RESUMEN EJECUTIVO

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

Empresa Textilera S.A

Junio 2016

Estudiante

Paula Andrea Maya Arango

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Área: Sistemas de Gestión de la Seguridad de la Información

Consultor: Antonio José Segovia

Profesor responsable de la asignatura: Carles Garrigues Olivella

Centro: Universitat Oberta de Catalunya

Fases del proyecto

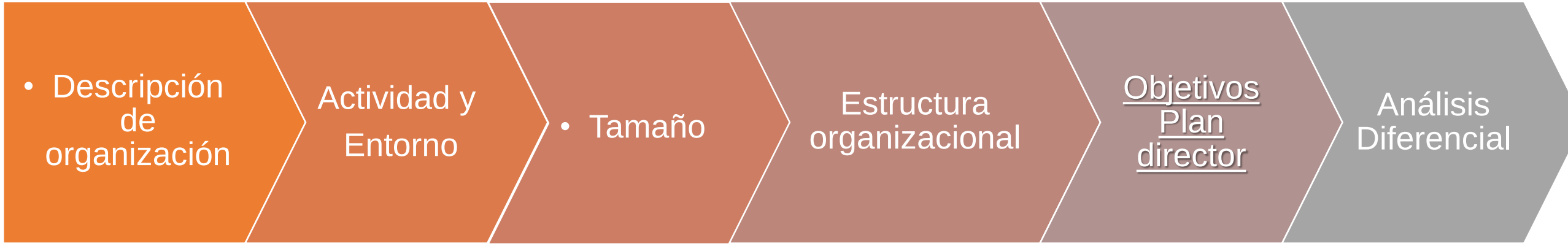
El proyecto plantea la implementación de un SGSI (Sistema de Gestión de la seguridad de la información). Para ello se abordaran las siguientes fases:

- Fase 1: Definición clara de la situación actual y los objetivos del SGSI.
- Fase 2: Esquema documental
- Fase 3:Analisis de Riesgos
  - Identificación y valoración de activos como punto de partida
  - Identificación de amenazas, evaluación y clasificación de las mismas.
- Fase 4:Propuesta de proyectos para conseguir una adecuada gestión de seguridad
- Fase 5:Evaluacion de nivel de cumplimiento de ISO/IEC 27001:2013
- Fase 6:Presentacion de Informes.

Fase 1. Situación Actual

- **Descripción de la organización**: la empresa Textilera S.A, es una empresa ubicada en el municipio de Girardota, a 28 kilómetros de la ciudad de Medellín, Colombia. Dedicada a la industria Textil.
- **Actividad y Entorno:** Se produce y comercializa polímeros y fibras químicas de Poliéster y Nylon, materias primas para la industria, en forma de gránulos, fibras, filamentos textiles e industriales y lona para llantas. Actualmente, se ha convertido en el mayor fabricante de fibras sintéticas del Grupo Andino, ampliando su oferta de productos, atendiendo también a la industria química y del plástico.
- **Tamaño:** Textil S.A es una empresa con dos sedes una en el poblado y otra en Girardota y cuenta con 1600 empleados.
- **Estructura Organizacional:** La compañía cuenta con un presidente y las vicepresidencias de : Gestión humana, producción, ventas y Administrativa y Financiera. Cada Vicepresidencia cuenta a su vez con Divisiones y estas con áreas especializadas.

Fase 1. Situación Actual



Objetivos del plan director:

Objetivo General: Planear, diseñar y recomendar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) enfocado a los procesos de las áreas de: División informática, control interno, administración servicios al personal, seguridad física en Textilera S.A

Objetivos Específicos:

- Identificar el estado actual de los procesos existentes en el área de TI, control interno: en cuanto a administración de pólizas, manejo de activos, manejo de contratistas. administración servicios al personal: proceso de contratación. Seguridad física: control de acceso.
- Establecer controles para minimizar los riesgos significativos y de alto impacto para el negocio, como el robo o fuga de información, accesos no autorizados, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial, la alteración o modificación de la misma, y en general la continuidad de las operaciones.
- Establecer la brecha de seguridad entre los procesos y el SGSI bajo la norma ISO27001:2013.
- Establecer claramente al interior de la compañía los roles y responsabilidades en términos de seguridad de la Información.
- Desarrollar y mantener una cultura en seguridad de la Información orientada a la identificación y análisis de riesgos, a través de la sensibilización a los funcionarios y contratistas.
- Realizar un análisis diferencial del estado actual de seguridad de los activos de la compañía, versus el cumplimiento de la norma ISO/IEC 27001 e ISO/IEC 27002, para que a partir de este análisis se identifiquen los recursos necesarios y se puedan establecer los planes de trabajo con el fin de cumplir la norma.

Fase 1. Situación Actual

- Descripción de organización
- Actividad y Entorno
- Tamaño
- Estructura organizacional
- Objetivos Plan director
- Análisis Diferencial

Análisis Diferencial

- Teniendo como base está definición de la norma ISO 27001:2013, este trabajo estará enfocado en analizar todos los controles y requerimientos de seguridad
- Los hallazgos descritos , son resultados del análisis de las medidas de seguridad y la normativa que tiene la organización en relación a la seguridad de la información.
- Esta verificación se centró en la revisión de los diferentes controles de las áreas del alcance.
- Se agrega un valor a cada control en base al estado en el que se encuentra:
  - No esta implementado = 0
  - Esta parcialmente implementado = 1
  - Esta casi completamente implementado = 2
  - Completamente implementado = 3

EL documento base es el Anexo: Análisis Hoja de Verificacion.xlsx

Fase 2. Sistema Gestión Documental

Política de seguridad de la información

- Se describirá la política de seguridad de la información de la organización: Para la organización la seguridad de la información de los sistemas que se gestionan y/o operan es de vital importancia y se protegerá de cualquier pérdida en su confidencialidad, integridad y disponibilidad.
- Textilera S.A, ha definido la política institucional y una serie de políticas específicas de seguridad de la información, las cuales hacen parte del SGSI y se encuentra en documentos anexos. *Ver anexo: PW-15-007 Política de seguridad de la información .doc*

Documentación del SGSI

- Como parte de la documentación del Sistema de Gestión de Seguridad de la Información, tenemos entre otros los siguientes documentos considerados procedimientos de seguridad

- Procedimientos de Auditorías Internas
- Gestión de Indicadores
- Procedimiento de Revisión por la Dirección
- Gestión de Roles y Responsabilidades
- Metodología de Análisis de Riesgos

