MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TIC

Trabajo final de Máster

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

Alberto Morelo Palacios

Director: Antonio José Segovia Henares

UOC
Octubre 2015

Tabla de contenido

LISTA DE TABLAS

LISTA IMÁGENES

ÍNDICE DE ANEXOS

1. DESCRIPCIÓN DEL PROYECTO

Es indudable que las tecnologías de información y comunicación se han convertido en una herramienta indispensable para el desarrollo de las empresas, no obstante a los grandes beneficios que aporta la tecnología a la empresas, existe una amenaza latente a la implantación de un equipamiento tecnológico en una empresa y son los ataques cibernéticos de todo tipo perpetrado por personas que utilizan los medios tecnológicos para cometer todo tipo de delitos tales como suplantación de sitios web y de identidad, transferencia ilegal de dinero, robo de información sensible o crítica para la organización entre otros, que afectan los patrimonio, la imagen y en general la sostenibilidad y permanencia de la empresa; el presente proyecto aborda la elaboración de un sistema de gestión de seguridad de la información en una empresa dedicada al sector textil basado en la ISO/IEC 27001:2013.

La elaboración del proyecto contempla varias fases siendo la primera:

Fase 1 Situación actual: Contextualización, objetivos y análisis diferencial

La fase considera:

- Introducción al Proyecto
- Enfoque y selección de la empresa que será objeto de estudio
- Definición de los objetivos del Plan Director de Seguridad y Análisis diferencial de la empresa con respecto a la ISO/IEC 27001+ISO/IEC 27002 en su versión 2013

Los entregables de esta fase serán:

- Presentación de la empresa en estudio (objetivos, misión, visión, normatividad que la rige, procesos, esquema de red a alto nivel, estructura organizacional de la empresa).
- Alcance del SGSI ajustado para cumplir requisitos de ISO 27001:2013
- Objetivos del SGSI ajustados para cumplir requisitos de ISO 27001:2013
- Diagnóstico de seguridad frente a ISO 27001:2013 e ISO 27002:2013

Fase 2 Sistema de Gestión Documental

La fase considera:

- Elaboración de la Política de Seguridad.
- Declaración de aplicabilidad
- Documentación del SGSI

Los entregables de esta fase serán:

- Política de seguridad de la información
- Proceso de revisión por la dirección
- Roles y responsabilidades en seguridad de la información
- Proceso de gestión de indicadores
- Declaración de aplicabilidad
- Procedimiento de auditorías internas

Fase 3 – Análisis de riesgos

La fase considera:

- Elaboración de una metodología de análisis de riesgos.
- Identificación y valoración de activos, amenazas, vulnerabilidades.
- Cálculo del riesgo.
- Nivel de riesgo aceptable y riesgo residual.

Los entregables de esta fase serán:

- Riesgos de seguridad de la información identificados a partir del análisis de vulnerabilidades y amenazas sobre los activos de información considerados críticos por la empresa. Debido a las restricciones de confidencialidad que se tienen con la empresa, se mostrará un bosquejo general, dado que la empresa no autorizo entregar detalles sobre el análisis de riesgos y sus resultados.

Fase 4 - Propuesta de Proyectos La fase considera:

- Evaluación de proyectos que debe llevar a cabo la Empresa para alinearse con los objetivos planteados en el Plan Director.
- Propuesta plan de tratamiento de riesgos, proyectos de cara a conseguir una adecuada gestión de la seguridad de la información.
- Cuantificación económica y temporal de los mismos.

Los entregables de esta fase serán:

- Propuestas de planes de tratamiento ante los riesgos evidenciados

Fase 5 - Auditoría de Cumplimiento de la ISO/IEC 27002:2013

La fase considera:

- Evaluación de controles, madurez y nivel de cumplimiento.

Los entregables de esta fase serán:

- Informe de auditoría frente a la norma ISO 27002:2013.

  Este será un ajuste o segunda evaluación con respecto al realizado al inicio del proyecto en la fase de diagnóstico para ver las mejoras obtenidas en el desarrollo del proyecto.

Fase 6 - Presentación de Resultados y entrega de Informes

La fase considera:

- Consolidación de los resultados obtenidos durante el proceso de análisis.
- Realización de los informes y presentación ejecutiva a la Dirección.
- Entrega del proyecto final.

Los entregables de esta fase serán:

- Informe consolidado del proyecto
- Anexos realizados durante el proyecto

2. NORMAS ISO 27001 E ISO 27002 DE 2013.

2.1. ORIGEN E HISTORIA DE LAS NORMAS ISO/IEC 27001 y 27002

La Organización Internacional de estándares conocida como la ISO y la Comisión Electrotécnica Internacional por sus siglas IEC, son actualmente las principales organizaciones a nivel mundial para la estandarización de aspectos técnicos, de seguridad, entre otros. Dichas organizaciones, junto con otros organismos internacionales públicos o privados, participan en la realización de comités técnicos para establecer acuerdos y estándares en áreas específicas del conocimiento.

Las normas conocidas como ISO/IEC 27001 y 27002, que proporcionan un marco de gestión para la seguridad de la información aplicable por cualquier tipo de organización sin importar su naturaleza o tamaño, surgieron como resultado del Comité Técnico conjunto ISO/IEC JTC 1, llamado de las Tecnologías de la Información, subcomité 27 (SC 27), asociado con Técnicas

de seguridad. Estas normas se encuentran basadas en la antiguamente denominada norma BS 7799, elaborada por la BSI3 (Institución de estándares Británica) en 1995.

La BSI publicó su norma 7799 en dos partes, la primera conocida como BS 7799-1, se elaboró como una guía de buenas prácticas de seguridad de la información y no se encontraba enmarcada en un sistema de seguridad de la información ni se encontraba diseñada para ser una norma certificable. Posteriormente en 1998, la BSI publicó la segunda parte de su norma, conocida como BS 7799-2, en la cual definió los requisitos que permitirían obtener una certificación del sistema de seguridad de la información (SGSI) por parte de una entidad independiente.

Posteriormente, en el año 2000, la ISO adoptó la norma BS 7799-1 y la denominó ISO 17799, sin cambios representativos respecto a su predecesora de la BSI, y fue hasta el año 2005 donde la ISO adoptó y publicó la norma BS 7799-2 bajo el nombre de ISO 27001, revisando al mismo tiempo la norma ISO 17799 y renombrándola posteriormente como ISO 27002 en el año 2007.

En su versión de 2005, la norma ISO 27001 contenía 11 dominios, cobijando 33 objetivos de control y 133 controles,

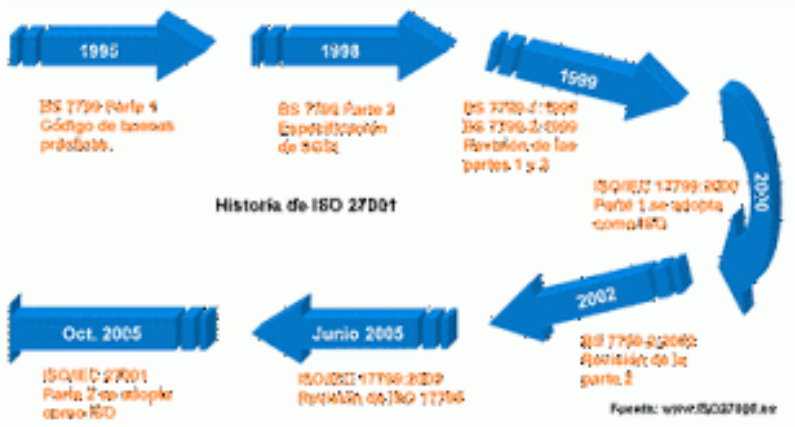

Imagen 1Evolución de la norma ISO 27001 y 27002

La última revisión, realizada el 25 de septiembre de 2013, se ha establecido un total de 14 Dominios, abordando 35 objetivos de control y 114 Controles.

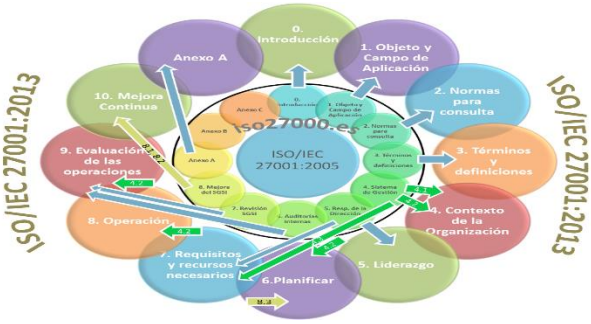

Imagen 2 Norma ISO 27001

La norma ISO 27001, describe como gestionar la seguridad de la información en una empresa. Está determina como gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información (SGSI).

La ISO 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar el SGSI, esta es la norma certificable por las empresas.

ISO 27002, corresponde a la guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Esta norma nos permite desarrollar: normas de seguridad organizativa, práctica efectivas de gestión de la seguridad y la confianza en las relaciones con terceras organizaciones además tiene en cuenta los aspectos de legislación y reglamentación que sean aplicables en los diferentes países.

Los numerales o capítulos en los cuales se divide la norma son los siguientes:

0. Introducción - 1. Alcance - 2. Referencias normativas - 3. Términos y definiciones - 4. Contexto de la organización - 5. Liderazgo - 6. Planeación - 7. Soporte - 8. Operación - 9. Evaluación del desempeño - 10. Mejora

Siendo los más relevantes los que se definen a continuación:

4. Contexto de la organización:

Entendimiento de la organización y su contexto, expectativas de las partes interesadas, alcance del SGSI.

5. Liderazgo:

Liderazgo y compromiso de la alta dirección, políticas, organización de roles, responsabilidades y autoridades.

6. Planeación:

Como abordar riesgos y oportunidades

7. Soporte:

Recursos, competencias, conciencia, comunicación e información documentada.

8. Operación:

Evaluación de riesgos de seguridad de la información, manejo de riesgos de seguridad de la información.

9. Evaluación del desempeño:

Evaluación de riesgos de seguridad de la información.

10. Mejora:

Monitoreo y auditorías internas, revisión de la alta dirección.

En resumen la norma presenta la siguiente estructura:

	ISO 27001
Dominios	**14**
Objetivos de control	**35**
Controles	**114**

Tabla 1 - Resumen NORMA ISO 27001

La siguiente tabla presenta los controles actuales de la norma ISO 27001 2013

A.5 Las políticas de seguridad de información		
	A.5.1 Dirección Gestión de seguridad de la información	
	A.5.1.1	Políticas para seguridad de la información
	A.5.1.2	Revisión de las políticas de seguridad De Información
A.6 Organización de seguridad de la información		
	A.6.1 organización interna	
	A.6.1.1	Los roles y las responsabilidades de seguridad de información
	A.6.1.2	La segregación de funciones
	A.6.1.3	El contacto con las autoridades

A.6.1.4	El contacto con los grupos de interés especial
A.6.1.5	Seguridad de la información en gestión de proyectos
A.6.2 dispositivos móviles y el teletrabajo	
A.6.2.1	Política dispositivo móvil
A.6.2.2	Teletrabajo
A.7 seguridad de los recursos humanos	
A.7.1 Antes de empleo	
A.7.1.1	Proyección
A.7.1.2	Términos y condiciones de empleo
A.7.2 Durante el empleo	
A.7.2.1	Responsabilidades de gestión
A.7.2.2	Conciencia de seguridad Información la educación y la forma
A.7.2.3	Proceso disciplinario
A.7.3 Terminación y el cambio de empleo	
A.7.3.1	Terminación o cambio de responsabilidades laborales
A.8 Gestión de activos	
A.8.1 Responsabilidad para activos	
A.8.1.1	Inventario de activos
A.8.1.2	La propiedad de los activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	retorno de los activos
A.8.2 Clasificación de la información	
A.8.2.1	Clasificación de la información A.8.2.1
A.8.2.2	Etiquetado de información
A.8.2.3	Manejo de activos
A.8.3 Manejo Medios	
A.8.3.1	Gestión de medios extraíbles
A.8.3.2	Eliminación de los medios de comunicación

A.8.3.3	Transferencia de medios Física
A.9 Control de acceso	
A.9.1 requisitos de negocio de control de acceso	
A.9.1.1	Política de control de acceso
A.9.1.2	Acceso a redes y servicios de red
A.9.2 gestión de acceso de usuario	
A.9.2.1	Registro de usuarios y de la matrícula
A.9.2.2	Acceso aprovisionamiento usuario
A.9.2.3	Gestión de derechos de acceso privilegiados
A.9.2.4	Gestión de la información de autenticación de secreto de usual
A.9.2.5	Revisión de los derechos de acceso de usuario
A.9.2.6	Remoción o ajuste de los derechos de accesos
A.9.3 Responsabilidades del usuario	
A.9.3.1	Uso de la información secreta de autenticación
A.9.4 Sistema de control de acceso y aplicación	
A.9.4.1	Restricción de acceso Información
A.9.4.2	inicio de sesión de Secure procedimientos
A.9.4.3	Sistema de gestión de contraseña
A.9.4.4	Uso de programas de utilidad privilegiados
A.9.4.5	Control de acceso a código fuente del programa
A. 10 Criptografía	
A.10.1 controles criptográficos	
A.10.1.1	Política sobre el uso de controles criptográficos
A.10.1.2	Gestión de claves
A.11 física y la seguridad del medio ambiente	
A.11.1 Áreas seguras	
A.11.1.1	perímetro de seguridad física
A.11.1.2	Controles de entrada físicas

A.11.1.3	Protección de oficinas, habitaciones e instalaciones
A.11.1.4	Protección contra amenazas externas y ambientales
A.11.1.5	Trabajar en zonas seguras
A.11.1.6	áreas de entrega y carga
A.11.2 Equipo	
A.11.2.1	Localización del equipo y protección
A.11.2.2	Utilidades Apoyo
A.11.2.3	Seguridad Cableado
A.11.2.4	El mantenimiento del equipo
A.11.2.5	La eliminación de los activos
A.11.2.6	Seguridad de equipo y activos fuera de las instalaciones
A.11.2.7	eliminación segura o la reutilización de los equipos
A.11.2.8	Equipos de usuario desatendida
A.11.2.9	Claro escritorio y política pantalla clara
A.12 Operaciones de seguridad	
A.12.1 Procedimientos y responsabilidades operacionales	
A.12.1.1	Procedimientos operativos Documentados
A.12.1.2	Gestión del cambio
A.12.1.3	Gestión de la capacidad
A.12.1.4	Separación de desarrollo, pruebas y entornos operativos
A.12.2 Protección del malware	
A.12.2.1	Controles contra el malware
A.12.3 Backup - copia de seguridad	
A.12.3.1	Información copia de seguridad

A.12.4 Registro y monitoreo	
A.12.4.1	Registro Evento - Eventlogging
A.12.4.2	Protección de información de registro
A.12.4.3	Administrador y registros del operador
A.12.4.4	sincronización del reloj
A.12.5 control de software operacional	
A.12.5.1	Instalación de software en los sistemas operativos
A.12.6 Gestión vulnerabilidad Técnica	
A.12.6.1	Gestión de vulnerabilidades técnicas
A.12.6.2	Restricciones sobre la instalación de software
A.12.7 Información Consideraciones de auditoría de sistemas	
A.12.7.1	Información controles de auditoría de sistemas
A.13 Seguridad Comunicaciones	
A.13.1 Gestión de la seguridad Red	
A.13.1.1	Controles red
A.13.1.2	Seguridad de los servicios de red
A.13.1.3	Segregación en redes
A.13.2 La transferencia de información	
A.13.2.1	Las políticas y los procedimientos de transferencia de información
A.13.2.2	Acuerdos en la transferencia de información
A.13.2.3	La mensajería electrónica
A.13.2.4	Confidencialidad o acuerdos de confidencialidad
A.14 Sistema de adquisición desarrollo y mantenimiento	
A.14.1 requisitos de seguridad de los sistemas de información	
A.14.1.1	Información A.14.1.1 análisis de los requisitos de seguridad y la especificación
A.14.1.2	Protección de los servicios de aplicación en las redes públicas
A.14.1.3	Protección de las transacciones de servicios de aplicaciones
A.14.2 Seguridad en los procesos de desarrollo y de apoyo	

A.14.2.1	política de desarrollo seguro
A.14.2.2	Procedimientos de control de cambios del sistema
A.14.2.3	Revisión técnica de aplicaciones después de la plataforma de funcionamiento
A.14.2.4	Restricciones sobre los cambios en los paquetes de software
A.14.2.5	sistema seguro principios de ingeniería
A.14.2.6	Secure entorno de desarrollo
A.14.2.7	Desarrollo Outsourced
A.14.2.8	Pruebas de seguridad Sistema
A.14.2.9	Pruebas de aceptación del sistema
A.14.3 Los datos de prueba	
A.14.3.1	Protección de datos de prueba
A.15 Relaciones con los proveedores	
A.15.1 Seguridad de la información en relaciones con los proveedores	
A.15.1.1	La política de seguridad de la información para relaciones con los proveedores
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores
A.15.1.3	Tecnología de la comunicación Información y cadena de suministro
A.15.2 Gestión de la prestación de servicios Proveedor	
A.15.2.1	Monitoreo y revisión de los servicios de proveedores
A.15.2.2	Gestión de cambios en los servicios de proveedores
A.16 Información gestión de incidentes de seguridad	
A.16.1 Gestión de incidentes de seguridad de la información y mejoras	

A.16.1.1	Responsabilidades y procedimientos
A.16.1.2	Los eventos de seguridad de información de Información
A.16.1.3	Reporting debilidades de seguridad de información
A.16.1.4	Evaluación de y decisión sobre los eventos de seguridad de información
A.16.1.5	Respuesta a incidentes de seguridad de información
A.16.1.6	Aprendiendo de los incidentes de seguridad de la información
A.16.1.7	Collection of evidence - El acopio de pruebas
A.17 Aspectos de seguridad Información de gestión de continuidad de negocio	
A.17.1 Información continuidad seguridad	
A.17.1.1	Planificación continuidad seguridad de la información
A.17.1.2	información Implementación de la continuidad de seguridad
A.17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad
A.17.2 despidos A.17.2	
A.17.2.1	disponibilidad de instalaciones de procesamiento de información
A.18 cumplimiento	
A.18.1 Cumplimiento con los requisitos legales y contractuales	
A.18.1.1	Identificación de la legislación aplicable y los requisitos contractuales
A.18.1.2	Los derechos de propiedad intelectual
A.18.1.3	Protección de los registros
A.18.1.4	Privacidad y protección de datos personales
A.18.1.5	Reglamento de controles criptográficos
A.18.2 Información revisiones de seguridad	

		A.18.2.1	Revisión independiente de seguridad de la información
		A.18.2.2	Cumplimiento con las políticas y estándares de seguridad
		A.18.2.3	revisión de cumplimiento técnico

Tabla 2-Controles de la Norma ISO 27001

3. PRESENTACIÓN DE LA EMPRESA

La empresa base para el desarrollo de este proyecto es una empresa dedicada a la representación de fábricas textiles en colombiano con proveedores internacionales de países como la india, Turquía. Esta cuenta con una trayectoria de más de 20 años, funciona como una sociedad limitada.

La empresa cuenta con empleados bilingües comprometidos con su labor.

La misión de la empresa está enfocada en representar fábricas Colombianas del sector textil, que necesitan de insumos o materia prima como hilos y tejidos para la elaboración de sus productos.

La visión, ser la representante número uno, de las fábricas textiles del mercado colombiano.

Los valores corporativos son el respeto, transparencia y lealtad.

3.1 Marco Jurídico

En Colombia desde hace algunos años existe una normatividad legislativa relacionada con el tema de seguridad de la información, esta legislación debe ser cumplida por las empresa objeto del estudio.

