DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENPRESA DE OBRA, CONSULTORÍA E INTERVENTORÍA DE OBRAS CIVILES

TRABAJO DE GRADO

PARTICIPANTES

ERIKA LORENA RODRIGUEZ ECHEVERRIA

COD. 1612010350

LUDIVIA GIRLEZA RUBIO SALCEDO

COD. 1612010383

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENPRESA DE OBRA, CONSULTORÍA E INTERVENTORÍA DE OBRAS CIVILES

TRABAJO DE GRADO

PARTICIPANTES

ERIKA LORENA RODRIGUEZ ECHEVERRIA

COD. 1612010350

LUDIVIA GIRLEZA RUBIO SALCEDO

COD. 1612010383

ASESOR

ALEJANDRO CASTIBLANCO CARO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, 24 de abril de 2017

TABLA DE CONTENIDO

LISTA DE CUADROS

LISTA DE FIGURAS

Introducción

En la actualidad es evidente que para las empresas lo más importante es la información, pues de esto depende la correcta efectividad del negocio, aunque existen muchos mecanismos para trasmitir, compartir y procesar esta información, no existen controles y elementos que garanticen la confidencialidad, integridad y disponibilidad de la misma, por consiguiente es necesario desarrollar una gestión adecuada de recursos y activos de información que cumpla, asegure y controle la información sensible de la organización.

De acuerdo a lo anterior, podemos considerar que las organizaciones están expuestas a un sin número de riesgos, los cuales se pueden materializar aprovechando las debilidades presentes al interior de la misma. Con el fin de mitigar estos riesgos es posible implementar diferentes mecanismos tecnológicos, pero su ejecución resulta limitada o insuficiente por sí misma. Por tanto es necesario implementar una gestión efectiva de seguridad, mediante el diseño de un Sistema de Gestión de Seguridad de la Información, en el cual se desarrolle un conjunto de políticas, lineamientos y procedimientos que permitan el mejoramiento continuo garantizando así el buen uso y la privacidad de la información en todas las operaciones que se realizan con los clientes.

Hoy en día, las organizaciones dedicadas a brindar servicios de consultoría e interventoría tienen la necesidad de garantizar la seguridad, confidencialidad, disponibilidad e integridad de la información ya que esta maneja datos sensibles de empresas públicas y privadas, por ende es preciso asegurar el tratamiento y uso de la información de las mismas, ya que una de las problemáticas más evidentes ahora con los avances tecnológicos es la fuga de información que

en muchas ocasiones se presenta por descuido o desconocimiento de empleados o terceros, causando grandes perjuicios a la organización y sus clientes externos.

El presente proyecto tiene como objetivo diseñar un SGSI para una empresa que presta servicios de obra, consultoría e interventoría de obras civiles. Apoyados en el marco de referencia ISO 27001/2013, se tendrá en cuenta un análisis de diagnóstico GAP en materia de seguridad de la información de la empresa, con el fin de proyectar y aplicar una metodología y análisis de riesgo organizacional para garantizar que se cumplan con los objetivos estratégicos y las necesidades del negocio buscando el crecimiento continuo y seguro de la misma.

El diseño del SGSI se realizará para una empresa real, pero por seguridad de la información de la empresa, el nombre que se utilizara es XY S.A

1. Resumen ejecutivo

XY S.A.S. es una empresa anónima que presta el servicio de Obra, Consultoría e Interventoría de obras civiles, en el sector público y privado a nivel nacional, la cual utiliza una metodología para la estructuración de proyectos donde brinda la solución de problemas y reduce costo para un mejor desempeño, mientras se minimiza los riesgos.

La entidad se encuentra vigilada y controlada por la Superintendencia de Industria y Comercio y otros entes de control como Fonade, Invias, entre otros, por ende, es necesario que cumpla con la Ley de protección de datos personales y a su vez diseñe, implemente, mantenga y mejore un Sistema de Gestión de Seguridad de la Información.

XY S.A.S cuenta con infraestructura tecnológica adecuada, pero no tiene implementados mecanismos de seguridad físicos, ni lógicos, razón por la cual no conoce el estado real de la organización frente a temas de seguridad de la información, aunque están definidos los procesos y las responsabilidades de su personal, no se cuenta con una identificación de activos de la información, ni un análisis de riesgos real que permita a la entidad actuar de forma adecuada si se presenta un incidente, lo cual puede llegar a comprometer la confidencialidad, integridad y disponibilidad de la información.

Con la implementación de la Ley No. 1581 del 2012 de protección de datos personales y los requisitos mínimos para realizar el registro Nacional de las bases de datos, se evidencio que la organización tenia algunos documentos base no oficiales de seguridad de la información pero no cuenta con un SGSI, razón por la cual no está cumpliendo a cabalidad con esta norma en cuanto al tratamiento que se le debe dar a los datos sensibles; por tanto surgió la necesidad de diseñar un Sistema de Gestión de Seguridad de la información, para que posteriormente la compañía lo implemente, lo mantenga y realice procesos constantes de mejora continua.

Adicionalmente se han presentado varios incidentes de fuga de información sensible en los procedimientos de licitaciones y consultorías de la organización y esta ha sido suministrada a la competencia razón por la cual se perdieron algunas licitaciones que la compañía ya estaba a punto de concretar, aunque se han tomado algunas medidas de aseguramiento tecnológico para evitar la nueva presentación de este evento, no se ha realizado una valoración de riesgo que permita a la entidad estar preparada para estos incidentes, ni mucho menos se tiene contemplado que puedan ocurrir otra serie de eventos que se puedan materializar.

Tras el diagnóstico realizado a la organización, se evidencio que no existe una estructura de Seguridad de la información en la cual apoyarse, esto se debe a la falta de interés de la alta dirección por avanzar en temas de seguridad por esta razón el personal no posee conocimiento al respecto, así mismo los recursos tecnológicos con los que cuentan están dedicados a mantener la operación y no a protegerla, generalmente cuando ocurre un evento de riesgo le dan solución pero no tienen en cuenta algunas otras medidas de seguridad pues esperan que no se presenten eventos posteriores. Debido a lo anterior no se tiene una identificación de activos, ni una clasificación de la información, por ende toda la información se comparte y distribuye sin ningún tipo de aseguramiento, por tanto, no cuentan con una visión clara de que tipo de información se debe salvaguardar, ni porque es importante hacerlo.

Además, no existe un área específica a cargo de seguridad de la información y la poca gestión que se ha ejecutado ha sido realizada por el área de tecnología quienes no tienen clara la diferencia entre seguridad de la información y seguridad informática.

Tras la problemática planteada el objetivo que enmarca este proyecto es "Diseñar un Sistema de Gestión de Seguridad de la información, por medio de un análisis diagnóstico organizacional de la empresa XY S.A.S". Aplicando los conocimientos adquiridos en la especialización y en las investigaciones realizadas en la empresa. Para desarrollar este objetivo se tendrán en cuenta los siguientes objetivos específicos:

- Realizar un diagnóstico del estado actual de la empresa XY S.A.S, en materia de seguridad de la información, mediante un GAP análisis enfocado en la norma ISO 27001.
- Diseñar e implementar una metodología para la identificación, clasificación y valoración del riesgo inherente de Seguridad de la Información.

- Desarrollar una matriz de riesgo inherente con los resultados obtenidos del análisis de riesgo organizacional.
- Diseñar un plan de tratamiento para la mitigar los riesgos en los procesos de la organización.
- Construir la política general del sistema de Gestión de Seguridad de la Información, teniendo en cuenta el alcance y objetivos organizacionales.
- Definir los roles y las responsabilidades del Sistema de Gestión de Seguridad de la Información.

De acuerdo a la problemática planteada anteriormente los sistemas de gestión de seguridad de la información son de gran utilidad ya que permite tener visión general del estado de la seguridad de la información y así conocer la efectividad de las medidas de seguridad que se implementen, esto con el fin de que la Alta Dirección pueda tomar decisiones, logrando así tener una mejor planeación, definición, identificación e implantación de medidas orientadas a salvaguardar la información.

Con lo anterior la empresa XY S.A.S requiere desarrollar una serie de políticas que le permitan asegurar la integridad, confidencialidad y disponibilidad de la información donde se garantice la protección de información sensible de la empresa. Mediante un SGSI, donde se dé a conocer el estado actual de la información mediante un análisis de riesgos, y se establezcan mecanismos que mitiguen el impacto de las vulnerabilidades.

Por consiguiente, la metodología empleada para el desarrollo del proyecto busca dar cumplimiento a los objetivos especificados anteriormente para lograr alcanzar el objetivo principal del proyecto, apoyados en el marco de referencia de la norma ISO/IEC 27001:2013 la

cual específica las actividades que se deben desarrollar para el diseño de un Sistema de Gestión de Seguridad de la Información.

Las etapas para resolver la problemática de la organización son:

Cuadro 1.
Etapas de metodología

Fases	Descripción
Planeación	Identificación y diagnóstico de la organización frente a Seguridad de la información
Diseño	Definición Alcance Definición de Estructura Desarrollo de Metodología de Riesgos Definición Políticas
Implementación	Clasificación de Activos de la Información Matriz de Riesgo Elaboración de Manual SGSI

***Fuente**:* Autores

Tras el desarrollo del proyecto se busca que la empresa implemente el sistema de Seguridad de la Información diseñado de acuerdo a la norma ISO/IEC 27001:2013, y de esta forma obtener los siguientes beneficios:

- Mejoramiento de Imagen Corporativa: Brindar un valor agregado a los clientes, en donde se garantiza que la información que se está procesando se está realizando con los mejores estándares de seguridad de la información.
- Diferencia frente a la Competencia: Al realizar la comparación con otras entidades se evidencia mejor gestión del servicio que se va a prestar.

- Asignación y Segregación de Responsabilidades: Delegar y especificar las funciones operativas del personal de la organización.
- Cumplimiento Disposición Legal: Evitar sanciones o multas por incumplimiento de algunas normas como la protección de datos personales.
- Mejora medidas de Seguridad: Garantizar que la información va a estar protegida frente a materialización de amenazas y mitigación de riesgos.

El alcance del presente proyecto comprende un diagnóstico inicial de toda la empresa XY S.A.S. mediante un GAP análisis respecto a seguridad de la información y el desarrollo de una metodología para la valoración de riesgos de los procesos involucrados en la organización (Gerencia General, Gerencia Comercial, Dirección Administrativa, Dirección Financiera y Dirección Tecnológica), por último el diseño de un SGSI adaptable a las características de la organización.

Para el desarrollo del proyecto se tomará como base la norma ISO/IEC 27001: 2013, la cual especifica los requisitos para establecer, implantar, mantener y mejorar un SGSI.

El proyecto consiste en el análisis y diseño del SGSI, pero no abarca la implementación, revisión, mantenimiento y mejora del mismo.

2. Justificación

La seguridad de la información y la protección de datos en una organización son fundamentales y obligatorias ya que su fin es garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos y el contenido de la información para evitar el abuso de esta. Demostrando el compromiso de la organización frente la seguridad de la información,

suministrando elementos requeridos para gestionar de manera eficiente los riesgos que puedan atentar contra la información sensible de una organización.

Con el diseño de un sistema de gestión seguridad de la información basado en la Norma ISO 27001:2013 permitirá estructurar bases que forjen un adecuado modelo de seguridad frente a una entidad mejorando las prácticas e implementando este tipo de sistema donde garantice la mejora continua y su debida permanencia. Ya que establece políticas y mecanismos para minimizar el impacto de materialización de riesgos, además permitirá fortalecer a la organización integralmente en cada uno de las áreas ya que según la ejecución de este plan de modelo de seguridad podrá mejorar la estrategia de negocio volviéndola más eficaz y proactiva.

De acuerdo a lo anterior y teniendo en cuenta algunas estadísticas propias de la organización, es posible evidenciar que actualmente XY S.A.S se ha visto afectada por una serie de amenazas como fuga de información, razón por la cual la compañía ha perdido prestigio y algunas negociaciones que han hecho que sus ingresos se reduzcan, a su vez se han presentado algunos incumplimientos normativos ante los entes de control, por no tener medidas de protección de datos implantadas en su organización, las razones principales de esta problemática se deben a que la Alta Gerencia no posee interés por la implementación de medidas en seguridad pues tiene conocimiento limitado en este tema y no desea invertir en un SGSI. A continuación se describen algunos indicadores que detallan la situación problema de la compañía en el siguiente cuadro:

Cuadro 2.
Indicador Problema

Indicador	Medición	Resultado	Fuente de Información
Liderazgo y Compromiso de la Alta Dirección en SI	• Encuestas Informales sobre temas de SI	N/A	• Encuesta Diligenciada
Capacitación de Empleados	• Número total de empleados/ empleados capacitados • Capacitados/evaluaciones aprobadas	Total empleados: 50 Capacitados: 17 Conocimientos Básicos SI: 5	• Listado de Asistencia • Evaluación de Capacitación
Licitaciones Ganadas y Prestigio Adquirido	• Encuesta de satisfacción del año anterior promedio con encuesta de satisfacción de año actual • Promedio de licitaciones Ganadas por año	80 clientes encuestados 2015 70 clientes encuestados 2016 Aumento insatisfacción del servicio en un 7%	• Encuesta de Satisfacción • Informe Comparativo
Perdida de Información	• Pérdida económica por perdida de la información	1 de cada 10 organizaciones sufrieron pérdidas económicas superiores a U$S 250.000	• Informe empresas consultoría
Metodología de Riesgo	• Porcentaje encuestas de resultados obtenidos tras la implementación.	solo el 21% de las organizaciones tiene proceso de planeación estratégica que se articula con la gestión de riesgos	• Informes de Empresas Expertas en Consultoría

***Fuente**:* Autores

Tras la medición de los indicadores relacionados en la tabla anterior, a continuación se muestran los resultados obtenidos:

- Liderazgo y Compromiso De La Alta Dirección En Seguridad De La Información: De acuerdo a reuniones realizadas con la alta gerencia, se evidencio que no tienen conocimiento respecto a temas de seguridad de la información y tienen poco interés de participar activamente en el proceso, sin embargo, se comprometen a trabajar en pro de la compañía, ya que si incumplen ante los entes regulatorios podrían perder algunas licitaciones o incurrir en multas o sanciones. De acuerdo a lo anterior en un informe del 2016 realizado por Deloitte sobre Tendencias en Gestión de Cyber Riesgos y Seguridad de la Información en Latinoamérica, se evidencio en Latinoamérica solo el 12% de la Alta Gerencia en las organizaciones, recibe un informe mensual de la situación de la empresa a nivel de Riesgos y de SI.
- Capacitación y Sensibilización a empleados: De un total de 50 empleados en XY S.A.S , el 25% que equivale a 17 personas se encuentran capacitados en temas de seguridad de la información, sin embargo de las 17 personas solo 5 personas tiene una concepción básica sobre el tema. Además en una encuesta global desarrollada por E&Y en el 2015, se considera que el 56% de los empleados son las fuentes más probables de un ataque.
- Licitaciones Ganadas y Prestigio Adquirido**:** De un total de 80 clientes encuestados durante el año 2015 y 70 clientes encuestados durante el año 2016, se puede evidenciar que ha aumentado la insatisfacción de los clientes en un 7%, lo cual indica menor participación en el mercado. Además en el informe anual de seguridad Cisco en el año 2016 se determinó que el 63% de las organizaciones se encuentran certificados en temas de seguridad y que debido a esta implementación muestran compromiso con mejoras de seguridad y poseen un valor agregado frente a sus competidores.