Declaración de Aplicabilidad

- En el documento anexo de declaración de aplicabilidad esta la tabla con todos los controles de la norma en donde se observa si existen controles y la razón de la selección de cada uno de ellos, resaltando si el control surge de un requerimiento legal de una obligación contractual, de un requerimiento de negocio o de las mejores prácticas; o si el control surge como resultado del análisis de riesgos realizado a los activo de información de la organización

- Ver anexo**: Declaración de aplicabilidad y hoja de verificacion.xlsx**

Fase 2. Sistema Gestión Documental
Documentación del SGSI

Procedimiento de auditorias internas

- Verificar si el sistema de gestión de seguridad de la información opera de acuerdo con los planes, procedimientos, registros y controles establecidos, si es conforme con los requisitos de la norma ISO 27001:2013 y es eficaz para satisfacer los requisitos relacionados con seguridad de la información
- Ver anexo: **PQ-01-171 .doc**

Gestión de Indicadores

- Se implementarán indicadores de gestión para mantener monitorizado y actualizado del SGSI, los cuales permitirán controlar el funcionamiento de las medidas de seguridad implementadas, eficacia y eficiencia.
- Ver anexo**: PQ-01-013.doc**

Procedimiento de Revisión por la Dirección

- El Sistema de Gestión de Seguridad de la Información contempla una evaluación periódica, sistemática y estructurada a cargo de la Alta Dirección que permite asegurar una adecuada planeación y la corrección de las desviaciones en el cumplimiento de los objetivos, y como tal incluye la toma de decisiones sobre acciones necesarias, que dentro de un marco de conveniencia razonable para la organización promueva el mejoramiento de productos, procesos y capacidades organizacionales que permitan alcanzar resultados de eficiencia, eficacia y efectividad.
- Ver anexo: **PQ-01-011.doc**

Fase 2. Sistema Gestión Documental
Documentación del SGSI

Gestión de Roles y Responsabilidades

- El Sistema de Gestión de Seguridad de la Información define los diferentes roles y funciones.
- Entre estas definiciones de roles y responsabilidades se podrán identificar alguno de los siguientes ítems:
  - Quien es el responsable de la ejecución de cada hito
  - Quien toma las decisiones, solo o conjuntamente con otros
  - Quien gestiona los recursos y controla el progreso del trabajo
  - Quien debe ser informado
  - Quien debe ser consultado
  - Quien debe participar
  - Quien debe dar apoyo o dotar de infraestructura al equipo
  - Quien asegura la calidad de los resultados
  - Ver anexo: **PQ-01-012.doc**

Metodología de Análisis de Riesgos

- De las diferentes metodologías existentes en el mercado, se optó por utilizar, Magerit.
- MAGERIT permite:
- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados

Fase 3. Análisis de Riesgos.

Inventario de Activos

Se analizan los activos vinculados a la información

Y se agrupan por ámbitos (instalaciones, Hardware, Aplicaciones….)

Valoración de Activos

- Se define una tabla de valoración de activos , las escalas de valoración quedan definidas por categorías y se da un rango de valores
- Igualmente se saca una tabla de elementos claves , clasificados por activo teniendo en cuenta criticidad, valor, categoría, servicios y misión

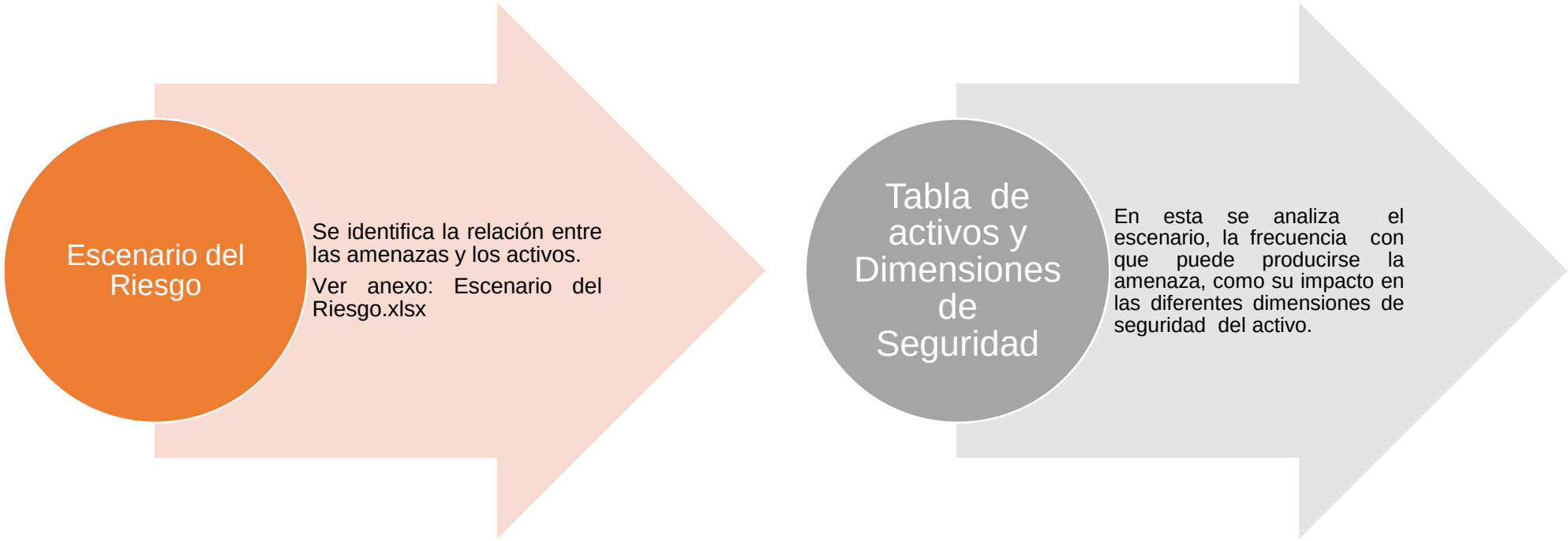
Dimensiones de Seguridad

Identificados lo activos se realiza la valoración ACIDA, dicha valoración mide la criticidad de las 5 dimensiones de seguridad Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad.

Se utiliza una escala de valores siguiendo los criterios de daño muy grave, grave, importante, menor, irrelevante.

Fase 3. Análisis de Riesgos.

Fase 3. Análisis de Riesgos.



Fase 3. Análisis de Riesgos.