NORMATIVIDAD JURIDICA EN COLOMBIA	
Leyes/Normas	Descripción
Ley 527 de 1999	Ley de Comercio Electrónico, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Ley 1273 de 2009	Ley de Delitos Informáticos, por medio del cual se busca la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
Ley 1266 de 2008	Ley de Hábeas Data, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
Ley 23 de 1982	Ley sobre los Derechos de Autor y de la Propiedad Intelectual.
Ley 1581 de 2012	Ley Estatutaria, por la cual se dictan disposiciones generales para la protección de datos personales

Tabla 3 -Normatividad Jurídica relacionada con la Seguridad de la Información en Colombia

3.2 Estructura organizacional de la empresa

A continuación se presenta la estructura organizacional de la empresa en estudio.

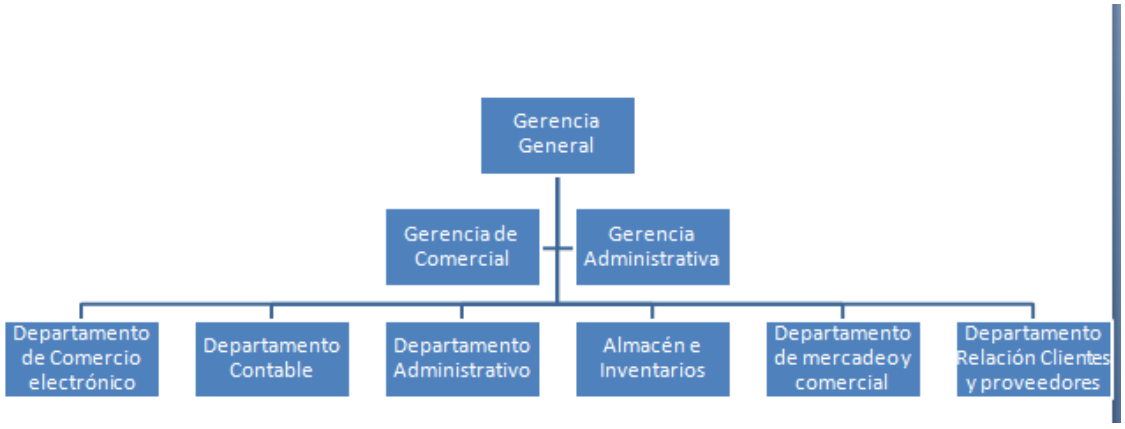

Imagen 3 Organigrama de la empresa seleccionada.

3.3 Mapa de procesos.

El mapa de procesos de la empresa con respecto a los departamentos que incluye esta fase de implementación del SGSI, está estructurado de la siguiente manera:

Departamento Comercio Electrónico: Gestiona las relaciones comerciales con clientes y proveedores a través de las tecnologías de información y comunicaciones.

Departamento Administrativa: Planea, organiza, coordina y controla todos los procesos administrativos de la empresa.

Departamento Contable: Administra y gestiona los procesos contables de la empresa.

Departamento de Almacén e Inventarios: Administra los activos fijos y lleva el archivo documental, registra los bienes muebles e inmuebles que adquiere la empresa.

Departamento de Mercadeo: Se encarga de definir y ejecutar estrategias de mercadeo de la empresa. Implementa los procesos que garanticen el establecimiento de un adecuado programa de mercadeo y comunicación, además de aplicar estrategias de mercadeo novedosas y dinámicas acordes con los objetivos de la empresa.

Departamento Relación con Clientes y Proveedores: Trabaja en coordinación con la sección de comercio electrónico, con la finalidad de gestionar las relaciones con los clientes y proveedores.

3.4 Diagrama de red a alto nivel

En cuanto al diagrama de red a alto nivel, la empresa en estudio solamente autorizó la elaboración de un diagrama general que se presenta a continuación.

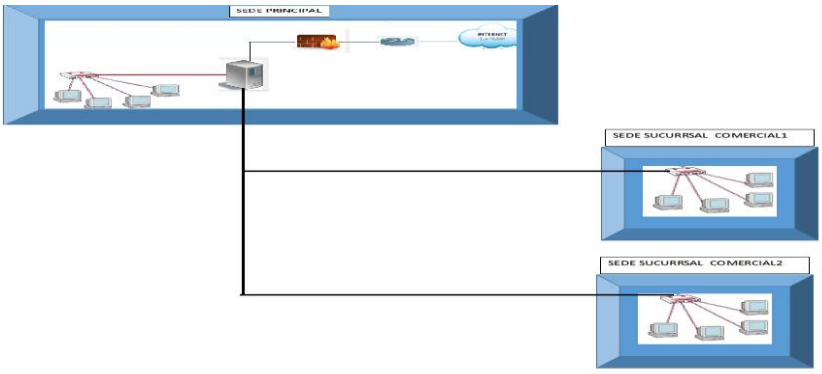

Imagen 4 - Diagrama de Red de Alto Nivel

4. ALCANCE DEL SGSI.

De acuerdo a la Norma ISO 27001, que establece que la empresa debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance y con mirar a delimitar la extensión del proyecto.

Para validar su alineación con la norma, a continuación se presenta el alcance actual para el Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa en estudio:

Según la declaración de aplicabilidad vigente, el límite del Sistema de Gestión de Seguridad de la información, está definido por los activos de información que apoyan los procesos, asociados al negocio de marketing y de comercio electrónico del portafolio accionario de la Empresa.

5. OBJETIVOS DEL SGSI.

De acuerdo a los requisitos que se definen en la norma ISO 27001 - 2013: La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

A continuación se presentan los principales objetivos del plan director de seguridad de la información.

- Crear un marco referencial para asegurar una protección efectiva de la información de la empresa XXXX**.**

- Acreditar a sus clientes y proveedores e interesados que se protege adecuadamente la información y las tecnologías empleadas para los negocios de la empresa XXXX.

- Precisar las medidas esenciales de seguridad de la información que la empresa XXXX, debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, con lo que se podrían evitar la materialización de algunos de los siguientes riesgos:

- Pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, etc.).
- Pérdida de imagen corporativa.
- Pérdida del negocio.

- Infundir a todo el personal de la empresa XXXX, la conciencia de la necesidad de la seguridad de la información y la comprensión de sus responsabilidades individuales.

- Suministrar a todo el personal de la empresa XXXX mecanismos y herramientas que facilite la toma de decisiones apropiadas relacionadas con las soluciones de seguridad de la información.

6. ANÁLISIS DIFERENCIAL SGSI

En este apartado realizaremos un Análisis Gap (Análisis diferencial) con el propósito de evaluar los controles implantados vs. controles necesarios no existentes en relación con la norma internacional **ISO/IEC 27001:2013 e ISO/IEC 27002:2013**, que desarrolla un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

6.1. ANÁLISI DIFERENCIAL BAJO LA NORMA ISO 27001:2013

La norma ISO 27001:2005 se compone de 7 puntos esenciales (del 4 al 10 ambos inclusive). Con el siguiente análisis veremos qué puntos de esta norma son aplicables a la empresa objeto de este estudio, y, veremos a qué nivel de implantación se encuentra.

Para realizar este análisis tuvimos en cuenta el **modelo de Capacidad y Madurez o CMM** (CapabilityMaturityModel), es un modelo de evaluación de procesos de una organización; desarrollado inicialmente para los procesos relativos al Software por la Universidad Carnegie-Mellon para el SEI (Software EngineeringInstitute).Con este modelo, podremos **averiguar el nivel de implantación actual**. Podemos ver esta configuración en la siguiente tabla

VALOR	EFECTIVIDAD	Significado	DESCRIPCIÓN
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	N/A	No aplica	

Tabla 4 - Valoración del nivel de implantación

ANÁLISI DIFERENCIAL BAJO LA NORMA ISO 27001:2013

SECCION	TITULO	APLICA	VALOR
4	**Contexto de la organización**		
4.1	Comprender la organización y su contexto	SI	L0
4.2	Comprender las necesidades y expectativas de las partes interesadas	SI	L0
4.3	Determinación del alcance del sistema de gestión de seguridad de información	SI	L0
4.4	Información de sistema de gestión de la seguridad	SI	L0
5	**Liderazgo**		
5.1	Liderazgo y compromiso	SI	L0
5.2	Política	SI	L0
5.3	funciones de organización, responsabilidades y autoridades	SI	L0
6	**Planificación**		
6.1	Acciones para hacer frente a los riesgos y oportunidades	SI	L0
6.1.2	fueron a materializarse;	SI	L0
6.1.3	Información de tratamiento de riesgos de seguridad	SI	L0
6.2	Objetivos de seguridad de la Información y la planificación para alcanzarlos	SI	L0
7	**Soporte**		
7.1	Recursos	SI	L0
7.2	Competencia	SI	L0
7.3	Conciencia	SI	L0
7.4	Comunicación	SI	L0
7.5	Información documentada	SI	L0
7.5.1	general	SI	L0
7.5.2	Creación y actualización	SI	L0
7.5.3	Control de la información documentada	SI	L0
8	**Funcionamiento**		
8.1	Planificación y control operacional	SI	L0
8.2	Evaluación del riesgo de seguridad Información	SI	L0
8.3	Información de tratamiento de riesgos de seguridad	SI	L0
9	**Evaluación Rendimiento**		
9.1	Monitoreo, medición, análisis y evaluación	SI	L0
9.2	La auditoría interna	SI	L0
9.3	Revisión Gestión	SI	L0
10	**Mejora**		
10.1	No conformidad y acciones correctivas	SI	L0
10.2	Mejora continua	SI	L0

Tabla 5 - Tabla I – Análisis diferencial norma ISO 27001

DOMINIO	% EFECTIVIDAD
4 -Contexto de la organización	**0%**
5- Liderazgo	**0%**
6- Planificación	**0%**
7- Soporte	**0%**
8 - Funcionamiento	**0%**
9 - Evaluación Rendimiento	**0%**
10 -Mejora	**0%**

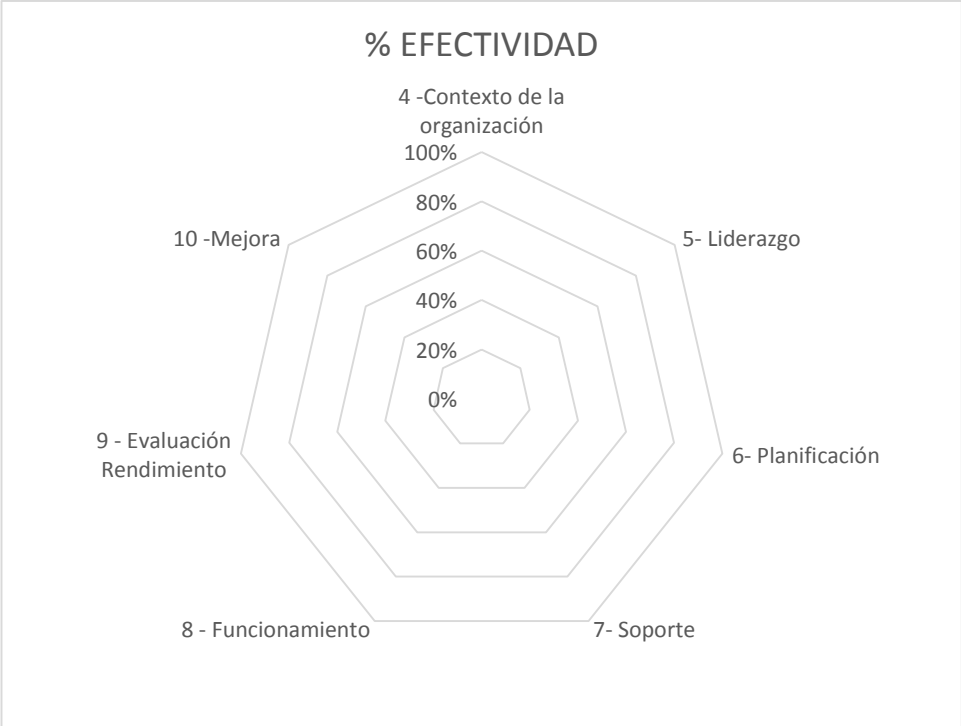

Imagen 5 - **Análisis GAP ISO 27001**

6.2. RESULTADO DEL ANALISIS DIFERENCIAL GAP -

Este análisis tiene como objetivo la verificación de la implantación, de los controles establecidos en la Norma con relación a los procesos de la empresa. Como resultado, se proponen una serie de recomendaciones cuya implantación es necesaria para mejorar la seguridad de la información, así como para priorizar la asignación de recursos sobre las áreas con mayor criticidad y optimizar los costes/beneficios.

El detalle de**l "Análisis diferencial SGS",** se encuentra en la carpeta de los ANEXOS, como:

ANEXO I - RESULTADO DEL ANALISIS DIFERENCIAL GAP 27001 Parte I –

ANEXO I - RESULTADO DEL ANALISIS DIFERENCIAL GAP 27002 Parte I -

El análisis GAP, presentó las siguientes conclusiones:

	r
A.5 Information security policies	0
A.6 Organization of information security	0
A.7 Human resource security	3
A.8 Asset management	2
A.9 Access control	2,25
A.10 Cryptography	0
A.11 Physical and environmental security	2
A.12 Operations security	0,86
A.13 Communications security	1
A.14 System acquisition, development and	0
A.15 Supplier relationships	1
A.16 Information security incident management	1
A.17 Information security aspects of business continuity management	0
A.18 Compliance	1

Tabla 6 - Conclusiones Análisis GAP

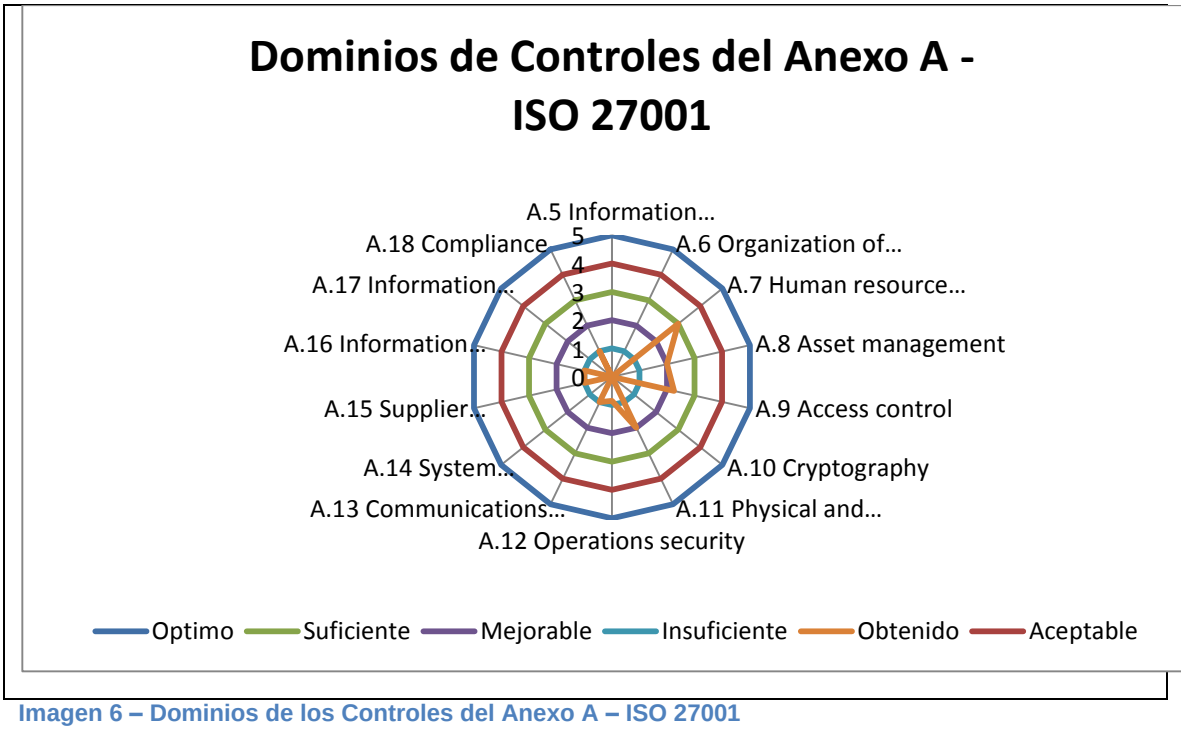

Imagen 6 – Dominios de los Controles del Anexo A – ISO 27001

GRÁFICO RESULTADO ANÁLISIS GAP –ISO 27002

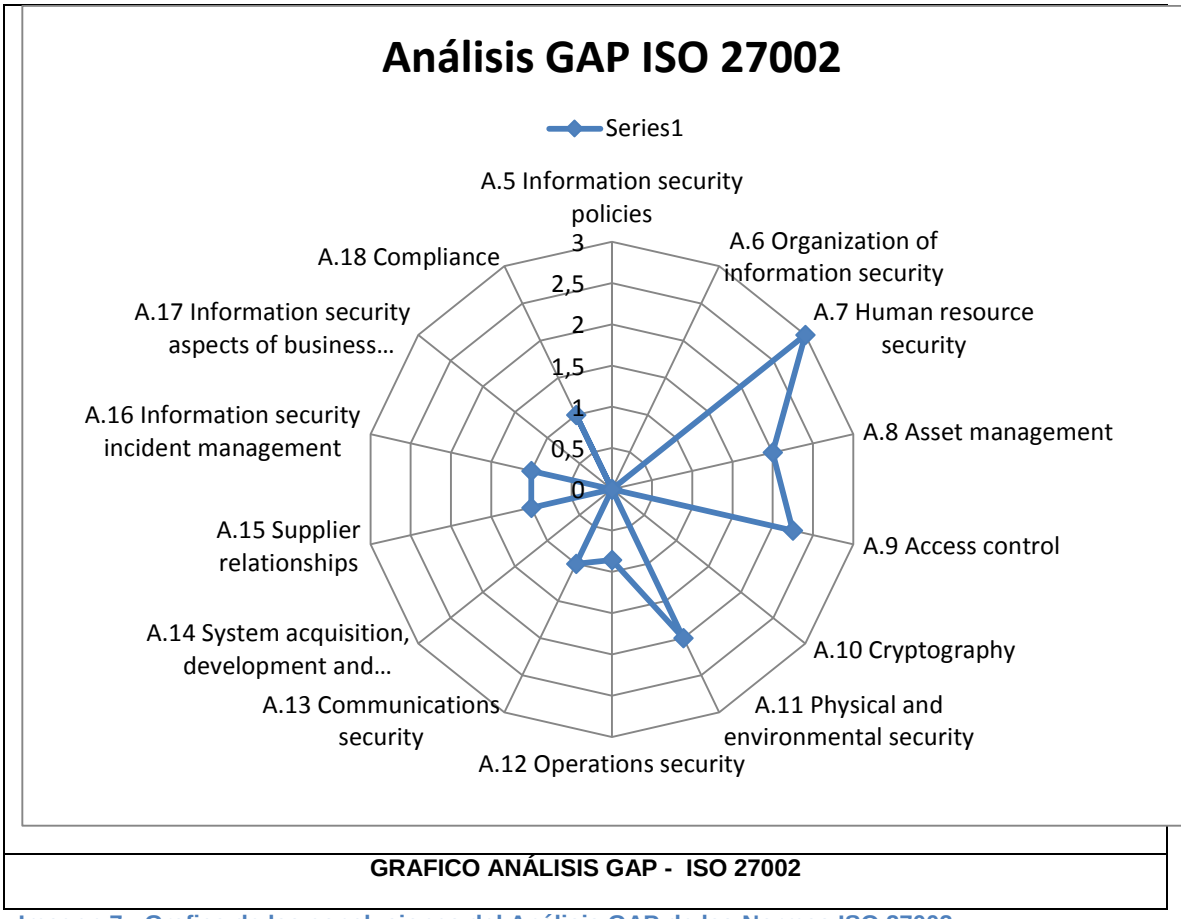

GRAFICO ANÁLISIS GAP - ISO 27002

Imagen 7 - Grafica de las conclusiones del Análisis GAP de las Normas ISO 27002

Conclusiones

De acuerdo a los resultados del Análisis GAP, se puede determinar que el 35,7% de los controles de la **norma ISO 27001 e ISO 27002**, no están implementados en la empresa de estudio y el 64,3% restantes son deficientes, por tal motivo en estos momentos la información de la empresa, es altamente vulnerable, lo que podría explicar la materialización de unos riesgo traducidas en incidente de seguridad de la información.

