplicación de la metodología 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.

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 MÁSTER, 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 MÁSTER 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 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 Máster 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.

- **Beneficios que aportaría la implementación del SGSI:**

  - 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.

- **Estructura de la norma ISO 27001**

1. Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.

2. Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de **ISO27001**.

3. Términos y Definiciones: Describe la terminología aplicable a este estándar.

4. Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del **SGSI**.

5. Liderazgo: Esta sección resalta la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar

una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.

6. Planificación: Esta es una sección que da visibilidad a la importancia de la determinación de riesgos y oportunidades a la hora de planificar un **Sistema de Gestión de Seguridad de la Información**, así como de establecer objetivos de **Seguridad de la Información** y el modo de lograrlos.

7. Soporte: En esta cláusula la norma señala que para el buen funcionamiento del **SGSI** la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.

8. Operación: Para cumplir con los requisitos de **Seguridad de la Información**, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la **Seguridad de la Información** y un tratamiento de ellos.

9. Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del **Sistema de Gestión de Seguridad de la Información**, para asegurar que funciona según lo planificado.

10. Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del **SGSI**.

Figura No 4. Estructura ISO 27001
Fuente:
https://s3.amazonaws.com/s3.timetoast.com/public/uploads/photo/11954207/image/53acbda2564159fdf6fdd2879d006091

12. METODOLOGIA

Como metodología en el plan de implementación del
SGSI se acuerda trabajar con Scrum, la cual implementa el Proceso de
Gestión de Riesgos dentro de un marco de trabajo para que los organismos de gobierno puedan tomar decisiones teniendo en cuenta los riesgos derivados del uso de TI". En el Scrum se presenta los siguientes objetivos:
Directos:
1-Asignación y manejo de plazos para cada sprint (pueden ser un día, una semana, un mes o lo que se establezca).
2-Elección de las herramientas de análisis para evaluar cada uno de ellos.
Sincronización de las actividades de cada miembro del equipo y monitoreo de cada una de ellas a fin de cumplir los objetivos asignados.
3-Análisis del desarrollo del proyecto: saber qué sucede con los problemas, riesgos, falta de recursos, entre otros detalles.
4-Revisión del proyecto: se estudia y evalúa qué aspectos cambiar, mejorar o eliminar para que los siguientes sprints sean más efectivos y ágiles.
5-Retrospectiva: repetir los análisis anteriores para pulir el proceso de trabajo y disminuir la cantidad de cambios.

Adicionalmente con el mismo acondicionamiento de la estructura de la seguridad de la información conforme al marco de referencia con la metodología Scrum

Con la metodología scrum, se busca identificar cada una de sus fases que permitan su aplicación a cada uno de sus componentes de SGSI
Con una previa identificación de datos para lograr hacer una correcta integración de estos para obtener una correcta visión, diseño, implementación, operación, seguimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

13. DESARROLLO DEL PROYECTO

Para la implementación de un sistema de gestión de seguridad de la información en la empresa Asesorías y consultorías Jurídicas S.A.S, se elaboró un análisis de los componentes de un SGSI Y de SCRUM, en dónde se organizó un marco de trabajo (Backlog) que cumpla con los objetivos de la implementación de un sistema de gestión de la seguridad de la información.

Figura No 5. Marco de trabajo

Fuente: Elaboración propia

BENEFICIO DE LA IMPLEMENTACION DE UN SGSI

Teniendo en cuenta las necesidades de la organización a la que se le implementa la propuesta del SGSI, se elabora una gestión de la seguridad por medio de esta se identifica y valora los riesgos presentes en la compañía, con el fin de implementar medidas, procesos y operaciones que ayuden a generar el adecuado control y se pueda generar una mejora continua en la empresa.

13.1 SCRUM SGSI – PRODUCT BACKLOG

En el estudio realizado, se estableció el siguiente backlog en donde se tendría previsto el cumplimiento de la norma ISO 27001:2013.

Tabla 1. PRODUCT BACKLOG

Ítem		estimación (Horas)
1	GESTIÓN ADMINISTRATIVA.	27
2	GESTION DE ACTIVOS.	27
3	GESTION DE RIESGOS.	27
4	GESTION DE RECURSOS HUMANO.	27
5	GESTION DE MEJORA CONTINUA.	27
	Total	135

Fuente: Fuente propia

13.2 SCRUM SGSI – GESTIÓN ADMINISTRATIVA

Para la elaboración del aspecto de Gestión Administrativa se elaboró el siguiente Sprint con la participación de la empresa Asesorías y consultorías Jurídicas S.A.S, para así obtener la información necesaria para poder conocer la situación en la que se encuentra actualmente.

Tabla 2. GESTIÓN ADMINISTRATIVA.