Impacto potencial

- Se calcula el riesgo actual, Para determinar el riesgo se multiplican los valores asignados a la probabilidad de una amenaza por los valores asignados a la magnitud del impacto, creando una matriz que se denomina mapa de riesgo
- Se define una escala de riesgos con los niveles Alto, Medio Alto, Medio, Medio Bajo, Bajo y las acciones que debe tomar la dirección y responsables.
- Se marca un nivel sobre la calificación de las Probabilidades/Frecuencias. Nivel 5 al 1 Siendo 5- Alto, 4-Medio Alto, 3-Medio, 2-Medio Bajo, 1-Bajo.
- Se marca un nivel sobre el impacto en la información (disponibilidad , confiabilidad, integridad)
- Con estos niveles se procede a realizar el calculo del riesgo que será la multiplicación entre la probabilidad y el impacto en la información. Se crea una tabla con escenario, probabilidad (nivel/calificación), Impacto operación (nivel/calificación), Resultado Riesgo.

Fase 3. Análisis de Riesgos.

Nivel de riesgo aceptable y residual

- Los criterios de aceptación de riesgo demandados por Textilera S.A, establece que riesgos de niveles “Alto” y “Medio Alto” se consideran inaceptables y deben ser tratados de forma inmediata con los recursos necesarios requeridos

- Así mismo para los niveles Medio y bajo su tratamiento depende del aporte del control para mitigar riesgos, la relación costo/beneficio y la contribución que este aporte al cumplimiento de los objetivos del negocio

- Teniendo estos criterios de aceptación se crea la matriz de riesgos donde se identifican los riesgos inaceptables que requieren tratamiento.

Ver anexo *MatrizRiesgos.xlsx*

Fase 4. Propuesta de Proyectos

Plan de tratamiento del riesgo

- Se establecen las medidas de protección, salvaguardas o contramedidas que se deben implementar para cada uno de los activos en función del impacto que representa la materialización de una amenaza.
- Se crea una tabla de tratamiento al riesgo analizando Riesgos Altos, Tratamiento (Aceptarlo, Evitarlo, Mitigarlo, Transferirlo), Plan de Monitoreo, Responsable, Resultado Esperado

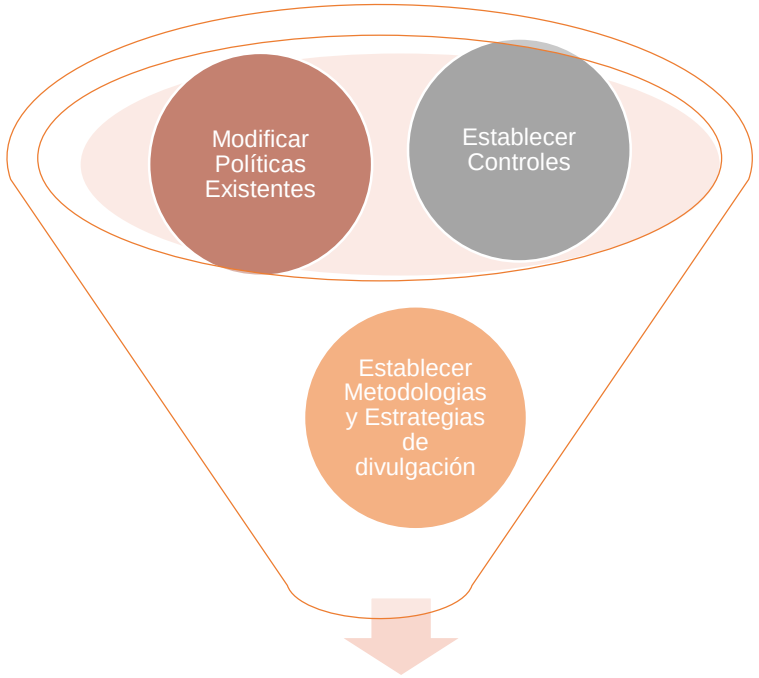
Riesgo Residual

- Se calcula el riesgo residual multiplicando el valor del activo por la probabilidad.*Ver Anexo. Calculo Riesgo Residual.xlsx*
- La organización determina que la aplicación del mejor o mejores controles para mitigar un riesgo aporta una disminución del mismo en un 90% en promedio, el valor restante deberá ser asumido por la organización en cada uno de los activos.

Planteamiento de proyectos

- Se plantea y detalla los proyectos a realizar para implementar las salvaguardas identificadas en el análisis de riesgos, basado en el objetivo establecido de los controles de la norma.
- Los proyectos más significativos serían los siguientes:
  - Proyecto Políticas de seguridad de la información
  - Proyecto Monitoreo SGSI
  - Proyecto Contratación legalidad
  - Proyecto control de acceso y seguridad física
  - Proyecto servicios de plataforma
  - Proyecto Desarrollo del software
  - Proyecto Clasificación/Gestión de Activos
  - Proyecto continuidad del negocio
  - Proyecto Análisis de Riesgos
  - Proyecto Criptografía
  - Se elabora por cada uno una carta de proyecto que contiene: descripción general, objetivos, Descripción del problema, identificación causa raíz, estimación de recursos, detalles de tareas, costos de proyecto, plan mitigación de riesgo, plan de comunicación, detalles del proyecto.

Fase 4. Propuesta de Proyectos
Proyecto Políticas de Seguridad de la Información



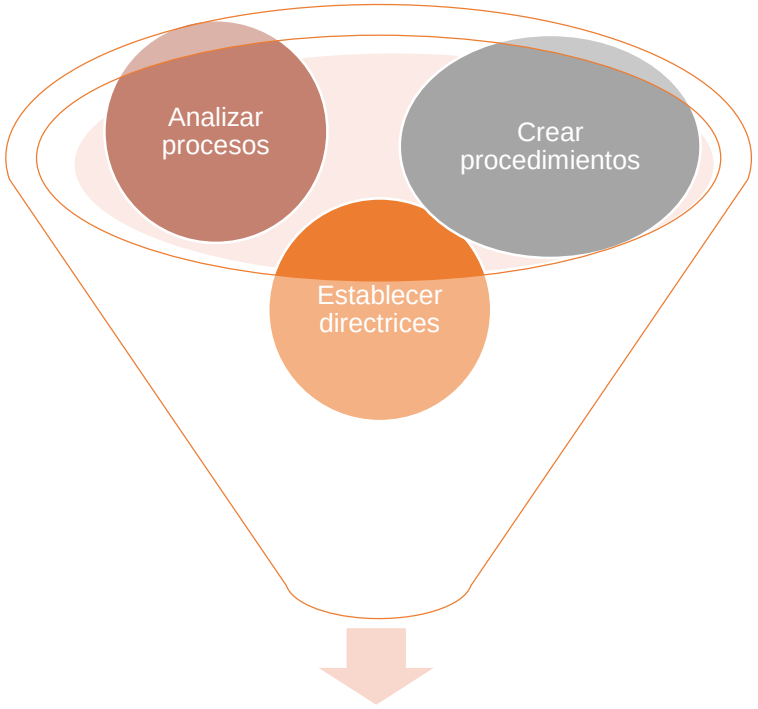
Proyecto Políticas de Seguridad de la información

Descripción General:
Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a políticas de seguridad de la información.
Creando políticas necesarias que permitan fortalecer el sistema de información.
Modificando políticas existentes de manera que sean claras y abarquen el contenido necesario que permita a la organización crear un sistema de gestión de la información conforme a estándares y leyes.