En los datos y gráficos mostrados anteriormente, vale la pena destacar que el dominio que tiene un mayor nivel de madurez en la implementación de controles es el A.7, asociado con la seguridad de los recursos humanos, ya que la empresa siempre se ha preocupado por establecer procedimiento como la verificación de antecedentes, de curriculum vitae, certificaciones del idioma inglés, entre otros con la finalidad de realizar una contratación idónea de

personal. De otra parte de observó que los controles A5, A6, A10, A14, A17, a la fecha no han sido implementados en esta empresa, por lo tanto su grado de madurez es inexistente o con ausencia total de los controles de la norma.

Metodología utilizada – Análisis GAP

El modelo de madurez empleado para la valoración de los controles es el definido por COBIT (Control Objectives for Information and related Technology) y basado en el CMM (Capability Marurity Model) desarrollado por la Carnegie MellonSchool.

ID	NIVEL	PRÁCTICAS DE GESTIÓN IT	IMPACTO SOBRE EL NEGOCIO
5	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de "*best practice*", sobre la base de una mejora continua.	Las IT son utilizadas de manera integrada para automatizar los workflows, proporcionando herramientas para mejorar la calidad y eficiencia, haciendo que la organización se adapte rápidamente.
4	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.	Es posible monitorizar y medir el cumplimiento con los procedimientos y tomar medidas cuando los procesos no funcionan de manera efectiva.
3	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.	Se deja a discreción del usuario seguir los procedimientos y es probable que no se detecten desviaciones respecto a los mismos.
2	REPETIBLE	Los procesos han evolucionado de forma que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.	Existe un alto grado de confianza en el conocimiento de los individuos y, por tanto los errores son probables.
1	INICIAL	No existen procesos estándar aunque sí planteamientos "*ad hoc*" que se utilizan en cada situación.	Existe evidencia de que la organización ha reconocido que debe contemplar la seguridad.
0	NO EXISTENTE	Ausencia total de procesos reconocibles.	La organización no es consciente de que debe gestionar la seguridad.

Tabla 7 - Nivel de valoración Análisis GAP

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En el numeral 5.2 Política**,** La norma ISO 27001:2013, establece los requisitos para su definición:

La política debe ser establecida por la alta dirección y debe considerar:

1) ser adecuada al propósito de la organización
2) incluir los objetivo de seguridad de la información o proporcione un marco de referencia para que estos se establezcan
3) incluya compromiso de cumplir requisitos aplicables relativos a seguridad de la información

4) la política debe estar disponible como información documentada
5) debe ser comunicada dentro de la organización
6) debe estar disponible para las partes interesadas

Con el objetivo de dar cumplimiento a los requerimientos de la norma con respecto a este punto, la Gerencia de la empresa redacto la política que se presenta a continuación:

Nota: El detalle de **la Política de Seguridad de la Información** y de **la Política de Alto Nivel,** se encuentra en la carpeta de los ANEXOS, como **ANEXO II - PO-01 POLITICA DE ALTO NIVEL y ANEXO III - PO-02 POLITICA DE SEGURIDAD DE LA INFORMACIÓN** respectivamente.

8. REVISIÓN POR LA DIRECCIÓN

En el numeral 9.3 Revisión por la dirección de la norma ISO 27001:2013 establece los siguientes requisitos:

1) la revisión debe realizarse a intervalos planificados, para asegurar su conveniencia, adecuación y eficacia continuas.
2) en las revisiones se deben incluir consideraciones sobre:

- el estado de las acciones con relación a las revisiones previas
- cambios en el contexto de la empresa que sean pertinentes al SGSI

El apartado que trata sobre la revisión de la Política de Seguridad de la empresa, se encuentra integrado en el documento de la política de seguridad de la información de la empresa.

La empresa objeto de estudio no tiene oficina de Dirección sino que cuenta con un Comité de Gerencia, quienes cumplen con la función de revisar la política de seguridad de la información, el texto se relaciona a continuación.

8.1 REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN POR LA GERENCIA DE LA EMPRESA

Anualmente, o ante un cambio relevante en los Sistemas de Información, el responsable de seguridad deberá realizar una revisión y o adecuación de la Política de Seguridad a la realidad de la Compañía, con la participación activa

del Comité de Seguridad de la Información y del apoyo de la Gerencia de la Empresa.

Las decisiones y acciones tomadas como resultado de las revisiones que la gerencia de la empresa realizara, quedan registradas en Actas bajo la responsabilidad del Comité de Seguridad de la Información, quienes velaran por la aplicación y cumplimientos de las mismas.

9. ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

En el numeral 5.3 de la norma ISO 27001:2013 - Roles, Responsabilidades y Autoridades en la organización, establece los siguientes requerimientos:

1) la alta dirección debe asegurar la asignación y comunicación de las responsabilidades y autoridades pertinentes para los roles del SGSI

2) la alta dirección debe asignar responsabilidad y autoridad para asegurar que el SGSI sea conforme con ISO 27001:2013

3) la alta dirección debe asignar responsabilidad y autoridad para tener una fuente que le reporte sobre el desempeño del SGSI A continuación se presenta la definición de los roles y responsabilidades:

9.1 DEFINICIÓN DE ROLES Y RESPONSABILIDADES

La empresa objeto de estudio observando la necesidad que implementar el Sistema de gestión de Seguridad de la Información, tomó la decisión de crear una estructura interna con responsabilidad directa sobre la seguridad de la información, para tal fin estableció los siguientes grupos de acción:

Nivel estratégico:

- Gerencia general
- Comité de gerencia

Nivel Táctico:

- Comité de seguridad de la información
- Responsable de las Auditorías Internas

- Responsable de Seguridad de la información

Nivel Operativo

- Líderes de procesos
- Colaboradores

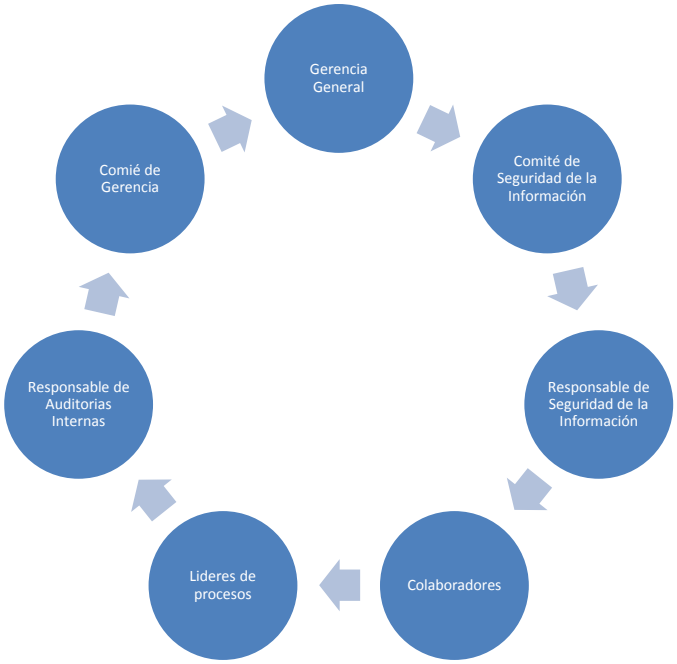

Imagen 8Organización de Seguridad de la información de la empresa

9.2 ROLES Y RESPONSABILIDADES DEFINIDOS POR LA EMPRESA EN ESTUDIO

Dentro de la organización interna de la seguridad, la empresa**,** determina que la función de administración de la seguridad de la información será realizada por el Comité de Seguridad de la Información y por el Responsable de la Seguridad de la Información, quienes tendrán la función general gestionar y controlar la aplicación y la operación de seguridad de la información dentro de la empresa.

9.3 GERENTE GENERAL

El Gerente General de la empresa en estudio, actúa como representante legal de la empresa, fija las políticas operativas, administrativas y de calidad. Es responsable ante los accionistas, por los resultados de las operaciones y el desempeño organizacional, junto con los demás gerentes funcionales planea, dirige y controla las actividades de la empresa

9.4 EL COMITÉ DE GERENCIA

La máxima autoridad en materia de seguridad de la información será ejercida por lo señores Gerentes de la empresa**,** quienes tienen la función principal de apoyar activamente la gestión de la seguridad de la información en la empresa.

9.5 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información, es un equipo de trabajo integrado por representantes de todas las áreas de la empresa, destinado a garantizar el apoyo manifiesto a las iniciativas de seguridad.

9.6 EL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Será la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la empresa que lo requieran.

Los empleados que cumplen la función y administración de la seguridad de la información son los responsables de velar por la implantación y desarrollo de las medidas relativas a esta. De igual manera se encargará de la definición y actualización de las políticas, normas, procedimientos y estándares relacionados con la seguridad informática, igualmente velará por la implantación y cumplimiento de las mismas.

Para realizar la función de administración de la seguridad los responsables se apoyarán en herramientas tecnológicas que permitan una adecuada administración, monitoreo y control de los recursos informáticos.

9.7 RESPONSABLES DE PROCESOS

Planear, coordinar, supervisar todas y cada una de las actividades que realizan los recursos humanos conforme a objetivos, políticas y procedimientos de Seguridad de la Información asignados.

9.8 COLABORADORES

Dentro del grupo de colaboradores se encuentran todos los demás empleados, quienes deberán contribuir con la implementación y mantenimiento del Sistema De Gestión de Seguridad de la Información.

Nota: Las funciones de los Roles principales como son: el Comité de Gerencia, el Comité de Seguridad de la Información y el Responsable de Seguridad de la Información, se encuentran detallada en la carpeta de ANEXOS así:

Anexo IV - Comité de Gerencia,
Anexo V - Comité de Seguridad de la Información
Anexo VI - Responsable de Seguridad de la Información.

10. PROCESO DE GESTIÓN DE INDICADORES

En la empresa objeto de estudio, los indicadores de gestión permitirá validar como se está llevando a cabo la implementación de la seguridad de la información, además determinara si las medidas y controles de seguridad fueron efectivas con respecto a los riesgo y amenazas identificadas. En este apartado la empresa validara que requiere ser medido, como se realizará la medición, cuales son las responsabilidades frente a esta medición y el proceso de evaluación de resultados en busca de la mejora del sistema.

A continuación se muestra el formato general para la gestión de los indicadores en esta empresa.

	EMPRESA			
	Titulo: INDICADOR DE GESTIÓN			
	Fecha: 10/03/2015	Clave: IND - 01	Versión: 01	Página: 1 de 1

INDICADOR		IDENTIFICADOR	
PROCESO			
PROPIETARIO			
OBJETIVO			
FORMULA CALCULO	OBTENCIÒN DE DATOS	FRECUENCIA	ARCHIVO
Observaciòn:			
Realizado por:	Nombres	Fecha	Firma

Tabla 8 - Formato Indicador de Gestión

Nota: Los indicadores de gestión definidos por la empresa en estudio, se encuentran detallados en la carpeta de ANEXOS, como **Anexo VII – Indicadores de Gestión Anual.**

11. DECLARACIÓN DE APLICABILIDAD

La actual declaración de aplicabilidad se encuentra enmarcada contra los controles del Anexo A de la norma ISO 27001:2005. De los 133 controles de esta norma están aplicando 88. Las exclusiones se dan sobre los controles:

A. Los controles definidos dentro de los puntos: A.6.1.2 - A.6.1.4 - A.6.1.5 y A.6.2, relacionados con el tema de la organización Interna, por el momento no se aplican a la empresa objeto de estudio. La empresa está en proceso de adquirir nuevo personal para implementar estos controles en una segunda fase del proyecto, además la empresa no utiliza el sistema de teletrabajo.

B. El control definido dentro del punto: A.9.4 y que se encuentra relacionados con el tema Sistema de control de acceso y aplicación, no se aplica en la empresa, toda vez que esta no cuenta con aplicaciones corporativas.
C. Los controles definidos dentro de los puntos: A.11.1.5 y A.11.1.6, relacionados con el tema Áreas Seguras, no se aplica en la empresa, esta no cuenta con zona de seguridad o de carga.
D. El control definido dentro del punto: A.12.1.4 y que se encuentra relacionados con el tema Operaciones de Seguridad, no se aplica a la empresa, esta no cuenta con Áreas de Separación de desarrollo, pruebas y entornos operativos.
E. El control definido dentro del punto: A.14 y que se encuentra relacionados con el tema Sistema de adquisición desarrollo y mantenimiento, no aplica a la empresa, esta no cuenta con secciones de desarrollo y mantenimiento.

El resto de controles **SI APLICAN** tal y como se muestra en el **ANEXO IX – A Declaración de Aplicabilidad.**

Nota: El documento de declaración de aplicabilidad, al igual que sus anexos, se encuentra detallado en la carpeta de ANEXOS así:

Anexo VIII – DAF – 01 - Declaración de Aplicabilidad
Anexo IX - A – Declaración de Aplicabilidad

12. PROCEDIMIENTO DE AUDITORÍAS INTERNAS

Una parte fundamental del mantenimiento del sistema de gestión de seguridad de la información es evaluar que los planes de tratamiento se han realizado, así como el seguimiento a la mejora del sistema mediante revisiones, y todo el proceso de mejora en la implementación inicial. Para ello se ha definido un procedimiento de auditorías internas que permita realizar este seguimiento.

Nota: El procedimiento de auditoría interna, se encuentra detallado en la carpeta de ANEXOS así:

Anexo X– Procedimiento de auditoría interna
Anexo X - A – Registros asociados con la Auditoría interna

13. METODOLOGÍA DE ANÁLISIS DE RIESGOS

La metodología de análisis y gestión de riesgos que será aplicada al interior de la empresa es la MAGERIT del Consejo Superior de Administración Electrónica y orientado a las administraciones públicas de España.

Este método propone la realización de la identificación y valoración de riesgos y amenazas sobre los activos de información de la organización, para luego determinar las medidas de control actuales y futuras que sean necesarias para realizar un tratamiento adecuado de los riesgos seleccionados.

Como protocolo de comunicación para obtener la información necesaria para adelantar la metodología cumpliendo con las etapas y actividades exigidas se utilizó la técnica lista de chequeo.

En el presente documento se relaciona la lista de chequeo elaborada para los procesos dentro del alcance del SGSI previo a la primera auditoría de cumplimiento ISO 27001:2013, denominada **ANEXO XI – VERIFICACIÓN DE ACTIVIDADES – ANALISIS DE RIESGO.**

Adicionalmente, en el **ANEXO XII - APLICACION METODOLOGIA DE ANALISIS DE RIESGO,** se encuentra un ejemplo paso a paso del desarrollo del método definido para un (1) activo dentro de un (1) proceso de la empresa.

13.1 Identificar activos de información

La primera etapa de esta metodología es la identificación de los activos de información, es decir los Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos que deben ser protegidos, de acuerdo al concepto definido en el método MARGERIT.

Después de realizar un análisis sobre los activos de información se obtuvieron las siguientes categorías:

- Equipos informáticos que permiten almacenar datos o información, o que permiten prestar el servicio o soportar la aplicación.
- Datos o información de la empresa
- Aplicaciones informáticas que permiten manejar datos
- Dispositivos de almacenamiento de datos o información
- Equipamiento y suministros eléctricos que suministran corriente eléctrica a los dispositivos y equipos informáticos
- Equipos de telecomunicación

- Instalaciones físicas
- Personal o empleados de la empresa

De lo anterior podemos concluir que es imperativo identificar todos los activos de información que posean valor para la empresa objeto de estudio.

Para adelantar la identificación de los activos, aplicamos la siguiente metodología.

Paso 1. En esta etapa trabajaremos con una matriz que contienen los siguientes campos: nombre del proceso, responsable del proceso, fecha de diligenciamiento, actividad, estado y observación.

Nombre del procesos	Venta de productos por internet a través del ecommerce	
Responsable del proceso	Departamento de comercio electrónico	
Fecha de diligenciamiento	10/04/2015	
Actividad	Estado SI/NO	Observación
Etapa 1: Activo de información	SI	
Actividad 1. Selección de proceso dentro del alcance	SI	Del alcance del SGSI se seleccionó el siguiente proceso primario: Venta de productos por Internet. Este proceso tiene como subproceso la Administración o Gestión de Seguridad de TI

Paso 2. Para desarrollar esta etapa se tomó uno de los activos identificados como de alto valor, creando una matriz con los siguientes campos: fecha de actualización, nombre del Proceso, consecutivo propio, depende del consecutivo, categoría del activo de información y nombre del activo de información (parte 2). Esta actividad también fue registrada en la matriz de verificación como se muestra a continuación (parte 1):

Parte 1

Actividad	Estado SI/NO	Observación
Actividad 2. Identificación de activo de Alto valor - Información y servicio	SI	Se realizó la identificación de un activo de alto valor que corresponde a la categoría de información o datos

fecha de actualización	nombre del Proceso	consecutivo propio	depende del consecutivo	categoría del activo de información	nombre del activo de información
10/04/2015	Venta de productos por internet	1000	N/A	Información o Datos	Base de datos de clientes

Paso 3. Con la finalidad de realizar un análisis completo, también fue incluido el subproceso o proceso de apoyo dentro de la evaluación, representada en la misma matriz de la actividad 2, como se muestra a continuación:
Parte 1.

Actividad	Estado SI/NO	Observación
Actividad 3. Identificación de activos de menor valor que sirven como apoyo al subproceso primario	SI	Se realizo la identificación de un activo de menor valor que corresponde a la categoría de equipo informático

Parte 2.

fecha de actualización	nombre del Proceso	consecutivo propio	depende del consecutivo	categoría del activo de información	nombre del activo de información
10/04/2015	Administración de Infraestructura tecnológica	1001	N/A	Equipo informático	Equipo informático principal del Área de Comercio electrónico

Paso 4. Se estableció una relación entre el activo de alto valor y el activo de menor valor como se muestra a continuación.

Consecutivo propio	Dependencia del consecutivo
1001	1000

Paso 5. En este paso se realizó la descripción de cada uno de los activos que fueron escogidos para la realización del ejercicio, como se muestra a continuación.

Descripción del activo de información	Responsable del activo de información
Base de datos que contiene la información de los clientes de la empresa	Director Departamento comercial
Equipo informático desde donde se realizan las operaciones principales relacionadas con la venta de los productos de la empresa	Director Departamento comercial

En el siguiente gráfico s muestra como quedó la tabla de identificación de activo, para este proyecto.