- Perdida de Información: De acuerdo al informe de Deloitte del 2016 sobre un Estudio de Seguridad de la información y ciber Riesgo, 1 de cada 10 organizaciones sufrieron brechas de seguridad de impacto alto y/o significativo, con pérdidas económicas superiores a U$S 250.000, más las perdidas reputacionales o por daño de imagen.
- Metodología de Riesgo: De acuerdo al informe anual de Benchmark De Gestión De Riesgos En Latinoamérica en el año 2015, aunque hay un gran número de participación de empresas con sistemas de gestión de riesgos, solo el 21% de las organizaciones tiene proceso de planeación estratégica que se articula con la gestión de riesgos.

Con la implementación de la Norma ISO 27001:2013 en XY S.A.S , se busca proyectar la compañía hacia un entorno más competitivo, en donde los clientes quieran invertir, porque sus procesos se desarrollaran con calidad, cumpliendo con estándares de reconocimiento internacional, posicionándola entre las mejores a nivel Nacional.

Un SGSI, le ayudará a XY S.A.S a medir, cuantificar y mejorar el nivel de cumplimiento de los indicadores establecidos en la situación problema, a continuación se exponen las mejoras en el siguiente cuadro:

Cuadro 3.
Apoyo SGSI a Indicadores

Nombre del Indicador	Apoyo Modelo SGSI
Porcentaje de Personas que laboran en la empresa debidamente capacitadas en políticas SGSI	• Promueve la divulgación y sensibilización de las políticas de seguridad. • Realiza un proceso efectivo de comunicación relacionado con la seguridad de la información
Pérdida de Prestigio	• Mejora la calidad servicio ofrecido, garantizando la confidencialidad de la información. • Mejora el reconocimiento y la competitividad frente a su competencia. • Genera valor y buena reputación en las políticas de gobierno corporativo.
Perdida de información	• Promueve procedimientos para la gestión de medios removibles. • Permite controlar el acceso a la red solo a personal autorizado. • Permite clasificar los activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la Entidad. • Fomenta el manejo de contraseñas utilizados por los usuarios de la organización le ayuda a manejar de forma segura su información de autenticación. • Fomenta el manejo de contraseñas utilizados por los usuarios de la organización le ayuda a manejar de forma segura su información de autenticación.
Metodología de Riesgo	• Permite prevenir y evitar eventos que atenten contra la Organización • Define Planes de Acción para estar preparados para responder ante un evento. • Promueve la reducción de costos y pérdidas organizacionales. • Mejora la gestión de Oportunidades.

Fuente: Autores

De acuerdo a lo anterior, el desarrollo de un SGSI suministra condiciones de gobernabilidad y viabilidad necesarias para lograr el objetivo deseable a la que pretende llegar.

3. Marco teórico y referentes

3.1. Marco teórico.

Con los avances de la tecnología se evidencia que para las organizaciones la información es un activo valioso ya que brinda grandes beneficios a las mismas, por ende proteger su integridad, confidencialidad y disponibilidad es esencial para alcanzar y lograr los objetivos del negocio.

Hoy en día, las nuevas tecnologías han presentado giros inesperados en el entorno a las organizaciones ya que se ha aumentado los riesgos y amenazas que atentan la seguridad lo cual ha causado que con estas herramientas tengan un fácil acceso a la información sensible que no ha sido autorizada, causando así graves perjuicios para las empresas.

Por consiguiente es necesario que las organizaciones protejan sus activos afrontando y mitigando las amenazas de una manera adecuada, para esto las organizaciones deben establecer un Sistema de Gestión de Seguridad de la Información que le permitirá implantar políticas, procedimientos y controles con el objeto de reducir los riesgos presentados que afecte los activos de la organización, con lo cual logre obtener una gestión adecuada con el fin de conseguir beneficios como: reducción de riesgos, ahorro de costos, mejoramiento del ciclo metodológico, aseguramiento del cumplimiento de la legislación vigente ,mejoramiento en la competitividad del mercado y mejorar la imagen y confianza con los clientes.

Por lo anterior el marco teórico, que se desarrollara a continuación, permitirá conocer los conceptos necesarios para el entendimiento del desarrollo de este proyecto**.**

3.1.1. Seguridad de la información. La seguridad de la información1, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

La información sensible, junto a los procesos y sistemas, son activos muy importantes de una organización ya que pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial para lograr los objetivos de la organización y así asegurar beneficios económicos[2].

Las entidades como los sistemas de información, están expuestos a un sin número de amenazas con lo cual aprovechan cualquier vulnerabilidad para dañar algún activo de la información causando de esta manera voluntaria e involuntariamente riesgos o incidentes de seguridad dentro de la organización.

La seguridad de la información [3]consiste en asegurar los recursos del sistema de información de la empresa donde garantiza el buen uso del sistema y el acceso de información que se encuentra contenida en ella, así como controlar que la modificación

[1]http://www.iso27000.es/download/doc_sgsi_all.pdf
[2] http://admondeinformacion.blogspot.com.co/
[3] http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

solo sea posible por personas autorizadas para tal fin y por supuesto dentro de los límites de la autorización.

La seguridad de la información[4] es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

El objetivo de la seguridad de la información[5] es proteger los activos de información ya que son elementos esenciales de las organizaciones las cuales son:

- Información: es el objeto de mayor valor para la empresa.
- Equipos: suelen ser software, hardware y la propia organización.
- Usuarios: son las personas que usan la tecnología de la organización.

La seguridad de la información en si es un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran así como el impacto que puede tener para de esta manera implementar medidas y controles de seguridad adecuados que permitan el monitoreo, revisión y mejora de los activos de la organización esto con el fin de lograr cumplir a cabalidad los objetivos del negocio**.**

[4]https://prezi.com/xftqz8li4znf/mecanismo-para-la-seguridad-e-integridad-de-la-informacion/
[5] http://www.pmg-ssi.com/2015/05/iso-27001

3.1.2. Sistema de Gestión de Seguridad de la Información. Un sistema de gestión de seguridad de la información (SGSI) consiste en la planificación de controles que permite reducir el riesgo, ejecución, rectificación y mejora continua de controles que permitan mitigar los riesgos de incidentes de seguridad.

El proceso que constituye un SGSI es garantizar que la seguridad de la información sea gestionada correctamente la cual debe hacer uso de un proceso sistemático, documentado y conocido por la organización partiendo del enfoque de riesgos empresariales. El SGSI ayuda a establecer políticas y procedimientos en relación con los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir[6].

Un sistema de gestión de seguridad de la información[7] ayuda a las organizaciones de una manera eficaz que la seguridad de la información sea evaluada con el propósito de evitar inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa causado por la desestimación de riesgos, por falta de contramedidas, controles mal implementados, por costos más elevados del necesario o por el retraso en las medidas de seguridad.

[6] http://www.iso27000.es/sgsi.html
[7] http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

Un sistema de gestión de seguridad de la información[8] ayuda a las organizaciones gestionar de forma efectiva mitigar y reducir los riesgos asociados a los activos de información, lo cual brinda y muestra confianza a los entes de la organización ya que evidencia que los procesos que se realizan acabo son debidamente gestionados y solucionados para resolver la problemática presenta. También permite a las organizaciones obtener una visión global del estado de los sistemas de información para poder observar las medidas de seguridad aplicadas y que resultados obtenidos tuvieron aplicando los elementos para tomar mejores decisiones estratégicas que permitan la mejora continua de la organización[9].

Con la implementación de un sistema de gestión de seguridad de la información contribuirá a las organizaciones disponer de una metodología que brinda continuidad de negocio con el cual se pueda contar con procesos definidos para evaluar, implementar, mantener y administrar la seguridad de la información causando así diferencia entre otras organizaciones logrando satisfacer los requerimientos de clientes, proveedores y organismos de control.

3.1.3. International Organization for Standarization (ISO). La ISO **[10]** es una federación internacional para la creación de estándares internacionales. Su sede está en Ginebra, Suiza, hasta el 2015 trabajaba con institutos de normalización de 196 países (uno por cada país). Esta organización promueve el uso de estándares propietarios, industriales y

[8]https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/
[9] http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3777/1/20904541.pdf
[10]https://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n

comerciales a nivel mundial, es una organización no gubernamental puesto que el origen de los institutos de normalización nacionales es diferente en cada país.

Las normas ISO surgen para facilitar la creación de productos y servicios que sean seguros, fiables y de calidad, armoniza la gran cantidad de normas sobre gestión de calidad y seguridad que aparecen en diferentes países. Los estándares de normalización de los diferentes países causan normas que van a consensos entre el representado del estado y la industria de igual forma las normas de la ISO sale de aprobación entre representantes de diferentes países integrados e incorporados a la ISO.

3.1.4. Norma ISO 27000. La información es un activo valioso para las organizaciones, ya que hoy en día cada vez sufren de grandes amenazas en cuanto la confiabilidad y su resguardo, de igual manera es de confirma que la información es vital para el éxito y continuidad de las organizaciones en el mercado. Por esta razón todo indica que el principal objetivo de las entidades es el aseguramiento de dicha información, así como también de los sistemas que procesan y ejecutan cada activo de la organización.

Para que exista una adecuada gestión de seguridad de la información al interior de las organizaciones [11] , es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

[11] http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO/IEC 27000 [12]es un conjunto de estándares desarrollados o en fase de desarrollo por ISO e IEC, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Este estándar proporciona y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información. El diseño e implementación de este estándar debe ser tomada en cuenta estratégicamente para la organización ya que se pretende que el SGSI extienda con el tiempo soluciones y mejoras a las necesidades de la organización.

La ISO 27000 a semejanza de otras normas es una serie de estándares[13] relacionados con sistema de gestión de seguridad de la información las cuales son:

- ISO/IEC 27000**:** Esta norma tiene estándares que contienen términos y definiciones que se emplean en toda la serie 27000 con el fin de que eviten distintas interpretaciones de conceptos técnicos y de gestión.
- ISO /IEC 27001: Esta norma tiene los diferentes requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información, contiene a la vez valoración y tratamiento de riesgos de seguridad de la información adoptada a las necesidades de la organización.
- ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
- ISO/IEC 27003: Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

[12] https://estandarisosevolucion.wordpress.com/iso-27000/
[13] http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ISO27.php

- ISO/IEC 27004: Guía de las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.
- ISO/IEC 27005: Guía que está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ISO/IEC 27006: Guía que Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- ISO/IEC 27035: Proporciona una guía sobre la gestión de incidentes de seguridad en la información.

3.1.5. Norma ISO /IEC 27001: 2013. Es una norma internacional emitida por la Organización Internacional de Normalización (ISO)[14] 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.

ISO 27001[15] puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación

[14] https://advisera.com/27001academy/es/que-es-iso-27001/
[15] http://auditoriasistemas10141.blogspot.com.co/2015/11/segundo-corte-norma-27001.html

independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO[16] es un estándar que proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Protege la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

El origen de la Norma ISO 27001 [17]está en el estándar británico BSI (British StandardsInstitution) BS7799- Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de Octubre de 2005.

Los beneficios que aporta la ISO 27001 a la organización son:

- Cumplir con los requerimientos legales
- Obtener una ventaja comercial
- Menores costos
- Brindar una mejor organización
- Mejoramiento de imagen y reputación frente a clientes o proveedores

[16] http://www.iso27000.es/download/doc_iso27000_all.pdf
[17] https://es.wikipedia.org/wiki/ISO/IEC_27001

3.1.6. Ciclo De Mejora Continua. Es una estrategia de mejora continua de la calidad[18], basada en un concepto ideado por Walter A. Shewhart. Es muy utilizado por los sistemas de gestión de la calidad (SGC) y los sistemas de gestión de la seguridad de la información (SGSI).

Los resultados de la implementación de este ciclo permiten a las empresas una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costos, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad de la empresa u organización[19].

Figura 1. Ciclo de mejora continua

Fuente: (http://www.iso27000.es/download/doc_sgsi_all.pdf)

- Plan (planificar): establecer el SGSI.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI.

[18] http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html
[19] https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

3.1.6.1. Descripción de los ciclo de mejora continua PHVA.[20]

3.1.6.1.1. Planificación.

- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología que define el alcance y los límites del SGSI.
- Definir política de seguridad: incluye el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección.
- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.
- Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

[20] http://www.iso27000.es/download/doc_sgsi_all.pdf

- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable o requiere tratamiento.
- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido, eliminado, aceptado o transferido
- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento.
- Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control.

3.1.6.1.2. Implementación.

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.

- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

3.1.6.1.3. Seguimiento.

- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado
- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.
- Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001.
- Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

3.1.6.1.4. Mejora Continua.

- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

3.2. Marco conceptual

- Amenaza**:** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos.
- Confidencialidad**:** aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.
- Disponibilidad: aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
- Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- ISO 27001/2013: es 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.
- Perdida de información o datos: se presenta por factores como la incapacidad de acceder a cualquier dato desde un sistema de computación en funcionamiento o una copia de seguridad, la supresión accidental de archivos o la sobrescritura de estructuras de control de datos, archivos dañados o con acceso bloqueado debido al funcionamiento anormal, errores humanos, condiciones adversas del entorno o falla de dispositivos de computo.
- Seguridad informática: Identifica vulnerabilidades de sistemas brindado con esto controles o medidas que eviten diferentes vulnerabilidades o amenazas a sistemas de cómputo.

- Sistemas de gestión de seguridad de la información (SGSI): es un conjunto de políticas de administración de la información. es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission.
- Virus Informático: son sencillamente programas maliciosos (**malwares)** que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo.
- Vulnerabilidad: es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.
- Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.
- Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.
- Causa: Razón por la cual el riesgo sucede.
- Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.
- Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico
- Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

- Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

4. Metodología

Para dar solución a la situación problema expuesta en XY S.A.S, la metodología planteada busca dar cumplimiento a los objetivos específicos definidos para alcanzar el objetivo general, teniendo en cuenta el marco de referencia de la norma ISO/IEC 27001:2013, eso con el fin de cumplir con los requerimientos necesarios para diseñar un Sistema de Gestión de Seguridad e la Información, la cual tiene como base la tecnología de la información, técnicas de seguridad, gestión de la seguridad de la información y los requisitos básicos para dar cumplimiento a la norma.

Para realizar el diagnóstico inicial de la Organización fue empleado el método de investigación de campo mediante entrevistas con la alta dirección, los funcionarios y la documentación existente en la organización, además se tuvieron en cuenta algunos textos, libros y documentación existentes sobre el diseño de un SGSI.