Objetivo General

Actualizar el documento actual de políticas de seguridad de la información de Textilera S.A estableciendo controles y métodos de divulgación.
Para ver el detalle de la carta del proyecto:
Ver anexo. ProyectoPoliticasSeguridad.docx

Fase 4. Propuesta de Proyectos
Proyecto Monitoreo SGSI



Proyecto
Monitoreo SGSI

Descripción General:

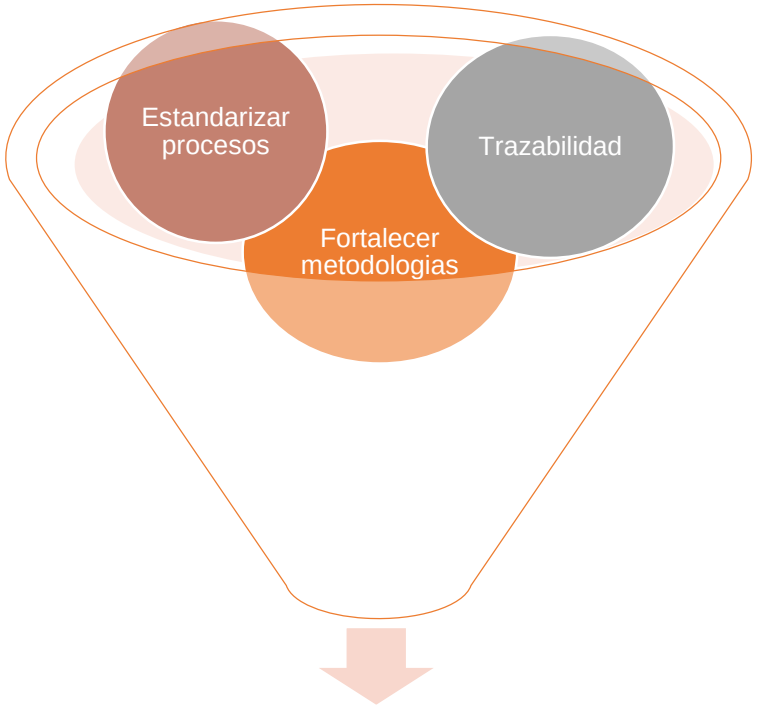
Este proyecto pretende analizar los procesos actuales de revisión que se realizan al sistema de gestión de seguridad de la información identificando las falencias, sugiriendo nuevos controles y procesos enfocados al cumplimiento de la norma ISO 27001:2013.

Objetivo General

Fortalecer dentro del sistema de gestión de la información los controles y procedimientos orientados a la revisión, monitoreo de los procesos y sistemas sensibles orientados al cumplimiento de la norma ISO 27001:2013

Para ver el detalle de la carta del proyecto:
Ver anexo. ProyectoMonitoreoSGSI.docx

Fase 4. Propuesta de Proyectos
Proyecto control de acceso y seguridad física



Proyecto control de acceso y seguridad física

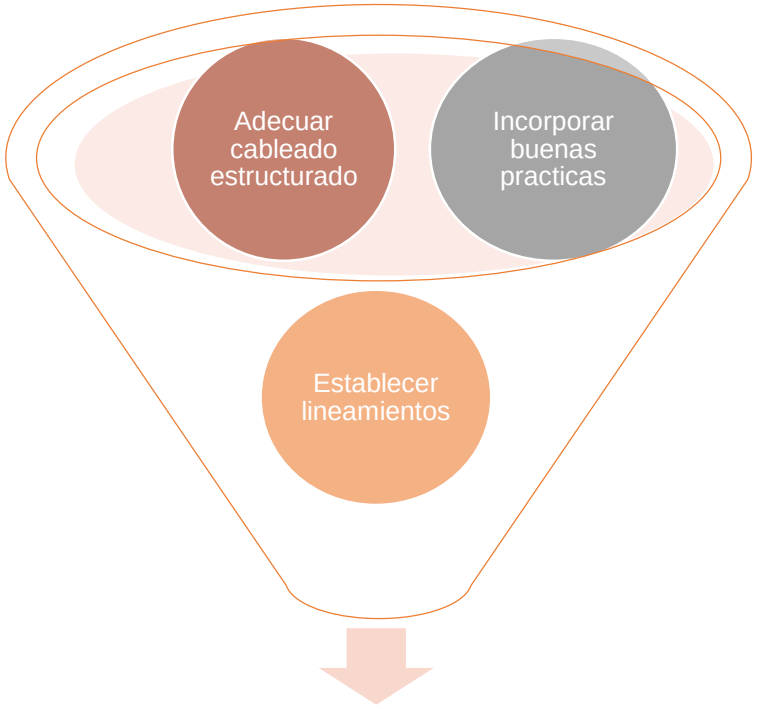
Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos y controles existentes de la organización, orientados hacia los controles de acceso y seguridades físicas establecidas en el manejo de activos y sistemas de información.

Objetivo general

Fortalecer y documentar los procesos que intervienen en las actividades de seguridad física y control de acceso a los sistemas de información.