Fecha de Actualización (dd/mm/aaaa)	Proceso	Consecutivo Propio	Depende del Consecutivo	Categoría del activo de información	Nombre del activo de información	Descripción del activo de información	Responsable del activo de información
10/04/2015	Venta de productos y servicios por Internet	1006	No Aplica	Servicio	Servicio de puntos de venta de Ventas por Internet	Servicio que permite radicar la compra de productos o servicios e imprimir la tirilla de pago, relacionando con el medio de pago utilizado por el cliente (Tarjeta débito, crédito, efectivo, consignación bancaria, etc).	Gerente de Ventas por Internet
10/04/2015	Venta de productos y servicios por Internet	1002	No Aplica	Información o datos	Base de datos de proveedores	Incluye la información solicitada a los proveedores que tienen una relación actual o pasada con la empresa	Departamento relación cliente y proveedor
10/04/2015	Vinculación, promoción y desvinculación de personal	1007	No Aplica	Información o datos	Base de datos personales y laborales de empleados	Incluye información personal de los empleados directos de la organización, incluyendo nombres completos, número de identificación, fecha de nacimiento, fecha de ingreso a la empresa, salario actual, cargo, ubicación en la empresa, dirección de residencia, teléfono personal, entre otras	Gerencia administrativa
10/04/2015	Vinculación, promoción y desvinculación de personal	1008	1007	Aplicación	Sistema de control de nómina	Permite acceder a consultar, incluir, modificar o eliminar datos de los empleados.	Gerencia administrativa
10/04/2015	Gestión de Seguridad de TI	1009	No Aplica	Servicio	Acceso a Internet	Servicio de acceso controlado a Internet	Departamento de comercio electrónico
10/04/2015	Gestión de Seguridad de TI	1010	No Aplica	Equipo Informático	Consola de Antivirus	Consola de Antivirus y Antispyware corporativo	Departamento de comercio electrónico
10/04/2015	- Venta de productos y servicios por Internet - Recibo, alistamiento y	1003	No Aplica	Información o datos	Base de datos de inventarios, precios y costos	Contiene los números de inventario (SKU) de todos los productos que vende la empresa, junto con su precio de venta y costo de	

Tabla 9 - Identificación de Activos de Información

Para continuar con el proceso de identificación de los activos de información asociados a los diferentes procesos de la empresa objeto de estudio, se diligenció una matriz con los Activos de Información, que puede ser consultada en el **ANEXO XI – VERIFICACIÓN DE ACTIVIDADES – ANALISIS DE RIESGO) y ANEXO XIII - ANEXO XIII - IDENTIFICACIÓN -VALORACIÓN DE ACTIVOS-CALCULO DE RIESGO INHERENTE Y RESIDUAL.**

13.2. Valoración activos de información

Para efectuar la valoración de los activos de información, inicialmente se debe tener presente que de forma natural existe una dependencia entre activos, definida como la medida en que un activo se puede ver afectado por un

incidente de seguridad materializado en otro activo. De allí surgen los conceptos de activos superiores y activos inferiores, siendo superior aquel que transmite sus necesidades de protección a los demás activos, llamados inferiores, pues la materialización de una amenaza en el activo inferior perjudica al activo superior.

En general, el valor de los activos superiores, como la información o los servicios que presta un sistema, es propio del activo y debe ser definido con base en la pérdida que puede causar al negocio una afectación a la seguridad en alguna de sus dimensiones, sea confidencialidad, integridad o disponibilidad. Por otro lado, el valor de los activos inferiores no será calculado de forma propia, sino que será calculado como el correspondiente valor acumulado de los activos superiores que dependen o se apoyan en éste.

La valoración de los activos, sea propia o acumulada por dependencias, puede ser presentada de forma cualitativa o cuantitativa, existiendo un rango de valores cuantitativos que generan determinado valor cualitativo. Adicionalmente se contempla un valor promedio cuantitativo para cada valor cualitativo. En la tabla siguiente se documenta la relación entre la valoración cualitativa del activo y su estimado valor cuantitativo.

VALOR CUALITATIVO	VALOR CUANTITATIVO	
	Rango de valores (USD)	Valor promedio (USD)
Extremo	valor > 300.000	500.000
Muy alto	100.000 < valor > 300.000	200.000
Alto	50.000 < valor > 100.000	75.000
Medio	5.000 < valor > 50.000	25.000
Bajo	100 < valor > 5.000	2.500
Despreciable	valor < 100	100

Tabla 10 - Valores Cuantitativos y Cualitativos

La valoración de los activos debe ser realizada de forma independiente por cada una de sus tres dimensiones de seguridad, identificando el impacto o daño que causaría a la empresa un incidente de seguridad asociado con cada una de dichas dimensiones de seguridad.

Para determinar los niveles de impacto del negocio asociados con cada activo en cada dimensión de seguridad se deben hacer las siguientes preguntas:

Confidencialidad: ¿Qué impacto causaría a la empresa que el activo de información fuera publicado o que fuera conocido por quien no debe?

Integridad: ¿Qué impacto causaría a la empresa que el activo de información, estuviera dañado, corrupto o que fuera alterado sin autorización?

Disponibilidad: ¿Qué impacto causaría a la empresa no tener el activo de información o no poder utilizarlo cuando se requiere y donde se requiere?

Este procedimiento fue aplicado de la siguiente manera:

Paso 1. En la siguiente matriz se realizó una posible valoración del impacto ante la materialización de los riesgos asociados a cada uno de los activos seleccionados. El análisis fue realizado teniendo en cuenta el impacto en la confidencialidad, integridad y disponibilidad de los activos.

Confidencialidad - Impacto posible					
Afectación de clientes	Incumplimiento de leyes	Pérdidas económicas	Interrupción de las ventas	Interrupción de reabastecimiento de mercancía	Pérdida de confianza
Alto USD 50.000	Alto USD 50.000	Extremo USD 500.000	Extremo USD 500.000	Depreciable USD 200	Extremo USD 500.000
Integridad - Impacto posible					
Afectación de clientes	Incumplimiento de leyes	Pérdidas económicas	Interrupción de las ventas	Interrupción de reabastecimiento de mercancía	Pérdida de confianza
Extremo USD 500.000	Depreciable USD 200	Muy alto USD 220.000	Depreciable USD 200	Depreciable USD 200	Extremo USD 500.000
Disponibilidad - Impacto posible					
Afectación de clientes	Incumplimiento de leyes	Pérdidas económicas	Interrupción de las ventas	Interrupción de reabastecimiento de mercancía	Pérdida de confianza
Extremo USD 500.000	Depreciable USD 200	alto USD 50.000	Extremo USD 500.000	Extremo USD 500.000	alto USD 50.000

Seguidamente, se escogieron los impactos para el activo de nivel inferior, que en este caso son los mismos del activo de nivel superior del cual depende.

Paso 2. Se diligenciaron las columnas asociadas con el valor cuantitativo y cualitativo de cada activo, escogiendo el máximo valor de los impactos en cada dimensión, cuyo resultado se muestra a continuación.

Confidencialidad Valor Cualitativo del Activo	Confidencialidad Valor Cuantitativo del Activo ($ USD)	Integridad Valor Cualitativo del Activo	Integridad Valor Cuantitativo del Activo ($ USD)	Disponibilidad Valor Cualitativo del Activo	Disponibilidad Valor Cuantitativo del Activo ($ USD)
Extremo	$500.000	Extremo	$500.000	Extremo	$500.000
Extremo	$500.000	Extremo	$500.000	Extremo	$500.000

A continuación se muestra el gráfico del proceso de valoración realizado para este proyecto.

Confidencialidad Clasificación	Confidencialidad Valor Cualitativo del Activo	Confidencialidad Valor Cuantitativo del Activo ($ USD)	Confidencialidad - Posibles impactos					
			Afectación a Clientes o al Público	Incumplimiento de Leyes o Regulaciones	Intereses Comerciales o Pérdidas Económicas	Interrupción de las ventas	Interrupción del reabastecimiento de mercancía	Pérdida de confianza (reputación)
Público	Despreciable	$100	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)
Confidencial	Muy Alto	$200.000	Muy Alto (US $200.000)	Alto (US $75.000)	Muy Alto (US $200.000)	Despreciable (US $100)	Despreciable (US $100)	Alto (US $75.000)
Confidencial	Muy Alto	$200.000	Muy Alto (US $200.000)	Muy Alto (US $200.000)	Medio (US $25.000)	Despreciable (US $100)	Despreciable (US $100)	Alto (US $75.000)
Confidencial	Muy Alto	$200.000	Muy Alto (US $200.000)	Muy Alto (US $200.000)	Medio (US $25.000)	Despreciable (US $100)	Despreciable (US $100)	Alto (US $75.000)
Público	Despreciable	$100	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)
Público	Despreciable	$100	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)	Despreciable (US $100)
Confidencial	Extremo	$500.000	Despreciable (US $100)	Extremo (US $500.000)	Alto (US $75.000)	Despreciable (US $100)	Despreciable (US $100)	Extremo (US $500.000)

Tabla 11 - Valoración de activos

Se debe tener en cuenta que los niveles de cada impacto son excluyentes entre sí, definiendo que para la valoración de cada activo en cada dimensión siempre primará el mayor valor posible de impacto para el negocio. ANEXO XI – VERIFICACIÓN DE ACTIVIDADES – ANALISIS DE RIESGO) y ANEXO XIII - ANEXO XIII - IDENTIFICACIÓN -VALORACIÓN DE ACTIVOS-CALCULO DE RIESGO INHERENTE Y RESIDUAL.

13.3 Clasificación de los activos de información

Posteriormente a la etapa de valoración se debe asociar un nivel de clasificación a cada uno de los activos de información en cada una de las dimensiones de seguridad establecidas en la empresa. Esta clasificación permite entre otras, conocer las necesidades de protección de los activos y permitirá priorizar la implementación de medidas de control de acuerdo con dichas necesidades. En la tabla siguiente se aprecia la relación que existe entre el valor del activo y su clasificación en cuanto a Confidencialidad, Integridad y Disponibilidad.

VALOR CUALITATIVO	CLASIFICACIÓN		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Extremo	CONFIDENCIAL	ALTA	MISIÓN CRÍTICA
Muy Alto			
Alto	USO INTERNO	MEDIA	CRÍTICA
Medio			
Bajo		BAJA	NO CRITICA
Despreciable	PÚBLICO		

Tabla 12 - valoración de activos

En General, cuando el valor del activo es Extremo o Muy Alto, la clasificación será la más alta posible en cada dimensión, así mismo si el valor del activo en cada dimensión es Alto o Medio, la clasificación será intermedia, y cuando el valor del activo sea Bajo o Despreciable la clasificación será la menor posible, excepto para la dimensión de Confidencialidad (Ver nota inferior). Esto debe ser analizado por cada una de las dimensiones de forma independiente pues es posible que un mismo activo tenga valores diferentes por cada una de sus dimensiones, y por ende tenga requisitos de protección (clasificación) diferentes por cada dimensión. La clasificación menor posible en la dimensión de confidencialidad (Público) implica que el activo puede ser conocido por el público en general, y para ello se requiere que no exista un impacto previsible al momento de una divulgación no autorizada. Lo anterior implica que el único valor del activo que haría viable una divulgación general del activo es "Despreciable", y el valor "Bajo" se asocia al nivel de confidencialidad "Uso Interno" dado que aún genera impactos para la empresa ante una posible divulgación del activo. ANEXO XI – VERIFICACIÓN DE ACTIVIDADES – ANALISIS DE RIESGO) y ANEXO XIII - ANEXO XIII - IDENTIFICACIÓN - VALORACIÓN DE ACTIVOS-CALCULO DE RIESGO INHERENTE Y RESIDUAL.

Confidencialidad Clasificación	Confidencialidad Valor Cualitativo del Activo	Confidencialidad Valor Cuantitativo del Activo ($ USD)	Integridad Clasificación	Integridad Valor Cualitativo del Activo	Integridad Valor Cuantitativo d Activo ($ USD)	Disponibilidad Clasificación	Disponibilidad Valor Cualitativo del Activo	Disponibilidad Valor Cuantitativo del Activo ($ USD)
Público	Despreciable	$100	Alta	Extremo	$500.000	Misión Crítica	Extremo	$500.000
Confidencial	Muy Alto	$200.000	Alta	Muy Alto	$200.000	Misión Crítica	Extremo	$500.000

Tabla 13 - Clasificación de Activos

13.4 Identificación de Amenazas

El siguiente paso del método de análisis de riesgos consiste en identificar las posibles amenazas que puedan llegar a afectar a cada uno de los activos de información identificados.

Para tal efecto se debe tener en cuenta las siguientes consideraciones:

De origen natural: Accidentes naturales (terremotos, inundaciones, etc.).

Del entorno: Desastres industriales (contaminación, fallos eléctricos, etc.)

Defectos de las aplicaciones: Corresponden a las llamadas vulnerabilidades técnicas propias del diseño o implementación del sistema.

Causadas por las personas de forma accidental: Causadas típicamente por errores u omisiones no intencionales.

Causadas por las personas de forma deliberada: Incluyendo ataques deliberados; ya sea con el ánimo de beneficiarse a sí mismo, beneficiar a otros, o para causar daños y perjuicios a la empresa.

PARTE 2. IDENTIFICACIÓN DE AMENAZAS Y VALORACIÓN DEL RIESGO INHERENTE	Activos
	Pricipio de Seguridad
Amenazas	Valor Activo
[N.1] Fuego Incendios: posibilidad de que el fuego acabe con recursos del sistema.	
[N.*] Desastres naturales Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.	
[I.2] Daños por agua Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	
[I.*] Desastres industriales Otros desastres debidos a la actividad humana: Explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, etc.	
[E.8] Difusión de software dañino Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	
[E.20] Vulnerabilidades de los programas (software) Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la	
[A.6] Abuso de privilegios de acceso Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su	
[A.11] Acceso no autorizado El atacante consigue acceder a los recursos del sistema sin	

Tabla 14 - Identificación de Amenazas

Las amenazas identificadas fueron registradas a manera de ejemplo en los ANEXO XI – VERIFICACIÓN DE ACTIVIDADES – ANALISIS DE RIESGO) y ANEXO XIII - ANEXO XIII - IDENTIFICACIÓN -VALORACIÓN DE ACTIVOS-CALCULO DE RIESGO INHERENTE Y RESIDUAL.

13.5 Valoración de Amenazas (Frecuencia e Impacto)

Es necesario valorar inicialmente la frecuencia de ocurrencia de una amenaza para cada activo por cada dimensión de seguridad sin tener en cuenta la aplicación de controles (actuales o futuros), para ello se debe establecer una escala de valores de frecuencia de ocurrencia de la amenaza por año, teniendo en cuenta 6 posibles valores frecuencias (cantidad de veces que podría materializarse la amenaza en el transcurso del año).

Frecuencia		
Descripción	Valor	Valor Anual
Muy frecuente	1 vez x mes	12
Frecuente	1 vez x trimestre	4
Normal	1 vez x año	1
Poco Frecuente	1 vez cada 4 años	0,25
Muy poco frecuente	1 vez cada 10 años	0,1

Tabla 15 - Frecuencia de ocurrencia de amenazas

Adicionalmente es necesario determinar el impacto que generará a la empresa la eventual materialización de cada amenaza sobre cada activo. Dicho impacto será calculado con base en la degradación del activo, es decir, el porcentaje (%) del valor del activo que se pierde por la materialización de una amenaza. Esta labor debe realizarse por cada amenaza en cada una de las dimensiones de seguridad y para cada activo.

Frecuencia		
Descripción	Rango de valores	Valor
Muy alta	80% - 100%	100%
Alta	50% - 80%	80%
Media	25% - 50%	505
Baja	10% - 25%	25%
Muy baja	< 10%	10%

Tabla 16 - Evaluación de degradación de activos

Una vez se ha estimado el valor de la degradación para cada posible amenaza sobre un determinado activo, es necesario estimar el valor del impacto, es

decir, la pérdida en la que incurriría la organización ante una eventual materialización de determinada amenaza. Dicho impacto se puede valorar de forma cualitativa o cuantitativa, siendo esta última la multiplicación numérica del valor del activo en $USD y el porcentaje de degradación del activo.

Impacto	Degradación del Activo				
	Muy baja	Baja	Media	Alta	Muy Alta
	10%	25%	50%	80%	100%
Extremo	Medio	Alto	Muy alto	Muy alto	Muy alto
USD 500.000	50.000	125.000	250.000	400.000	500.000
Muy alto	Bajo	Medio	Alto	Alto	Muy alto
USD 200.000	20.000	50.000	100.000	160.000	200.000
Alto	Bajo	Bajo	Medio	Medio	Alto
USD 75.000	7.500	18.750	37.500	60.000	75.000
Medio	Bajo	Bajo	Bajo	Bajo	Medio
USD 25.000	2.500	6.250	12.500	20.000	25.000
Bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Bajo
USD 2.500	250	625	1.250	2.000	2.500
Despreciable	Muy Bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo
USD 100	10	25	50	80	100

Tabla 17 - Impacto cualitativo

En general se observa que existen cinco (5) posibles niveles de impacto: Muy Alto, Alto, Medio, Bajo y Muy Bajo.

13.6. Determinación del Riesgo Inherente

De igual manera, para determinar el impacto que tiene sobre la empresa la materialización de una amenaza, teniendo en cuenta la frecuencia con la que esto podría ocurrir en un (1) año y sin considerar los posibles controles implementados para mitigarlo, es decir, para determinar la medida del riesgo inherente, es necesario establecer una relación para cada activo entre la probabilidad de ocurrencia y el impacto que podría causar la materialización de cada amenaza en cada una de las dimensiones de seguridad analizadas para el activo.

La empresa ha determinado que realizará estimaciones cualitativas y cuantitativas del riesgo inherente, siendo esta última la multiplicación numérica entre la probabilidad y el valor en (USD) calculado previamente del Impacto de cada amenaza en cada activo. Este cálculo se debe registrar por cada activo respecto a cada amenaza, de forma cualitativa el nivel de riesgo, se debe utilizar como referencia la siguiente tabla, donde se relacionan los valores cualitativos de probabilidad e impacto.

IMPACTO	PROBABILIDAD				
	Muy poco Frecuente	Poco Frecuente	Normal	Frecuente	Muy frecuente
Muy Alto	Apreciable	Importante	Crítico	Crítico	Critico
Alto	Bajo	Apreciable	Importante	Crítico	Crítico
Medio	Bajo	Bajo	Apreciable	Importante	Crítico
Bajo	Despreciable	Bajo	Bajo	Apreciable	Importante
Muy bajo	Despreciable	Despreciable	Despreciable	Bajo	Apreciable

Tabla 18 - Estimación del riesgo cualitativo

De otra parte la estimación del riesgo se puede calcular también de manera cuantitativa, como se muestra en la imagen:

RIESGO	VALOR (USD)
Crítico	>= 500.000
Importante	Entre 125.000 y 499.999
Apreciable	Entre 30.000 y 124.000
Bajo	Entre 6.250 y 29.999
Despreciable	< 6.250

Tabla 19 - Cálculo de estimación cuantitativa de riesgo

En la siguiente tabla se muestra la aplicación del método que fue aplicado para el cálculo del riesgo Inherente.

Para cada uno de los activos seleccionados por ejemplo Base de datos de clientes, identificado con el código interno 1000, le fue calculado el riesgo inherente de acuerdo a los principios de seguridad como son la confidencialidad, integridad y su disponibilidad.

1000 Base de datos de clientes		
Confidencialidad	Integridad	Disponibilidad
$500.000	$500.000	$500.000

Tabla 20 - Selección de activo

Para cada activo seleccionado se determino a qué tipo de amenaza está expuesto, por ejemplo, el activo Base de datos de clientes presenta las siguientes amenaza, [A.6] Abuso de privilegios de acceso y [A.11] Acceso no autorizado.

PARTE 2. IDENTIFICACIÓN DE AMENAZAS Y VALORACIÓN DEL RIESGO INHERENTE	Activos	1000 Base de datos de clientes		
	Pricipio de Seguridad	Confidencialidad	Integridad	Disponibilidad
Amenazas	Valor Activo	$500.000	$500.000	$500.000
sobrecarga eléctrica, fluctuaciones eléctricas, etc.		$0	$0	$0
[E.8] Difusión de software dañino Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.		$0 $0	$0 $0	$0 $0
[E.20] Vulnerabilidades de los programas (software) Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la		$0 $0	$0 $0	$0 $0
[A.6] Abuso de privilegios de acceso Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su		12 100% $500.000 $6.000.000	12 100% $500.000 $6.000.000	12 100% $500.000 $6.000.000
[A.11] Acceso no autorizado El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.		12 100% $500.000 $6.000.000	12 100% $500.000 $6.000.000	 $0 $0
		Total RIESGO x CONFIDENCIALIDAD ACTIVO	Total RIESGO x INTEGRIDAD ACTIVO 3	Total RIESGO x DISPONIBILIDAD ACTIVO 3
		$12.000.000	$12.000.000	$6.000.000
	TOTAL RIESGO x ACTIVO	Total RIESGO ACTIVO N		
		$30.000.000		

Tabla 21 – Calculo del Riesgo Inherente para el activo Base de datos de clientes

Por último obtuvimos el cálculo del riesgo inherente y total para el conjunto de activos que fueron seleccionados como se observa en la siguiente tabla.