Para el desarrollo del proyecto se establecieron las siguientes fases:

Figura 2. Fases para el diseño del SGSI de la entidad

Fuente: Autores

4.1. Fase 1 – Planeación

Se refiere a las actividades realizadas para identificar el estado actual de la organización, respecto a temas de seguridad de la información de acuerdo a los lineamientos de la norma ISO/IEC 27001:2013.

Para el desarrollo de esta fase se emplearan los siguientes mecanismos:

- Entrevistas con la alta dirección, esto con el fin de percibir que concepción tienen respecto a la Seguridad.
- Revisión de documentación existente y oficializada en la organización, tal como procesos, procedimientos, definición de roles y perfiles entre otros.
- Revisión de Organigrama, objetivos estratégicos y conocimiento de la organización, mediante visita a las áreas y algunas entrevistas con los empleados de la organización.

- Análisis de GAP, para determinar con una serie de preguntas el estado actual de la organización.

4.2. Fase 2– Diseño

Contempla las actividades de definición y alcance del diseño del Sistema de Gestión de Seguridad de la Información, a continuación se describen las acciones a desarrollar:

- Definición del alcance, reunión con la alta dirección para determinar hasta donde esperan llegar con el diseño de SGSI.
- Definición de estructura, como estará enfocado el SGSI, como se definirán los roles y las responsabilidades del mismo.
- Definición de políticas, determinar que políticas se aplicaran y como se enfocaran para la organización.
- Desarrollo de metodología de riesgos, para determinar cómo se realizara la evaluación de riesgos.

4.3. Fase 2– Implementación

En esta fase se desarrollaran todos los entregables para la organización, a continuación se enumeran las actividades a desarrollar:

- Identificación y clasificación de activos de información, se realizaran entrevistas con los líderes de área y se determinaran cuales activos poseen y su nivel de criticidad.
- Análisis de riesgo, con la metodología planteada en la fase de diseño, se realizara un análisis de riesgo inherente y se determinara a que riesgos altos se encuentra expuesta la organización.

- Se desarrollara el manual del Sistema de Gestión de Seguridad de la Información.

5. Resultados y discusión

De acuerdo a la metodología planteada en el capítulo anterior, a continuación, se describen cada una de las fases desarrolladas para lograr los objetivos propuestos.

En este capítulo de resultados y discusión se planteará paso a paso los diferentes elementos, datos recolectados y realizados para el desarrollo de cada una de las actividades de las fases de la metodología.

5.1. Fase 1 – Planeación

Teniendo en cuenta la metodología anterior en esta fase se realizó un estudio general de la compañía, esto con el fin de conocer sus procesos y el core del negocio, así mismo determinar la madurez en la que se encuentra la empresa respecto a temas de seguridad de la información, para esto se desarrolló un GAP análisis apoyados en la norma ISO 27001, a continuación, se describe claramente cómo se encuentra compuesta la compañía:

5.1.1. Conocimiento de la entidad. XY S.A.S. Es una empresa anónima que presta el servicio de Obra, Consultoría e Interventoría de obras civiles, en el sector público y privado a nivel nacional, la cual utiliza una metodología para la estructuración de proyectos donde brinda la solución de problemas y reduce costos para un mejor desempeño, mientras se

minimiza los riesgos. Esta empresa se encuentra vigilada y controlada por la Superintendencia de Industria y Comercio y otros entes de control como Fonade, Invias.

Misión: es una empresa que presta el servicio de Obra, Consultoría e Interventoría de obras civiles, en el sector público y privado a nivel nacional, con alto grado de calidad en sus servicios. Son una empresa enfocada a proteger el ambiente, controlar los recursos y brindar seguridad a los recursos humanos, esto con el fin de poder cumplir con las actividades especificadas para así satisfacer a sus clientes.

Visión: Ser una de las principales empresas de obra, interventoría y consultoría a nivel nacional e internacional, enfocándose en el desarrollo de proyectos de calidad.

Servicios que ofrece: XY S.A.S ofrece servicios para proyectos de obra civil, consultoría, interventoría, gerencia y estructuración de proyectos tanto del servicio público como privado, teniendo en cuenta las normas vigentes que regulen los respectivos servicios

De los servicios que se describieron anteriormente, la empresa XY S.A.S los cataloga de la siguiente manera:

Cuadro 4.
Servicios que ofrece XY S.A.S

CONSTRUCCION	INTERVENTORIA	CONSULTORIA
• Edificaciones. • Alcantarillado. • Vías. • Acueducto. • Obras de urbanismo, parques, espacio público.	• Obras de edificaciones • Obras de alcantarillado • Obras de vías • Obras de acueductos	• Obras de edificaciones • Obras de alcantarillado • Obras de vías • Obras de acueductos • Obras civiles (urbanismo, parques, espacio público).

Fuente: Autores

5.1.1.1. Estructura organizacional.

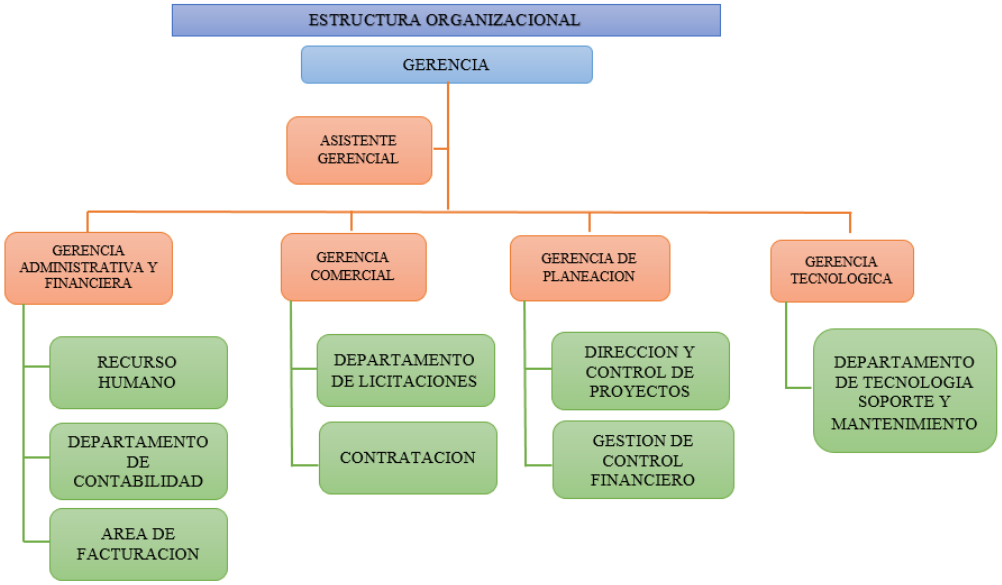

Figura 3. Organigrama de la entidad

Fuente: La entidad

5.1.1.2. Mapa de procesos.

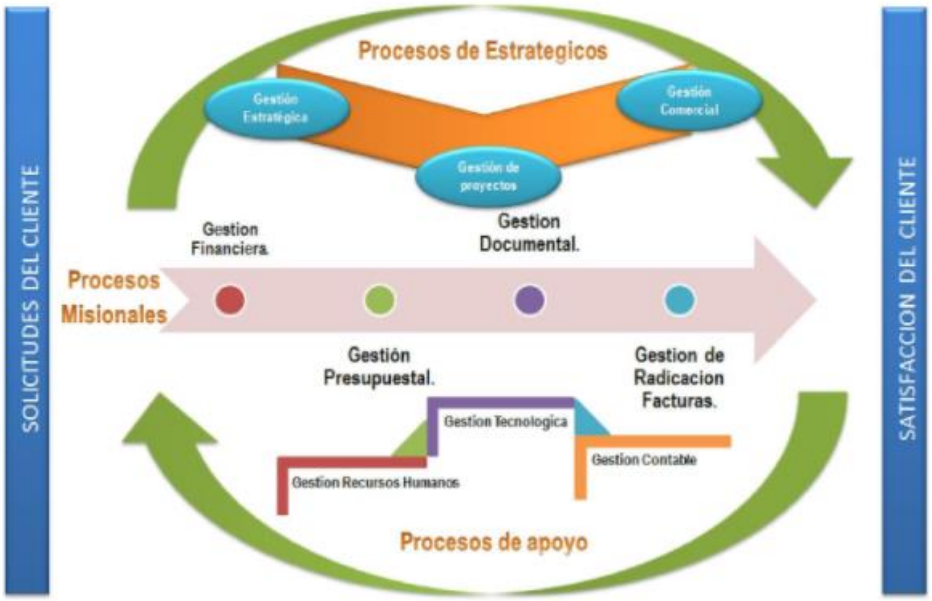

Figura 4. Mapa de procesos de la Entidad

Fuente: La Entidad

5.1.1.3.Descripción de las áreas de la entidad.

- Gerencia General: Ejerce la representación legal de la empresa donde define y dirige la estrategias organizacionales y lineamientos de calidad con lo cual controla la correcta asignación de los recursos para la operación de los procesos, garantizando así el logro de las estrategias corporativas. Es responsable ante los accionistas e inversionistas, por los resultados de los proyectos, consultorías e interventorías y el desempeño de las actividades organizacionales de la entidad.
- Gerencia administrativa y financiera: Dirige los procesos y procedimientos de acuerdo a las estrategias, políticas, normas, directrices y programas con el fin alcanzar los objetivos de la organización Planea, coordina y controla los recursos y

la información financiera de la Organización, con el fin de garantizar el rendimiento disponibilidad, uso adecuado de los recursos financieros para el desarrollo normal de las operaciones, maximiza la rentabilidad de los mismos y asegurar la viabilidad financiera a largo plazo. Esta área es responsable abastecer de recursos financieros a la organización para cumplir con los proyectos y servicios que ofrece para así contribuir al desarrollo organizacional donde el área brinde a la entidad información clara, confiable, exacta y responsable de la contabilidad para que la gestión de recurso humano realice sus procesos establecidos por la organización para su buen funcionamiento.

- Gerencia Comercial: Planifica, organiza, dirige, controla y coordina eficientemente la gestión comercial, administrando la fuerza de ventas que permita el logro de los objetivos estratégicos y corporativos de mercado, con el fin de garantizar el cumplimiento de metas comerciales y garantizar los estándares y niveles de servicio generando satisfacción a sus clientes. Esta área es responsable de contribuir con la entidad para el desarrollo organizacional con la aportación en estudios de mercadeo para la gerencia de proyectos también mantiene e incrementa la imagen de la organización y elabora estudios en materia para la integración de proyectos de inversión.
- Gerencia de planeación: Elabora, gestiona y supervisa proyectos donde administra riesgos e integra y elabora informes. Esta área es responsable de la entrega en tiempo y forma de los proyectos constructivos con los resultados establecidos o mejorados también en contribuir con propuestas de proyectos constructivos innovadores y altamente rentables para el desarrollo organizacional.

- Gerencia tecnológica: Coordina, soporta, mantiene y controla los recursos tecnológicos, es responsable de salvaguardar y proteger los activos de la organización, a través de planes, políticas y estrategias tecnológicas para la adquisición, uso y creación de tecnología esto para cumplir con planes y procedimientos tecnológicos.

5.1.1.4. Recursos de la entidad.

Cuadro 5.
Descripción de recursos de la entidad XY.S.A.S

PARÁMETROS DE EVALUACIÓN	**RESPUESTA**	**OBSERVACIONES**
Presupuesto de la entidad	5.000.000.000 a 10.000.000.000 COP	Para el 2015 fuente: La entidad
Número total de computadores	50 computadores en total De la cual 15 son de escritorio y 35 portátiles	Dato adquirido del departamento tecnología
Número de Servidores	5 servidores 2 Linux y 3 Windows en total	Dato adquirido del departamento tecnología
Número impresoras	10 impresoras en total De la cual están distribuidas de a dos en cada área de la organización	Dato adquirido del departamento tecnología
Número Empleados	50 empleados en total De la cual son todos los empleados.	Dato adquirido del departamento recursos humanos

Fuente: Autores

5.1.2. Diagnóstico identificado después de conocer la organización. En esta primera fase se realizó el conocimiento previo de la organización, en donde se identificó que la empresa cuenta con un presupuesto que oscila entre 5.000.000.000 a 10.000.000.000 COP, a pesar de que con una licitación ganada pueden obtener altos ingresos, se identificó que estos han disminuido por incumplimientos en la normatividad de protección de datos personales y por desprestigio, debido a algunos incidentes de seguridad que se han materializado.

Además se observó que aunque la empresa no sobrepasa los 50 empleados ya que cada proyecto se tercerizara, la socialización y el conocimiento en temas de seguridad de la información es escaso, esto debido a que la alta gerencia no le daba importancia a estos temas, por tanto como recomendación general se sugiere incluir el sistema de gestión de seguridad de la información dentro de los objetivos estratégicos de la organización, teniendo en cuenta la afectación que se está generando por el incumplimiento de lineamientos básicos de seguridad.

De acuerdo a lo anterior y a las evidentes amenazas a las que se enfrentaba la organización, se realizó un análisis de GAP teniendo en cuenta los lineamientos de la Norma ISO27001, esto con el fin de realizar un diagnóstico estadístico del estado actual de la organización frente a seguridad de la información.

Un análisis de GAP es un análisis de brecha que permite identificar el estado real de una organización frente a un tema en específico, la construcción de este documento se realizó tomando la norma ISO27001 y por cada uno de los numerales generales y de los anexos

se propuso una pregunta específica, adicionalmente se ingresaron valores de calificación cuantitativa a cada una de las preguntas planteadas, cada numeral contiene una series de preguntas y representan un porcentaje de acuerdo a la respuesta seleccionada por ejemplo:

El numeral de la norma A5 describe todo lo relacionado con políticas de la seguridad de la información y se divide en dos sub numerales, en este caso el A.5.1.1 y el A.5.1.2 de cada uno de estos sub numerales se desprenden una serie de preguntas a las cuales se les da un valor de calificación, si la respuesta es no, pues tendrá un valor de 0% y si por el contrario es si tendrá un valor especifico de acuerdo a las preguntas, el resultado de todas debe ser igual a un 100% cuando se termine la evaluación, el análisis arrojo qué porcentaje de madurez en el que se encuentra la organización.