Para ver el detalle de la carta del proyecto:
Ver Anexo. ProyectoControlAccesoySeguridaFisica.docx

Fase 4. Propuesta de Proyectos
Proyecto servicios de plataforma



Proyecto servicios de plataforma

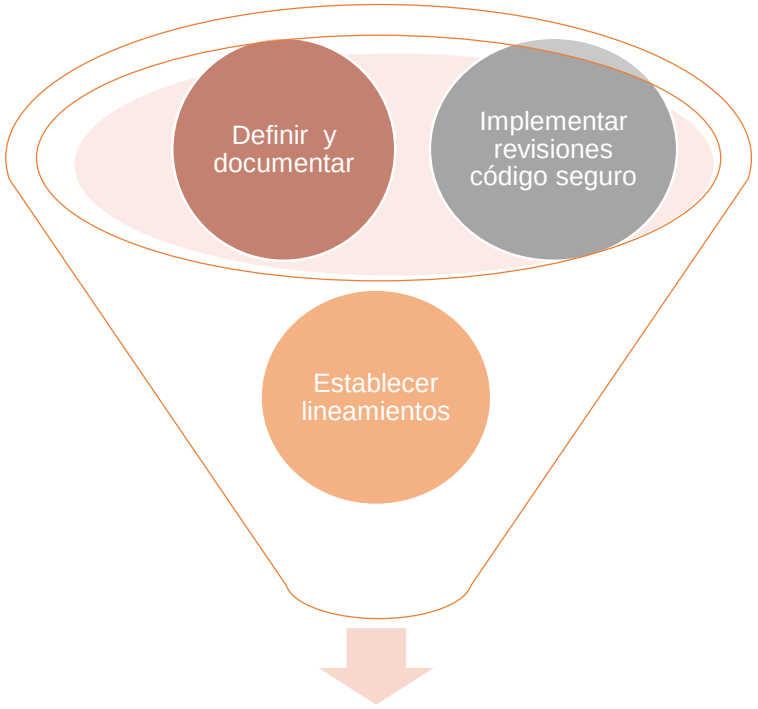
Este proyecto pretende analizar los procesos actuales de plataforma y definir las necesidades conforme a la norma ISO 27001:2013 enfocados al cumplimiento y creación de controles.

Objetivo General

Fortalecer dentro del proceso de plataforma los controles y procedimientos ya existentes y crear los necesarios orientados al cumplimiento de la norma ISO 27001:2013

Para ver el detalle de la carta del proyecto:
Ver Anexo. ProyectoServiciosPlataforma.docx

Fase 4. Propuesta de Proyectos
Proyecto Desarrollo del software



Proyecto Desarrollo del software

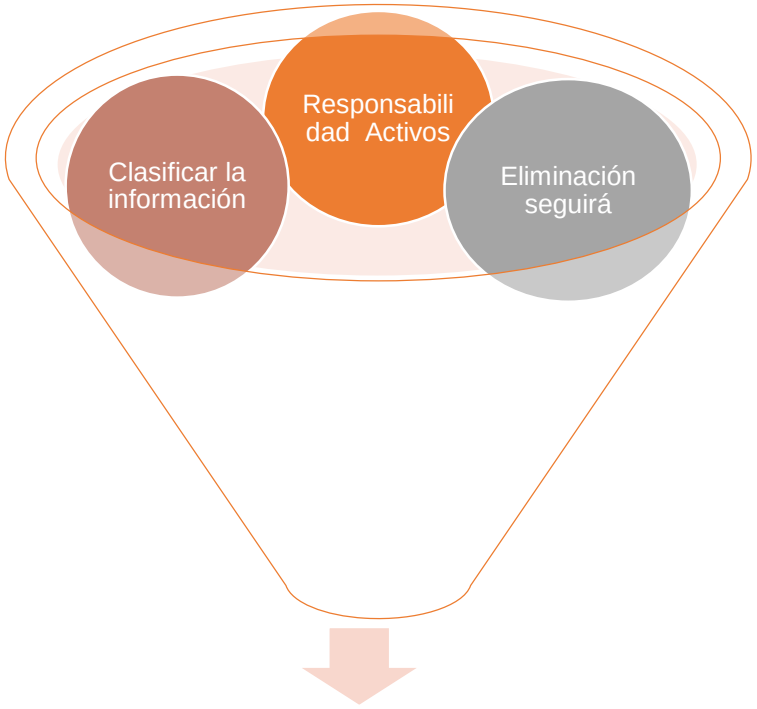
Este proyecto pretende analizar los procesos actuales de desarrollo de software en el sistema de gestión de seguridad de la información, que se aplican identificando las falencias, sugiriendo nuevos controles y procesos enfocados al cumplimiento de la norma ISO 27001:2013.

Objetivo General

Fortalecer dentro del sistema de gestión de la información los controles y procedimientos ya existentes en el proceso de desarrollo de software, además de proponer la creación de nuevos que contribuyan al cumplimiento de la norma ISO 27001:2013.

Para ver el detalle de la carta del proyecto:
Ver Anexo. ProyectoDesarrolloSoftware.docx

Fase 4. Propuesta de Proyectos
Proyecto Clasificación/Gestión de Activos



Proyecto
Clasificación/Gestión de Activos

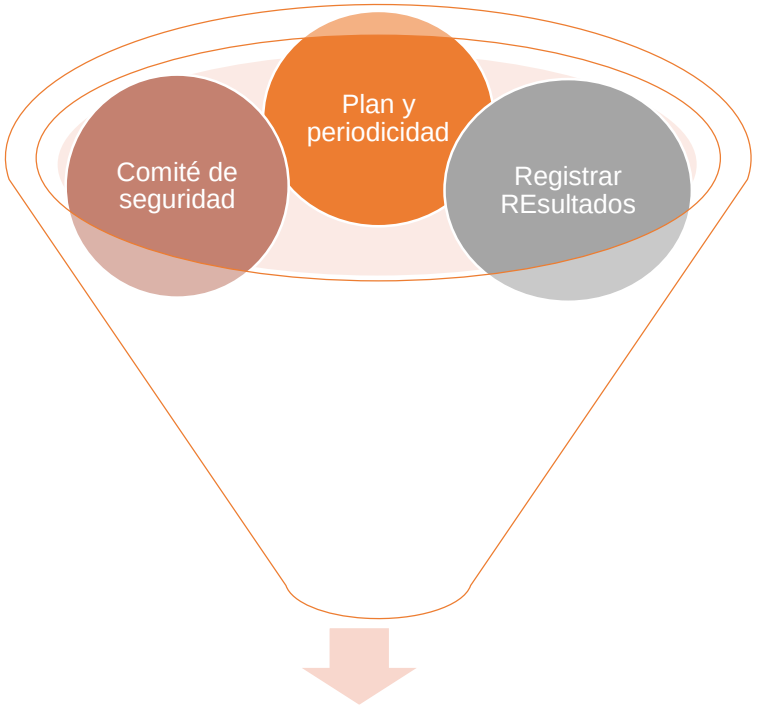
Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a la clasificación y el manejo de activos en un sistema de gestión de seguridad de la información.
Fortaleciendo procesos ya existentes, creando nuevos y apoyándose en controles que puedan responder a un ciclo de clasificación, diferenciación, uso y dar de baja los activos informáticos de la compañía.