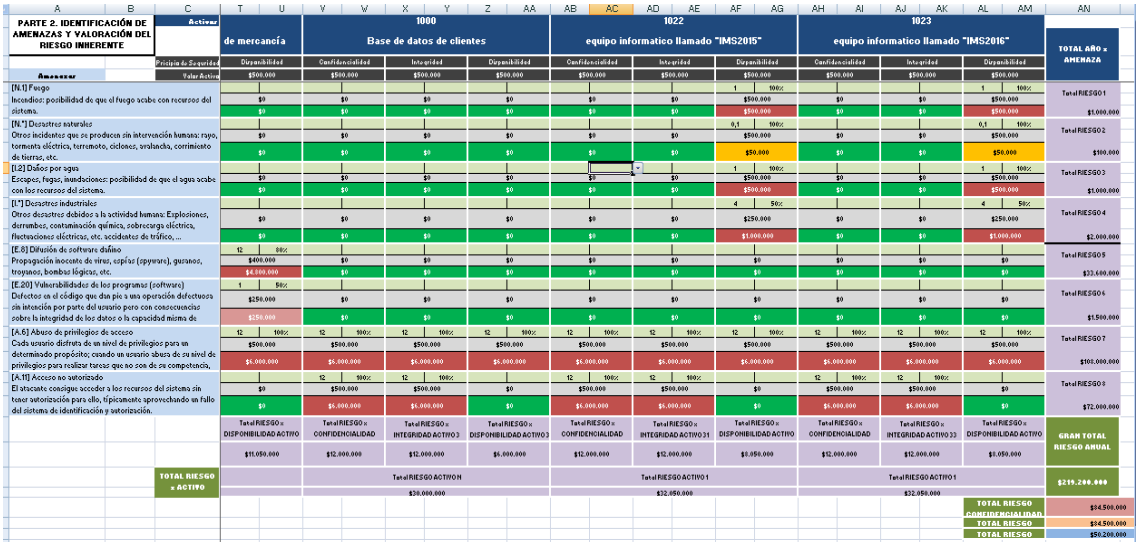

Tabla 22 - Riesgo Inherente

Para determinar el cálculo total del riesgo inherente anual, es necesario primero totalizar (sumar) cada uno de los riesgos inherentes causados por cada amenaza y finalmente sumar dichos valores. ANEXO XI – VERIFICACIÓN DE ACTIVIDADES – ANALISIS DE RIESGO) y ANEXO XIII-IDENTIFICACIÓN - VALORACIÓN DE ACTIVOS-CALCULO DE RIESGO INHERENTE Y RESIDUAL.

13.7. Determinación del Riesgo Residual

Para determinar el riesgo residual, es decir, el valor del riesgo al que la empresa se verá sometido teniendo en cuenta los posibles controles aplicables actualmente (sin tener en cuenta planes de acción futuros), es necesario determinar primero el valor de la efectividad de los controles de seguridad, es decir, el porcentaje (%) en el que se podría reducir el riesgo, ya sea reduciendo la frecuencia de ocurrencia o el impacto (degradación), al aplicar medidas de control. Se debe tener en cuenta que el riesgo nunca va a llegar a cero (0), por lo que la disminución del impacto o frecuencia nunca será del 100%.

Disminución del nivel de degradación o la frecuencia		
Descripción	Rango de valores	Valor
Alta	60% - 99%	90%
Media	40% - 60%	60%
Baja	20% - 40%	40%
Despreciable	< 20%	20%

Tabla 23 - Criterios de efectividad de controles

El valor del riesgo residual debe calcularse teniendo en cuenta la posible reducción de probabilidad o impacto causada por todos los controles aplicables, realizando una multiplicación numérica entre el valor de probabilidad resultante y el valor en (USD) del impacto reducido por controles. El cálculo de la reducción de probabilidad o impacto se debe registrar por cada riesgo inherente respecto a cada control, en cada una de las celdas donde aparecen las frases “Reducción de impacto (%) y Reducción de Frecuencia (%)”.

Después de determinar el riesgo inherente de cada uno de los activos, continuamos con la determinación del riesgo residual, por ejemplo para el activo anterior identificado con el código 1000 se le realizó la evaluación sobre el riesgo - Riesgo 1000 - [A.9] Acceso no autorizado sobre la Base de datos de clientes.

A	B	C	D	BA	BB	BC	BD
PARTE 3. IDENTIFICACIÓN DE CONTROLES Y VALORACIÓN DEL RIESGO RESIDUAL		**Riesgo: Amenaza vs Activo**		**Riesgo 1000 - [A.9] Acceso no autorizado sobre la Base de datos de clientes**			
		Principio de Seguridad		Confidencialidad		Integridad	
Controles Actuales		Frecuencia Inherente	Impacto Inherente	12	$500.000	12	$500.000
		Riesgo Inherente		$6.000.000		$6.000.000	
A.12.2.1. Controles contra el código malicioso (Reductor de frecuencia de ocurrencia)				Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto
A.12.3.1. Copias de seguridad de la información (Reductor de impacto)				Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto 90%
A.13.1.1. Controles de red (Reductor de frecuencia de ocurrencia)				Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto
A.9.4.1. Restricción del acceso a la información (Reductor de frecuencia de ocurrencia e impacto)				Reducción de Frecuenci 40%	Reducción de Impacto 40%	Reducción de Frecuenci 40%	Reducción de Impacto 40%
A.7.1.2. Investigación de antecedentes (Reductor de frecuencia de ocurrencia)				Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto
A.7.2.2. Concienciación, formación y capacitación en seguridad de la información (Reductor de frecuencia de ocurrencia)				Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto
		Frecuencia Residual	Impacto Residual	1,47456	**$300.000**	1,47456	**$30.000**
		TOTAL RIESGO RESIDUAL AÑO		$442.368		$44.237	

Tabla 24 - Riesgo 1000 - [A.9] Acceso no autorizado sobre la Base de datos de clientes.

Una vez realizada la evaluación para cada uno de los riesgos que fueron seleccionados y teniendo en cuenta a nivel general los posibles controles aplicables actualmente (sin tener en cuenta planes de acción futuros), es necesario determinar primero el valor de la efectividad de los controles de seguridad, es decir, el porcentaje (%) en el que se podría reducir el riesgo, ya sea reduciendo la frecuencia de ocurrencia o el impacto (degradación), al aplicar medidas de control. A continuación se muestra la tabla de riesgo residual.

PARTE 3. IDENTIFICACIÓN DE CONTROLES Y VALORACIÓN DEL RIESGO RESIDUAL	Riesgo: Amenaza vs Activo	Riesgo 1004 - [A.7] Difusión de software dañino sobre la Aplicación para la gestión de inventarios, precios y costos						Riesgo 1004 - [A.7] Abuso de privilegios de acceso sobre la Aplicación para la gestión de inventarios, precios y costos						Riesgo 1004 - [A.9] Acceso no autorizado sobre la Aplicación para la gestión de inventarios, precios y costos			
	Principio de Seguridad	Confidencialidad		Integridad		Disponibilidad		Confidencialidad		Integridad		Disponibilidad		Confidencialidad		Integridad	
Controles Actuales	Frecuencia Inherente	12	$500.000	12	$500.000	12	$400.000	12	$500.000	12	$500.000	12	$500.000	12	$500.000	12	$500.000
	Impacto Inherente																
	Riesgo Inherente	$6.000.000		$6.000.000		$4.800.000		$6.000.000		$6.000.000		$6.000.000		$6.000.000		$6.000.000	
A.12.2.1. Controles contra el código malicioso (Reductor de frecuencia de ocurrencia)		Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto
A.12.3.1. Copias de seguridad de la información (Reductor de impacto)		Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto 90%	Reducción de Frecuenci	Reducción de Impacto 90%	Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto 90%	Reducción de Frecuenci	Reducción de Impacto 90%	Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto 90%
A.13.1.1. Controles de red (Reductor de frecuencia de ocurrencia)		Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto
A.9.4.1. Restricción del acceso a la información (Reductor de frecuencia de ocurrencia e impacto)		Reducción de Frecuenci 40%	Reducción de Impacto 40%	Reducción de Frecuenci 40%	Reducción de Impacto 40%	Reducción de Frecuenci 40%	Reducción de Impacto 40%	Reducción de Frecuenci 40%	Reducción de Impacto	Reducción de Frecuenci 40%	Reducción de Impacto 40%	Reducción de Frecuenci 40%	Reducción de Impacto 40%	Reducción de Frecuenci 40%	Reducción de Impacto 40%	Reducción de Frecuenci 40%	Reducción de Impacto 40%
A.7.1.2. Investigación de antecedentes (Reductor de frecuencia de ocurrencia)		Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci 40%	Reducción de Impacto	Reducción de Frecuenci	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto	Reducción de Frecuenci 60%	Reducción de Impacto
A.7.2.2. Concienciación, formación y capacitación en seguridad de la información (Reductor de frecuencia de ocurrencia)		Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto	Reducción de Frecuenci 20%	Reducción de Impacto
	Frecuencia Residual	1,8432	$300.000	1,8432	$30.000	1,8432	$24.000	1,8432	$300.000	1,8432	$30.000	1,8432	$30.000	1,47456	$300.000	1,47456	$30.000
	Impacto Residual																
	TOTAL RIESGO RESIDUAL AÑO	$552.960		$55.296		$44.237		$552.960		$55.296		$55.296		$442.368		$44.237	

Tabla 25 - Calculo Riesgo Residual

Para determinar el cálculo total del riesgo residual anual, es necesario primero totalizar (sumar) cada uno de los riesgos residuales producto de la aplicación de controles y finalmente sumar dichos valores. ANEXO XI – VERIFICACIÓN DE ACTIVIDADES – ANALISIS DE RIESGO) y ANEXO XIII - ANEXO XIII - IDENTIFICACIÓN -VALORACIÓN DE ACTIVOS-CALCULO DE RIESGO INHERENTE Y RESIDUAL.

13.8. Aceptación del Riesgo

En la empresa objeto de estudio se definió que todos los riesgos cuya evaluación cualitativa sea superior o igual a “Importante” deben ser tratados de forma inmediata. Así mismo determina que los riesgos cuya evaluación resulte como “Apreciable” deben contar por lo menos con un plan de tratamiento de riesgo a mediano plazo y los riesgos definidos como de impacto igual o inferior a “Bajo” deberían contar con mediciones periódicas para garantizar que se mantengan en dichos niveles y podrán ser aceptados por la empresa sin definir acciones a corto o mediano plazo para su remediación.

14. PLAN DE TRATAMIENTO DE RIESGOS

Uno de los objetivos primordiales del Sistema de Gestión de Seguridad de la Información es establecer un plan operativo, que permita abordar las amenazas o riesgos de acuerdo a su importancia y urgencia para la seguridad de la información de la empresa.

Este plan incluye la implementación de proyectos de seguridad de la información orientada principalmente en la mitigación de riesgos, agregando nuevos controles o mejorando los actuales, y a su vez, permitirán aumentar el nivel de madurez de Seguridad de la información en la empresa.

De acuerdo a la disponibilidad de los recursos requeridos y complejidad para desarrollar cada una de las fases que constituyen el plan de tratamiento, se han definido 14, los cuales serán desarrollados a corto y largo plazo. A continuación se relacionan los títulos de los proyectos categorizados por su tiempo de implementación, en un diagrama de Gantt y una tabla en la pagina 59.

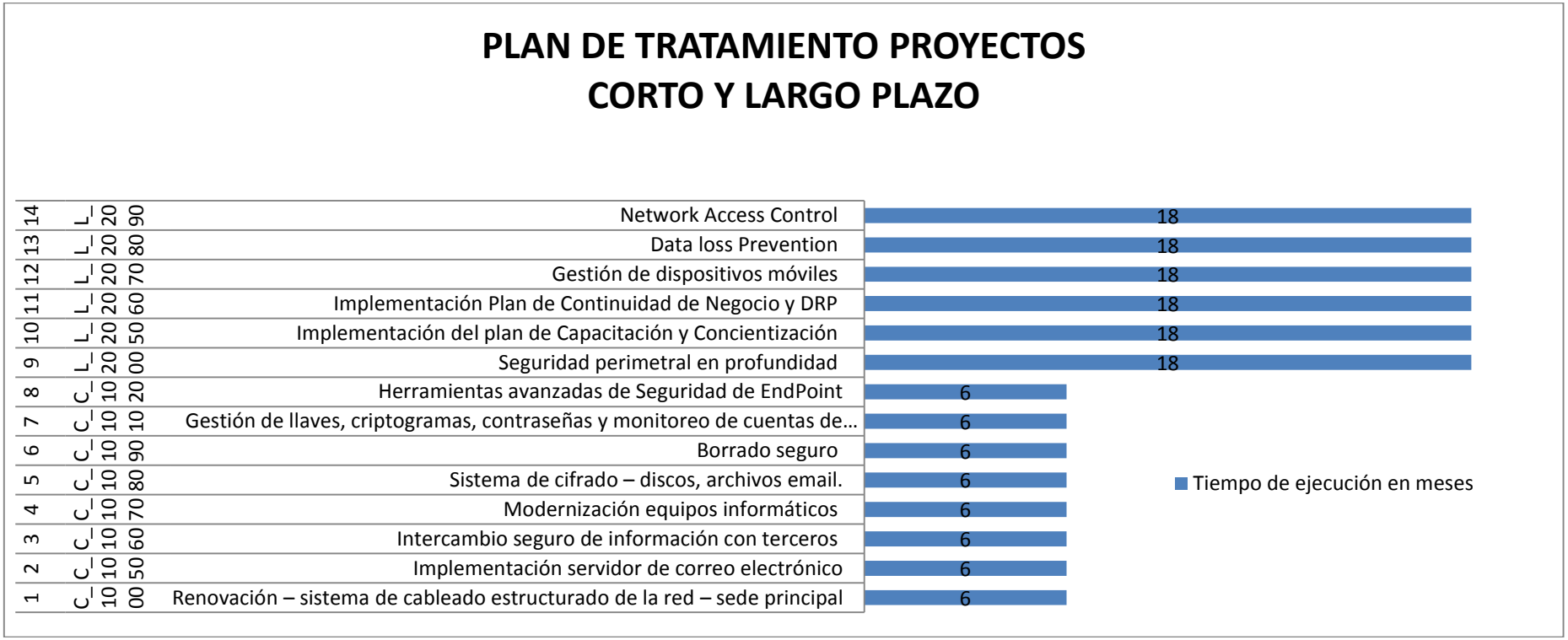

Tabla 26 Plan de proyecto con tiempo de ejecución en diagrama de Gantt.

Nota: para calcular la línea de tiempo de los proyecto de largo plazo se tomó el promedio entre 12 y 36 meses, es decir entre 1 y 3 años, que duraría la ejecución de esos proyectos, que sería igual a 18 meses. En la tabla 27, se muestra un mapeo entre los controles de la norma ISO 27001 y los proyectos planteados.

En la siguiente tabla (27) se muestra la correlación que existe entre los proyectos que serían implementados en la empresa con los controles de la norma ISO 27001. El objetivo es observar mediante que proyecto se le dará cumplimiento a cada control de la norma seleccionado.

Correlación entre los proyecto y los controles de la norma ISO 27001:2013

Tipificación	# Sección	Nombre	Nombre Proyecto
Control	A.5.1.1	Documento de política de seguridad de la información	Políticas de Seguridad de la Información
Control	A.5.1.2	Revisión de la política de seguridad de la información	Políticas de Seguridad de la Información
Control	A.6.1.1	Asignación de responsabilidades relativas a la seguridad de la información	Implementación del plan de Capacitación y Concientización
Control	A.13.2.4	Confidencialidad o acuerdos de confidencialidad	Intercambio seguro de información con terceros
Control	A.11.2.3	Seguridad Cableado	Renovación – sistema de cableado estructurado de la red – sede principal
Control	A.9.1.2	Acceso a redes y servicios de red	NAC (Network Access Control)
Control	A.13.2.2	Acuerdos en la transferencia de información	Intercambio seguro de información con terceros
Control	A.13.2.3	La mensajería electrónica	Intercambio seguro de información con terceros
Control	A.8.1.3	Uso aceptable de los activos	Implementación del plan de Capacitación y Concientización
Control	A.8.2.2	Etiquetado y manipulado de la información	Implementación del plan de Capacitación y Concientización
Control	A.11.2.6	Seguridad de equipo y activos fuera de las instalaciones	Cifrado de discos
Control	A.11.2.7	eliminación segura o la reutilización de los equipos	Borrado seguro
Control	A.10.1.1	Política sobre el uso de controles criptográficos	Sistema de cifrado – discos, archivos email.
Control	A.10.6.1	Controles de red	NAC (Network Access Control)
Control	A.13.2.3	La mensajería electrónica	Implementación servidor de correo electrónico
Control	A.10.6.2	Seguridad de los servicios de red	NAC (Network Access Control)
Control	A.8.3.1	Gestión de soportes extraíbles	Herramientas avanzadas de Seguridad de EndPoint
Control	A.8.3.1	Gestión de medios extraíbles	Cifrado de discos
Control	A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Intercambio seguro de información con terceros
Control	A.13.2.1	Las políticas y los procedimientos de transferencia de información	Intercambio seguro de información con terceros
Control	A.15.1.3	Tecnología de la comunicación Información y cadena de suministro	Intercambio seguro de información con terceros
Control	A.11.4.1	Política de uso de los servicios en red	NAC (Network Access Control)
Control	A.11.4.3	Identificación de los equipos en las redes	NAC (Network Access Control)
Control	A.10.1.2	Gestión de claves	Sistema de cifrado – discos, archivos email.
Control	A.11.4.6	Control de la conexión a la red	NAC (Network Access Control)

Control	A.13.2.2	Acuerdos en la transferencia de información	Implementación servidor de correo electrónico
Control	A.13.2.3	La mensajería electrónica	Sistema de cifrado – discos, archivos email.
Control	A.13.2.2	Acuerdos en la transferencia de información	Sistema de cifrado – discos, archivos email.
Control	A.8.3.1	Gestión de medios extraíbles	Gestión de dispositivos móviles
Control	A.10.1.2	Gestión de claves	Gestión de llaves, criptogramas, contraseñas y monitoreo de cuentas de superusuarios
Control	A.8.2.3	Manejo de activos	DLP (Data loss Prevention)
Control	A.13.2.1	Las políticas y los procedimientos de transferencia de información	Implementación servidor de correo electrónico
Control	A.16.1.2	Notificación de eventos de seguridad de la información	Implementación del plan de Capacitación y Concientización
Control	A.16.1.3	Notificación de puntos débiles de seguridad	Implementación del plan de Capacitación y Concientización
Control	A.16.1.5	Respuesta a incidentes de seguridad de información	Implementación del plan de Capacitación y Concientización
Control	A.17.1.1	Planificación continuidad seguridad de la información	PCN y DRP
Control	A.17.1.2	información Implementación de la continuidad de seguridad	PCN y DRP
Control	A.17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	PCN y DRP
Control	A.8.3.2	Eliminación de los medios de comunicación	Borrado seguro
Control	A.8.3.1	Gestión de medios extraíbles	Borrado seguro
Control	A.8.3.3	Transferencia de medios Física	DLP (Data loss Prevention)
Control	A.11.2.4	El mantenimiento del equipo	DLP (Data loss Prevention)
Control	A.11.2.6	Seguridad de equipo y activos fuera de las instalaciones	Gestión de dispositivos móviles
Control	A.9.3.1	Uso de la información secreta de autenticación	Gestión de llaves, criptogramas, contraseñas y monitoreo de cuentas de superusuarios
Control	A.9.2.3	Gestión de la información de autenticación de secreto de usuario	Gestión de llaves, criptogramas, contraseñas y monitoreo de cuentas de superusuarios
Control	A.9.1.2	Acceso a redes y servicios de red	Herramientas avanzadas de Seguridad de EndPoint
Control	A.9.2.3	Gestión de derechos de acceso privilegiados	Herramientas avanzadas de Seguridad de EndPoint
Control	A.11.1.4	Protección contra amenazas externas y ambientales	Herramientas avanzadas de Seguridad de EndPoint
Control	A.11.2.1	Localización del equipo y protección	Herramientas avanzadas de Seguridad de EndPoint
Control	A.11.2.1	Localización del equipo y protección	Modernización equipos informáticos
Control	A.12.2.1	Controles contra el malware	Modernización equipos informáticos
Control	A.12.2.1	Controles contra el malware	Herramientas avanzadas de Seguridad de EndPoint
Control	A.12.4.2	Protección de información de registro	Herramientas avanzadas de Seguridad de EndPoint

Tabla 27 - Mapeo entre los controles de la norma ISO 27001 y los proyectos planteados

Nota: El Cronograma de implementación de proyectos de seguridad de la información que se encuentra en la carpeta de ANEXOS, fueron detallados los proyectos mencionados anteriormente.