Cuadro 6.
Análisis de GAP

Numeral	Control y controles		Respue	nplin
A.5	**POLITICAS DE LA SEGURIDAD DE LA INFORMACIÓN**			**17%**
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información			17%
A.5.1.1	Politicas para la seguridad de la información	¿La organización cuenta con un documento de politicas de SI?	NO	0%
		¿Existen procedimientos relativos a seguridad de la información?	SI	17%
		¿Existe una comunicación formal a todos los colaboradores de la organización de la politica de SI?	NO	0%
		¿La politica de SI se encuentra aprobada por la dirección?	NO	0%
		¿La politica de SI se encuentra publicada y es de facil acceso para los funcionarios y partes externas pertinentes?	NO	0%
A.5.1.2	Revisión de las politicas para la seguridad de la informació	¿Las politicas de seguridad de la información son revisadas durante intervalos de tiempo regulares?	NO	0%

Fuente: Autores

Después de realizar el formato de análisis de GAP para cuantificar el estado de la organización frente a seguridad de la información, se realizaron reuniones con la alta dirección y las diferentes áreas de la organización, de acuerdo a los procesos identificados. El análisis realizado podrá ser consultado en el Anexo A.GAP análisis XY.S.A.S 27001, con base a la información recopilada, a continuación, se muestran los resultados obtenidos:

Aunque la compañía tiene alguna documentación oficial en cuanto a los procesos de la organización y que además de esto se han realizado algunas implementaciones de seguridad, la empresa solo cumple con el 30% de los controles solicitados por la norma, esto se debe a que no hay un área específica que se dedique a trabajar en temas de seguridad de la información, adicionalmente nunca se ha realizado una valoración de riesgos o un inventario base de activos de la información.

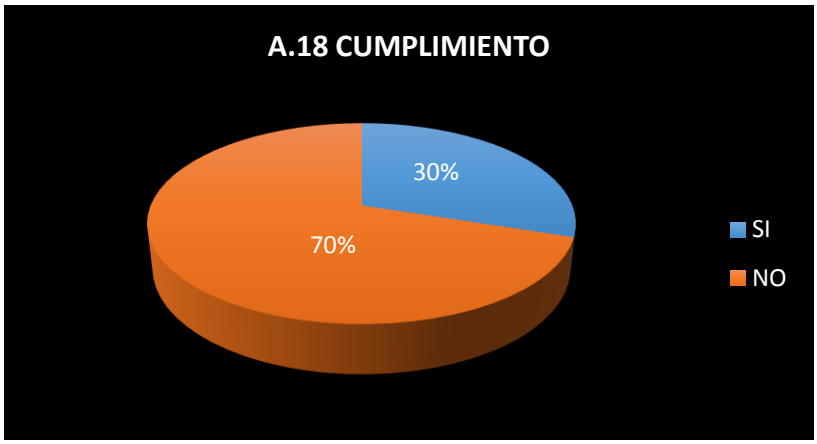

Figura 5. Nivel de cumplimiento control Anexo A ISO 27001:2013

Fuente: Autores

Lo anterior implica que la organización no tiene la madurez suficiente en temas de seguridad, lo cual implica que deben realizar un esfuerzo considerable para conseguir un cambio satisfactorio, muchos de los cambios e implementaciones que deben realizarse son cambios referentes a la percepción de la organización en temas de seguridad de la información, para lo cual deberá hacerse una inversión considerable de tiempo y de presupuesto para las mejoras del sistema.

Con el análisis de GAP realizado se pueden hacer varias aproximaciones y definiciones, esto con el fin de conocer el porcentaje de cumplimiento por procesos así:

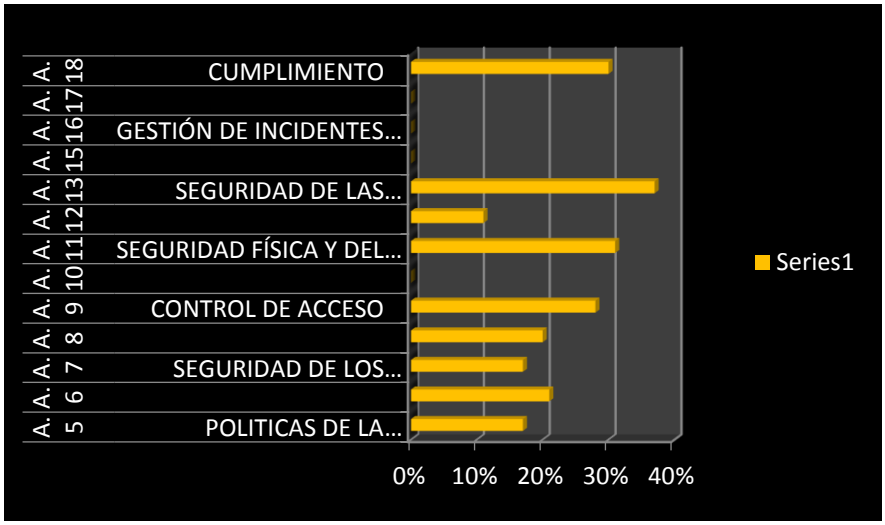

Figura 6. Niveles de controles de anexo A ISO 27001

Fuente: Autores

Como se puede observar ningún porcentaje con respecto al anexo A de la norma se encuentra en porcentaje alto de cumplimiento, de acuerdo a lo anterior se han presentado algunos incidentes de seguridad en la organización, lo cual refleja que, aunque hay algunos controles implementados, estos no proveen los resultados esperados dentro de la empresa.

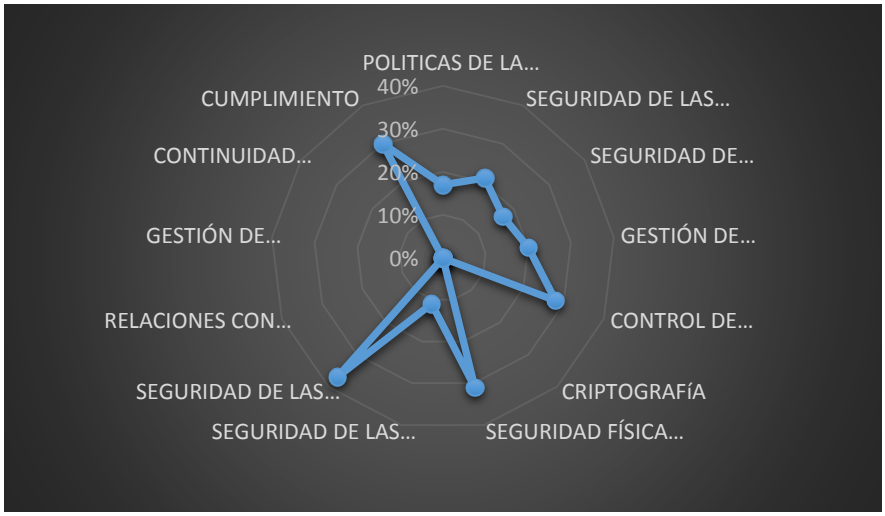

Figura 7. Nivel cumplimiento todos los controles anexo A ISO 27001:2013

Fuente: Autores

Cuadro 7.
Descripción de porcentajes de control de Anexo A

ANEXO	CONTROL	%
A.5	Políticas de la seguridad de la información	17%
A.6	Seguridad de las comunicaciones	21%
A.7	Seguridad de los recursos humanos	17%
A.8	Gestión de activos	20%
A.9	Control de acceso	28%
A.10	Criptografía	0%
A.11	Seguridad física y del entorno	31%
A.12	Seguridad de las operaciones	11%
A.13	Seguridad de las comunicaciones	37%
A.15	Relaciones con los proveedores	0%
A.16	Gestión de incidentes de seguridad de la información	0%
A.17	Continuidad del negocio	0%
A.18	Cumplimiento	30%

Fuente: Autores

De acuerdo a los resultados obtenidos por el análisis de GAP a continuación se describe el porcentaje de cumplimiento en cuanto el anexo y la razón del incumplimiento.

- A5 Políticas de Seguridad de la información (17%): Aunque existen algunos documentos o políticas no formales, estas no han sido divulgadas a todos los empleados y no han sido actualizadas ni aprobadas por la alta dirección.
- A6 Seguridad de las Comunicaciones (21%): Actualmente existen servicios segmentados por VLAN, pero no se han implementado algunos controles específicos para proteger la información o los sistemas, además la transferencia de información con proveedores se realiza de forma convencional, sin tener en cuenta ninguna política de transferencia segura, es aquí donde claramente se

evidencia un incumplimiento en la normatividad exigible por la ley en cuanto a protección de datos personales. Si bien existen acuerdos de confidencialidad con empleados y proveedores y regularmente se revisan y se documentan estos acuerdos, es necesario implementar ciertas medidas adicionales de protección de información.

- A7 Seguridad de los recursos humanos (17%): Durante el proceso de contratación se realiza un estudio exhaustivo de los antecedentes y del historial del candidato, además durante la contratación se hace firmar un acuerdo de confidencialidad, pero no hay un plan formal de capacitación para la toma de conciencia, a su vez no existe un comité disciplinario formal para emprender acciones en contra de empleados que atenten contra la seguridad de la información, de acuerdo a lo anterior, la organización se encuentra expuesta a fuga de información, ya sea por desconocimiento de los empleados o por manipulación de los mismos.
- A8 Gestión de Activos (20%): Existe un inventario detallado de activos con un propietario establecido, pero no se tiene un procedimiento claro de cómo clasificar estos activos, o de cómo proceder para realizar la devolución de los recursos tecnológicos cuando se termina la labor del empleado, además todos los dispositivos removibles se conectan a los equipos de cómputo sin ningún tipo restricción, este evento de riesgo puede generar grandes afectaciones de fuga de información o infección en los equipos de cómputo.
- A9 Control de Acceso (28%): En este momento no existen políticas de control de acceso definidas, ni un proceso formal de registro y cancelación de usuarios,

muchos usuarios registrados en el sistema se encuentran activos, pero ya no laboran en la organización, aunque existen unas restricciones de acceso a los sistemas, no son suficientes para garantizar el acceso a usuarios no autorizados.

- A10 Criptografía (0%): Actualmente la organización no cuenta con una política de cifrado de información y toda la información que se comparte se realiza a través de correo electrónico o mediante medios removibles, sin ningún tipo de aseguramiento, es necesario implementar algunos controles básicos de seguridad que permitan compartir información de forma segura, de acuerdo al tamaño de la organización y que no están interesados en realizar una gran inversión en seguridad, se deben implementar controles básicos como poner contraseñas a los documentos de texto y enviar las carpetas comprimidas con contraseña.
- A11 Seguridad Física y del Entorno (31%): En este momento existen algunos perímetros de seguridad física designados y la organización cuenta con controles de acceso biométricos, estos mecanismos no se usan correctamente y los usuarios no son conscientes de registrar su ingreso cada vez que accedan a cualquier zona de las instalaciones, además no hay una matriz de perfilamiento para el control de acceso.
- A12 Seguridad de las Operaciones (11%): Existen procedimientos operacionales formalizados y se utilizan los recursos para asegurar el buen desempeño del sistema, pero los cambios realizados al sistema se realizan de forma no controlada causando indisponibilidad a la operación, además los ambientes de producción y pruebas no se encuentran separados.

- A13 Seguridad de las comunicaciones (37%): Aunque los servicios de red se encuentran segmentados por VLANS, no existen acuerdos de nivel de servicio en la red y no existen controles para proteger el sistema core del negocio frente a una caída.
- A14 Adquisición, Desarrollo Y Mantenimiento Del Sistema: En la organización no se realiza desarrollo del sistema, por lo tanto, el análisis de este anexo de la norma no fue tenido en cuenta durante el presente análisis.
- A15 Relaciones con los proveedores (0%): no existen políticas para mitigar el riesgo de acceso de la información por parte de los proveedores, ni se tienen en cuenta los riesgos existentes por parte de los proveedores, razón por la cual es importante velar porque terceras partes garanticen la prestación del servicio de una manera adecuada y favorable para la organización.
- A16 Gestión de incidentes de seguridad de la información (0%): Debido a que la organización no tiene implementado una metodología de análisis de riesgo, no tiene contemplado como gestionar, registrar incidentes de seguridad, los eventos ocurridos con anterioridad son atacados sin ningún tipo de control, y si medir resultados a fin de que no se vuelvan a materializar, en ese orden de ideas la implementación eficaz del procedimiento de gestión de incidentes apoyara la mitigación de riesgos en la organización.
- A17 Continuidad del negocio (0%): Debido a la madurez de la organización en temas de seguridad de la información, no se tiene contemplado un plan de continuidad del negocio, cuando ocurren eventos por corte de fluido eléctrico simplemente se detiene la operación hasta que los servicios se restablezcan, se

cuenta con una UPS con duración máxima de 30 minutos para apagado de equipos y servidores, esto con el fin de no causar tanta afectación a la operación.

- A18 Cumplimiento (30%): De acuerdo al análisis anterior, es posible determinar que el cumplimiento de la organización frente a los controles establecidos en la Norma ISO/IEC 27001:2013, se están incumpliendo en un 70%, si en este momento se hiciera una revisión de algún ente regulador, los resultados no serían satisfactorios, lo cual podría incurrir en multas o sanciones legales, por esta razón es importante diseñar un Sistema de Gestión de Seguridad de la Información que apoye las mejoras y la implementación de ciertos controles mínimos para ser una organizaci0on competente en temas de seguridad

Tras el diagnostico general de la organización se identificó que se han presentado varios eventos de seguridad debido a la perdida de información sensible, además se presentan algunos incumplimientos de la ley de protección de datos personales, a continuación, se muestran algunos factores detallados de la situación problema:

- Falta de interés de alta gerencia en temas de Seguridad de la Información
- Conocimiento limitado de los empleados en temas de seguridad.
- No existe una metodología de valoración de eventos.
- Se presentan eventos de perdida de información
- Perdida de licitaciones por incumplimientos normativos
- Las herramientas tecnológicas no están configuradas para brindar aseguramiento.
- Existe poca documentación acerca de Seguridad de la información en la entidad.

Cuando se identificó el panorama real de la organización en temas de seguridad, a que se dedica, cuáles son sus procesos más críticos y que medidas de seguridad de la información se encuentran implementados, se determinó que el Diseño de Un sistema de Gestión de Seguridad de la Información apoyaría sustancialmente a la organización a tener un enfoque real y consecuente de cómo gestionar este tipo de temas y a adquirir un poco más de madurez de la que actualmente posee.

Con la ejecución del análisis de GAP, no se tuvieron inconvenientes, ya que las preguntas planteadas en el GAP fueron concisas y los ejecutivos de cada proceso tenían las respuestas claras, lo cual acelero el proceso de conocimiento de la organización en temas de seguridad.

El anexo A cumple con el alcance del objetivo general del proyecto, ya que antes de construir un manual de SGSI es necesario conocer la empresa y saber el nivel de madurez que posee en temas de seguridad de la información.

A continuación, en la fase de diseño se describirán como se realizó paso a paso el diseño del SGSI.

5.2. Fase 2– Diseño

Para iniciar la fase de diseño se tuvieron en cuenta los alcances de la organización, los servicios que presta, la identificación de sus principales proveedores y su fuente de ingreso, después de este análisis se determinó que para la compañía es muy importante cumplir con algunas normativas legales como “la ley de protección de datos”, entre otras, para mejorar su

competitividad y lograr ganar más licitaciones de las que hasta el momento ha ganado, partiendo de esta premisa se le indica a la alta dirección que el tema de protección de datos personales no consiste solo en realizar el registro ante la superintendencia de industria y comercio, sino que además es necesario mantener seguridad de la información sobre todas las bases registradas.