Objetivo General

Fortalecer el proceso de identificación, clasificación y cuidados especiales de activos de información más relevantes de la compañía conforme al ciclo de vida del mismo.

Para ver el detalle de la carta del proyecto:
Ver Anexo. ProyectoClasificacionGestion Activos.docx

Fase 4. Propuesta de Proyectos
Proyecto continuidad del negocio



Proyecto continuidad del negocio

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto al modelo de continuidad de negocio, analizando los procesos más críticos que se involucran en el soporte a la cadena de valor y a los sistemas.

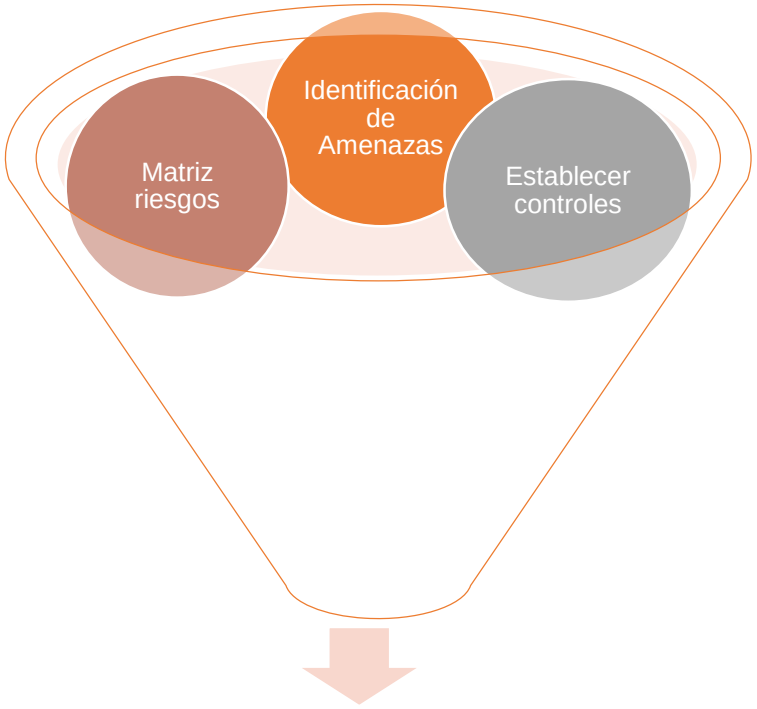
Objetivo General

Implementar un modelo de continuidad de negocio que involucre los procesos críticos de la compañía y asegure frente a un evento externo o interno el sostenimiento de la misma.

Para ver el detalle de la carta del proyecto:

Ver Anexo. ProyectoContuinidadNegocio.docx

Fase 4. Propuesta de Proyectos
Proyecto Análisis de Riesgos



Proyecto Análisis de Riesgos

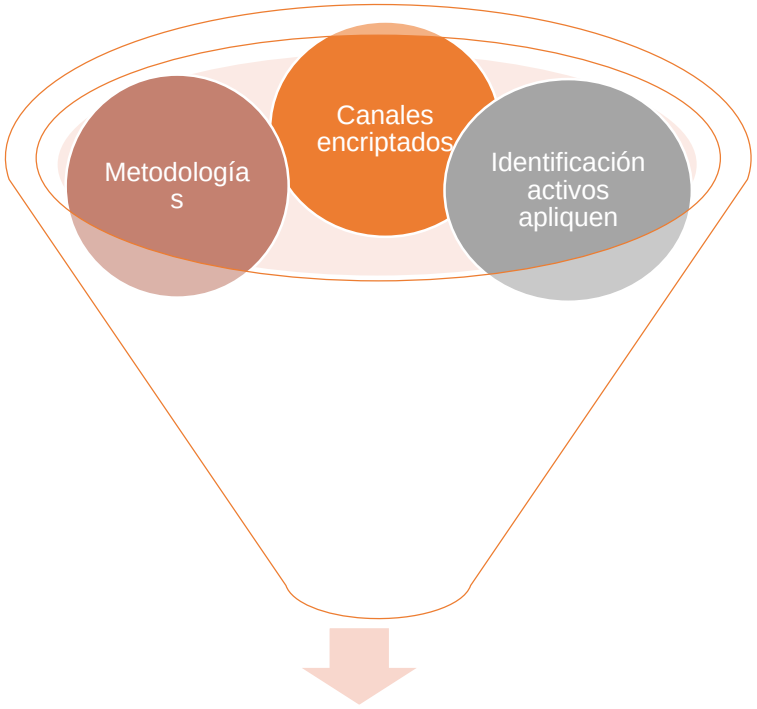
Este proyecto pretende analizar los procesos actuales orientados a las revisiones de vulnerabilidades al sistema de gestión de seguridad de la información identificando falencias, sugiriendo la creación de nuevos controles y procesos enfocados al cumplimiento de la norma ISO 27001:2013

Objetivo General

Analizar y documentar dentro del sistema de gestión de seguridad de la información los riesgos que afectan los activos de información con el fin de identificar amenazas, vulnerabilidades y fuentes y con estas generar salvaguardas y contingencias que ayuden a disminuir el impacto y la probabilidad de los mismos para dar cumplimiento de la norma ISO 27001:2013.
Para ver el detalle de la carta del proyecto:

Ver Anexo. ProyectoAnalisisRiesgos.docx

Fase 4. Propuesta de Proyectos
Proyecto Criptografía



Proyecto Criptografía

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a la necesidad de cifrar canales e información en los procesos más críticos de la compañía.