SPRINT 1	GESTIÓN ADMINISTRATIVA.	
ITEM	Descripción	Estimado (horas)
1	Conceptualización en Seguridad de la información	5
2	Análisis actual en seguridad de la información.	5
3	Alcance del SGSI, cumplimiento legal y normativo.	7
4	Política y Objetivo del SGSI.	5
5	Lineamientos para la gestión de recursos.	5
	Total	27

Fuente: Fuente propia

13.3 SCRUM SGSI – GESTIÓN DE ACTIVOS

Se realiza la gestión de activos en la empresa ya que es un papel muy importante, por que se identifica los activos de información con los que cuenta la empresa y formaran parte del sistema de gestión.

Tabla 3. GESTIÓN DE ACTIVOS.

SPRINT 2	GESTION DE ACTIVOS.	
ITEM	Descripción	Estimado (horas)
1	Identificación y Clasificación de Activos.	14
2	Valoración de activos.	13
	Total	27

Fuente: Fuente propia

13.4 SCRUM SGSI – GESTIÓN DE RIESGOS

En la gestión de riesgo se permitirá conocer las falencias, vulnerabilidades y amenazas que se encuentren presentes en la organización y las contramedidas que pueden ayudar a evitar estos riesgos.

Tabla 4. GESTIÓN DE RIESGOS.

SPRINT 3	GESTION DE RIESGOS.	
ITEM	Descripción	Estimado (horas)
1	Análisis y Selección de la metodología de gestión de riesgos.	6
2	Identificación de riesgos.	5
3	Evaluación y valoración de riesgos.	5
4	Plan de tratamiento de riesgo.	6
5	Plan de gestión de incidentes.	5
	Total	27

Fuente: Fuente propia

13.5 SCRUM SGSI – GESTIÓN DE RECURSOS HUMANOS

Para lograr los objetivos que tienen previstos en la organización, el recurso humano es uno de los puntos más importantes que tienen la empresa, por lo tanto, contar con personal capaz en el desarrollo de las actividades establecidas en la empresa, garantiza la mejora continua en la organización.

Tabla 5. GESTIÓN DE RECURSOS HUMANOS.

SPRINT 4	GESTION DE RECURSOS HUMANOS.	
ITEM	Descripción	Estimado (horas)
1	Plan de capacitación y sensibilización.	10
2	Cultura organizacional y gestión del cambio.	7
3	Evaluación de desempeño del recurso humano.	10
	Total	27

Fuente: Fuente propia

13.6 SCRUM SGSI – GESTIÓN DE MEJORA CONTINUA

Para obtener un SGSI funcional, es necesario que se realice una verificación, análisis y evaluación de forma periódica a los procesos implementados en el sistema de gestión de seguridad de la información, para identificar las falencias que tenga el SGSI y poder realizar mejoras en el proceso.

Tabla 6. GESTIÓN DE MEJORA CONTINUA.

SPRINT 5	GESTION DE MEJORA CONTINUA.	
ITEM	Descripción	Estimado (horas)
1	Plan de auditoría.	8
2	Plan de Seguimiento de acciones correctivas y preventivas.	7
3	Formación de auditores internos en SGSI.	12
	Total	27

Fuente: Fuente propia

Grafica 1: Gestión

Fuente: Fuente propia

14. CRONOGRAMA

Teniendo en cuenta los tiempos programados para cada sprint, se establece un cronograma de fechas en el que se realizaran los diferentes sprint teniendo en cuenta las horas en que se elabora cada ítem que compone cada sprint.

Tabla 7. CRONOGRAMA

Sprint	Horas	Fecha inicio	Fecha final
1	27	1/11/2021	3/11/2021
2	27	4/11/2021	8/11/2021
3	27	9/11/2021	11/11/2021
4	27	12/11/2021	16/11/2021
5	27	17/11/2021	19/11/2021