De acuerdo a lo anterior, en reunión con la alta gerencia se determinó el alcance que tendría el SGSI, ya que este alcance se define de acuerdo a las necesidades de la organización y teniendo en cuenta la norma ISO 27001, en la cual se determinó que por el tamaño reducido de la misma es viable implementar este alcance para todos los procesos de la organización, teniendo en cuenta el lugar donde se encuentra ubicada, sus activos de información y la tecnología con la que cuenta, es así como se construyó el siguiente alcance para la empresa XY S.A.S.

5.2.1. Definición De Alcance SGSI. De acuerdo a la Norma ISO/IEC 27001:2013, la compañía debe determinar los límites de aplicabilidad del SGSI, por esta razón, el alcance definido para la empresa XY S.A.S se demarca a continuación:

Alcance SGSI

El diseño del sistema de gestión de seguridad de la información de la empresa XY S.A.S, abarca todos los procesos de la organización, por tanto, es de aplicación general para todos los empleados y las personas que directa o indirectamente tengan algún vínculo con la compañía.

El sistema de gestión de seguridad de la información estará administrado y actualizado por el área de tecnología, siempre y cuando no exista un área de riesgo o de seguridad de la información asociada a la compañía.

5.2.2. Definición de Estructura de roles. En el desarrollo de la estructura que tendrá el SGSI, se realizó una reunión con la alta dirección en donde se les expusieron varios aspectos generales, como, que la implementación de un SGSI debe tener una estructura de participantes activos en donde cada quien tenga clara su función para lograr que el sistema se mantenga y alcance la madurez que se espera obtener , tras esta reunión y de acuerdo al diagrama de procesos, se estableció la siguiente estructura donde la organización definió roles y responsabilidades que involucran a todos los niveles de la Organización (Directivo, estratégico y operacional).

La definición de estructura de roles de la empresa XY S.A.S estará incluido dentro de este documento el cual se referencia como Anexo B. Definición de estructura de roles.

De acuerdo a lo anterior el Anexo B de definición de estructura de roles se define a continuación:

Cuadro 8.
Definición de estructura roles y responsabilidades

Nivel	Rol	Responsabilidad
Directivo	Alta Gerencia	▪ Suministrar los recursos que permitan establecer, implementar, operar hacer seguimiento, revisar, mantener y mejorar el SGSI de la Compañía, para que las iniciativas relacionadas con la Gestión de Seguridad de la Información se lleven a cabo y para que los lineamientos definidos se implementen. ▪ Promocionar la Cultura de Seguridad al interior de la Compañía, teniendo en cuenta el cumplimiento de las Políticas y lineamientos definidos en materia de Seguridad de la Información y Protección de Datos Personales. ▪ Aprobar el alcance, políticas, lineamientos, normas, directrices y procedimientos, así como herramientas, manuales, modelos de

Nivel	Rol	Responsabilidad
		operación, metodologías y estructuras organizacionales empleadas para la gestión del SGSI, seguimiento a su cumplimiento y actualización permanente.
Táctico	Comité Disciplinario	▪ Determinar la procedencia de abrir procesos disciplinarios por el incumplimiento de políticas y lineamientos de seguridad de la información-protección de datos personales y/u ocurrencia de incidentes de seguridad de la información que involucren a un funcionario de la Compañía. ▪ Reportar al tercero cuando correspondan a funcionarios no vinculados a la Compañía para iniciar el proceso disciplinario a que haya lugar, por el incumplimiento de las políticas y lineamientos de Seguridad de la Información y Protección de Datos Personales.
Operacional	Gerencia de Tecnología	▪ Adquirir y administrar las herramientas de Seguridad Informática necesarias para el aseguramiento y/o monitoreo de la infraestructura tecnológica de la organización. ▪ Implementar las políticas, lineamientos, normas, estándares y procedimientos sobre Seguridad Informática. ▪ Participar en la mitigación de riesgos y vulnerabilidades de Seguridad de la Información. ▪ Gestionar proyectos que permitan mitigar riesgos de Seguridad Informática. ▪ Propender por incentivar la Cultura de reporte a todos los empleados y terceros con los que tenga relación la Compañía.
	Gerencia Administrativa	▪ Gestionar proyectos de Seguridad Física y relacionada con Gestión Documental.

Nivel	Rol	Responsabilidad
		▪ Implementar políticas, lineamientos, normas, estándares y procedimientos sobre Seguridad Física, relacionada con Gestión Documental, procesos de Gestión Humana y gestión de proveedores que permitan mitigar riesgos de seguridad de la información. ▪ Propender por incentivar la Cultura de reporte a todos los empleados y terceros con los que tenga relación la Compañía.
	Todos los procesos, áreas Funcionarios, Contratistas, Proveedores y Terceros	▪ Conocer y cumplir las disposiciones y lineamientos de Seguridad de la Información y Protección de Datos Personales que gestionan en cumplimiento de sus labores en la Compañía y según aplique en cada caso. ▪ Informar cualquier incidente de seguridad que evidencie dentro de las actividades diarias.

Fuente: Autores

Con la identificación de los roles no se tuvieron inconvenientes ya que en la página web de la entidad se pudo encontrar con mayor facilidad el mapa de procesos y este se tomó como guía para identificar con mayor facilidad la estructura, adicionalmente las reuniones con la alta gerencia fueron efectivas para definir los roles y responsabilidades de cada proceso.

Teniendo en cuenta el anexo B aporto una de las definiciones principales del manual de seguridad de la información, ya que con la identificación de los roles se asignaron funciones a cada proceso de la organización.

5.2.3. Política de Seguridad de la Información. Para el desarrollo de la política, se tomó como base los lineamientos básicos bajo los cuales se regirá la organización para

implementar el sistema de seguridad de la información, con el fin de demostrar el compromiso de la alta dirección son ellos los que deben construirla en dicha política se deben incluir, los objetivos de Seguridad de la Información, se debe contemplar el compromiso y la mejora continua del sistema, además esta política debe estar documentada y comunicada a todos los integrantes de la organización. La política SGSI de la empresa XY S.A.S estará incluida dentro de este documento la cual se referencia como Anexo C.Política SGSI - definición de políticas.

De acuerdo a lo anterior el Anexo C de la política del Sistema de Seguridad de la Información que se definió para la compañía seria:

POLITICA SGSI

Teniendo en cuenta que para la empresa XY S.A.S, la información es un activo fundamental para la prestación de los servicios y consientes de las necesidades actuales XY S.A.S implementa un modelo de Gestión de Seguridad de la información en cumplimiento de su misión para satisfacer las necesidades de sus clientes y colaboradores, en cumplimiento con la normatividad, requerimientos legales, contractuales, regulatorios y de negocio vigentes.

De acuerdo a lo anterior es preciso tener en cuenta que dentro de los activos de información, se incluyen las bases de datos que contienen Datos Personales, a las cuales se les deben brindar medidas de protección apropiadas, con el fin de cumplir con los requerimientos establecidos en la Ley 1581 de 2012 respecto al tratamiento de dicha información, por lo cual cada proceso, será responsable del apropiado manejo de estos datos, con el fin de garantizar los principios de veracidad, calidad, seguridad, confidencialidad, acceso y circulación restringida. Es por ello que la alta dirección, se compromete con la protección de la confidencialidad, integridad y disponibilidad de la

información, para lo cual se debe implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013 y fundamentado en el pertinente análisis de riesgos a los cuales ésta se encuentra expuesta, apuntando al cumplimiento de los requisitos legales vigentes, reglamentarios y contractuales que en la materia sean aplicables a la Organización

Por lo anterior la compañía busca cumplir con los siguientes objetivos:

- Cumplir con los principios de seguridad de la información.
- Conservar la confianza de sus clientes y empleados.
- Proteger los activos de la información.
- Establecer las políticas, procedimientos para propender la seguridad de la información.
- Sensibilizar y generar cultura en materia de seguridad de la información a todos los funcionarios y personas que desarrollen sus labores al interior de la organización.

Así mismo, se propenderá por el mantenimiento del Manual del sistema de Gestión de Seguridad de la Información, aportando los recursos humanos y técnicos necesarios para la implementación de acciones formativas y de sensibilización destinadas a que se conozcan y cumplan las responsabilidades en esta materia, se gestionen los incidentes en seguridad de la información y se implementen los controles necesarios para la mitigación de los riesgos relacionados.

El cumplimiento de las directrices en seguridad de la información consignadas en el manual, es obligatorio para todos los funcionarios, proveedores y/o contratistas que tengan relación directa o indirecta con la seguridad de información en cada uno de los

procesos, y en caso de violaciones a las mismas, la organización se reserva el derecho de tomar las medidas administrativas y/o disciplinarias a que exista lugar.

5.2.3.1. Definición de Políticas. Después de tener definida la política general, se creó la necesidad de construir una serie de políticas que cumplieran con los lineamientos expuestos en la norma ISO/IEC 27001:2013, para construir cada una de estas políticas fue necesario reunirse con todas las áreas en general, pero especialmente con el área de tecnología y de acuerdo a las necesidades de la organización y a los mecanismos que ya se tenían, se empezaron a desarrollar cada una de estas políticas, a continuación se menciona a nivel general en que consiste cada una de las ellas:

- Política de selección, vinculación y desvinculación de funcionarios: se establecen lineamientos generales de selección, vinculación y desvinculación de funcionarios, estableciendo políticas de cumplimiento en temas de Seguridad de la Información, esto incluye al personal provisto por terceras partes o contratistas, cuando termine la vinculación con la organización se debe hacer una entrega formal del cargo, incluyendo los recursos tecnológicos que le fueron asignados y realizar una eliminación formal de sus accesos y cuentas de usuarios.
- Política Gestión Activos de Información: Se establecen lineamientos para la clasificación, calificación de activos de información, esto con el fin de determinar la criticidad del activo y proceder con la clasificación adecuada de la información, esta clasificación debe ser desarrollada por el responsable de cada uno de los activos de la información con el fin de protegerlos y salvaguardarlos de acuerdo a su calificación.

- Política Gestión de Medios Removibles: Se establecen lineamientos para el control, monitoreo y restricción de medios removibles de acuerdo al esquema de clasificación de los activos de la información definidos en la política de gestión de activos de la información, cada permiso de acceso de medio removible debe estar justificado por el jefe inmediato del funcionario, además los medios que contienen información categorizada como restringida deben protegerse de accesos no autorizados.
- Política de Control de Acceso: Se establecen lineamientos para monitorear, supervisar y proteger el acceso lógico en la organización, esto con el fin de proteger la información, implementando controles para redes LAN e inalámbricas, además se contempla el acceso de los usuarios al sistema y los controles establecidos para evitar la fuga de información por accesos no autorizados.
- Política de Criptografía: Se establecen lineamientos básicos para controlar él envió o transferencia de información, aunque la organización no esté dispuesta a realizar una gran inversión se deben establecer medios gratuitos y básicos de criptografía, a fin de garantizar la confidencialidad de la información.
- Política de Seguridad Física: Se establecen lineamientos de control para el acceso físico a las instalaciones y la definición de zonas seguras en la organización, entendiendo por zonas seguras las áreas donde se procesa información sensible.
- Política Gestión de Recursos Tecnológicos: Se establecen lineamientos para la asignación, mantenimiento y devolución de los recursos tecnológicos asignados al personal para el desarrollo de sus funciones, garantizando el aseguramiento de

los mismos ante cualquier evento de riesgo que se pueda llegar a presentar a fin de proteger la información que se procesa en el equipo.

- Política de Seguridad en las Operaciones: Se establecen lineamientos para asegurar la documentación de las funciones específicas y propias del negocio, así como la implementación de mecanismos que permitan controlar los cambios realizados en la operación que puedan causar indisponibilidad en los servicios prestados, esto con el fin de garantizar la continuidad de la prestación del servicio a los clientes.
- Política Respaldo de la Información: Establece lineamientos para la implementación de copias de respaldo de equipos de cómputo y servidores de la información crítica de la organización.
- Política de Gestión de Vulnerabilidades: Establece lineamientos para el monitoreo y la ejecución de mecanismos tecnológicos para ejecutar análisis de vulnerabilidades sobre los recursos de la plataforma tecnológica, además incluye la mitigación y corrección de las vulnerabilidades encontradas.
- Política de Gestión con Terceros: Se establecen lineamientos para la contratación, vinculación y desvinculación con terceras partes, esto con el fin de asegurar la información y protegerla de personas externas a la organización, pero que tienen algún vínculo con la compañía, además asegura la prestación del servicio mediante la inclusión de parágrafos relativos a acuerdos de niveles de servicio en el contrato acordado.
- Política de Gestión de incidentes de Seguridad: Establece lineamientos para el reporte, registro, tratamiento y mitigación de incidentes de seguridad.

- Política de Gestión de Continuidad del Negocio: Establece lineamientos y parámetros para garantizar la respuesta efectiva de funcionarios y elementos necesarios ante una contingencia por la materialización de algún evento que afecte la operación normal de las operaciones.

Las políticas descritas anteriormente están atadas al sistema de gestión de seguridad de la información y serán tenidas en cuenta para ser descritas específicamente en el manual SGSI.

Con el desarrollo del anexo C, se presentaron algunos inconvenientes en cuanto a la definición, ya la alta dirección no estaba relacionada con el tema de seguridad de la información, para esto fue necesario realizar varias reuniones que permitieran involucrarlos en este tema, a su vez enfatizar mucho en que la construcción y el desarrollo de un sistema debe ir con la colaboración y participación activa de la alta gerencia, esto con el fin de obtener buenos resultados.

Con la elaboración del Anexo C se contribuyó a la definición de la política general sobre la cual se basa el manual de seguridad de la información, en donde se especificó sobre que principios o lineamientos que se basaría para la ejecución del manual del SGSI en la empresa XY.S.A.S.

5.2.4. Metodología de Riesgo a implementar. Con las definiciones anteriores y teniendo en cuenta que la organización no cuenta con un análisis de riesgo, se creó una metodología teniendo en cuenta las características del negocio, se tomó como base la norma ISO 31000 y la ISO 25000, esta metodología servirá para analizar que riesgos se pueden materializar dentro de la organización por tanto se definieron en las siguientes etapas:

5.2.4.1. Identificación. Esta etapa inicia con la identificación de los activos de información de la Compañía, para desarrollar esta etapa de identificación, se realizaron mesas de trabajo y entrevistas con cada uno de los procesos.

La identificación de estos activos permitirá a la compañía entender que es lo más representativo para su trabajo y que activo posee una mayor criticidad, priorizando las áreas y la información que maneja la organización.

En la tercera fase, la fase de implementación se explicara detalladamente que factores se tuvieron en cuenta para determinar la criticidad de los activos y como se realiza la evaluación de los mismos.

Tras tener el listado de los activos de información se procede con la identificación de los riesgos, los cuales son eventos que pueden llegar a materializarse, o que ya se materializaron y el daño o la perdida que eso puede traer a la organización, por consiguiente se analiza como estos riesgos se pueden mitigar, esto con el fin de planear y estar atentos a minimizar nuevos eventos que se puedan materializar.