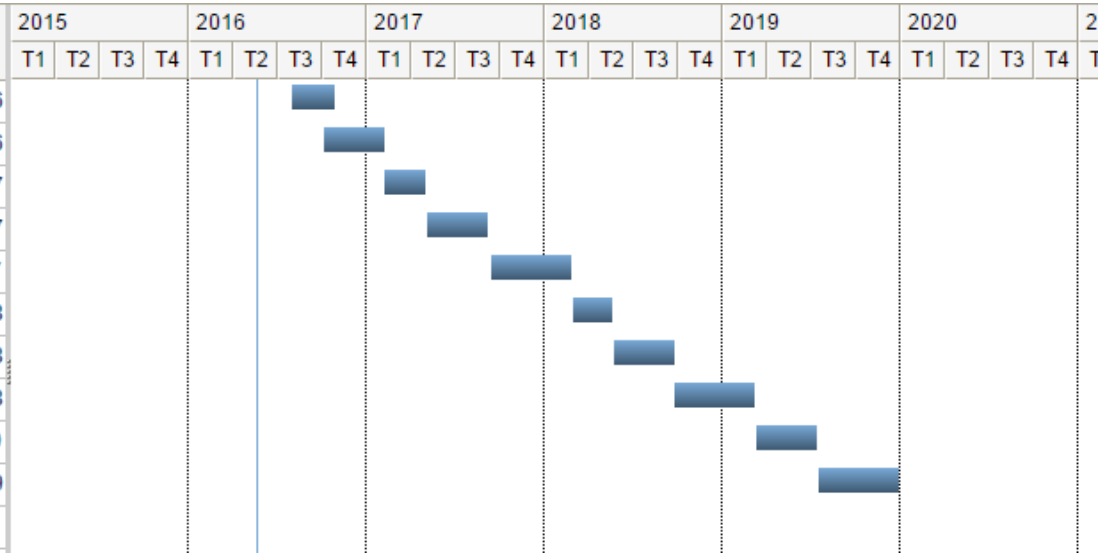
Objetivo General

Establecer dentro de los servicios controles criptográficos para los sistemas de información y activos de información que lo requieran.

Para ver el detalle de la carta del proyecto:
Ver Anexo. ProyectoCriptografia.docx

Fase 4. Propuesta de Proyectos
Estimación de tiempos realización de proyectos

		Nombre	Duración	Inicio
1		Proyecto Políticas de seguridad de la información	64d	01/08/2016
2		Proyecto Monitoreo SGSI	90d	03/10/2016
3		Proyecto Contratación legalidad	62d	06/02/2017
4		Proyecto control de acceso y seguridad física	90d	03/05/2017
5		Proyecto servicios de plataforma	120d	11/09/2017
6		Proyecto Desarrollo del software	60d	26/02/2018
7		Proyecto Clasificación/Gestión de Activos	90d	21/05/2018
8		Proyecto continuidad del negocio	120d	24/09/2018
9		Proyecto Análisis de Riesgos	90d	11/03/2019
10		Proyecto Criptografía	120d	15/07/2019



Fase 5. Auditoria de Cumplimiento

Metodología

- Para ejecutar la auditoria de cumplimiento, se usará el modelo de madurez de la capacidad (CMM) como metodología para el análisis del grado de madurez en la implementación del SGSI .

Evaluación de Madurez

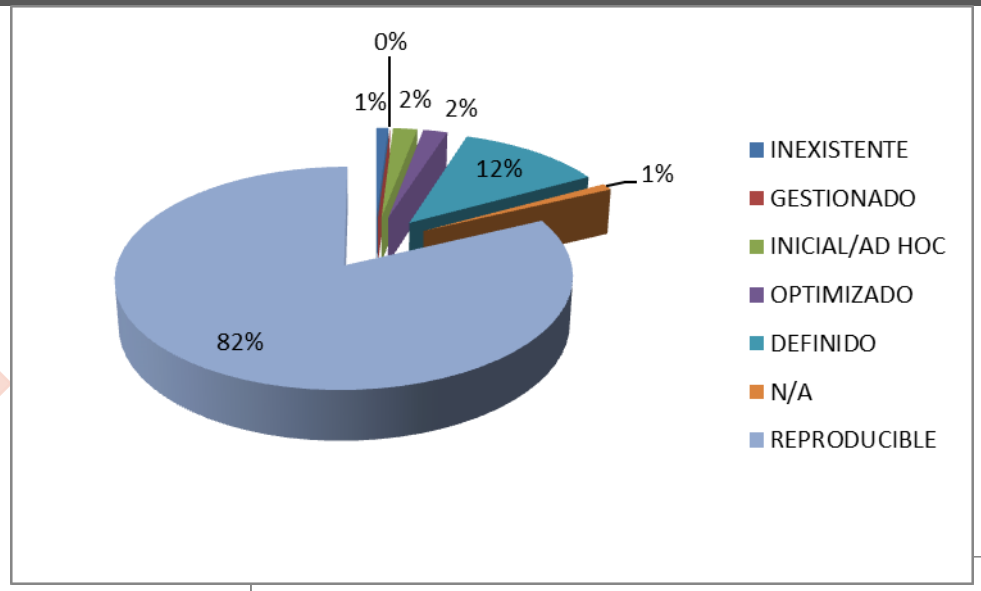
- Se realiza una auditoria y por cada control se identificaron de acuerdo a los hallazgos positivos y negativos:
- El CMM y efectividad
- El grado de cumplimiento (Cumplido, No conformidad Mayor, Menor, requiere Observación/ Corrección, Posibilidad de Mejora, Punto fuerte.
- Observación del grado de cumplimiento
- Asociación al proyecto a desarrollarse

- Ver detalle en el anexo: EvaluaciondeMadurez.xlsx

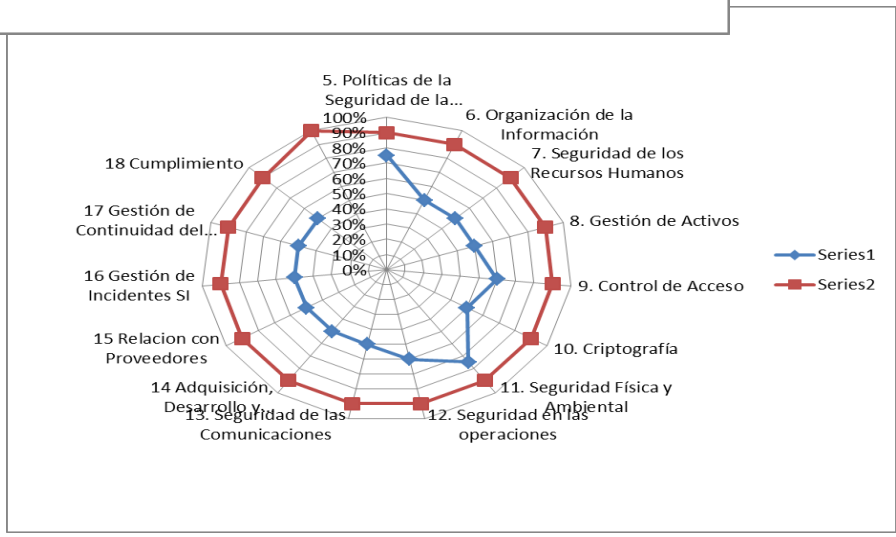
Fase 5. Auditoria de Cumplimiento

Presentación de Resultados

- La mayoría de controles se encuentran en un nivel (L2) seguido de controles de procesos definidos (L3). Esto indica que hay en su mayoría procesos que están parcialmente definidos, que se evidencian buenas prácticas y seguimientos en muchos de los controles planteados en la ISO 27002 pero que carecen en su mayoría de documentación, entrenamiento, comunicación, consolidación de información, definición de responsables y caracterizaciones de proceso.



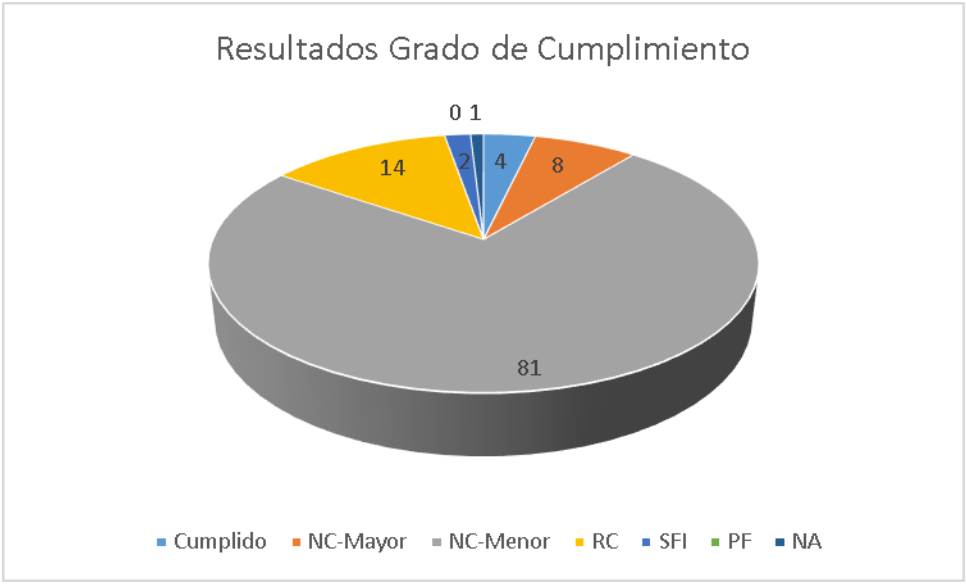
el nivel de cumplimiento por capitulo ISO, Anticipándonos a las medidas, compara el estado actual con el estado deseado. Las series1 al grado actual de madurez CMM%; la series2 corresponde al grado post- implementacion de madurez CMM %. Para la organización el nivel deseado de los dominios es de un 90% en una etapa inicial e ir mostrando el proceso de mejora continua y optimizar hasta tener un cumplimiento de un 100%.



Fase 5. Auditoria de Cumplimiento

Resumen de hallazgos de la auditoria

- Cumplido (C) =4. Se da cumplido a lo requerido en el control.
- No conformidades – Meyores (NC-Meyor)=8. Estas no conformidades es el incumplimiento de un apartado completo de la norma, en este caso el control.
- No conformidades – Menores (NC-Menor)=81.Las no conformidades Menores en su mayoría corresponden a procesos que tienen evidencias y registros que dan cumplimiento al control pero no existe documentación del proceso, ni difusión del mismo, por lo que se tiene un incumplimiento de un punto de la norma.
- Requiere Correccion/Observacion (RC)= 14.No existe incumplimiento pero se requiere la revisión en este caso de los procedimientos y documentación facilitada, se encuentran incompletos y hay falta de detalle en el proceso. Si no se corrige podría convertirse en una no conformidad en una auditoria futura.
- Posibilidad de Mejora (SFI)=2. Se muestra como una recomendación del auditor, no existe incumplimiento de la norma.
- Punto Fuerte (PF)=0. Aun cuando se notan procesos de buenas practicas y un esfuerzo de mejora en el SGSI no se destaca ningún control.
- No aplica (NA)=1. Solo un control se considera que no aplica para la organización.



Fase 6. Presentación de Resultados y Entrega de Informes

Conclusiones

- La implementación de un sistema de gestión de seguridad de la información SGSI, conformara un mecanismo de optimización de recursos, ahorro de costos y mejora continua que permitirá a Textilera S.A alcanzar los objetivos y metas planteadas.

- Las mejoras al sistema Gestión de seguridad de la información posibilitara alcanzar niveles de madurez fijados por la organización, al mismo tiempo que permitirá un mayor acercamiento para realizar la certificación del SGSI mediante la norma ISO 27001:2013.

- Un SGSI conlleva a cambios de procesos y estructuras pero hace que la integridad, confidencialidad y disponibilidad estén enmarcadas como uno de los mayores activos dentro de una compañía y para Textilera S.A esto es de vital importancia para su crecimiento.

- El análisis y la gestión de riesgos ha permitido la correcta identificación de los activos en riesgo, determinando sus dependencias y el impacto potencial de la materialización de las amenazas, desarrollando y cuantificando las medidas de protección, ya sean operativas, técnicas y humanas que permiten mitigar, aceptar o transferir los riesgos.

Conclusiones

- Con las visitas realizadas a Textilera S.A se identificaron procesos no existentes a implementar al SGSI.
- Con las diferentes auditorías realizadas a los procesos y áreas existentes se logró identificar las evidencias, hallazgos positivos, negativos y grado de cumplimiento para cada uno de los controles aplicables a la norma ISO 27001:2013 en miras al fortalecimiento del SGSI.
- A través del análisis de riesgos de los activos más críticos de la empresa Textilera S.A se logró identificar los proyectos a desarrollarse en miras al cumplimiento de la norma ISO 27001:2013.
- Se presentaron las cartas de los diez proyectos resultantes como punto de partida de la gestión de proyectos necesarios para el cumplimiento de la norma ISO 27001:2013 en el fortalecimiento de SGSI.

Conclusiones

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

- La presentación de la asesoría realizada a Textilera S.A genero un impacto positivo al personal de TI y cumplió con las necesidades planteadas.

- El apoyo de la dirección es un factor clave para la madurez del sistema de gestión de seguridad de la información.

- Se deberá contar con estrategias y medios que permitan la sensibilización del SGSI permanente con los usuarios ya que ellos son los responsables del manejo adecuado de la información.