ANEXO XIV - CRONOGRAMA DE PROYECTOS.

Teniendo en cuenta que uno de los objetivo primordial para la empresa en estudio es la protección, confidencialidad e integridad de la información sensible que se intercambia entre la empresa – clientes y proveedores internacionales.

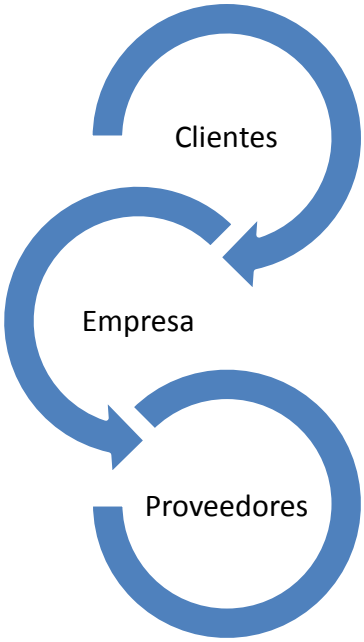

Imagen 9 Intercambio de información

Dentro del primer paquete de proyectos del plan de seguridad de la información a desarrollar a corto plazo, fueron incluidos los proyectos que darían solución a las amenazas y riesgo que afectan la información sensible con carácter de urgencia, toda vez que por solicitud de la empresa se le dará prioridad al tratamiento de estos riesgos.

Mejorar el grado de madurez de los de los controles implica un avance en general sobre de cada uno de los dominios de la ISO 27001. Dicha mejora puede ser comparada contra el nivel de implementación realizado en el análisis diferencial inicial (Tablas 4, figuras 4 y 5 del punto 6), sin embargo, dicho análisis fue realizado antes de dar inicio al plan de implementación del SGSI y por ende no incluye algunos aspectos que han mejorado en el transcurso de dicho plan. Dado lo anterior, y para determinar con mayor veracidad la mejora causada exclusivamente por los proyectos, fue necesario realizar una

actualización al análisis diferencial, la cual se encuentra en el ANEXO I - GAP 27001 y 27002 de 2013 - Parte II– Segundo análisis diferencial.

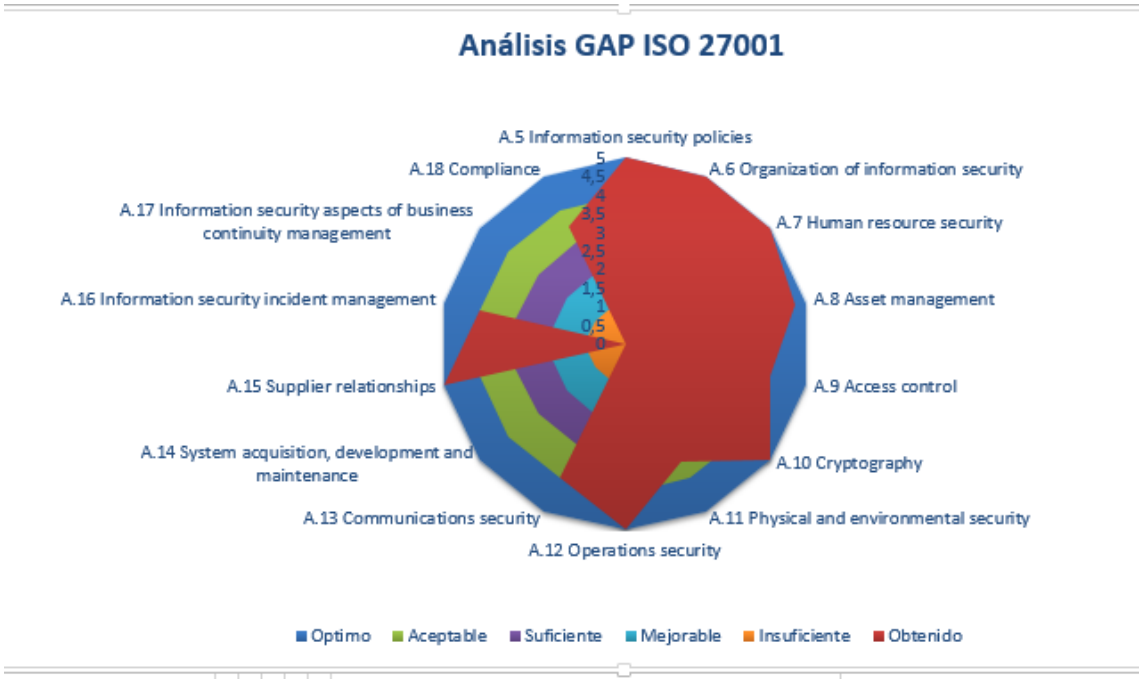

Imagen 10 Análisis GAP ISO 27001 Parte II _ Mejora

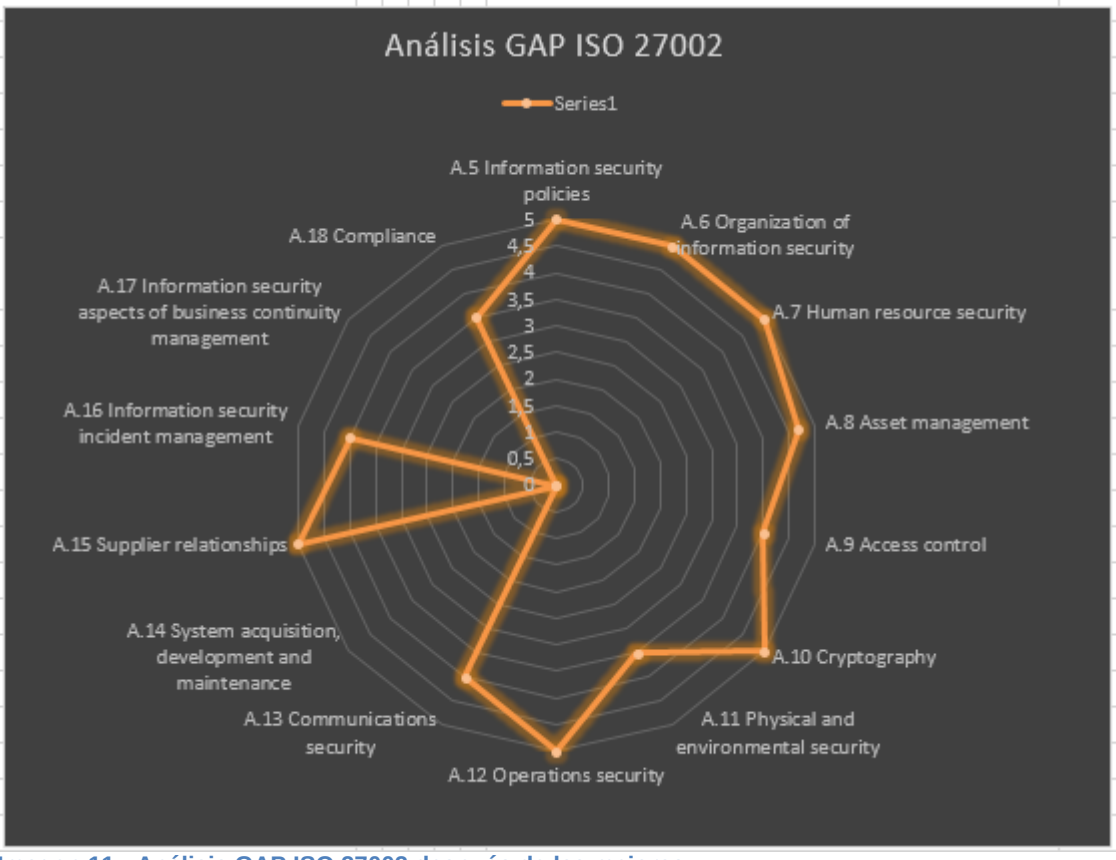

Imagen 11- Análisis GAP ISO 27002 después de las mejoras

En cuanto a la evaluación realizada del cumplimiento de los requisitos generales de la ISO 27001, en el segundo análisis diferencial se obtuvo que en promedio el 21% de éstos se encuentran implementados en la empresa. Al culminar la implementación de la primera fase del proyecto, se espera que lleguen a un 77% (Ver tabla 8).

Implementación de Requisitos Generales ISO 27001	
	% de Implementación
Antes de Proyectos	**21%**
Después de Proyectos	**83%**

Tabla 28 - Mejora en la implementación de requisitos generales de la ISO 27001 por los proyectos

El porcentaje de implementación de cada uno de los dominios de la norma ISO 27002 (Anexo A ISO 27001) en general aumentará para todos los dominios una vez se culminen los proyectos planteados. A continuación se muestra el estado de los dominios obtenido en el segundo análisis diferencial y la mejora esperada al implementar los proyectos planteados.

Mejora en la implementación de dominios ISO 27001 por los proyectos			
		% implementación	
Sección	**Dominios**	**Antes del proyecto**	**Después del proyecto**
A.5	**Information security policies**	0%	100%
A.6	**Organization of information security**	0%	100%
A.7	**Human resource security**	60%	100%
A.8	**Asset management**	40%	93%
A.9	**Access control**	45%	80%
A.10	**Cryptography**	0%	100%
A.11	**Physical and environmental security**	40%	70%
A.12	**Operations security**	17,10%	100%
A.13	**Communications security**	20%	80%
A.14	**System acquisition, development and maintenance**	N/A	N/A
A.15	**Supplier relationships**	20%	100%

A.16	**Information security incident management**	20%	80%
A.17	**Information security aspects of business continuity management**	0%	0%
A.18	**Compliance**	20%	70%

Tabla 29- Mejora en la implementación de dominios ISO 27001 por los proyectos

Para facilidad de interpretación de la información antes citada, la relación de los avances o el grado de implementación de las mejoras del sistema de gestión de seguridad de la información, se puede apreciar en la grafico que se presenta a continuación, en el cual se muestra el estado en que se encontraba la empresa y las mejoras que tendrá después de la ejecución de los proyectos a corto plazos.

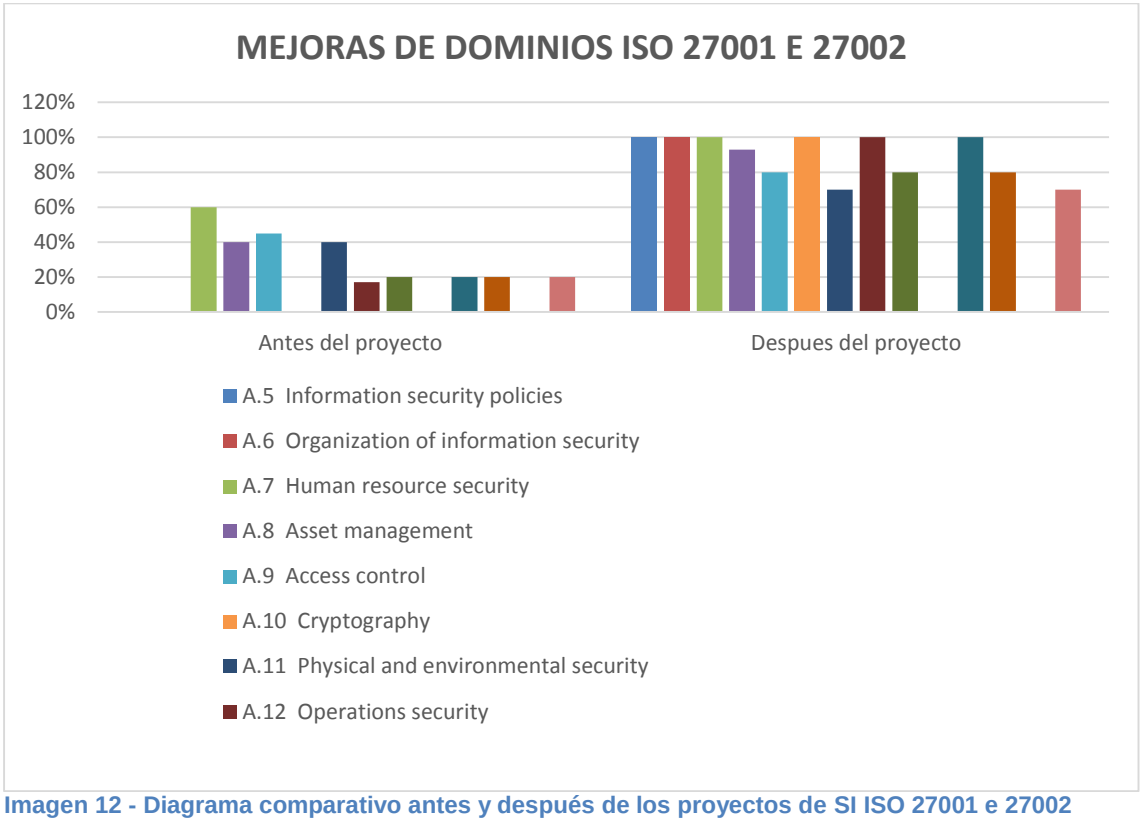

Imagen 12 - Diagrama comparativo antes y después de los proyectos de SI ISO 27001 e 27002

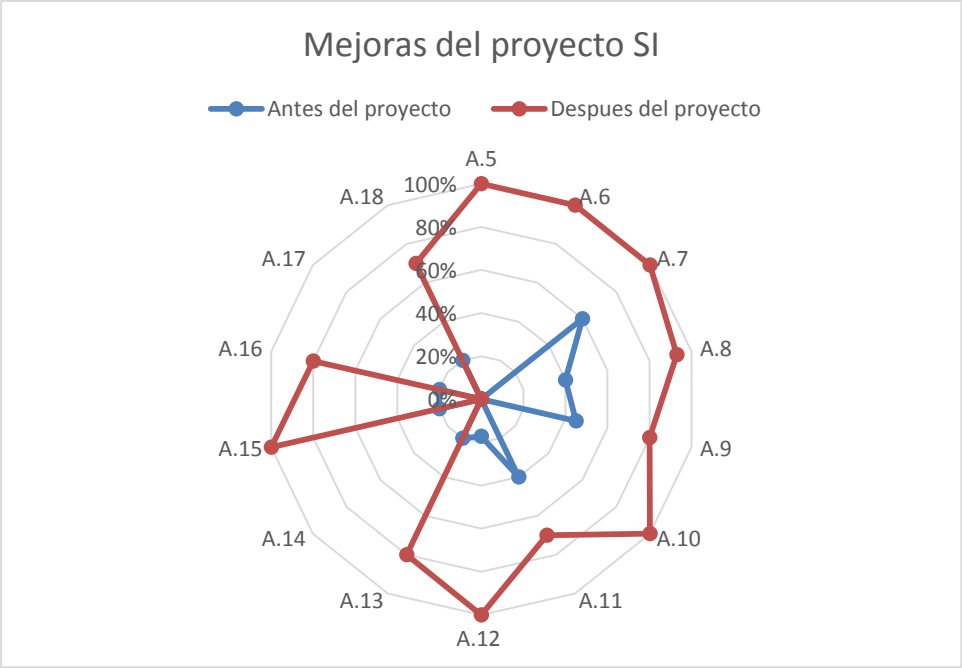

Imagen 13 - Diagrama radar de las mejoras del proyecto SGSI

En general se observa que al implementar los proyectos, se aumenta la eficacia de los controles en relación a la mitigación o disminución de los riesgos, lo que conlleva a una posible reducción de la frecuencia de ocurrencia de una amenaza. A continuación se relacionan algunos controles que reportan una mejora en su eficacia:

A.9. Control de Acceso: Aumenta su efectividad en la reducción de la frecuencia de ocurrencia del 45% al 80% para amenazas como el “Acceso no autorizado” y la “Difusión de software dañino”.

A.10. Controles Criptográficos: Aumenta su efectividad en la reducción de la frecuencia de ocurrencia y el impacto de amenazas como el “Acceso no autorizado de la información y perdida de la confidencialidad” de un 0%, es decir inexistente a un 100%, siendo este dominio uno de los primordiales para la empresa.

A.12. Seguridad en las Operaciones: Aumenta su efectividad en la reducción de la frecuencia de ocurrencia de todas las amenazas documentadas de un 17,10% a un 100%.

A.13. Seguridad en las Comunicaciones: Aumenta su efectividad en la reducción de la frecuencia de ocurrencia de todas las amenazas documentadas de un 20% a un 80%, teniendo en cuenta la importancia que revierten las comunicaciones entre sus clientes y proveedores, espera lograr un 100%, en la ejecución de los proyectos de largo plazo.

A.15. Relación con los Proveedores: Aumenta su efectividad en la reducción de la frecuencia de ocurrencia y el impacto de amenazas como el “Acceso no autorizado de la información y perdida de la confidencialidad” de un 0%, es decir inexistente a un 100%, siendo este dominio uno de los primordiales para la empresa.

14.1 PLANIFICACIÓN ECONÓMICA PARA LA EJECUCIÓN DE LOS PROYECTOS

En la siguiente tabla 30 podemos ver la planificación económica para la ejecución de los Proyectos definidos en la presente FASE 4.