5.2.4.2. Medición. Cada activo de la información posee una clasificación en este caso se toman todos los activos de la información, llámese activo de la información a todo lo que contenga información y tenga algún valor para la organización, ya sea, hardware, software, instalaciones, personas, comunicaciones y procesos e información, una vez identificados se evaluaran los tres principios fundamentales de seguridad de la información como lo son: la Confidencialidad, la integridad y la disponibilidad y a cada uno de los principios se le realiza una inspección de acuerdo a la siguiente clasificación:

Cuadro 9.
Descripción de calificación de probabilidad del activo

CALIF	CONFIDENCIALIDAD			INTEGRIDAD		DISPONIBILIDAD	
	CATEGORIA	SUBCATEGORIA	DESCRIPCIÓN	CATEGORIA	DESCRIPCIÓN	CATEGORIA	DESCRIPCIÓN
4	PRIVADA	Restringida	Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información para estricto cumplimiento de sus funciones	Muy Alta	La alteración del dato causa gran afectación en la organización y no es posible que el dato modificado vuelva a estar en su estado inicial, ejemplo cambios	2 Horas	Por un periodo de tiempo de dos horas de indisponibilidad podria causar perdidas significativas
3		Reservada	Es información crítica y solamente podrá ser conocida al interior de la Entidad ya que el conocimiento externo de la misma podrá ocasionar	Alta	La alteración del dato causa afectación y su recuperación puede hacerse con algunass perdidas	4 Horas	Por un periodo de tiempo de cuatro horas de indisponibilidad podria causar perdidas significativas
2		Interna	podra ser conocida por los empleados de la organización	Media	La alteración del dato se puede recuperar, las perdidas son manejables	8 Horas	Por un periodo de tiempo de ocho horas de indisponibilidad podria causar perdidas
1	PUBLICA	Publica	podra ser conocida por todas las personas que tengtan alguna relación con la organización llamese	Baja	La alteración del dato no genera ningun tipo de afectacióon se puede trabajar con el dato	24 Horas o Mas	Por un periodo de tiempo de veinticuatro horas de indisponibilidad podria causar

Fuente: Autores

Teniendo en cuenta la tabla anterior se determinó la criticidad del activo es decir que tanto perjudica a la organización que el activo no se encuentre disponible, así la criticidad es el cálculo automático que determina el valor general del activo, de acuerdo a la clasificación del activo de información.

Por consiguiente con el listado de activos se identifican la probabilidad de que un evento de riesgo se materialice en este activo, es decir la cantidad de veces que el evento ocurre en un periodo determinado, la medición se realiza de la siguiente forma:

Cuadro 10.
Medición de los factores de frecuencia

Nivel		**Significado**	**Cantidad de Eventos**	**% Máx.**
Detalle	**Valor**			
Muy Frecuente	4	Es seguro que el evento ocurra en la mayoría de circunstancias	Mayor a 3	80%
Frecuente	3	Hay buenas razones para creer que ocurrirá según circunstancias.	2 a 3	60%
Moderado	2	Puede ocurrir en algún momento	1 (2 años seguidos)	40%

Nivel		Significado	Cantidad de Eventos	% Máx.
Detalle	**Valor**			
Poco Frecuente	1	Eventualidad poco común	1	20%

Fuente: Autores

El Porcentaje Máximo (% Max.) indica el grado de participación que el evento tiene respecto a la totalidad de eventos reportados en el Horizonte de Tiempo, de forma tal, que a una mayor participación se genera un aumento del Nivel de Frecuencia en el modelo.

Después de determinar la probabilidad se analiza el impacto es decir que tanto me puede afectar esta materialización, las consecuencias de pérdida para la empresa. El impacto que se analizara en este caso estará dado por la siguiente medición:

Cuadro 11.
Medición de los impactos

Nivel		Impacto		
Detalle	Valor	Reputacional	Financiero	Legal
Catastrófico	4	Nacional	Gran magnitud	Intervención
Crítico	3	Sector	Significativas	Si
Moderado	2	Local	Moderadas	Si
Menor	1	No	Bajas	No

Fuente*:* Autores

Existen, muchos tipos de impacto que pueden afectar a una organización, en este caso la empresa XY S.A.S analiza 3 elementos fundamentales de impacto:

- Impacto Reputacional: que destruye valor y percepción de marca para la Empresa.
- Impacto Financiero: Impacto sobre los Estados Financieros y rentabilidad de la Empresa.

- Impacto Legal: Acota las Glosas y sanciones que el Ente de Vigilancia ejecute contra la Empresa por fallos de acción u omisión en los procedimientos y normas.

Después de tener el inventario de los activos de información y la probabilidad o frecuencia y el impacto que le puede causar a la organización, se multiplican estos valores para identificar el riesgo inherente

Figura 8. Formula del riesgo inherente

Fuente: Autores

Dado lo anterior, la fórmula determina la probabilidad de incidencia del Riesgo Asociado, respecto a los Eventos de Riesgos relacionados con éste y los restantes tipos de Riesgo, para lo cual, se ubicará en el corte entre Frecuencia e Impacto en la siguiente matriz o Mapa de Calor:

R. INHERENTE		0 a 20%	20% a 40%	40% a 60%	60% a 80%	> 80%
		Impacto				
	Frecuencia	Insignificante 0 20%	Menor 0 40%	Moderado 0 60%	Crítico 0 80%	Catastrófico 0 100%
> 80%	Muy Frecuente 0 100%	Bajo 0 20%	Moderado 0 40%	Alto 0 60%	Muy Alto 0 80%	Muy Alto 0 100%
60% a 80%	Frecuente 0 80%	Bajo 0 16%	Moderado 0 32%	Alto 0 48%	Muy Alto 0 64%	Muy Alto 0 80%
40% a 60%	Moderado 0 60%	Bajo 0 12%	Moderado 0 24%	Moderado 0 36%	Alto 0 48%	Alto 0 60%
20% a 40%	Poco Frecuente 0 40%	Bajo 0 8%	Bajo 0 16%	Moderado 0 24%	Moderado 0 32%	Moderado 0 40%
0 a 20%	Inusual 0 20%	Bajo 0 4%	Bajo 0 8%	Bajo 0 12%	Bajo 0 16%	Bajo 0 20%

Figura 9.Mapa de calor

Fuente Autores

5.2.4.3. Control. En esta etapa, se determinó con los Líderes de Proceso, los Planes de Acción para controlar el Riesgo Inherente a los que se ve expuesta por el proceso particular de estudio a fin de mitigar la Frecuencia de Ocurrencia y el Impacto previamente medidos.

Para determinar la Eficacia del Control se tiene en cuenta un Rating implementado con tal objetivo, el cual pondera lo siguiente:

- Cobertura del control.

  Para llevar a cabo la calificación de los controles, existen cinco variables con unos pesos (%) parametrizables, a su vez cada variable posee unas categorías con un peso internamente que no son parametrizables, los cuales son

Cuadro 12.
Cobertura de control

Variable	Categoría
Clase Control	Preventivo Correctivo Detectivo
Tipo Control	Automático Semiautomático Manual
Frecuencia	Rara vez Periódico Permanente

Fuente: Autores

5.2.4.4.Monitoreo. Esta fase debe ser implementada por la empresa ya que se deben hacer validaciones del funcionamiento de los controles aplicados, es necesario realizar un monitoreo periódico de los Riesgos y de las exposiciones a pérdidas debe cumplir, como mínimo, con los siguientes requisitos:

- Facilitar la pronta detección y corrección de las deficiencias encontradas en la Organización; dicho seguimiento debe ser proporcional a los eventos de Riesgo potencial y materializado, así como con la frecuencia y naturaleza de los cambios en el entorno operativo.
- Establecer indicadores descriptivos y/o prospectivos que evidencien los potenciales Eventos de Riesgo.
- Garantizar que los controles estén funcionando en forma oportuna y efectiva.

5.3. Fase 3 - Implementación

En esta fase se describirán los procesos realizados con los cuales se identificaron los activos de información, la identificación de riesgos y controles aplicados en la organización.

5.3.1. Clasificación de activos de información. Tras realizar algunas entrevistas con las áreas de la organización y conocer un poco de la misma, se realizó un inventario de activos, estos activos están descritos en detalle en el documento de Anexo D. Inventario de activos/ Matriz de riesgo, del presente trabajo.

Para dar inicio a la implementación se realizó una clasificación y se determinó que activos se tendrían en cuenta para proceder con el levantamiento de la información, el análisis se realizó de acuerdo a la norma ISO 27005 e ISO 31000 teniendo en cuenta la siguiente descripción:

Cuadro 13.
Descripción de activos

Tipo de Activo	Descripción
Hardware	Hardware. Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Software	Programas, aplicativos, desarrollos, software base, sistema de información.
Personas	Personas relacionadas con los procesos de la organización.
Instalaciones	Lugares donde se desarrollan las actividades realizadas.
Comunicaciones	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro
Procesos	Documentación formal aprobada por la organización para el desarrollo de las funciones.
Información	Documentos no formales pero que son relevantes para el negocio.

Fuente: Autores

Tras realizar el análisis anterior, se definió el tipo de impacto a través del cual se evaluaría el activo de la información, para la organización lo más crítico en este caso sería el impacto Financiero, Reputacional y Legal, a continuación se describe el grado de criticidad, siendo 5 el mayor valor de pérdida y así sucesivamente en forma descendente:

Cuadro 14.
Impactos para evaluar el activo

Tipo de Activo	Descripción de Valoración	Criterio de Valoración	Valor
Financiero	Pérdidas económicas para la empresa.	Menor o igual a 0.25%	1
		Mayor a 0.25% y menor o igual a 5%	2
		Mayor a 5% y menor o igual a 20%	3
		Mayor a 20% y menor o igual a 50%	4

		Mayor al 50%	5
Reputacional	Pérdida de Prestigio y confiabilidad de la empresa.	Conocido solo por la empresa	1
		Atención de algunas partes interesadas a nivel local que potencialmente puede afectar a la empresa	2
		Media atención de las partes interesadas a nivel local y regional.	3
		Alta Atención de las partes interesadas a nivel local, regional y nacional.	4
		Conocimiento general a nivel nacional e internacional.	5
Legal	Incumplimiento de normatividad y legislación	No tiene repercusión frente a normatividad y contratos.	1
		Genera llamados de atención por parte de los entes de control.	2
		Genera posibles sanciones menores por parte de los entes de control y/o reclamos por parte de terceros.	3
		Genera sanciones económicas por parte de los entes de control y/o demandas por parte de terceros.	4
		Genera sanciones mayores por parte de entes de control, cancelación de contratos, suspensión de licencias, cierre de líneas de negocios.	5

Fuente: Autores

Tras la definición anterior de los impactos para la evaluación los activos de la información, se procedió a terminar el esquema de calificación para la confidencialidad, integridad y disponibilidad de la siguiente forma:

Cuadro 15.
Evaluación de criticidad del activo

Criterio Evaluación	Criticidad	
	Valor	**Nivel**
Activos de la información en los cuales la clasificación de cualquiera de las 3 está entre calificación 4 y 5	>4	Muy Alto
Activos de la información en los cuales la clasificación de cualquiera de las 3 propiedades en calificación 4	>3 y<=4	Alto
Activos de información en los cuales la clasificación de la información de cualquiera de las 3 propiedades en calificación 3	>2 y <=3	Medio
Activos de información en los cuales la clasificación de la información de cualquiera de las 3 propiedades en calificación 1 y 2	>=1 y<= 2	Bajo

Fuente: Autores

Para el desarrollo de los activos de información inicialmente se construyó una metodología, en la cual se listan todos los activos de la información y a este se le asigna un valor de acuerdo a la confidencialidad, integridad y disponibilidad, especificando por ejemplo:

Clasificación Activo	Nombre Activo	Proceso Responsable	Subproceso Responsable	Cargo del Responsable	Confidencialidad		
					Legal	Reputacional	Financiero
Hardware	Equipo de Computo Gerente Gral	Gerencia General	Gerencia General	Gerente General	3	4	4

Figura 10. Ejemplo para dar un valor calificativo a un activo clasificado

Fuente: Autores

Se tiene un activo de la información llamado Equipo de Cómputo de Gerente General de clasificación hardware, el cual se encuentra a cargo del proceso de la gerencia general, para medir la confidencialidad se analiza que tan grave sería en un valor de 1 a 4 en donde 1 es el menos crítico y 4 el más crítico a nivel legal, reputacional o financiero de que ocurriera un evento como el robo de la información de este equipo, y así se debe realizar con la integridad y la disponibilidad, luego se saca el valor total de cada uno en este caso el que tenga el valor más alto así:

Clasificación Activo	Confidencialidad			Integridad			Disponibilidad			T. Confidencialidad	T.Integridad	T.Disponibilidad	Criticidad del Activo	Nivel de Criticidad
	Legal	Reputacional	Financiero	Legal	Reputacional	Financiero	Legal	Reputacional	Financiero					
Hardware	3	4	4	4	3	4	2	1	2	4	4	2	4	Alto

Figura 11. Ejemplo de sacar valor total del activo teniendo en cuenta su nivel de criticidad

Fuente: Autores

De acuerdo a la imagen anterior se consolido el total del valor de la confidencialidad, integridad y disponibilidad para calcular el nivel de criticidad alto, este procedimiento se realizó con todos los activos identificados y se puede visualizar en el Anexo D, después de realizar todo el análisis, se obtuvieron los siguientes resultados:

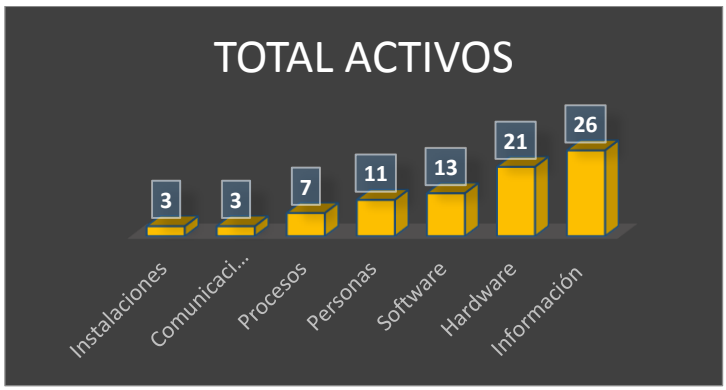

Figura 12. Resultados de valoración de activos

Fuente: Autores

De un total de 84 activos identificados, se evidencia que el 26% corresponden a información de documentos de licitaciones y documentos sensibles para la organización, los cuales no se encontraban valorados, por tanto no se utilizan medios para proteger esta información del riesgo al que puedan estar expuestos, además se encontró un porcentaje de 21% para hardware ya que no se realizan mantenimientos a los equipos de cómputo de los empleados, ni mucho menos a los servidores core del negocio, si no se tienen programados mantenimientos preventivos, es posible que se presente indisponibilidad de los servicios esenciales de la compañía, lo cual representaría detener la operación mientras se cubre la indisponibilidad, haciendo que la organización pierda dinero.