Fuente: Fuente propia

15. GESTION FINANCIERA.

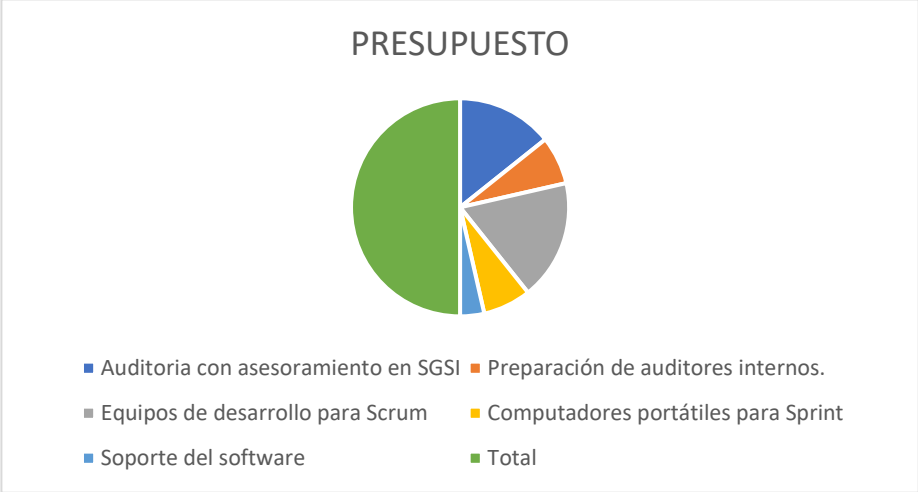
Se tiene como objetivo dar un eso adecuado y rentable a los servicios para la implementación del sistema SGSI incluyendo el modelo Scrum. Se considera un presupuesto aproximado a 14.000.000, el cual será asignado al desarrollo del proceso.

Tabla 8. GESTION FINANCIERA.

	GESTION FINANCIERA.	
ITEM	DESCRIPCCIÓN	PRESUPUESTO
1	Auditoria con asesoramiento en SGSI	4.000.000
2	Preparación de auditores internos.	2.000.000
3	Equipos de desarrollo para Scrum	5.000.000
4	Computadores portátiles para Sprint	2.000.000
5	Soporte del software	1.000.000
	Total	14.000.000

Fuente: Fuente propia

Grafica 2: Gestión Financiera



Fuente: Fuente propia

16. CONCLUCIONES Y RECOMENDACIONES.

-La empresa contará con un sistema de seguridad SGSI para dar mas fiabilidad de confidencialidad a los datos de sus clientes y procesos.

-La seguridad de la información es un aspecto que debe ser parte de la cultura organizacional, es inherente que las actividades de parte humana ya sea con cursos, seminarios y talleres no bastan, hay que profundizar en las personas de la organización, la necesidad y beneficios de dicha cultura estratégica, así como los riesgos de no tenerla.

-En el estudio realizado de los activos con los que cuenta la empresa, se debería efectuar un modelo de control que ayude a minimizar en gran manera el riesgo constante al que se ve afectados los activos de información con los que cuenta la organización.

-Una empresa que pueda implantar un SGSI, estará cumpliendo con los estándares internacionales logrando certificar sus procesos de seguridad debido a que identifico, gestiono y minimizo los riesgos que posee la seguridad de la información.

BIBLIOGRAFÍA

- Iso27000.es
  https://www.iso27000.es/sgsi.html

- Sistemas de Gestión Normalizados
  https://thinkandsell.com/servicios/consultoria/software-y-sistemas/sistemas-de-gestion-normalizados/

- https://conceptodefinicion.de/confidencialidad/

- Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad,1 febrero, 2018, obtenido de: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

- Belkis Echemendía Tocabens, Rev Cubana Hig Epidemiol vol.49 no.3 Ciudad de la Habana sep.-dic. 2011, Definiciones acerca del riesgo y sus implicaciones, obtenido de: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1561-30032011000300014

- Conceptos de amenazas, vulnerabilidad y riesgo. https://www.tdx.cat/bitstream/handle/10803/6219/04Capitulo2.PDF?sequence=4&isAllowed=y

- https://advisera.com/27001academy/es/que-es-iso-27001/
- Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001 obtenido de: https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf
- https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/
- https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

- Henares, J. S. (2016). Elaboración de un plan de implementación de

la ISO/IEC 27001:2013 en un ayuntamiento. Recuperado a partir de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/45704/7/jturhTFM0116 memoria.pdf

- Ministerio de Hacienda y Administraciones Públicas. versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado a partir de 2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8%20(1).pdf
- Luis Gómez Fernández y Pedro Pablo Fernández Rivero. Edición 2018. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. PUB_DOC_Tabla_AEN_12450_1.pdf
- La norma ISO 27001: Aspectos claves de su diseño e implantación. https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf
- Flávia Estélia Silva Coelho Luiz Geraldo Segadas de Araújo Edson Kowask Bezerra. Gestión de la seguridad de la información. https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf
- Ana Andrés y Luis Gómez. 2009. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. http://www.varios.cen7dias.es/documentos/documentos/90/iso.pdf
- Henrik Kniberg. SCRUM Y XP DESDE LAS TRINCHERAS. http://www.proyectalis.com/wp-content/uploads/2008/02/scrum-y-xp-desde-las-trincheras.pdf
- Juan Palacio. Octubre – 2008. Flexibilidad con Scrum. https://www.scrummanager.net/files/flexibilidad_con_scrum.pdf