	PLAN DE TRATAMIENTO PROYECTO A CORTO Y LARGO PLAZOS				
	Tipo de Contrato - Corto Plazo				
Código	**Descripción del proyecto**	**Tiempo de ejecución**	**Coste**	**Año**	**Coste/Año**
C_1000	Renovación – sistema de cableado estructurado de la red – sede principal	6 Meses	15.000	2015	91000 USD
C_1050	Implementación servidor de correo electrónico	6 Meses	8.000		
C_1060	Intercambio seguro de información con terceros	6 Meses	4.000		
C_1070	Modernización equipos informáticos	6 Meses	40.000		
C_1080	Sistema de cifrado – discos, archivos email.	6 Meses	5.000		
C_1090	Borrado seguro	6 Meses	4.500		
C_1010	Gestión de llaves, criptogramas, contraseñas y monitoreo de cuentas de superusuarios	6 Meses	3.500		
C_1020	Cifrado de discos	6 Meses	4.000		
C_1030	Herramientas avanzadas de Seguridad de EndPoint	6 Meses	7.000		
			91.000		
	Tipo de Contrato - Largo Plazo				
Código	**Descripción del proyecto**	**Tiempo de ejecución**	**Coste**	Año	Coste/Año
L_2000	Seguridad perimetral en profundidad	Entre 1 y 3 años	9.000	2016	42500 USD

L_2050	Implementación del plan de Capacitación y Concientización	Entre 1 y 3 años	1.000		
L_2060	Implementación Plan de Continuidad de Negocio y DRP	Entre 1 y 3 años	20.000		
L_2070	Gestión de dispositivos móviles	Entre 1 y 3 años	2.500		
L_2080	Data loss Prevention	Entre 1 y 3 años	4.700		
L_2090	Network Access Control	Entre 1 y 3 años	5.300		
			42.500		
			Costo Total del Proyecto	133.500 USD	

Tabla 30 - Planificación económica del proyecto

Finalmente el costo total del proyecto se estima en 133.500 (USD. En cuanto al retorno de la de los proyectos de seguridad propuestos. Al valor de pérdidas posibles por materialización de riesgos en un año se le conoce como ALE (Annual Loss Expectancy) y el retorno de inversión para la empresa causado por las inversiones de seguridad se denomina ROSI (Return Of Security Investment). A continuación se muestra el cálculo del ROSI y adicionalmente se estimará la cantidad de años que tardará la empresa en recuperar dicha inversión:

ALE	$10463590
ALE incluyendo proyectos (ALEnuevo)	$928954
Costo Total Proyectos	$133.500
Ahorro anual por riesgos no materializados = ALE - ALEnuevo	$ 9534636

Con los datos anteriores es posible determinar la cantidad de años que le tomaría a la empresa recuperar la inversión realizada en el plan de tratamiento de riesgos (Proyectos de seguridad):

Años de retorno de inversión = (Costo Total Proyectos) / (Ahorro anual por riesgos no materializados)
Años de retorno de inversión = $133.500 / $9534636 = 0,015 años

Lo anterior significa que en menos de 1 año (0,015 años) la empresa vería claramente el retorno de la inversión de los proyectos de seguridad planteados. Por otro lado, para calcular la tasa de retorno de la inversión (ROSI) se utilizará la siguiente fórmula:

ROSI = (ALE – ALEnuevo – Costo Total Proyectos) / Costo Total Proyectos
ROSI = ($9534636 - $133.500) / $133.500 = 70,4

El ROSI obtenido es del 70,4. Lo que indica que los proyectos son altamente rentables a través del tiempo.

15. INFORME DE AUDITORÍA INTERNA DE CUMPLIMIENTO

Parte importante del mantenimiento del sistema de gestión de seguridad de la información es evaluar que los planes de tratamiento se han realizado, así como el seguimiento a la mejora del sistema mediante revisiones, y todo el proceso de mejora en la implementación inicial. Para ello se ha definido un procedimiento de auditorías internas que permita realizar este seguimiento. En el presente informe se plasman los resultados de la auditoría efectuada sobre los procesos incluidos en el alcance del SGSI, como preparación para la obtención de la certificación ISO 27001:2013. Adicionalmente se presenta de forma estructurada y ordenada los resultados de la evaluación del nivel de madurez de seguridad de la información realizado para los controles de seguridad de acuerdo a la norma ISO 27002.

En el ANEXO XV, del presente trabajo se incluye el detalle de dicho análisis.
Los hallazgos realizados fueron priorizados y son presentados de forma ordenada de acuerdo a la siguiente escala de impactos establecida en común acuerdo con la empresa durante la reunión de inicio:

Clasificación		Tipo de Hallazgo	Cantidad de Hallazgo
Informativo	Fortalezas identificadas	Corresponde a aquellos puntos identificados como muy positivos por la auditoría y sobre los cuales la empresa debería enfocarse en mantener a través del tiempo.	
Impacto Alto	No conformidad Mayor	Se debe brindar atención inmediata, estableciendo planes de acción a corto plazo. Por su severidad implican la no obtención de la certificación ISO 27001.	
Impacto Medio	No conformidad Menor	Se deben establecer planes de acción a corto y mediano plazo. Implican un aplazamiento en la obtención de la certificación ISO 27001.	
Impacto Bajo	Oportunidad de Mejora	Se recomienda establecer planes de acción a mediano y largo plazo. Corresponden a las recomendaciones del auditor sobre algunos aspectos que el auditor encuentra conforme a la norma pero que podrían ser mejoradas para elevar el nivel de madurez de seguridad de la empresa y reducir los riesgos asociados.	

Objetivo y Alcance de la Auditoria

Dentro de los objetivos y alcance general de la auditoria se propusieron los siguientes:

1. Verificar en sitio la correcta implementación de los controles definidos en la declaración de aplicabilidad de acuerdo con el alcance del SGSI.

2. Realizar una evaluación del nivel de madurez de los controles de seguridad de la información, tomando como base la norma ISO 27002 y la declaración de aplicabilidad de la empresa.

15.2. Metodología empleada

Con base a los requisitos de la norma ISO 27001:2013, fueron identificados los hallazgos y con base en la verificación de la implementación de los controles declarados en el documento GAP 27001 y 27002, realizado en la empresa objeto de estudio. De igual manera se efectuó una revisión a alto nivel de la madurez en seguridad de la información de la empresa, respecto a los dominios de la norma ISO 27002 y teniendo como referencia el esquema de valoración de madurez CMM.
En esta auditoría de cumplimiento se realizó una validación completa de los controles de acuerdo a la declaración de aplicabilidad, y se espera que una vez sean implementados todos los proyectos el nivel de madures y de seguridad sean excelente.

La auditoría fue desarrolla siguiendo las siguientes fases:

Recolección de información: El principal objetivo de esta fase fue obtener la mayor cantidad de información asociada con el Sistema de Gestión de Seguridad de la Información de la empresa objeto de estudio, recolectar la documentación asociada y efectuar la asignación de recursos para cada fase de la auditoría.

Verificación de documentación del SGSI: Se verificó al detalle cada uno de los documentos enmarcados dentro de los requisitos de la certificación ISO 27001.

Verificación de eficacia de controles: Se validó la implementación de los controles estipulados en el documento GAP 27001 (declaración de aplicabilidad) para los procesos y en las instalaciones físicas incluidas en el alcance del SGSI.

Ejecución de auditoría in situ a procesos dentro del alcance: Se validó la existencia, el estado de implementación y de concientización de los procedimientos y procesos asociados con el Sistema de Gestión de Seguridad

de la Información en los siguientes procesos de negocio, incluidos dentro del alcance: venta de Productos y Servicios por Internet, recibo, alistamiento y despacho de mercancía, gestión de Seguridad de la Información, Seguridad de los recursos informáticos, etc.

Verificación de eficacia de controles: Se validó la implementación de los controles estipulados en el documento GAP 27001 (declaración de aplicabilidad) para los procesos y en las instalaciones físicas incluidas en el alcance del SGSI.

Análisis de información recopilada: Se analizaron los documentos recibidos y las evidencias recolectadas para determinar el estado general de seguridad de la información (Nivel de madurez) y se documentaron y clasificaron los hallazgos.

Elaboración, presentación y entrega del informe de auditoría: Fase estimada para la elaboración del informe de auditoría y su respectiva concertación con las áreas de seguridad previa formalización y presentación a la dirección.

15.3. Resultados de la evaluación del nivel de madurez de seguridad de la información en la empresa.

La valoración del nivel de madurez fue realizada para cada control de la declaración de aplicabilidad, la cual se encuentra basada en ISO 27002, teniendo en cuenta las entrevistas realizadas a los responsables de los procesos junto con las visitas in situ realizadas por los auditores y expertos técnicos que apoyaron la labor de auditoría.

Efectividad	CMM	Significado	Descripción
0%	L0	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	L1	Incial/Ad hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	L2	Reproducible pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	L3	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	L4	Gestionado	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	L5	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 31 - Nivel de madurez CMM

El resultado acumulado corresponde al promedio matemático de cada uno de los objetivos de control que lo componen, que a su vez se calculó con el

promedio de los valores de efectividad (madurez porcentual) de cada uno de los controles que lo componen.

Controles	Efectividad (%)	Nivel de madurez	Nivel de madurez (CMM)
A.5 Informationsecuritypolicies	100	5	Optimizado
A.6 Organization of information security	100	5	Optimizado
A.7 Human resourcesecurity	100	5	Optimizado
A.8 Assetmanagement	93,3	4,66666667	Proceso definido
A.9 Access control	80	4	Reproducible pero intuitivo
A.10 Cryptography	100	5	Optimizado
A.11 Physical and environmental security	70	3,5	Reproducible pero intuitivo
A.12 Operationssecurity	100	5	Optimizado
A.13 Communicationssecurity	80	4	Reproducible pero intuitivo
A.14 System acquisition, development and maintenance	0	0	Inexistente
A.15 Supplierrelationships	100	5	Optimizado
A.16 Information security incident management	80	4	Reproducible pero intuitivo
A.17 Information security aspects of business continuity management	0	0	Inexistente
A.18 Compliance	70	3,5	Reproducible pero intuitivo
Promedio SGSI	76,66428571	3,833333333	Reproducible pero intuitivo

Tabla 32 Resultado de evaluación por nivel de madurez dominios de seguridad norma 27001 y 27002

En el cuadro anterior, se puede observar que en la mayoría de los dominios la empresa, con la implementación de los proyectos de corto plazo, se encuentra algunos en nivel cinco optimizado y otro grupo en nivel dos reproducible pero intuitivo, de acuerdo con el grado de efectividad establecido por el nivel de madurez CMM, de igual manera se observa que a nivel general los proyectos se encuentra aplicados con un promedio general de 3,8, equivalente a un 77%, el cual se proyecta que aumente de manera significativa al finalizar todos los proyectos de la primera fase, en los meses de julio y agosto, fecha en la cual se recomendara a la empresa actualizar la auditoria.

El mismo análisis anterior puede ser visto en las siguientes figuras, que corresponden a la representación en un diagrama de radar y en un diagrama de área, donde se observa la brecha existente entre los niveles actuales de madurez de seguridad de la empresa y los niveles a los que la empresa desea llegar a estar.

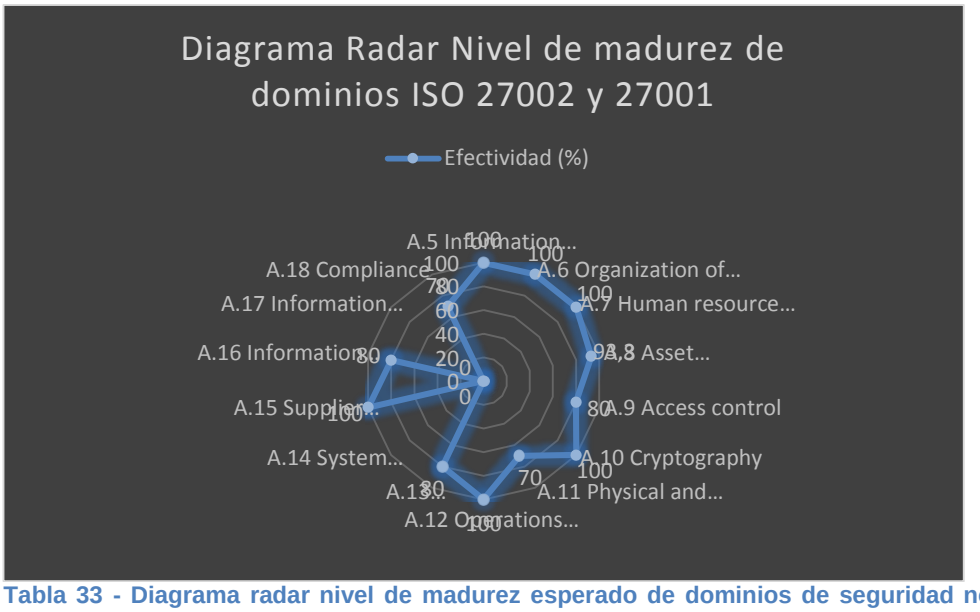

Tabla 33 - Diagrama radar nivel de madurez esperado de dominios de seguridad norma 27001 y 27002

De igual manera a continuación se muestra un diagrama de área que al igual que el diagrama en barra permite apreciar el nivel de madurez esperado con la ejecución de los primeros proyectos delineados dentro de la fase de corto plazo.

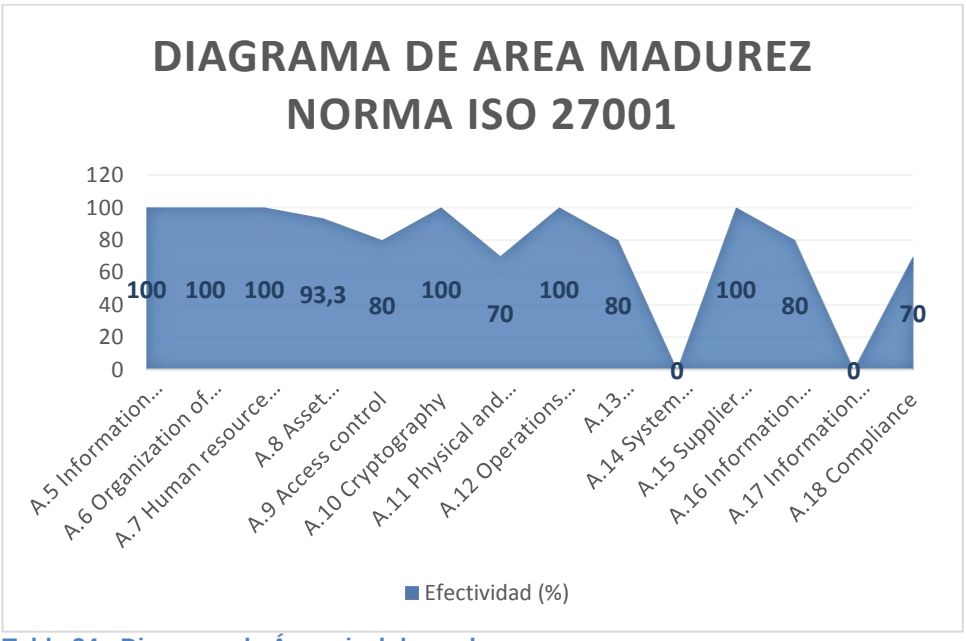

Tabla 34 - Diagrama de Área nivel de madurez

Hallazgos de Auditoria.

Para facilidad de comprensión los hallazgos de auditorías que fueron encontrados se relacionaron en la tabla que se muestra a continuación:

HALLAZGOS DE AUDITORIAS	
TIPO DE HALLAZGO	DESCRIPCIÓN DEL HALLAZGO
PUNTOS FUERTES	
APOYO DE LA DIRECCION	La Gerencia de la empresa objeto de estudio, generó unos documentos en donde apoyo de manera incondicional los proyectos que buscan mejorar la seguridad de la información en la empresa.
COMITÉ DE SEGURIDAD	El Comité de Seguridad de la Información, fue integrado por los responsable y coordinadores de Departamento, con lo cual se obtiene un grupo interdisciplinario y homogéneo que llevara el liderazgo en todo lo relacionado con la seguridad de la información
GESTIÓN DE RECURSO HUMANO	Se evidencian procedimientos y controles orientados a proporcionar una adecuara gestión antes durante y después del empleo.
CONCIENTIZACIÓN DE EMPLEADOS	Se evidencia un alto grado de conciencia y de compromiso de parte de los empleados de la empresa con los proyectos del SGSI
PARTICIPACIÓN DE EMPLEADOS	Se evidencia un alto grado de participación y colaboración de los empleados de la empresa en los proyectos SGSI.
GESTION DE ACTIVOS DE INFORMACIÓN	Se evidencio que después de la implementación de los proyectos fase I del plan de tratamiento de los riesgo, la gestión de los activos de la empresa es óptima y eficiente

SEGURIDAD CRIPTOGRAFICA	Se evidencia que después de la aplicación de los planes de tratamiento relacionados con sistemas criptográficos, la seguridad de la información tanto en los equipos locales como en su transmisión, mejoro de manera considerable, lo que les permitió aumentar sus niveles de seguridad.
GESTIÓN DE RELACIÓN CON PROVEEDORES	Se evidenció una excelente relación entre la empresa objeto de estudio proveedores y clientes, en especial en cuanto al tratamiento adecuado y seguro de la información.
NO CONFORMIDADES MAYORES	
PLAN DE CONTINUIDAD DEL NEGOCIO	A la fecha de realización de la auditoria, la empresa no cuenta con una Plan de Continuidad del Negocio, no obstante hay que recordar que en los planes de tratamiento de los riesgo se encuentra un proyecto en caminado a subsanar esta falencia, de manera gradual con un tiempo total de duración de 3 años aproximadamente.
NO CONFORMIDADES MENORES	
GESTIÓN DE SEGURIDAD FISICA	Se evidencia una notable mejoría en la seguridad física, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 70%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.

GESTION DE CONTROL DE ACCESO	Se evidencia una notable mejoría en la gestión del control de acceso, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 80%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.
GESTIÓN SEGURIDAD EN COMUNICACIONES	Se evidencia una notable mejoría en la gestión de seguridad de las comunicaciones, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 80%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.
GESTIÓN DE INCIDENTES DE SEGURIDAD	Se evidencia una notable mejoría en la gestión de los Incidentes de Seguridad, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 80%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.

GESTIÓN DE CUMPLIMIENTO	Se evidencia una notable mejoría en el cumplimiento de las normas y leyes regulatoria del país en temas de seguridad de la información, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 70%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.
OPORTUNIDADES DE MEJORAS	
CAPACITACIÓN SEGURIDAD INFORMÁTICA	Se evidencio que la empresa objeto de estudio está realizando contrataciones sobre capacitaciones en seguridad informática, con empresa proveedoras de software y herramientas de seguridad.
ACUERDOS DE CONFIDENCIALIDAD	Se evidencio que la empresa objeto de estudio realiza acuerdos de confidencialidad con el personal que ejerce funciones sensibles y dentro de las nuevas políticas estos acuerdos serán extendidos a todos los empleados de la empresa.

15.4. Conclusiones y recomendaciones de la auditoría interna

En conclusión fueron evidenciadas una cantidad significativa de puntos fuertes que fueron posibles gracias a la implementación de más del 80% de los proyectos del plan de tratamiento de los riesgos ejecutado a la fecha de realización de ésta auditoría, lo que nos indica que los controles esta alineados de manera acertada con las necesidades (riesgos y amenazas) de la empresa.

De otra parte era de esperarse que dentro de las no conformidades mayores se encontrase el Plan de Continuidad del Negocio, no obstante también hay que tener en cuenta la siguiente consideración: dentro de los proyectos del Plan de

Tratamiento de Riesgo, fue definido un proyecto para subsanar esta falencia, el cual tiene como objetivo, implementar el PCN, en un plazo no mayor a los 3 año.

En cuanto a las no conformidades menores, se evidencio que en su mayoría se encuentran con un porcentaje de implementación de alrededor de 70% o 80%, debido a que los proyectos que se encuentra relacionados con estos controles, se encuentra todavía en ejecución, con lo cual se espera que una terminados, se cumpla con el 100% de aplicación década uno de los controles que fueron relacionados dentro de las no conformidades menores.

Cabe destacar que la empresa objeto de estudio también presenta unas oportunidades de mejoras, destacándose las capacitaciones y charlas en seguridad informática que la empresa está contratando con empresa reconocidas en este medio, además como iniciativa propia ya se encontraban aplicando acuerdos de confidencialidad en algunos empleados para evitar amenazas como la fuga de información.

Por último, se considera que el resultado de la evaluación del nivel de madurez de seguridad de la información en la empresa es muy satisfactorio en cuanto a que la mayoría de procesos y controles se encuentran entre los niveles optimizado y Reproducible pero intuitivo, con un porcentaje entre 70% y 100%. Lo anterior permite evidenciar que los grandes esfuerzos que ha realizado la organización en la definición e implementación del SGSI han dado los resultados esperados y totalmente alineados con la norma ISO 27001:2013.