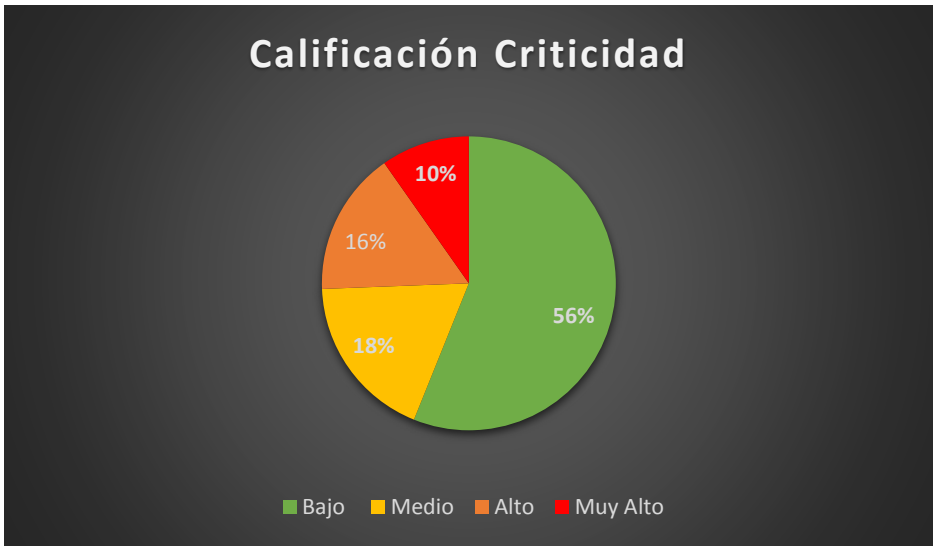

Figura 13. Resultados de valoración de activos con criticidad

Fuente: Autores

Al determinar la criticidad del activo, se puede evidenciar que el 10% de los activos es decir 8 activos de información están categorizados como activos muy altos, estos corresponden a la aplicación core del negocio, el acceso biométrico, el cuarto de

comunicaciones, el servidor de producción , los swhitches, el firewall y el servidor de antivirus, razón por la cual estos son prioritarios para la organización y es necesario asegurarlos de la mejor manera, pues si se materializa algún evento de riesgo en estos activos esto puede representar pérdidas significativas.

A su vez existen 13 activos de información con calificación de criticidad alta, dentro de los cuales se encuentra la red lan, algunos documentos informales con los que trabaja la compañía, el servidor de backups y el de dominio y en cuanto a instalaciones el área restringida de financiero.

Aunque del 100% de los activos solo el 26% están categorizados con criticidad alta y muy alta, es importante garantizar que estos activos están siendo protegidos de la mejor forma y que hay controles y planes de contingencia oportunos para minimizar el riesgo que implica su pérdida o indisponibilidad.

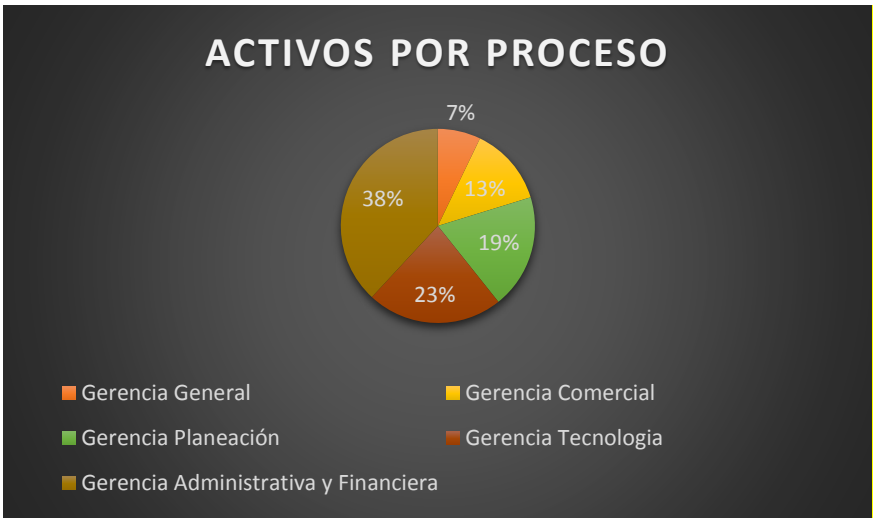

Figura 14. Activo de información identificados por proceso

Fuente: Autores

De acuerdo a la reunión realizada con cada uno de los procesos, se identificó que el proceso con más activos de información es la gerencia administrativa y financiera, con un 38% de participación, como sugerencia se solicita ser más asertivos y realistas durante la consolidación de los activos, se deben evaluar todos los impactos a los que puede estar expuesto el activo, a su vez es necesario disminuir el uso de documentos informales de la compañía, ya que la mayoría de activos identificados corresponde a documentos informales de la entidad, de acuerdo a la información dada, es necesario desarrollar una valoración de riesgo con el fin de identificar los riesgos a los que se encuentran expuestos los activos de información. La calificación y consolidación de los activos se podrá encontrar en el documento Anexo D.

Cuadro 16.
Matriz de riesgo

Clasificación Activo	Nombre Activo	Subproceso Responsable	Cargo del Responsable	Ley	Reputacional	Financiera	Ley	Reputacional	Financiera	Ley	Reputacional	Financiera	T. Confidencialidad	T.Integridad	T.Disponibilidad	Criticidad del Activo	Nivel de Criticidad
Hardware	Equipo de Computo Gerente Gral	Gerencia General	Gerente General	3	4	4	4	3	4	2	1	2	4	4	2	4	Alto
Software	Metricas de qqqplaneación Vias	Gerencia General	Gerente General	2	4	4	3	4	4	1	1	2	4	4	2	4	Alto
Información	Estados Financieros	Gerencia Administrativa y Financiera	Gerente Administrativo y Financiero	4	4	4	4	3	4	4	1	4	1	4	4	4	Alto
Información	Presupuesto Anual	Gerencia Administrativa y Financiera	Gerente Administrativo y Financiero	1	1	3	4	2	4	4	4	4	3	4	4	4	Alto
Información	Balance General	Gerencia Administrativa y Financiera	Gerente Administrativo y Financiero	2	3	3	4	3	4	3	2	3	3	4	3	4	Alto
Instalaciones	Zona Restringida Financiera	Gerencia Administrativa y Financiera	Gerente Administrativo y Financiero	2	1	4	2	2	3	2	2	3	4	3	3	4	Alto
Software	SIIGO- Software Contable	Gerencia Administrativa y Financiera	Coordinador Contable	1	1	3	3	1	4	2	1	5	3	4	5	5	Muy Alto
Personas	Coordinador Contable	Gerencia Administrativa y Financiera	Gerente Administrativo y Financiero	3	4	1	3	1	3	1	1	2	4	3	2	4	Alto
Software	SIIGO- Software Nomina	Recurso Humano	Analista de Nomina	2	1	3	3	1	3	2	1	5	3	3	5	5	Muy Alto
Software	SIIGO- Facturación	Facturación	Analista Facturación	3	1	3	4	3	4	1	2	5	3	4	5	5	Muy Alto
Instalaciones	Cuarto de Comunicaciones	Gerencia Tecnologia	Gerente Tecnologia	1	1	3	2	1	4	1	1	5	3	4	5	5	Muy Alto
Comunicaciones	Red Lan	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	1	1	3	2	2	3	2	2	4	3	3	4	4	Alto
Comunicaciones	Red Wifi Corporativa	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	1	1	3	2	2	3	2	2	4	3	3	4	4	Alto
Software	Servidor de Producción	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	3	4	4	4	4	5	4	3	5	4	5	5	5	Muy Alto
Software	Servidor de Domino	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	2	3	3	2	2	3	3	4	4	3	3	4	4	Alto
Software	Servidor de Backup	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	2	3	3	2	2	3	2	3	4	3	3	4	4	Alto
Software	Servidor de Correo	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	3	3	4	4	3	4	4	4	4	4	4	4	4	Alto
Comunicaciones	Swicthes	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	1	1	3	2	2	3	2	2	5	3	3	5	5	Muy Alto
Software	Firewall	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	5	4	4	5	5	5	4	5	5	5	5	5	5	Muy Alto
Software	Antivirus	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	2	3	3	2	5	5	1	4	4	3	5	4	5	Muy Alto
Software	File Server	Tecnologia, Soporte y mantenimiento	Coordinador de Tecnologia	4	4	4	4	4	4	2	3	3	4	4	3	4	Alto

Fuente: Autores

Teniendo en cuenta los activos de la información analizada se realizó la valoración de riesgos, de acuerdo a la metodología descrita en la fase de diseño, se tuvieron en cuenta algunas amenazas y vulnerabilidades generales que se describen en la norma ISO 27005, a continuación se muestran cuales fueron estas generalidades escogidas:

Con la identificación y clasificación de los activos de información se tuvieron algunos inconvenientes de comprensión en cuanto al significado del activo de la información y como valorarlo, ya que la empresa nunca había desarrollado un levantamiento de esta información y no tenía los conceptos claros, razón por la cual fue necesario incluir dentro del plan de trabajo varias sesiones de capacitación a los funcionarios de cada proceso.

Con la identificación de los activos de la empresa XY.S.A.S, se logró identificar la cantidad de activos, lo cual contribuyo a identificar los riesgos de cada activo con mayor precisión.

Tipo	Amenazas
Daño físico	Fuego
	Daño por agua
	Contaminación
	Accidente importante
	Destrucción del equipo o los medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado
	Pérdida de suministro de energía
	Falla en el equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometedoras
	Espionaje remoto
	Escucha subrepticia
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Falla del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de los datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal

Figura 15. Lineamientos de la ISO 27005:2013 para la valorización de riesgos

Fuente: https://es.scribd.com/doc/124454177/ISO-27005-espanol

Para iniciar con el análisis de riesgo se tomaron todos los activos de información y se le asignó un evento de riesgo, algunos eventos de riesgo fueron propuestos, es decir se planteó que llegaría a suceder si se materializara en realidad un evento, y otros si corresponde a eventos ya materializados dentro de la compañía, después de consolidar esta información se relacionaron algunas amenazas y vulnerabilidades, en cuanto a la criticidad del activo se consolido con la probabilidad del impacto, de acuerdo a este resultado se realizó la relación de probabilidad con impacto y se obtuvo un valor resultante este valor final es el que se aplica para conocer la calificación real para el riesgo uno, en total se consolidaron 120 riesgos asociados a los activos.

Clasificación del Activo	Proceso Responsable	Activo	Evento Riesgo	Amenaza	Vulnerabilidad	Criticidad del Activo	Impacto	Criticidad X Impacto	Probabilid	Dim. Ries	Riesgo N
Hardware	Gerencia General	Equipo de Computo Gerente Gral	Equipo de computo abandonado en la sala de juntas sin bloqueo de sesión	Abuso de derechos	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	4	4	4	3	Alto	R1

Figura 16. Ejemplo de calificación del riesgo de un activo

Fuente: Autores

Como podemos observar en la figura anterior, el riesgo R1 ocurrió porque el equipo del gerente general fue abandonado en una sala de reuniones sin bloquear la sesión de usuario, la amenaza identificada en este caso corresponde a abuso de derechos y la vulnerabilidad que pudo explotar la amenaza fue Falta de terminación de la sesión cuando se abandona la estación de trabajo, la criticidad de este activo es 4 es decir criticidad alta, el impacto puede ser alto ya que pueden sustraer información sensible de este equipo y la probabilidad de ocurrencia es media, es decir 3, ya que en ocasiones el gerente general bloquea la sesión del equipo, pero en algunas oportunidades se le olvida de hacerlo, seguido de esta identificación se multiplica la probabilidad por el impacto y se determina la dimensión del riesgo inherente, así el riesgo 1 (R1) tiene una dimensión alta.

Por tanto la medición anterior se realizó para los 120 eventos de riesgos identificados de los cuales se obtuvieron los siguientes resultados generales:

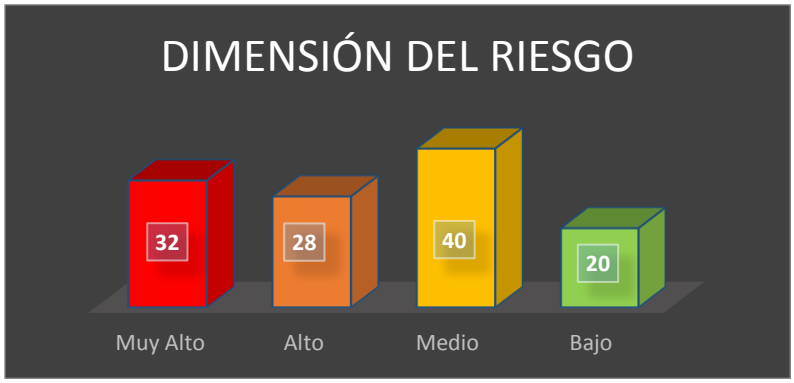

Figura 17. Dimensión del riesgo

Fuente: Autores

De acuerdo a los 120 riesgos encontrados, la mayoría de los riesgos son de calificación media, lo cual asegura un poco de normalidad dentro del comportamiento organizacional, sin embargo existen 32 riesgos muy altos y 28 en alto, los cuales deben ser mitigados lo antes posible.

Los riesgos por procesos se encuentran identificados así:

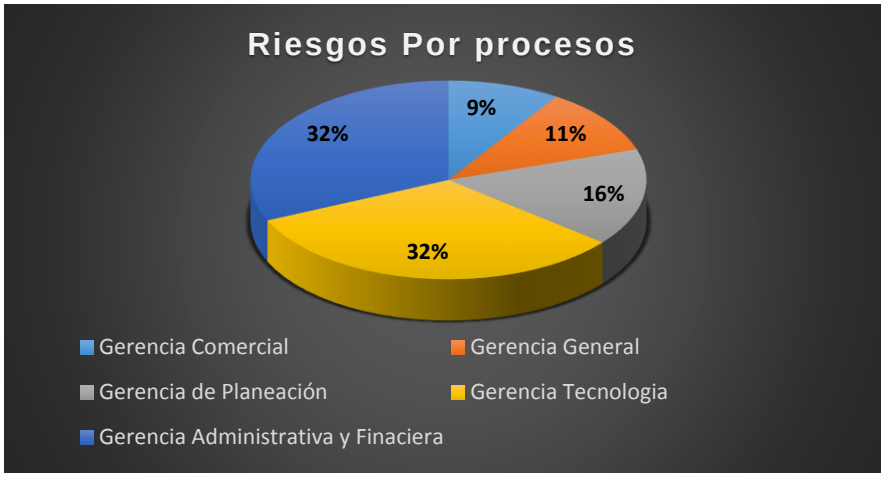

Figura 18. Riesgo por procesos

Fuente: Autores

De acuerdo a al grafica anterior tecnología tiene un 32% de riesgos que corresponden a 39 riesgos, seguido de la gerencia administrativa y financiera con 38 riesgos, en cuanto a la gerencia comercial es donde menos riesgos se han identificado, teniendo en cuenta lo anterior es necesario darle prioridad a los procesos con mayor cantidad de riesgos, pero también es importante validar donde se concentran los riesgos con dimensión muy alta y alta.

A continuación se categorizan los riesgos por procesos y por dimensión de riesgo.

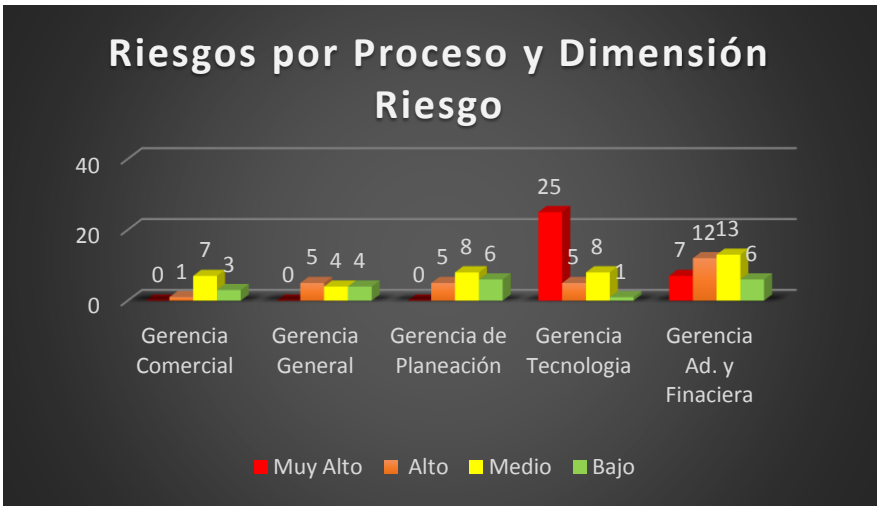

Figura 19. Riesgo por procesos y Dimensión Riesgo

Fuente: Autores

Como se puede observar en la gráfica anterior los procesos que tienen registrados riesgos muy altos son la gerencia administrativa y financiera y la gerencia de tecnología, razón por la cual es importante atacar inicialmente estos riesgos, con el fin de establecer controles que permitan la mitigación del mismo.

De acuerdo a los resultados obtenidos se consolidaron los riesgos en un mapa de calor por proceso, de la siguiente forma:

Para los procesos de gerencia administrativa y financiera se encontraron 38 riesgos de los cuales 2 se encuentran en alto y 4 en muy alto, lo cual implica que se debe realizar tratamiento y seguimiento a estos riesgos para tratar de disminuir su valor en cuanto a dimensión.

GERENCIA ADMINISTRATIVA Y FINANCIERA					
PROBABILIDAD	IMPACTO				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Alta			1	2	4
Alta	1	1	3	3	
Media		5	6	4	
Baja	2	4	2		
Muy Baja					

Figura 20. Mapa de calor por proceso gerencia administrativa y financiera

Fuente: Autores

En cuanto a la gerencia comercial se identificaron 11 riesgos los cuales se encuentran en medio como podemos observar no hay riesgos muy altos, ni altos, para lo cual se deben aplicar controles pero no son críticos para la organización.

GERENCIA COMERCIAL					
PROBABILIDAD	IMPACTO				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Alta					
Alta				1	
Media		5	1		
Baja		3	1		
Muy Baja					

Figura 21. Mapa de calor por proceso gerencia comercial

Fuente: Autores

Para le procesos de gerencia general se identificaron 13 riesgos pero ninguno esta categorizado como riesgo alto o muy alto.

GERENCIA GENERAL					
PROBABILIDAD	IMPACTO				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Alta					
Alta			2	3	
Media		3	1		
Baja		4			
Muy Baja					

Figura 22.Mapa de calor por proceso gerencia gerencial

Fuente: Autores

En cuanto a la gerencia de planeación, se identificaron 19 riesgos, de los cuales están ubicados en una dimensión de riesgo bajo y medio.

GERENCIA PLANEACIÓN					
PROBABILIDAD	IMPACTO				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Alta					
Alta			1	4	
Media	1	2	3		
Baja	1	3	2		
Muy Baja	2				

Figura 23. Mapa de Calor por proceso gerencia planeación

Fuente: Autores

Para los procesos de tecnología se encontraron 39 riesgos de los cuales 9 se encuentran en alto y 13 en muy alto, lo cual implica que se debe realizar tratamiento y seguimiento especial a estos riesgos para tratar de disminuir su valor en cuanto a dimensión.

GERENCIA TECNOLOGIA					
PROBABILIDAD	IMPACTO				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Alta		1	2	9	11
Alta				4	2
Media			7	1	
Baja		1	1		
Muy Baja					

Figura 24.Mapa de calor por proceso gerencia tecnológica

Fuente: Autores

Con la valoración de riesgos no se tuvo ningún inconveniente para esta valoración, ya que la empresa XY.S.A.S, ya tenía claros cuales eran los eventos que se habían materializado, y a proponer nuevos eventos que se podrían materializar en un futuro, tenían claro como esto podría afectar a cada proceso.

Con el desarrollo de la valoración de riesgo aportó al objetivo general ya que realiza una medición real de los riesgos presentados sobre los activos, con la valoración del riesgo colaboro a la construcción de un manual de seguridad de la información, ya que este manual brinda lineamientos para brindar soluciones a los riesgos presentados.

Después de la realizar el análisis de riesgos se implementaron una serie de controles, esto con el fin de minimizar el nivel de riesgo inherente.

Para la remediación de los riesgos se identificaron 122 controles pero su evaluación y monitoreo dependerá de la organización y con esto se medirá su efectividad o se implementaran nuevos controles. El consolidado de los controles para minimizar los riesgos se podrá encontrar en el documento de Anexo D aquí se describe un control como ejemplo:

Referencia Control	Nombre Control	Reduce Riesgo	Subproceso que implementa	Clase control	Tipo Control	Frecuencia
1	Capacitación Seguridad de la Información	Equipo de computo abandonado en la sala de juntas sin bloqueo de sesión	Gerencia Tecnologia	Preventivo	Manual	Periódico

Figura 25.Ejemplo de control para minimizar riesgo

Fuente: Autores

Para el primer riesgo, el control aplicado es capacitar al gerente general en temas referentes a seguridad de la información, esto se realizara de manera periódica y esta categorizado como un control preventivo, ya que aunque se ha encontrado el equipo sin bloqueo de sesión no se han materializado eventos de pérdidas representativas.

Con el cálculo de todos los controles, se pudo identificar en la siguiente figura cuantos controles le pertenecen a cada proceso de la entidad XY S.A.S:

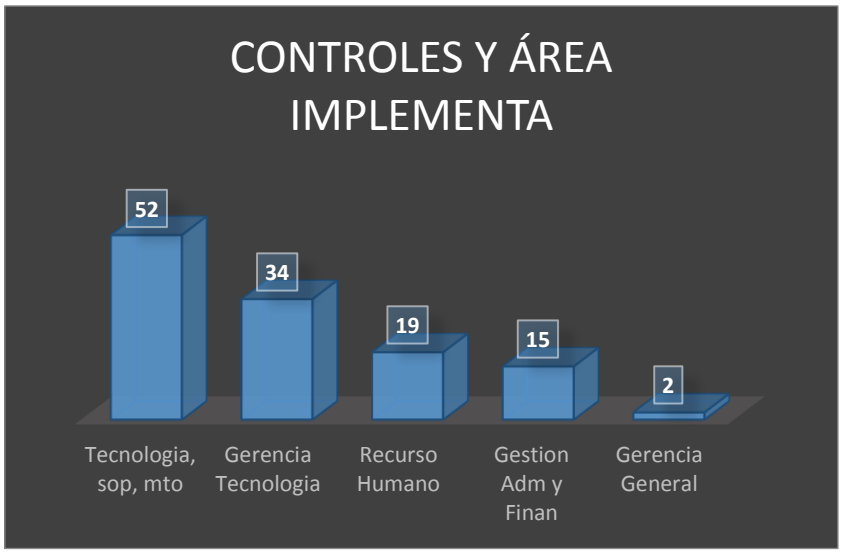

Figura 26. Calculo de controles implementados en cada proceso de la entidad

Fuente: Autores

Como se puede a observar en la anterior grafica la mayor cantidad de controles los implementara el área de tecnología ya que el proceso que presenta más riesgos altos y muy altos, a su vez los controles describen una configuración que se debe realizar a los recursos tecnológicos con los que ya cuenta la organización, pero estos no se habían tenido en cuenta pues no había una valoración de riesgo que determinara a que estaba expuesta la organización, a su vez no existe un área de seguridad de la información que

apoye estos cambios, ya que el área de tecnología solo se dedica a asegurar que las herramientas tecnológicas funcionen y no necesariamente que lo hagan de forma segura.

Figura 27. Calculo del tipo de control implementado en la entidad XY S.A.S

Fuente: Autores

De los controles a implementar un 71% corresponden a controles correctivos, lo cual indica que la organización ha sido víctima de varios eventos de materialización de riesgos.

Para el desarrollo del consolidado de los controles descritos en el Anexo D se presentaron algunos inconvenientes para su implementación, ya que la alta gerencia no está dispuesta a realizar una gran inversión en cambios significativos con respecto a seguridad de la información, razón por la cual los controles aportados solo especifican cambios en los procesos ya existentes.

La descripción de los controles brindara a la empresa XY.S.A.S medidas de seguridad que permitan proteger a la organización, aunque aún faltan muchos controles por

implementar este es un inicio para medir el resultado de estos controles, tras su aplicación.

Después de realizar la identificación de los activos, la matriz de riesgo y aplicar los controles para minimizar el riesgo de cada activo se construyó finalmente un Manual de Seguridad de la Información, lo cual hará que la organización tenga como base un documento formal para que empiece a trabajar en temas de seguridad de la información en este documento se omitió el numeral de la norma A.14, ya que la empresa no realiza implementaciones de desarrollo de software.

Con este manual se espera que se establezcan lineamientos básicos orientados a fomentar la Seguridad de la Información ya que este tema es nuevo para la organización, por tanto se sugiere contratar a una empresa especializada que les brinde una capacitación general a todos los funcionarios de la compañía, en la cual se enfatice en la importancia de la seguridad, esto con el fin de obtener toda la ayuda necesaria por parte de los empleados.

Esta información del manual SGSI se encontrará en el Anexo E. Manual SGSI.

En cuanto a la realización del ANEXO E, se presentaron algunas demoras en su construcción, ya su desarrollo implicaba reunión constante con las áreas para determinar que implementaciones se iban a realizar y que aportes significativos se podían tomar para crear y general las políticas, a su vez la alta dirección informo que por el momento no iba a realizar una inversión significativa para apoyar el tema de seguridad de la información.

La construcción del manual de SGSI aporta el objetivo general de este proyecto porque brindara a la empresa XY.S.A.S lineamientos de seguridad de la información que mejoren los procesos de la empresa para mitigar los eventos de riesgo.

6. Conclusiones

- La implementación de mecanismos de seguridad de la información, se ha convertido en un elemento vital para la estrategia del negocio de las organizaciones.

- El diseño de un Manual de Seguridad de la información es un aporte significativo para las empresas que desea enfocar la estrategia de su negocio hacia otro rumbo, aunque el camino es largo y abarca muchos temas específicos, su implementación permitirá construir un sistema con un grado de madurez sostenible.

- Para que la implementación de un sistema de seguridad de la información sea efectivo debe contar con todo el apoyo y la participación de la alta gerencia, ya que sus directrices son las que permiten que toda la organización este trabajando activamente. Por un mismo propósito.

- Un análisis de GAP aplicado a la Norma ISO 27001:2013 le permite a una organización, conocer el estado real de madurez en temas de Seguridad de la Información.

- En el análisis de riesgo realizado a todos los procesos de la empresa XY. S.A.S, se identificaron eventos de riesgo que no habían sido contemplados por la organización, ya que, al no tener una metodología de riesgo aplicada, un evento era visto como un suceso normal que se remediaba sin ningún tipo de seguimiento y control.

- Los controles propuestos para mitigar los riesgos identificados en el análisis de riesgo corresponden en su mayoría a configuraciones básicas de los recursos tecnológicos con los que la empresa XY S.A.S cuenta, pero estos no se habían implementado por falta de recursos humanos que se dedicaran analizar la raíz del problema y a plantear soluciones.

- Actualmente la empresa XY S.A.S no tiene un área de seguridad de la información, razón por la cual no hay avances significativos que apoyen esta labor, para que la organización avance en estos temas, es necesario crear esta figura encargada de apoyar y asesorar esta implementación.

- La informalidad de las remediaciones y medidas de seguridad realizadas en la empresa XY S.A.S, no eran suficientes para mitigar los eventos de riesgos que se materializaron.

- Para lograr resultados eficaces en la implementación del Sistema de Seguridad de la Información, la empresa XY S.A.S debe realizar un esfuerzo considerable, ya que a la fecha tiene un porcentaje de cumplimiento de la norma de un 30%, lo cual muestra menos de la mitad del cumplimiento.

7. Bibliografía

[1] *iso27000.es*. (s.f.). Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

[2] *blogspot*. (24 de 10 de 2011). Obtenido de http://admondeinformacion.blogspot.com.co/

[3] Excellence, I. (21 de 05 de 21). *pmg-ssi*. Obtenido de http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[4] *prezi.com*. (14 de 7 de 2014). Obtenido de https://prezi.com/xftqz8li4znf/mecanismo-para-la-seguridad-e-integridad-de-la-informacion/

[5] *pmg-ssi.com*. (4 de 05 de 2015). Obtenido de http://www.pmg-ssi.com/2015/05/iso-27001-analizar-y-gestionar-riesgos-sgsi/

[6] *iso27000*. (s.f.). Obtenido de http://www.iso27000.es/sgsi.html

[7] ceeisec. (2010). *ceeisec*. Obtenido de http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

[8] Federico, P. (10 de 09 de 2010). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

[9] *stadium.unad.edu.co*. (s.f.). Obtenido de http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3777/1/20904541.pdf

[10] wikipedia. (16 de 04 de 2017). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n

[11] iso27000. (s.f.). *iso 27000.es*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

[12]*estandarisosevolucion.wordpress*. (11 de 2014). Obtenido de https://estandarisosevolucion.wordpress.com/iso-27000/

[13] *redyseguridad.fi-p.unam.mx*. (s.f.). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ISO27.php

[14] *Advisera*. (s.f.). Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

[15] *blogspot.com*. (8 de 11 de 2015). Obtenido de http://auditoriasistemas10141.blogspot.com.co/2015/11/segundo-corte-norma-27001.html

[16] iso27000. (s.f.). *iso 27000.es*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

[17] Wikipedia. (18 de 04 de 2017). *wikipedia*. Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27001

[18] *calidad-gestion*. (s.f.). Obtenido de http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html

[19] *wikipedia.org*. (s.f.). Obtenido de https://eshttps://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming/wiki/C%C3%ADrculo_de_Deming

[20] *iso27000.es*. (s.f.). Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Anexos