15.5. Anexos del informe de auditoría interna

El análisis detallado del nivel de madurez de seguridad de la información realizada sobre cada uno de los controles con el nombre de ANEXO XV - AUDITORIA DE CUMPLIMIENTO - EVALUACION NIVEL DE MADUREZ.

16. PRESENTACIÓN DE RESULTADOS Y ENTREGA DE INFORMES

16.1 Introducción

Un entregable es cualquier producto medible y verificable que se elabora para completar un proyecto, los cuales son representados por esquemas, prototipos, análisis, sistemas, entre otros.

Los entregables tienen que estar enmarcados entre los requisitos del plan de implementación y los objetivos definidos.

Los entregables que se entregaran dentro de este proyecto son:

- **Informe ejecutivo:** Se debe presentar un breve análisis de los aspectos más importantes del Plan de Implementación de la ISO/IEC 27001:2013, se antepone antes de la presentación y tiende hacer uno de los aspectos más importantes para la alta dirección, por lo que debe ser concisa incluyendo la motivación, el enfoque del plan y las principales conclusiones.

- **Memoria descriptiva:** Corresponde el documento final que contiene las fases desarrolladas, con los respectivos anexos que servirán de evidencia de los resultados obtenidos.

16.2 Entregables

6.2.1 Informe Ejecutivo

Medellín – Colombia

Referencia: INFORME EJECUTIVO

Fecha: Diciembre de 2015

El TFM ha consistido en la elaboración de un Plan de Implementación de la ISO/IEC 27001:2013, en una empresa del sector textil con una trayectoria de más de 25 años de funcionamiento.

La empresa objeto de estudio esta situada en Colombia y tiene sus oficinas principales en la ciudad de Medellín. Al momento cuenta con un número considerable de empleados distribuidos en todas sus sedes.

En nuestro país desde el año 2009, existe una toma de conciencia frente a las amenazas informáticas situación que la empresa estudiada tiene deseo de aprovechar.

Por lo tanto, la empresa está consciente que es un momento decisivo donde hay que tomar acciones encaminadas a reforzar la seguridad de la información alineadas al plan estratégico de la empresa y el marco normativo vigente.

Una vez el comité de gerencia de la empresa tomó la decisión de aceptar la propuesta de implementar el plan y brindar todo el apoyo ante el mismo, se debió identificar si se iba a trabajar con personal interno o se iba a contratar asesoría. Debido a la carencia de conocimientos relacionados con el tema la empresa decidió con tratar asesores externos para que trabajaran con empleados internos quienes conformarían el Comité de Seguridad de la Información, quine sería el encargado de la ejecución y supervisión del plan.

Se realizaron las reuniones de inicio del proyecto para concienciar al personal de la empresa sobre de la importancia de su implementación y de su apoyo para que su ejecución se realice correctamente, en este sentido, la decisión de que el personal interno se encargue del desarrollo del plan ha facilitado el análisis.

A continuación se presentan las fases realizadas del Plan de Implementación de la norma ISO/IEC 27001:2013:

- Se realizó el análisis diferencial (GAP Analysis) comparando los controles implantados en la empresa vs los controles necesarios en base a la norma ISO/IEC 27001 e ISO/IEC 27002:2013, con el objetivo de conocer el estado actual de la empresa y definir el alcance y objetivos de la implantación del Sistema de Gestión de Seguridad de la Información.

- Alcance: La implementación de la seguridad de la información se va a realizar en la sede principal de la empresa, que se encuentra ubicada en la ciudad de Medellín, bajo el siguiente escenario:

- De acuerdo a la Norma ISO 27001, que establece que la empresa debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance y con mirar a delimitar la extensión del proyecto. Para validar su alineación con la norma, a continuación se presenta el alcance actual para el Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa en estudio: Según la declaración de aplicabilidad vigente, el límite del Sistema de Gestión de Seguridad de la información, está definido por los activos de información que apoyan los procesos, asociados al negocio de marketing y de comercio electrónico del portafolio accionario de la Empresa.

- Posterior se definió la documentación necesaria y básica para implementar el SGSI, ya que es fundamentar disponer de una normativa

común de seguridad que regule la documentación, además de identificar los documentos mínimos.

- Luego se realizó la Valoración de Activos y Dimensiones de Seguridad, donde por cada activo se estableció el valor que tendría que la amenaza sea explotada por alguna vulnerabilidad. Con esta información se procedió a identificar el nivel de riesgo aceptable, el mismo que fue Aprobado por parte del Consejo Superior según resolución.

- Implementación del Plan de gestión de riesgos, en donde se presenta una propuesta de proyectos que servirán para reducir la presencia del riesgo. La empresa, debe estar consciente que con dichas medidas no va a eliminar la presencia del riesgo, sino se va a controlar en caso de presencia.

Las fases fueron desarrolladas siguiendo las directrices de la norma ISO/IEC 2700:2013 y las metodologías seleccionadas.

Cuando se han realizado todas las fases de implementación de los proyecto se determinó el estado de cumplimiento de los mismos mediante una Auditoría, que realizó personal externo de la empresa, cuyos resultados fueron avalados por el Comité de Seguridad de la Información.

Los datos obtenidos de la auditoría fueron presentados al Comité de Gerencia de la empresa, quienes fueron los encargados de tomar las decisiones pertinentes sobre el proyecto.

A continuación se presentan algunos no conformidades que fueron detectadas con base a diferentes metodologías de pruebas y recolección de información como entrevistas, encuestas, análisis de documentación interna y externa, pruebas en el sistema, entre otros.

PUNTOS FUERTES	
APOYO DE LA DIRECCION	La Gerencia de la empresa objeto de estudio, generó unos documentos en donde apoyo de manera incondicional los proyectos que buscan mejorar la seguridad de la información en la empresa.

COMITÉ DE SEGURIDAD	El Comité de Seguridad de la Información, fue integrado por los responsable y coordinadores de Departamento, con lo cual se obtiene un grupo interdisciplinario y homogéneo que llevara el liderazgo en todo lo relacionado con la seguridad de la información
GESTIÓN DE RECURSO HUMANO	Se evidencian procedimientos y controles orientados a proporcionar una adecuara gestión antes durante y después del empleo.
CONCIENTIZACIÓN DE EMPLEADOS	Se evidencia un alto grado de conciencia y de compromiso de parte de los empleados de la empresa con los proyectos del SGSI
PARTICIPACIÓN DE EMPLEADOS	Se evidencia un alto grado de participación y colaboración de los empleados de la empresa en los proyectos SGSI.
GESTION DE ACTIVOS DE INFORMACIÓN	Se evidencio que después de la implementación de los proyectos fase I del plan de tratamiento de los riesgo, la gestión de los activos de la empresa es óptima y eficiente
SEGURIDAD CRIPTOGRAFICA	Se evidencia que después de la aplicación de los planes de tratamiento relacionados con sistemas criptográficos, la seguridad de la información tanto en los equipos locales como en su transmisión, mejoro de manera considerable, lo que les permitió aumentar sus niveles de seguridad.

GESTIÓN DE RELACIÓN CON PROVEEDORES	Se evidenció una excelente relación entre la empresa objeto de estudio proveedores y clientes, en especial en cuanto al tratamiento adecuado y seguro de la información.
NO CONFORMIDADES MAYORES	
PLAN DE CONTINUIDAD DEL NEGOCIO	A la fecha de realización de la auditoria, la empresa no cuenta con una Plan de Continuidad del Negocio, no obstante hay que recordar que en los planes de tratamiento de los riesgo se encuentra un proyecto en caminado a subsanar esta falencia, de manera gradual con un tiempo total de duración de 3 años aproximadamente.
NO CONFORMIDADES MENORES	
GESTIÓN DE SEGURIDAD FISICA	Se evidencia una notable mejoría en la seguridad física, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 70%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.
GESTION DE CONTROL DE ACCESO	Se evidencia una notable mejoría en la gestión del control de acceso, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 80%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.

GESTIÓN SEGURIDAD EN COMUNICACIONES	Se evidencia una notable mejoría en la gestión de seguridad de las comunicaciones, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 80%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.
GESTIÓN DE INCIDENTES DE SEGURIDAD	Se evidencia una notable mejoría en la gestión de los Incidentes de Seguridad, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 80%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.
GESTIÓN DE CUMPLIMIENTO	Se evidencia una notable mejoría en el cumplimiento de las normas y leyes regulatoria del país en temas de seguridad de la información, desde la auditoria previa, a la auditoria de cumplimiento, se denotan la implementación de los nuevos controles exigidos por la norma de seguridad, que han permitidos elevar su efectividad a un 70%, se espera que llegue al 100% una vez se terminen de implementar los proyectos del plan de tratamiento.

Todos los documentos fueron desarrollados bajo el manual de documentación, e información que poseía la empresa en materia de seguridad fue adaptada.

Para concluir deseo señalar que todo el proceso fue adelantado cumpliendo con todos los procedimientos y protocolos que la empresa tenía establecido para este tipo de situaciones y en los casos en los que no los hubieron, los procedimientos fueron aprobados por el Comité de Seguridad de la Información con el aval del Comité de Gerencia.

La propuesta de implementación del SGSI dio a la Alta Dirección una visión sobre la importancia de la seguridad en la información, y una oportunidad inigualable para contener las amenazas y riesgos de seguridad que se le venían presentado desde hace varios meses con unas pérdidas económicas bastante significativa, además del impacto negativo de esta situación ante sus clientes.

16.2.2 Memoria descriptiva

En la memoria descriptiva se incluye a detalle todo el proceso para la Implementación del Sistema de Gestión de Seguridad de la Información.

A continuación se encuentran las fases de las que está conformado:

- **Fase 1: Situación Actual: Contextualización, Objetivos y Análisis Diferencial:** Descripción la situación actual de la IES según la normativa ISO/IEC 27001:2013 e ISO/IEC 27002:2012.

- **Fase 2: Sistema de Gestión Documental:** Establecimiento de la documentación básica inicial para implementar el Sistema de Gestión de Seguridad de la Información según la norma ISO 27001.

- **Fase 3: Análisis de Riesgos:** Identificación de los activos de la empresa, las vulnerabilidades y amenazas a las que se encuentra expuesto.

- **Fase 4: Propuestas de Proyectos:** Definición e implementación de los controles adecuados, con los responsables y el presupuesto, con el objetivo de evitar los daños intrínsecos al factor de riesgo.

- **Fase 5: Auditoría de Cumplimiento:** Verificación de los controles, realizado por un auditor con el fin de comprobar si se han cumplido el objetivo establecido.

16.2.3 Presentaciones

- **Presentación inicial a la empresa:** Presentación antes de abordar el Plan de Implementación del SGSI donde se establecen las claves del mismo y se expone la importancia de su implementación.

- **Presentación del estado de cumplimiento de los controles de seguridad:** Presentación donde se establece el estado de cumplimiento de los controles de seguridad en la empresa, que posterior serán los objetivos a cumplir. El objetivo de la presentación es servir de base para la aprobación de los proyectos propuestos.

- **Presentación final a la empresa:** Presentación donde se expone el plan a realizar, los aspectos organizativos, el plan de acción, los principales resultados del estudio y el resumen del cumplimiento e impacto de la ejecución de los proyectos.

CONCLUSIONES DEL PROYECTO

Aunque los motivos iníciales para desarrollar el Sistema Gestión de Seguridad de la Información no fue una toma de conciencia sobre la importancia de la seguridad de la información de parte de la empresa, sino la materialización de algunos riesgo que revirtieron en pérdidas económicas significativas, la empresa terminó aceptando que los niveles de seguridad con los que contaba en su momento, eran precarios los cuales presentaron para esa fecha los siguientes resultados: “el 35,7% de los controles de la norma ISO 27001 e ISO 27002, no están implementados en la empresa de estudio y el 64,3% restantes son deficientes, por tal motivo en estos momentos la información de la empresa, es altamente vulnerable”.

De otro lado, con el Plan de Implementación de la ISO/IEC 27001:2013, adoptado por la empresa se presentó la oportunidad de mejor dichos resultados, hoy en día la empresa ha alcanzado el 100% en varios controles y dominios y se espera que una vez culmine la ejecución de todos los proyectos de corto y largo plazo que fueron estipulado en el Plan de Tratamiento, los demás dominios y controles de la norma ISO/IEC 27001:2013 que están siendo desarrollados por la empresa también alcance el 100%.Esto evidencia la efectividad que tendrá la implementación de los proyectos de seguridad definidos en el plan de tratamiento de riesgos y permite de alguna manera sustentar la inversión realizada. Adicional a esto, se espera que la implementación de dichos proyectos permitirá reducir significativamente los riesgos y la materialización de amenazas sobre los principales activos de la empresa, estimando que de una pérdida inicial estimada de $10.463.590 llegaría a tan solo $928.954 al año.

De otra parte, al realizar la auditoria de cumplimiento fueron hallados unas fortalezas y oportunidades, que nos permiten inferir que la implementación de este SGSI, es altamente positivo para la empresa, lo que ha permitido disminuir sus riesgo a niveles considerables, así mismo fueron hallados unas no conformidades las cuales están siendo subsanadas con la ejecución de los proyectos definidos en el plan de tratamiento.

En conclusión, con la implementación de este plan, la empresa adquiere unos niveles adecuados de seguridad y protección, ajustados a la norma ISO 27001 y a los dominios de la ISO 27002, lo que le permitirá hacerle frente a las amenazas y riesgos que fueron identificados en esta empresa.

GLOSARIO DE TÉRMINOS

Autenticidad: Aseguramiento de la identidad u origen [MINIST06]

Análisis del riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [ISO05]
Análisis de impacto: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización [MINIST06]
Activo: Cualquier cosa que tiene valor para la organización. [ISO05]
Amenaza: Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las amenazas se pueden materializar y transformarse en agresiones. Pueden afectar a la integridad, confidencialidad o disponibilidad. [ARTOOL08]
Consecuencia: Resultado de un evento [CNSS10]

Confidencialidad: El objetivo de seguridad que genera requerimientos para protección de intentos intencionales o accidentales para realizar lectura de datos no autorizados. La confidencialidad cubre datos en almacenamiento, durante el procesamiento y en tránsito. [NIST02]

Control: Proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo negativo o potenciar oportunidades positivas. [NTC06]

Continuidad del negocio: Prevenir, mitigar y recuperarse de una interrupción. Los términos “planear la reanudación del negocio”, “planear la recuperación después de un desastre” y “planear contingencias” también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad. [COB07]

Criterio de riesgo: Términos de referencia con lo que el riesgo es valorado [ISO02]

Ciclo Deming: El ciclo PDCA consiste en la secuencia encadenada de planificar, hacer, medir y actuar para mejorar, es muy conocido en el mundo de la calidad, fue explicado con cierto detalle por Shewhart en la segunda década del siglo pasado y es universalmente conocido como el ciclo o Rueda de Deming por que fue este autor quien profundizó en él, lo desarrolló y lo dio a conocer de sus escritos en los términos que se conoce hoy [CERVERA02]

Control de acceso: Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace [SEGREDES02]

Dimensión de seguridad: Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor [MINIST06]

Disponibilidad: El objetivo de seguridad que genera los requerimientos para protección contra:

1. Intentos intencionales o accidentales de (1) realizar la destrucción no autorizada de datos o (2) de otra forma causar una denegación de servicios o datos
2. El uso no autorizado de recursos del sistema[NIST02]

Degradación: Pérdida de valor de un activo como consecuencia de la materialización de una amenaza [MINIST06]

Estimación del riesgo: Proceso usado para asignar valor a la probabilidad y consecuencias de un riesgo [ISO02]

Evento: Ocurrencia de un conjunto particular de circunstancias [NTC06]

Integridad: El objetivo de seguridad que genera requerimientos de protección contra cualquier intento intencional o accidental de violar la integridad de los datos (la propiedad que tienen cuando no han sido alterados de forma no autorizada) o la integridad de los sistemas (la calidad que un sistema tiene cuando se lleva a cabo su función prevista en una forma irreprochable, libre de manipulación no autorizada) [NIST02]

Frecuencia: Tasa de ocurrencia de una amenaza [MINIST06]

Infraestructura tecnológica: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones. [COB07]

Identificación del riesgo: Proceso para encontrar, listar e identificar los elementos de riesgo. [ISO08]

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza [MINIST06]

Impacto residual: Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información [MINIST06]

Incidente: Evento con consecuencias en detrimento de la seguridad del sistema de información [MINIST06]

Información: “Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto,

disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones" [IDALBE05]

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [ISO05]

Política de seguridad de la información: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión de la seguridad de la información [ISO11]

Probabilidad: Medida de la oportunidad de ocurrencia expresada como un número entre o y 1 [NTC06]

Riesgo residual: Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información [MINIST06]

Riesgo: El impacto neto considerando (1) la probabilidad de que una fuente de amenaza particular (explote accidental o intencionalmente) una vulnerabilidad particular del sistema de información y (2) el impacto resultante en caso de que esto ocurra. El riesgo relacionado con TI se deriva de la responsabilidad legal o perdida de misión debido a:
a. Divulgación no autorizada (intencional o accidental), modificación, o destrucción de información
b. Errores y omisiones no intencionales
c. Interrupciones de TI a causa de desastres naturales o causados por el hombre
d. El no ejercer el debido cuidado y diligencia en la implementación y operación de sistema de TI. [NIST02]

El potencial de que una amenaza específica explote las vulnerabilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia. [COB07]

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad. [ISO05]

Sistema de información: “Un sistema de información es un conjunto de elementos o componentes interrelacionados para recolectar (entrada), manipular (proceso) y diseminar (salida) datos e información y para proveer un mecanismo de retroalimentación en pro del cumplimiento de un objetivo” [ISO05]

Sistema de Gestión de Seguridad de la Información (SGSI): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. [ISO05]

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quien hizo que y en qué momento [MINIST06]

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo. [ISO05] Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo. [ISO05]

Vulnerabilidad: “Una vulnerabilidad es una debilidad de seguridad en un sistema informático que suele encontrarse en programas y sistemas operativos. La presencia de vulnerabilidades conocidas en sistemas informáticos puede dejar estos sistemas expuestos a los ataques de malware. Esto se debe a que los programas que aprovechan las vulnerabilidades conocidas, normalmente llamados exploits, a menudo están disponibles públicamente como código origen, que se puede personalizar para crear una herramienta de malware o de hacking.” [TRENDM08]

BIBLIOGRAFIA

Adicional a los conocimientos y experiencia previamente adquiridos, y al material proporcionado por el instructor de la materia, fueron requeridas las siguientes fuentes de consulta:

1. [ARTOOL08] AR-TOOLS - Glosario de seguridad informática. AR-TOOLS, 2008

2. [CERVERA02] CERVERA, Josep. "*La transición a las nuevas ISO 90002000 y su implantación: Un plan sencillo y práctico con ejemplos*", Publicado por Ediciones Díaz de Santos, 2002, pág. 31

3. [COB07] Instituto de Gobierno de TI. COBIT 4.1. "Marco de Trabajo - Objetivos de control – Directrices Generales – Modelos de Madurez", 2007

CIBERBIBLIOGRAFÍA

1. http://www.iso27000.es
2. www.iso27001standard.com/es/que-es-iso-27001
3. https://es.wikipedia.org/wiki/ISO/IEC_27001
4. http://inzafe.cl/analisis-gap/
5. https://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n
6. https://www.ismsforum.es/
7. http://www.defensa.gob.es/politica/infraestructura/seguridad-informacion/
8. http://planeameinto-estrategico.blogspot.com/2010/05/metricas-e-indicadores-gestion.html
   - Introduction to Return on Security Investment. ENISA (European Network and Information Security Agency), 2012.
9. http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf
   - La importancia de la Declaración de aplicabilidad para la norma ISO 27001. Dejan Kosutic, 2 de Junio de 2011.
10. http://planeameinto-estrategico.blogspot.com/2010/05/metricas-e-indicadores-gestion.html
11. https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport