MASTER INTERUNIVERSITARIO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

TRABAJO FINAL DE MÁSTER: SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ELABORACIÓN DE UN PLAN DE IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2013

ESTUDIANTE:

ING. MIGUEL ARTURO ARCOS ARGUDO

DIRECTOR:

MÁSTER ANTONIO JOSÉ SEGOVIA HENARES

FECHA DE REALIZACIÓN:

Septiembre 2014 – Enero 2015

Agradecimiento

Primeramente a Dios en quién he confiado siempre y quién también ha confiado en mí a pesar de mis debilidades. A mi esposa Kelly, por haberme empujado a empezar esta “loca aventura” con el fin de tener la vida que siempre quisimos y poder cristalizar nuestros sueños que van mucho más allá de lo económico, gracias por haberme sostenido en todo este tiempo, la mitad de este logro es tuya. A David, mi hijo y mi mejor amigo, gracias porque con tu inocencia y tu ternura me has dado siempre fuerzas para seguir adelante cuando todo se veía más fuerte que yo, perdona todo el tiempo que te he quitado por dedicarme a estudiar. A mi hermano Rudolf, gracias por el apoyo durante todo este camino, hubiera sido mucho más difícil sin ti. A toda mi familia, mis padres, hermanas, cuñados, sobrinos, gracias por entender y soportar mi ausencia en muchos momentos importantes para nosotros cuando tenía que pasar las interminables horas de estudio. A mi director de este trabajo, Máster Antonio Segovia, realmente tengo muy pocos profesores de los que puedo tener tan buen concepto, gracias por esa capacidad de guiar y de alentar a seguir adelante, y por supuesto, gracias por todas esas oportunas correcciones, ojalá nos volvamos a ver más adelante. Finalmente gracias a todos mis compañeros del MISTIC, ya que me he enriquecido cuando han compartido sus conocimientos en cada asignatura, gracias por la ausencia de egoísmo y la abundancia de solidaridad.

Dedicatoria

Este trabajo va dedicado a mi esposa Kelly y a mi hijo David, mi razón de vivir, de superarme y de querer ser mejor, todo esto fue por nuestro pequeño hogar. Los amo.

Resumen

La seguridad de la información es considerada actualmente como uno de los aspectos más importantes dentro de toda organización y al que se dedica gran cantidad de recursos, es más, en muchos casos llega a ser uno de los procesos más críticos que ameritan mucha investigación, inversión y actualización.

La información es considerada hoy en día, un activo intangible, pero de gran valor para la empresa, en ella reside, en muchos casos, el éxito dentro de la competencia en el mercado; cualquier fuga, manipulación o pérdida de la misma podría implicar grandes pérdidas de diferente índole para la compañía. Es por ello que se vuelve imprescindible la existencia de un Sistema de Gestión de Seguridad de la Información (SGSI), este sistema ayudará a que la empresa se dote de controles que le permitan gestionar los riesgos a los que esté expuesta la información, ya sea evitándolos o reduciéndolos a índices aceptables.

El presente trabajo consiste en la implementación de un SGSI basado en la norma ISO/IEC 27001:2013 en un empresa que se ha interesado en proteger su información mediante la identificación de los riesgos a los que está expuesta, y la definición de procesos para controlar dichos riesgos, así como determinar un plan de mejora continua para la seguridad de su información.

Abstract

The security of the information is now considered as one of the most important aspects of any organization and that a large amount of resources is dedicated, in many cases becomes one of the most critical processes which deserve a lot of research, investment and upgrade.

The information is currently considered an intangible asset, but of great value to the company, it's in many cases, success in competition in the market, any escape, tampering or loss of it could involve big losses of various kinds for the company. That is why the existence of a Management System of Information Security (ISMS) becomes necessary, this system will help the company shall be equipped with controls that allow it to manage risks to which information is displayed, either avoiding them or reduce them to acceptable indexes.

The present work consists of the implementation of an ISMS based on ISO / IEC 27001: 2013 on a company that was interested in protecting its information by identifying the risks to which they are exposed, and the definition of processes to control such risks and determine a plan of continuous improvement to the security of its information.

Índice

1. Introducción

El presente documento representa un diseño e implementación de un SGSI para el sistema de información interno de la empresa **Mariscos S. A**., tomando como base la norma ISO/IEC 27001:2013, dicho sistema de información ha sido analizado y se ha desarrollado una serie de recomendaciones para garantizar la disponibilidad, integridad y confidencialidad de la información en todo momento. De la misma manera se presenta las acciones que se deben realizar cuando alguna eventualidad ha ocurrido afectando al sistema de información para una pronta recuperación.

1.1 Norma ISO/IEC 27001 e ISO/IEC 27002

La norma ISO/IEC 27001 describe los requisitos que debe tener todo SGSI que aspire a obtener dicha certificación. Este estándar fue publicado como tal por la ISO (International Organization of Standarization) en 2005, y en la actualidad es el único aceptado para la gestión de la seguridad de la información, sin embargo es producto de toda una evolución.

1.1.1 Breve reseña histórica de la norma ISO/IEC 27001 e ISO/IEC 27002

El origen de la norma ISO/IEC 27001 se encuentra en la norma BS 7799-1:1995 que fue desarrollado como un manual de buenas prácticas para la seguridad de la información de las empresas británicas, esta guía no ofrecía una certificación.

En 1999 esta norma es revisada y recién se convierte en una norma certificable como BS 7799-2:1999.

En el año 2000 la ISO la toma como base y publica la norma ISO/IEC 17799:2000, sin embargo no implementan cambios significativos.

En Reino Unido, durante el año 2002 se actualiza la norma BS, y se publica la versión BS 7799-2:2002, la misma que sirve para la certificación de varias empresas de distintos países.

En 2005 la norma ISO/IEC 17799 es revisada, y aparece la norma certificable ISO/IEC 27001:2005.

En 2007 la norma ISO/IEC 17799 es renombrada como ISO/IEC 27002. Esta norma es una guía de buenas prácticas que describe los controles (133 controles) que pueden ser implementados para la gestión de la seguridad de la información. No es una norma certificable.

En 2007 se publica una versión de la norma ISO 27001 traducida al castellano, esto sucedió en España.

En 2009 se publica un documento de modificaciones adicionales a la norma ISO 27001 llamado ISO/IEC 27001:2005/1M:2009.

En 2013 se vuelve a revisar la norma ISO 27001 en la que se incluyen cambios significativos y se publica la norma ISO/IEC 27001:2013.

1.1.2 Comparación entre la norma ISO/IEC 27001:2005 y la norma ISO/IEC 27001:2013

La principal modificación entre la versión de la norma del año 2005 y la versión del año 2013 radica en la estructura. La norma ISO/IEC 27001:2005 tiene cinco secciones principales (desde la 4 hasta la 8), mientras que la norma ISO/IEC 27001:2013 presenta siete secciones principales (desde la 4 hasta la 10), esto es debido a que la nueva versión ya utiliza el formato de Anexo SL, formato que deberán implementar todas las normas según la disposición de la ISO.

La nueva versión es mucho más concreta, a pesar de tener más apartados, lo que le permite ser mucho más fácil de manejar.

Uno de los cambios más significativos tiene que ver con la eliminación del sub-apartado que la antigua norma contenía sobre el enfoque de procesos y la explicación sobre el PDCA, la nueva norma asume que no es necesario entender estos conceptos para implementarla.

También desaparece las exigencias sobres acciones preventivas, pues se ha determinado que resulta un trabajo redundante el implementar controles que ya actúan como acciones preventivas, y luego implementar más acciones preventivas.

Otro aspecto eliminado es la distinción entre documentos y registros, ahora solamente se refiere a ellos como “información documentada”.

Algo que la nueva norma incorpora es el concepto de “Contexto”, ahora es necesario que se entienda el contexto de la organización antes de implementar un SGSI.

La nueva norma también pide en el apartado 4.1 que se consulte a la norma ISO/IEC 31000 como estándar para la gestión de riesgos.

1.1.3 La Norma ISO/IEC 27001 en Ecuador

En Ecuador, a la fecha actual (noviembre de 2014) existe una cantidad casi nula de empresas que poseen una certificación ISO 27001 en sus SGSI, sin embargo sí existe una entidad que otorga dicho certificado, el INEN (Instituto Ecuatoriano de Normalización – www.normalización.gob.ec) es el organismo estatal que se encarga de vigilar la calidad de productos y servicios que se ofrecen en todo el territorio ecuatoriano, aquellos productos que poseen el sello de calidad INEN garantizan haber aprobado altas exigencias de calidad, la norma ISO 27001:2005 consta entre las certificaciones que este organismo ofrece para las empresas que se interesen.

El mismo INEN es el encargado de la traducción de las normas ISO, lo hace con la nomenclatura **NTE INEN-ISO/IEC XXXXX**, sin embargo son pocas las normas traducidas, de hecho la norma ISO/IEC 27001 no ha sido traducida en Ecuador.

1.2 Enfoque y descripción de la empresa

La empresa Mariscos S. A. es una organización con una experiencia de quince años dentro del mercado, que se dedica principalmente a la venta y distribución de mariscos y carnes dentro de toda la región sur del Ecuador, con su sede en la ciudad de Cuenca, provincia del Azuay. Es una compañía pionera en la ciudad, razón por la cual goza de un prestigio bien alto dentro de la región y cuya clientela sigue en expansión, debido a esto su volumen de información ha crecido considerablemente en los últimos cinco años. La empresa dispone también de un comisariato ubicado en un sector estratégico de la ciudad, en el que además comercializa productos de otra

naturaleza tales como: productos de primera necesidad, artículos de limpieza, confitería, embutidos, etc., esto con la intención de completar el servicio a los clientes locales.

A continuación se muestra el organigrama de la organización:

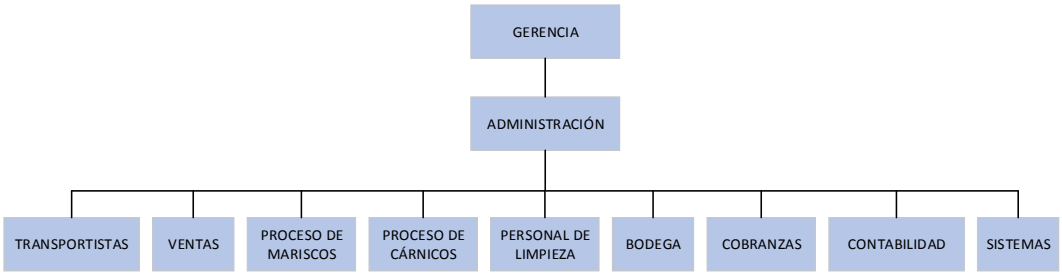

Figura 1.1: Organigrama de la empresa

Los clientes a los que se atiende con prioridad, y en donde el proceso suele ser crítico son aquellos que tienen restaurantes, empresas de catering, comedores de fábricas, etc., es decir todo aquel que potencialmente pueda hacer o hace compras en volúmenes altos.

El sistema de información existente maneja los módulos necesarios para el manejo del negocio, los principales se enumeran a continuación:

a. Clientes
b. Proveedores
c. Inventarios
d. Compras
e. Ventas
f. Contabilidad
g. Bancos
h. Pagos / Cobros

Cabe recalcar también que la empresa no es tan amplia en cuanto a espacio físico ni en cuanto a personal, dentro de su país se le considera como microempresa, sin embargo es de las más conocidas dentro del mercado local. La figura 1.2 muestra el Organigrama Funcional de la empresa.

Inicialmente la seguridad de la información de la empresa se puede considerar en un estado aceptable, ya que nunca se han detectado robos, y cuando ha habido pérdidas se ha podido recuperar un alto porcentaje de la misma, sin embargo se evidencia que hay muchos aspectos que se debe mejorar.

Los datos más importantes para la compañía que se han identificado son:

a. Datos de los clientes (personas claves de contacto).
b. Precios de compra
c. Precios de venta
d. Datos de proveedores
e. Estados financieros
f. Asuntos legales

La compañía dispone de un sistema de información adquirido, este sistema funciona a nivel interno, la empresa no maneja un sitio web por lo que los riesgos de su información se reduce a lo que pueda pasar a nivel local, es decir, es muy poco probable que remotamente se lleve a cabo un ataque ya que el servidor principal nunca se conecta a internet. Existen algunos terminales que si tienen conexión con

la web, pero lo hacen para tareas muy específicas, como enviar alguna información solicitada por algún cliente por medio de correo electrónico o para realizar alguna consulta o descarga por parte del departamento de sistemas. El sistema de información en realidad no es grande, es por ello que prácticamente no existe documentación sobre las políticas de seguridad. La actualización del sistema está a cargo de la empresa que lo desarrolló, es decir dentro de la organización no existe un departamento de desarrollo de software, solamente de mantenimiento y soporte técnico. La figura 1.2 muestra el diagrama de red de la empresa.

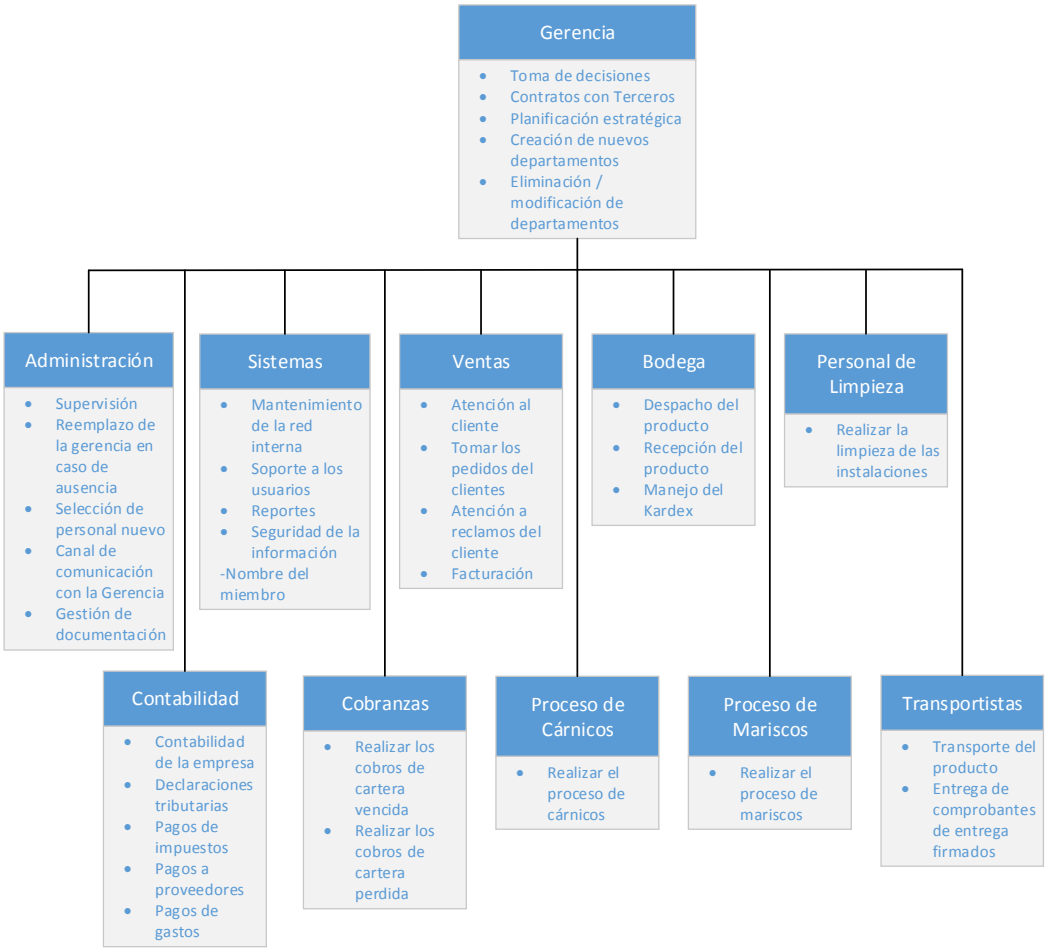

Figura 1.2: Organigrama Funcional del al empresa

A pesar de no tener documentación, a lo largo de este tiempo el sistema ha tenido una aceptable administración desde el punto de vista de que cada miembro del personal tiene claro cómo se debe manejar la seguridad de la información, pero está claro que esto a su vez significa un riesgo. La seguridad de la información está a cargo del Responsable de la Seguridad de la Información, empleado que labora dentro del departamento de Sistemas y que tiene sus obligaciones especificadas en su contrato de trabajo.

Sobre la empresa rigen leyes impuestas por el gobierno ecuatoriano que abarcan varios campos, sin embargo el sistema de información se ve afectado únicamente

por las exigencias del Servicio de Rentas Internas (SRI), por el Instituto Ecuatoriano de Seguridad Social (IESS) y por el Ministerio de Relaciones Laborales (MRL). En cuanto al SRI establece varios requerimientos para los procesos de:

- Facturación
- Compras
- Inventarios
- Declaraciones de Impuestos

El IESS por su lado exige el aseguramiento de cada empleado y el pago a tiempo de los aportes mensuales. Por último el MRL obliga a mantener la información sobre los contratos de los empleados, roles de pago y entrega de beneficios de ley.

El sistema de información debe tomar en cuenta todas estas exigencias para no presentar anomalías legales. Los demás organismos estatales que afectan a la empresa son entidades en las que solamente hay que tramitar permisos de funcionamiento y no tienen mayor influencia en el sistema de información.

A partir de estas premisas se procederá a describir el SGSI que se propone para implementar y garantizar la seguridad del sistema de información.

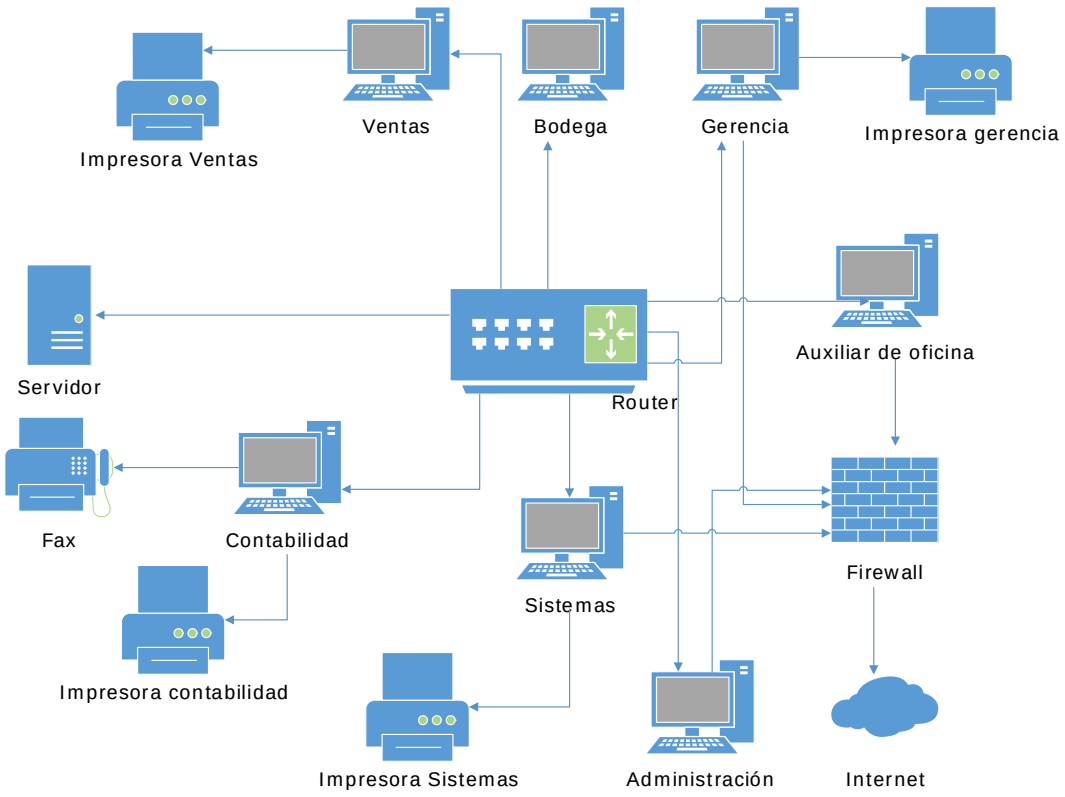

Figura 1.3: Diagrama de red de la empresa

2. Alcance del Proyecto

Los sistemas de información que dan soporte a todos los procesos de negocio de Mariscos S. A., según la declaración de aplicabilidad vigente.

El alcance incluye un profundo análisis y diagnóstico del sistema de información existente y su nivel de seguridad, se debe verificar:

a. Los requisitos y controles existentes implementados correctamente.
b. Los requisitos y controles existentes implementados incorrectamente.
c. Los requisitos y controles inexistentes.

Una vez obtenidos estos resultados se corregirán los requisitos y controles mal implementados y se implementarán de una manera correcta los que no existan.

Las áreas de la empresa que el proyecto alcanzará son aquellas en la que se maneja información relevante para la empresa, estos departamentos a su vez son los identificados cómo “partes interesadas” cuyas expectativas tienen relación con la consecución de los objetivos del negocio, estos departamentos son las siguientes:

a. Gerencia
b. Administración
c. Ventas
d. Bodega
e. Cobranzas
f. Contabilidad
g. Sistemas

Los departamentos: Transportistas, Proceso de Mariscos, Proceso de Cárnicos y Personal de Limpieza manejan información que no amerita protección, ya que en unos casos es pública (Transportistas) y en otros casos es irrelevante.

El alcance del proyecto también incluirá y tomará en cuenta todos los aspectos que estén relacionados con la naturaleza y cultura del negocio, así como todos los aspectos legales vigentes en la República del Ecuador.

3. Objetivos de Seguridad

El presente proyecto persigue los siguientes objetivos:

a. Mejorar la seguridad de la aplicación adquirida por Mariscos S. A.
b. Proteger de forma efectiva la información de los clientes depositada en la Organización.
c. Disminuir a niveles aceptables las probabilidades de robos o fugas de información ocasionados por el personal proveniente de la empresa proveedora del sistema de información.
d. Garantizar que los datos referentes a los productos como precio, stock, kardex, etc., mantengan su integridad.
e. Garantizar que el personal de ventas pueda realizar su actividad de atención al cliente de manera ininterrumpida.

4. Análisis Diferencial

A continuación desarrollaremos un análisis diferencial entre el estado actual del sistema de información de Mariscos S. A. en comparación con las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013. La intención de éste capítulo es ver cuáles de los requisitos de las normas de éstos estándares se cumple, cuáles no se cumple y cuales no se necesita cumplir.

4.1 Análisis diferencial respecto a la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013

El Análisis Diferencial está desarrollado sobre una plantilla que utiliza el modelo de madurez para la valoración de los controles definido por COBIT (Control Objectives for Information and related Technology), en la tabla 4.1 se detalla esta valoración.

Estado	Descripción
Se desconoce	No se ha revisado aún
No existe	Ausencia total de la implementación
Inicial	El desarrollo apenas ha comenzado y requerirá un importante trabajo para cumplir con los requisitos
Limitado	El desarrollo del requisito ha progresado pero aún no está completa su implementación
Definido	El desarrollo es casi completo pero a detalle aún falta y aún no está totalmente implementado
Gestionado	El desarrollo está completo y su funcionamiento ha empezado recientemente
Optimizado	El requisito se ha cumplido totalmente. Su funcionamiento es bueno, se está monitorizando y mejorando constantemente
No aplicable	En el caso de la ISO/IEC 27001 todos los ítems son obligatoriamente aplicables. En el caso de la ISO/IEC 27002 no todos son obligatoriamente aplicables.

Tabla 4.1: Valoración de los controles para el Análisis Diferencial

El resultado del análisis diferencial se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Análisis Diferencial.xlsx

Una justificación del análisis diferencial se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Justificación Análisis Diferencial.docx

La figura 4.1 muestran los resultados del análisis diferencial de manera gráfica, en los mismos se pueden observar el porcentaje del cumplimiento de las exigencias de la norma ISO/IEC 27001:2013 según la tabla 4.1. De este gráfico se puede deducir que un poco más de la mitad de las exigencias están ya funcionando, sin embargo tiene un importante porcentaje de exigencias por trabajar. En cuanto a la figura 4.2, muestra el porcentaje de controles implementados, el porcentaje de controles por implementar y el porcentaje de controles no aplicables, de la misma manera se

deduce que hay una importante cantidad de controles por implementar para el adecuado funcionamiento del SGSI.

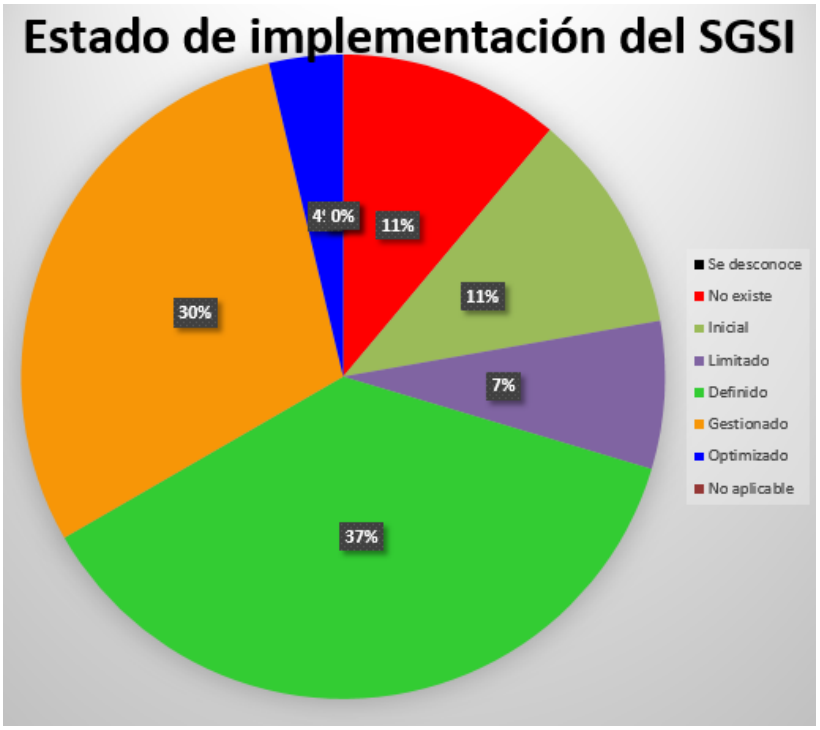

Figura 4.1: Cumplimiento de las exigencias de la norma ISO/IEC 27001:2013

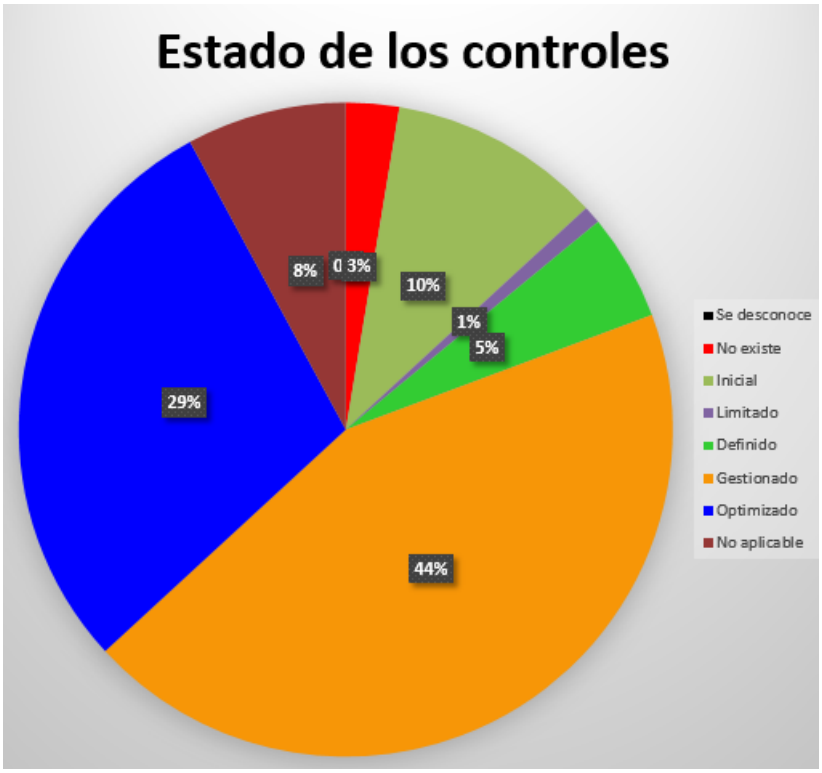

Figura 4.2: Cumplimiento de los controles de la norma ISO/IEC 27002

5. Esquema Documental

Este apartado reúne todo el cuerpo documental que requiere la norma ISO/IEC 27001, los mismos que son evidencia del funcionamiento del SGSI de Mariscos S. A., los documentos aquí descritos sirven de base para llevar a cabo las diferentes actividades de la implementación.

5.1 Política de Seguridad

La información es considerada por Mariscos S. A. como su activo intangible más valioso, por lo tanto considera que implementar procesos para garantizar su seguridad es una tarea imprescindible. Es por esta razón que se ha desarrollado el documento sobre políticas para la seguridad de la información, en el que constan todas las disposiciones aprobadas por la gerencia de la empresa y a la que todo el personal que labore bajo su mando deberá regirse, sin excepción de persona, cuando requiera acceder, consultar, ingresar, eliminar, modificar o realizar cualquier acción sobre todas clase de información sin importar su estado.

EL documento de políticas para la seguridad de la información deberá ser revisado una vez al año, o cada vez que sea necesario por el Comité de Seguridad.

El documento de políticas para la seguridad de la información será distribuido a todo el personal pertinente por medio de su correo electrónico como medida ecológica con el fin de evitar impresiones innecesarias, además habrá una sola copia impresa disponible 24 horas del día en la oficina del Departamento de Sistemas de la empresa para cualquier miembro del personal que necesite acceder al documento.

El Documento de Políticas para la Seguridad de la información se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA.pdf

5.2 Procedimiento de Auditorías Internas

La implementación de un SGSI comprende una fase de comprobación en la que se debe revisar y verificar que todas sus políticas para la seguridad de la información y controles establecidos se estén ejecutando de una manera adecuada y sus resultados sean los esperados. El objetivo de esta tarea es identificar los errores del SGSI con respecto a la norma ISO/IEC 27001 y determinar las medidas necesarias para posteriormente la empresa pueda corregir dichas falencias, retomando la línea del negocio y del propósito del SGSI. A esta fase se le conoce como Auditoría Interna, en ella se realiza una revisión de todo del SGSI, ya sea completo o de determinada área. No tiene un propósito de certificación de ningún tipo, más bien podría ser una preparación previa a pasar una Auditoría de Certificación ISO/IEC 27001. La auditoría interna debe ser ejecutada por un equipo auditor que no pertenezca al equipo que haya implementado el SGSI para garantizar su objetividad. La auditoría interna del SGSI se llevará a cabo anualmente, para cada nueva auditoría se deberá tener en cuenta los resultados de las auditorías realizadas anteriormente con el objeto de tener una mejora continua.

El Documento que describe el Procedimiento de Auditorías Internas se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Procedimientos de Auditorías Internas.pdf

5.3 Gestión de Indicadores

La implementación de un SGSI comprende la tarea de definir los indicadores que permitirán determinar el nivel de eficacia de los controles de seguridad que se han implementado y la metodología que se utilizará para medirlos. Estos indicadores proporcionan valiosa información para la toma de decisiones, la calidad de estas decisiones estará directamente relacionada con la calidad de la información que se ha utilizado para tomarlas.

El Documento que describe el Procedimiento de Gestión de Indicadores se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Gestión de Indicadores.pdf

5.4 Revisión por Dirección

La Dirección de la organización es la más interesada en el correcto funcionamiento de su SGSI, pero no necesariamente está conformada por personal experto en seguridad de información. Es por ello que se requiere un marco referencial en el que se puedan apoyar para determinar con un grado aceptable de exactitud la conveniencia de su sistema con el propósito del negocio. Este documento pretende brindar el apoyo necesario a la Dirección para que puedan cumplir con esta tarea.

El Documento que describe el Procedimiento de Revisión por Dirección se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Revisión por dirección.pdf

5.5 Gestión de Roles y Responsabilidades

Este documento definirá las diferentes personas o equipos de personas que estarán encargadas de implementar, mantener, supervisar y mejorar continuamente el SGSI, así como las responsabilidades que serán asumidas por cada uno de ellos.

La Gestión de Roles y Responsabilidades se encuentra descrito en el apartado 1 del archivo:

ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA.pdf

5.6 Metodología de Análisis de Riesgos

La implementación de un SGSI comprende la tarea de definir la metodología con la que se llevará a cabo el análisis de los riesgos para la seguridad de la información que la empresa identifique antes, durante y después de la implementación del SGSI y que debe incluirse en el plan de mejora cíclica. Se considera que la gestión de riesgos es la piedra angular en las guías del buen gobierno. Esta metodología permitirá a la empresa determinar el nivel de protección que tiene ante cierto riesgo, apoyando a la toma de decisiones a la administración de seguridad de la información ya que permite establecer prioridades.

El Documento que describe el Procedimiento de la Metodología de Análisis de Riesgos se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Metodología de Análisis de Riesgos.pdf

5.7 Declaración de Aplicabilidad

En este documento se define todos los controles de la norma ISO/IEC 27002 que se implementarán en el SGSI, y por supuesto, también se definen los controles que no se implementarán, cada uno deberá tener una justificación muy corta y concreta.

El Documento que describe el Procedimiento de la Declaración de Aplicabilidad se encuentra en el archivo adjunto:

ArcosArgudoMiguel-TFM-SGSI-Declaración de Aplicabilidad.xlsx

6. Análisis de Riesgos

El propósito del análisis de riesgos es determinar, para intereses de la empresa, el nivel de riesgo que se enfrenta, con las salvaguardas implementadas. El análisis de riesgos está descrito en el archivo *ArcosArgudoMiguel-TFM-SGSI-Metodología de Análisis de Riesgos.pdf*, de acuerdo a este documento se desarrollará este análisis.

6.1 Inventario de Activos

La tabla 6.2 muestra el listado de los activos que afectan a SGSI. Cabe recalcar que los activos se han agrupado según su naturaleza y su valoración.

Los grupos que se han utilizado se definen en la tabla 6.1:

Nombre del Grupo	Abreviatura
Datos o Información	[D]
Servicios	[S]
Aplicación	[SW]
Hardware	[HW]
Información Digital o impresa	[Media]
Redes	[COM]
Instalaciones	[L]
Personal	[P]

Tabla 6.1: Definición de Grupos de los activos

El inventario de activos se muestra a continuación:

Id	Nombre	Descripción	Grupo	Responsable
AC-D-001	Contabilidad	Contabilidad de la empresa: Estados financieros, Balances generales, utilidades, pérdidas, impuestos, etc.	[D]	Gerencia
AC-D-002	Base de Datos	Base de datos que almacena toda la información digitalizada de la empresa.	[D]	Jefe de Sistemas
AC-D-003	Cobranzas	Control de pagos de clientes.	[D]	Jefe de Recaudación
AC-D-004	Ventas	Ventas de mercadería (Facturación).	[D]	Jefe de Ventas
AC-D-005	Compras	Compras de mercadería	[D]	Jefe de Compras
AC-COM-006	Internet	Conexión a internet Wii 2400Kbps de bajada	[COM]	Jefe de Sistemas
AC-D-007	Bodega	Inventario y despacho de productos	[D]	Jefe de Bodega
AC-S-008	Correo electrónico	Servicio de correo electrónico para los usuarios.	[S]	Jefe de Sistemas
AC-Media-09	Documentación del negocio	Documentos físicos: Facturas de compra, facturas de venta, retenciones	[Media]	Administrador

		en la fuente, notas de crédito, etc.		
AC-HW-010	Servidor	Servidor de Base de Datos MySQL 5.6 con discos en RAID 1	[HW]	Jefe de Sistemas
AC-HW-011	Computadores de usuarios	12 Computadores de usuarios con Windows XP SP3	[HW]	Jefe de Sistemas
AC-SW-012	Sistema Operativo del servidor	Windows 2008 Server	[SW]	Jefe de Sistemas
AC-SW-013	Sistema operativo los terminales	Windows XP Service Pack 3	[SW]	Jefe de Sistemas
AC-HW-014	Impresoras	4 Impresoras Epson LX-300	[HW]	Jefe de Sistemas
AC-015	Router	1 Router de 20 puertos 100/1000	[HW]	Jefe de Sistemas
AC-HW-016	Fax	1 Fax para envío y recepción de documentos	[HW]	Jefe de Sistemas
AC-Media-017	Respaldos	Banco de respaldo de documentos de la empresa	[Media]	Jefe de Sistemas
AC-SW-018	Firewall	ZoneAlarmFree Firewall	[SW]	Jefe de Sistemas
AC-Media-019	Documentación técnica	Documentos referentes al SGSI: manuales, etc.	[Media]	Jefe de Sistemas
AC-SW-020	Antivirus	Aplicación antivirus instalada en la empresa – ESET Nod32	[SW]	Jefe de Sistemas
AC-L-021	Edificio	Edificio en el que funciona la empresa	[L]	Gerencia
AC-P-022	Personal directivo	Personal estratégico para la empresa	[P]	Gerencia
AC-P-023	Personal técnico	Personal para soporte técnico del sistema de información	[P]	Gerencia
AC-P-024	Resto del personal	Resto de personal que labora en la empresa	[P]	Gerencia

Tabla 6.2: Inventario de los activos

6.2 Valoración de los activos

La valoración de los activos se ha basado en el coste invertido en cada uno de ellos, en el coste que representaría su reposición en caso de que haya sido comprometido y las relaciones de dependencia que tienen con otros activos, este último se ha utilizado sobre todo para la valoración cuantitativa de activos intangibles que es algo más compleja.

6.2.1 Análisis de dependencias de activos

El análisis de las dependencias de activos se establece mediante la generación de árboles, en los cuales el nodo superior se ubica el tipo activo más crítico, y luego en

los siguientes niveles se ubican los tipos activos de los que depende, logrando obtener una jerarquía de activos, para el caso de la empresa en estudio los activos esenciales son: [D] Datos o Información.

Los activos referentes a Personal [P] son transversales, es decir, influyen en todo el árbol por lo que no se les ubica en ningún nivel.

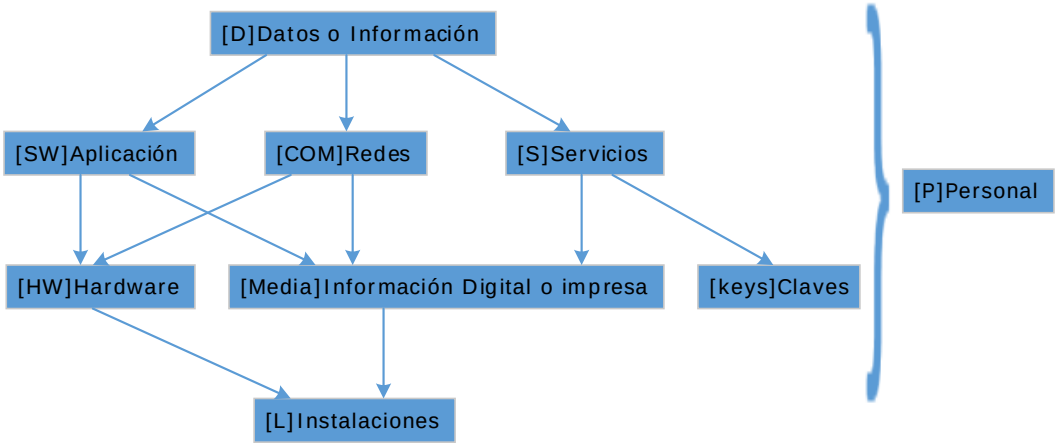

Figura 6.1: Árbol de dependencias de activos

6.2.2 Tabla de Valoración de activos

Del árbol que se muestra en la figura 6.1 se deduce que el activo más importante para la empresa es la Contabilidad de la organización, ya que al ser una empresa con fines de lucro, lo que más le interesa a la dirección son los resultados de las transacciones que se realizan, es decir, la rentabilidad del negocio. De esta misma tabla se define la valoración de los activos, cabe recalcar que se toma como moneda el Dólar Americano, que circula actualmente en la República del Ecuador.

La tabla 6.3 muestra la valoración de los activos, pero para poder definirla se tiene que basar en la tabla 5.2 del archivo *ArcosArgudoMiguel-TFM-SGSI-Metodología de Análisis de Riesgos.docx* que se muestra a continuación, esta tabla define los rangos para los valores de los activos:

Rangos para el Valor de los activos		
Descripción	**Rango**	**Abreviatura**
Despreciable	Menor que $500 USD	D
Muy Bajo	Mayor o igual a $500 USD y menor o igual que $1000 USD	MB
Bajo	Mayor que $1000 USD y menor que $10000 USD	B
Medio	Mayor o igual a $10000 USD y menor que $25000 USD	M
Alto	Mayor o igual a $25000 USD y menor que 50000$1USD	A
Muy Alto	Mayor que $50000 USD	MA

Tabla 5.2: Rangos para la definición del valor de los activos

La tabla de valoración de los activos resultante es la siguiente:

Id	Grupo	Nombre	Valoración cualitativa	Valoración cuantitativa
AC-D-001	[D]	Contabilidad	MA	$100.000 USD
AC-D-002	[D]	Base de Datos	A	$50.000 USD
AC-D-003	[D]	Cobranzas	A	$50.000 USD
AC-D-004	[D]	Ventas	A	$50.000 USD
AC-D-005	[D]	Compras	A	$50.000 USD
AC-COM-006	[COM]	Internet	MB	$1.000 USD
AC-D-007	[D]	Bodega	A	$50.000 USD
AC-S-008	[S]	Correo electrónico	MB	$1.000 USD
AC-Media-09	[Media]	Documentación del negocio	M	$25.000 USD
AC-HW-010	[HW]	Servidor	M	$25.000 USD
AC-HW-011	[HW]	Computadores de usuarios	B	$10.000 USD
AC-SW-012	[SW]	Sistema Operativo del servidor	MB	$1.000 USD
AC-SW-013	[SW]	Sistema operativo los terminales	MB	$1.000 USD
AC-HW-014	[HW]	Impresoras	MB	$1.000 USD
AC-015	[HW]	Router	MB	$1.000 USD
AC-HW-016	[HW]	Fax	MB	$1.000 USD
AC-Media-017	[Media]	Respaldos	MB	$1.000 USD
AC-SW-018	[SW]	Firewall	MB	$1.000 USD
AC-Media-019	[Media]	Documentación técnica	MB	$1.000 USD
AC-SW-020	[SW]	Antivirus	MB	$1.000 USD
AC-L-021	[L]	Edificio	A	$50.000 USD
AC-P-022	[P]	Personal directivo	A	$50.000 USD
AC-P-023	[P]	Personal técnico	M	$25.000 USD
AC-P-024	[P]	Resto del personal	M	$25.000 USD
AC-keys-025	[keys]	Claves de cada usuario del sistema de información	A	$50.000 USD

Tabla 6.3: Valorización de los Activos

6.3 Dimensiones de seguridad

Esta sección muestra el impacto que diferentes amenazas podrían causar en las cinco dimensiones de seguridad de cada activo, dichas dimensiones son Autenticidad [A], Confidencialidad [C], Integridad [I], Disponibilidad [D] y Trazabilidad [T]. La tabla 6.4 muestra los rangos de valoración de los impactos sobre cada activo, se establece una escala de 0 a 10.

Valor	Descripción del daño
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Tabla 6.4: Valorización de Dimensiones de Seguridad

6.3.1 Valoración de los impactos por activo

Entiéndase por impacto al daño que ha sufrido un activo luego de la materialización de una amenaza, se valora un impacto en la escala de 0 a 10, siendo 0 un impacto despreciables y 10 un daño total del activo. La tabla 6.5 muestra el valor del impacto que cada activo soportaría en cada una de sus dimensiones de seguridad:

Grupo	Id	Nombre del activo	Valoración cualitativa	[A]	[C]	[I]	[D]	[T]
[D]	AC-D-001	Contabilidad	MA	10	8	9	8	7
[D]	AC-D-002	Base de Datos	A	8	7	8	8	7
[D]	AC-D-003	Cobranzas	A	7	6	8	7	6
[D]	AC-D-004	Ventas	A	7	6	8	7	6
[D]	AC-D-005	Compras	A	7	6	7	7	6
[COM]	AC-COM-006	Internet	MB	5	5	5	8	6
[D]	AC-D-007	Bodega	A	7	6	8	7	6
[S]	AC-S-008	Correo electrónico	MB	8	6	6	6	6
[Media]	AC-Media-09	Documentación del negocio	M	9	6	8	7	5
[HW]	AC-HW-010	Servidor	M	5	7	7	9	7
[HW]	AC-HW-011	Computadores de usuarios	B	7	6	6	8	4
[SW]	AC-SW-012	Sistema Operativo del servidor	MB	5	7	7	9	7
[SW]	AC-SW-013	Sistema operativo los terminales	MB	7	6	6	8	4
[HW]	AC-HW-014	Impresoras	MB	0	0	0	4	4
[HW]	AC-015	Router	MB	0	0	0	5	7
[HW]	AC-HW-016	Fax	MB	0	0	0	2	2
[Media]	AC-Media-017	Respaldos	MB	7	8	7	4	2
[SW]	AC-SW-018	Firewall	MB	5	5	5	7	4
[Media]	AC-Media-019	Documentación técnica	MB	5	5	5	3	1
[SW]	AC-SW-020	Antivirus	MB	5	5	5	7	5
[L]	AC-L-021	Edificio	A	0	5	5	9	0
[P]	AC-P-022	Personal directivo	A	8	8	8	8	8
[P]	AC-P-023	Personal técnico	M	6	6	6	6	6
[P]	AC-P-024	Resto del personal	M	3	3	3	3	3

[keys]	AC-keys-025	Claves de cada usuario del sistema de información	A	8	8	8	8	8

Tabla 6.5: Tabla de valoración de los impactos por activo

6.4 Análisis de amenazas

El análisis de amenazas se ha desarrollado tomando el listado de amenazas de la metodología MAGERIT en libro 2 Apartado 5. Para cada una de estas amenazas se ha determinado los tipos de activos a los que puede afectar según la misma metodología, y se ha valorado el nivel de impacto que podría causar en cada una de las dimensiones de seguridad de los activos. Este análisis se muestra en la tabla 6.6.

Tabla de Análisis de Amenazas								
				Dimensiones de seguridad				
Código	**Amenaza**	**Frecuencia Anual**	**Tipo de Activo**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
[N]	**Desastres Naturales**							
[N.1]	Fuego	1	[HW]				60%	
			[Media]				60%	
			[L]				30%	
[N.2]	Daños por agua	1	[HW]				60%	
			[Media]				60%	
			[L]				30%	
[N.*]	Otros desastres naturales	1	[HW]				30%	
			[Media]				40%	
			[L]				20%	
[I]	**De origen industrial**							
[I.1]	Fuego	1	[HW]				60%	
			[Media]				60%	
			[L]				30%	
[I.2]	Daños por agua	1	[HW]				60%	
			[Media]				60%	
			[L]				30%	
[I.3]	Contaminación mecánica	1	[HW]				40%	
			[Media]				40%	
[I.4]	Contaminación electromagnética	1	[HW]				20%	
			[Media]				20%	
[I.5]	Avería de origen físico o lógico	1	[SW]				50%	
			[HW]				50%	
			[Media]				50%	
[I.6]	Corte de suministro eléctrico	2	[HW]				70%	
			[Media]				50%	
[I.7]	Condiciones inadecuadas de	1	[HW]				20%	
			[Media]				20%	

	temperatura y humedad							
[I.8]	Fallo de servicios de comunicaciones	2	[COM]				50%	
[I.9]	Interrupción de otros servicios y suministros esenciales	0						
[I.10]	Degradación de los soportes de almacenamiento de la información	1	[Media]				10%	
[I.11]	Emanaciones electromagnéticas	1	[HW]				30%	
			[Media]				70%	
			[L]				40%	
[I.*]	Otros desastres industriales	1	[HW]				10%	
			[Media]				10%	
			[L]				10%	
[E]	**Errores y fallos no intencionados**							
[E.1]	Errores de los usuarios	10	[D]		80%	90%	70%	
			[keys]		80%	90%	70%	
			[S]		10%	10%	10%	
			[SW]		60%	70%	50%	
			[Media]		70%	80%	60%	
[E.2]	Errores del administrador	3	[D]		60%	70%	80%	
			[keys]		50%	60%	70%	
			[S]		10%	10%	10%	
			[SW]		40%	50%	60%	
			[HW]		40%	50%	60%	
			[COM]		30%	40%	50%	
			[Media]		20%	30%	40%	
[E.3]	Errores de monitorización (log)	4	[D.log]			70%		
[E.4]	Errores de configuración (conf)	4	[D.conf]			60%		
[E.7]	Deficiencias y fallos en la organización	2	[P]				40%	
[E.8]	Difusión de software dañino	15	[SW]		50%	70%	90%	
[E.9]	Errores de [re-]encaminamiento	5	[S]		10%			
			[SW]		60%			
			[COM]		50%			
[E.10]		2	[S]			10%		

	Errores de secuencia		[SW]			30%		
			[COM]			20%		
[E.14]	Escapes de información	3	[D]		70%			
[E.15]	Alteración accidental de información	5	[D]			80%		
			[keys]			80%		
			[S]			10%		
			[SW]			50%		
			[COM]			40%		
			[Media]			40%		
			[L]			10%		
[E.18]	Destrucción de información	3	[D]				50%	
			[keys]				70%	
			[S]				10%	
			[SW]				60%	
			[COM]				50%	
			[Media]				50%	
			[L]				10%	
[E.19]	Fugas de información	5	[D]		80%			
			[keys]		80%			
			[S]		10%			
			[SW]		60%			
			[COM]		60%			
			[Media]		60%			
			[L]		30%			
			[P]		30%			
[E.20]	Vulnerabilidades de los programas (software)	5	[SW]		40%	80%	60%	
[E.21]	Errores de mantenimiento / Actualización de programas (software)	3	[SW]		50%	70%		
[E.23]	Errores de mantenimiento / Actualización de equipos (hardware)	5	[HW]				60%	
			[Media]				40%	
[E.24]	Caída del sistema por agotamiento de recursos	1	[S]				10%	
			[HW]				60%	
			[COM]				60%	
[E.25]	Pérdida de equipos	1	[HW]		80%		50%	
			[Media]		80%		60%	

[E.28]	Indisponibilidad del Personal	10	[P]				80%	
[A]	**Ataques intencionados**							
[A.3]	Manipulación de los registros de actividad (log)	3	[D.log]			70%		
[A.4]	Manipulación de la configuración	3	[D.log]	50%	70%	70%		
[A.5]	Suplantación de la identidad de un usuario	10	[D]	80%	90%	80%		
			[keys]	80%	90%	80%		
			[S]	10%	10%	10%		
			[SW]	60%	70%	60%		
			[COM]	60%	60%	60%		
[A.6]	Abuso de privilegios de acceso	10	[D]	80%	90%	80%		
			[keys]	80%	90%	80%		
			[S]	10%	10%	10%		
			[SW]	60%	70%	60%		
			[HW]	60%	60%	60%		
			[COM]	60%	60%	60%		
[A.7]	Uso no previsto	10	[S]		10%	10%	10%	
			[SW]		50%	40%	60%	
			[HW]		40%	30%	50%	
			[COM]		30%	20%	40%	
			[Media]		30%	20%	40%	
			[L]		20%	20%	30%	
[A.8]	Difusión de software dañino	10	[SW]		50%	70%	90%	
[A.9]	[Re-]encaminamiento de mensajes	10	[S]		10%			
			[SW]		70%			
			[COM]		60%			
[A.10]	Alteración de secuencia	8	[S]			10%		
			[SW]			60%		
			[COM]			50%		
[A.11]	Acceso no autorizado	10	[D]		50%	90%		
			[keys]		60%	80%		
			[S]		10%	10%		
			[SW]		50%	70%		
			[HW]		50%	70%		
			[COM]		50%	70%		
			[Media]		50%	70%		
			[L]		30%	50%		
[A.12]	Análisis de tráfico	10	[COM]		80%			
[A.13]	Repudio	10	[S]					10%
			[D.log]					60%

[A.14]	Intercepción de información (escucha)	10	[COM]		90%			
[A.15]	Modificación deliberada de la información	10	[D]			50%		
			[keys]			90%		
			[S]			10%		
			[SW]			70%		
			[COM]			70%		
			[Media]			70%		
			[L]			20%		
[A.18]	Destrucción de información	10	[D]				50%	
			[keys]				70%	
			[S]				10%	
			[SW]				60%	
			[Media]				50%	
			[L]				10%	
[A.19]	Divulgación de información	10	[D]		50%			
			[keys]		90%			
			[S]		10%			
			[SW]		70%			
			[COM]		70%			
			[Media]		70%			
			[L]		50%			
[A.22]	Manipulación de programas	10	[SW]		80%	70%	60%	
[A.23]	Manipulación de equipos	10	[HW]		80%		70%	
			[Media]		80%		70%	
[A.24]	Denegación de servicio	10	[S]				10%	
			[HW]				70%	
			[COM]				70%	
[A.25]	Robo	10	[HW]		50%		50%	
			[Media]		50%		50%	
[A.26]	Ataque destructivo	10	[HW]				50%	
			[Media]				50%	
			[L]				70%	
[A.27]	Ocupación enemiga	10	[L]		80%		80%	
[A.28]	Indisponibilidad del Personal	1	[P]				50%	
[A.29]	Extorsión	1	[P]		50%	70%	60%	
[A.30]	Ingeniería social (picaresca)	10	[P]		80%	80%	80%	

Tabla 6.6 Análisis de amenazas

Un respaldo del análisis de amenazas se encuentra en el archivo adjunto *ArcosArgudoMiguel-TFM-SGSI-Análisis de amenazas-Impacto de amenazas por activo.xlsx*.

6.5 Impacto potencial de las amenazas por cada activo de información

Recordamos que se entiende por impacto al nivel de daño que ha sufrido un activo después de la materialización de una amenaza. Para el caso de la empresa se analizará el impacto potencial por cada activo de información, en base a que su cantidad de activos no es muy amplia sería de mayor aporte al momento de elegir las salvaguardas. Para ello se tomará en cuenta los siguientes parámetros.

a. Cada activo se analizará con cada amenaza del listado sugerido por MAGERIT en su libro 2 apartado 5.
b. Se valorará el impacto tomando en cuenta las salvaguardas actualmente existentes en la empresa.
c. Se valorará a cada activo en sus 5 dimensiones (Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad) en la escala de 0 a 10, según la tabla 6.7.

Valor	Nivel de daño al activo
0 – 1	Daño irrelevante al activo de información.
2 – 3	Daño menor al activo de información.
4 – 5	Daño importante al activo de información.
6 – 7	Daño grave al activo de información.
8 – 9	Daño muy grave al activo de información.
10	Daño irreparable al activo de información.

Tabla 6.7: Rangos para definir los daños a los activos de información

d. El cálculo del impacto se calcula trasladando directamente el mayor valor del impacto en cualquiera de las dimensiones de seguridad del activo y multiplicándolo por 10. Por ejemplo: si un activo tiene los valores [A]=2, [C]=5, [I]=3, [D]=6, [T]=0, el valor del impacto será 60%.
e. El cálculo del impacto está en la pestaña ***Cálculo de riesgos por activo*** del archivo adjunto ***ArcosArgudoMiguel-TFM-SGSI-Análisis de amenazas-Impacto de amenazas por activo.xlsx***.

6.6 Cálculo del riesgo por activo

Ahora se calcula el riesgo por activo, el mismo que se ha realizado en base al valor del activo, a la máxima frecuencia de la ocurrencia de una amenaza, al máximo impacto para cada activo y a la probabilidad promedio de que una amenaza se materialice a diario. La tabla 6.8 muestra este cálculo.

Código	Nombre de activo	Valor activo	Valor del riesgo $ USD
AC-D-001	Contabilidad	$ 100.000	2465.75
AC-D-002	Base de Datos	$ 50.000	1232.88
AC-D-004	Ventas	$ 50.000	1232.88
AC-D-005	Compras	$ 50.000	1232.88
AC-D-007	Bodega	$ 50.000	1232.88
AC-keys-025	Claves de cada usuario	$ 50.000	1232.88
AC-L-021	Edificio	$ 50.000	1095.89
AC-P-022	Personal directivo	$ 50.000	958.90

AC-D-003	Cobranzas	$ 50.000	821.92
AC-Media-09	Documentación del negocio	$ 25.000	547.95
AC-HW-010	Servidor	$ 25.000	547.95
AC-P-024	Resto del personal	$ 25.000	479.45
AC-P-023	Personal técnico	$ 25.000	410.96
AC-HW-011	Computadores de usuarios	$ 10.000	136.99
AC-COM-006	Internet	$ 1.000	24.66
AC-SW-012	Sistema Operativo del servidor	$ 1.000	24.66
AC-SW-013	Sistema operativo los terminales	$ 1.000	16.44
AC-HW-014	Impresoras	$ 1.000	13.70
AC-015	Router	$ 1.000	8.22
AC-Media-017	Respaldos	$ 1.000	8.22
AC-Media-019	Documentación técnica	$ 1.000	8.22
AC-HW-016	Fax	$ 1.000	5.48
AC-SW-018	Firewall	$ 1.000	5.48
AC-S-008	Correo electrónico	$ 1.000	2.74
AC-SW-020	Antivirus	$ 1.000	2.74

Tabla 6.8: Cálculo del riesgo por activo

Según este cálculo se ha determinado la siguiente tabla para determinar el riesgo aceptable.

Nivel	Valor
Alto	Mayor a $2.000 USD
Medio	Entre $900 USD y $2.000 USD
Bajo	Entre $500 USD y $900 USD
Mínimo	Entre $200 USD y $500
Despreciable	Menor a $200

Tabla 6.9: Tabla de referencia para catalogar los niveles de riesgo de cada activo

El gráfico 6.2 muestra los valores de los riesgos de los activos, en él se puede ver su variación respecto al nivel de riesgo Bajo.

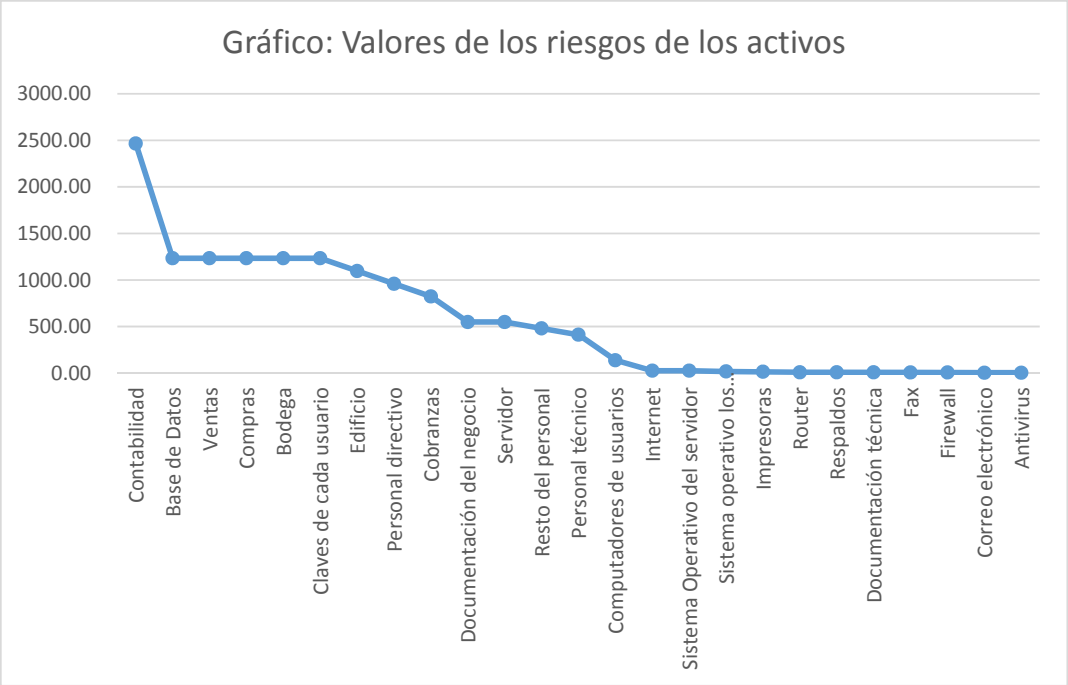

Gráfico 6.2: Gráfico de los valores de los riesgos de los activos

6.7 Nivel de riesgo aceptable y riesgo residual

Dados estos cálculos se determina que todo riesgo superior a $2.000 USD será tratado con alta prioridad. Todo riesgo superior a $900 USD será tratado con prioridad media. Todo riesgo que se menor a $900 USD no será tratado y por lo tanto será aceptado por la dirección de la empresa. Es decir, todo riesgo que sea por lo menos de nivel Bajo será catalogado como riesgo aceptable.

6.7.1 Documento de aprobación del riesgo residual

El presente documento es una constancia de aceptación por parte de la Gerencia de la empresa Mariscos S. A. del umbral del riesgo asumible, debido al coste de la implantación de las salvaguardas versus el coste de asumir el riesgo.

Dicho nivel de riesgo asumible fijado será el *Nivel Bajo* (inferior a $900 USD diario), los activos que se encuentran en este rango representan alrededor del 60% del total de los activos de información de la empresa. En consecuencia, todo activo que sean catalogados en los niveles *Medio* y Alto, que representan el 40% del total de los activos de información del SGSI entrarán en el tratamiento de riesgos.

Los activos que estén bajo el umbral aceptado serán asumidos por el Departamento de Gerencia de Mariscos S. A.

La Gerencia de Mariscos S. A. aprueba el presente documento sobre el riesgo residual a los 6 días del mes noviembre de 2014.

_____
La Gerencia.

7. Propuestas de mejoras para la seguridad de la información

El análisis de riesgos ha indicado cuáles son los activos cuyos riesgos no serán asumidos por la empresa, se ha identificado también cuáles son las principales amenazas que atentan contra estos activos, se debe entonces proponer proyectos que permitan mitigar estos riesgos, teniendo en cuenta los resultados de la Declaración de Aplicabilidad, que es en donde se definió los controles aplicables y los no aplicables, dicha declaración se encuentra en el archivo ***ArcosArgudoMiguel-TFM-SGSI-Declaración de Aplicabilidad.xlsx***, además los controles propuestos están pensados en tratar las amenazas identificadas.

Este apartado propondrá proyectos para implementar los controles necesarios de la norma ISO/IEC 27002 para mejorar la seguridad de los activos críticos de la información.

7.1 Gestión de los controles a implementar

Se definirán los procedimientos con los cuales se gestionarán los controles de la norma ISO/IEC 27002 a implementar.

7.1.1 Análisis del estado inicial

Primeramente se deberá recopilar toda la documentación existente en materia de seguridad dentro de la empresa, así como también documentar los procedimientos y controles de seguridad implementados pero no documentados. En esta etapa se planificará consolidar todas las salvaguardas de seguridad existentes y funcionales con la finalidad de obtener un solo documento que ayude a administrar los controles de seguridad.

7.1.2 Gestión de recursos para la implementación de controles

Según el tipo de control a implementar se decidirá si la mejor opción para la empresa es que sea implementado por el personal existente, sea implementado por personal contratado o empresa contratada puntualmente para ese control, ó, que se implementado por personal contratado de forma permanente. Esta decisión deberá contar con la aprobación expresa de la Gerencia de la empresa.

Los recursos económicos necesarios para implementar cada control se deberán solicitar a la Gerencia de la empresa por medio de un proyecto desarrollado por el Comité de Seguridad, en el cuál se debe indicar claramente el objetivo del control, los beneficios de implementarlo y las desventajas de no implementarlo.

Los demás recursos como los de espacio físico, tiempo, etc. serán coordinados por el jefe de seguridad de la información.

7.1.3 Desarrollo de los controles a implementar

Este es un paso crítico dentro de la empresa, ya que no existe la costumbre de documentar los controles que se implementarán dentro de ella, por lo que se procederá a que en el lapso de dos semanas, el mismo personal que está implementando el SGSI de formación durante una hora diaria a todo el personal que intervenga en materia de seguridad de la información divididos en grupos, sobre temas de normalización, redacción y documentación de controles que serán implementados en la empresa.

Una vez terminada esta capacitación, el formato de la documentación de controles deberá tener el siguiente formato:

1. Código del control
2. Riesgo que mitiga
3. Procedimientos para implementar el control
4. Porcentaje esperado de reducción del riesgo
5. Monto de inversión estimado
6. Indicadores para medir el control
7. Frecuencia de evaluación del control
8. Responsable del control
9. Fecha de inicio
10. Fecha de finalización

7.2 Sumario de las mejoras para la seguridad de la información identificadas

A continuación, en primera instancia, se realizará un sumario de las mejoras que se propondrán con el objetivo de identificar aquellos problemas que ya han sido resueltos durante la fase de la Gestión Documental. El presente sumario se ha desarrollado teniendo en cuenta la declaración de aplicabilidad, el mismo que contendrá un código para cada proyecto, el nombre, una breve descripción y los controles de la norma ISO/IEC 27002:2013 que se implementarán para gestionar la deficiencia.

MJ-001-A.5.1 Política de seguridad de la información

Redactar un documento que contenga las políticas para la seguridad de la información a la que tenga que regirse todo el personal de la empresa.

Nota: Este proyecto ya ha sido implementado en la fase de Gestión Documental en el documento **ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA.pdf**.

Controles implementados:

A.5.1.1 Documento de política de seguridad de la información

A.5.1.2 Revisión de política de seguridad de la información

MJ-002-A.7.2 Durante el empleo

Definir un plan de formación y concienciación al personal en materia de seguridad de la información, así como un proceso disciplinario también relacionado a la seguridad.

Controles a implementar:

A.7.2.2 Concienciación, educación y capacitación en seguridad de la información

A.7.2.3 Proceso Disciplinario

MJ-003-A.8.1 Responsabilidad de los activos

Definir un procedimiento que englobe el uso debido de cada activo, y un documento que indique el procedimiento para la devolución de activos.

Controles a implementar:

A.8.1.3 Uso aceptable de activos

A.8.1.4 Devolución de activos

MJ-004-A.8.2 Clasificación de la información

Definir un documento que de las directrices para que la información sea clasificada de manera adecuada, y otro documento que regule la manipulación de activos.

Controles a implementar:

A.8.2.1 Directrices de clasificación

A.8.2.3 Manipulación de activos

MJ-005-A.9.1 Requisitos del negocio para el control de accesos

Este control ya ha sido implementado en el documento **ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA.pdf** durante la fase de Gestión Documental, apartado 9.

Controles implementados:

A.9.1.1 Política de control de accesos

A.9.1.2 Control de acceso a las redes y servicios asociados

MJ-006-A.9.2 Gestión de acceso al usuario

Definir un método para gestionar los derechos de accesos a los usuarios que deban tener privilegios especiales a la información. Los usuarios deben ser autentificados mediante información confidencial. Sus derechos deben revisarse cada cierto período de tiempo.

Controles a implementar:

A.9.2.3 Gestión de los derechos de acceso con privilegios especiales.

A.9.2.4 Gestión de información confidencial de autenticación de usuarios.

A.9.2.5 Revisión de los derechos de acceso de los usuarios.

MJ-007-A.9.4 Control de acceso a sistemas y aplicaciones

Definir procedimientos para restringir el acceso a la información según la necesidad del usuario.

Controles a implementar:

A.9.4.1 Restricción del acceso a la información.

MJ-008-A.11.2 Seguridad en los equipos

Este control ya ha sido implementado en el documento **ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA.pdf** durante la fase de Gestión Documental, apartado 7.11.

Controles implementados:

A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia.

MJ-009-A.12.1 Responsabilidades y procedimientos de operación

Documentar los procedimientos operativos y ponerlos a disposición del usuario que lo necesite.

Controles a implementar:

A.12.1.1 Documentación de procedimientos de operación.

MJ-010-A.12.7 Consideraciones de las auditorías de los sistemas de información

Definir un procedimiento que establezca tomar los resultados de auditorías anteriores para apoyar a las nuevas auditorías como parte del PDCA.

Controles a implementar:

A.12.7.1 Consideraciones de las auditorías de los sistemas de información.

MJ-011-A.13.2 Transferencia de información

Este control ya ha sido implementado en el documento **ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA.pdf** durante la fase de Gestión Documental, apartado 8.7.

Controles implementados:

A.13.2.1 Políticas y procedimientos de intercambio de información.

MJ-012-A.14.2 Seguridad en los procesos de desarrollo y soporte

Definir los requerimientos a la empresa proveedora del sistema de información sobre las políticas de desarrollo seguro de software que deberán cumplir, especialmente la documentación de dichas políticas.

Controles a implementar:

A.14.2.1 Política de desarrollo seguro de software.

MJ-013-A.16.1 Gestión de incidentes de seguridad de la información y mejoras

Este control ya ha sido implementado en el documento **ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA.pdf** durante la fase de Gestión Documental, apartado 6.3.

Controles implementados:

A.16.1.5 Respuesta a los incidentes de seguridad.

MJ-014-A.17.1 Continuidad de la seguridad de la información

Definir procedimientos que garanticen la continuidad de la seguridad de la información aún en momentos críticos.

Controles a implementar:

A.17.1.2 Implantación de la continuidad de la seguridad de la información.

MJ-015-A.18.2 Revisiones de la seguridad de la información

Definir los requerimientos a la empresa proveedora del sistema de información sobre el cumplimiento de las políticas y normas de seguridad, así como la comprobación del cumplimiento.

Controles a implementar:

A.18.2.2 Cumplimiento de las políticas y normas de seguridad.

A.18.2.3 Comprobación del cumplimiento.

7.3 Desarrollo de las propuestas de mejoras para la seguridad de la información

Este apartado describirá los proyectos propuestos con los que se pretende implementar los controles de la norma ISO/IEC 27002:2013 que aplican a la empresa y que aún no han sido gestionados.

7.3.1 Controles para el apartado: MJ-002-A.7.2 Durante el empleo

Código del proyecto: MJ-002-A.7.2

Riesgo que mitiga: El personal de la organización no tiene una costumbre ni una cultura de seguridad de la información, debido a que nunca antes se ha implementado un SGSI en la empresa, razón por la cual desconocen casi por completo principios elementales de seguridad, padecen de falta de concienciación de la importancia de la seguridad y del valor de la información como tal. Esto conlleva el riesgo de que personal con acceso a información sensible no la proteja debidamente produciendo errores humanos.

Procedimientos para implementar el control:

- El personal recibirá un curso de capacitación inicial en materia de seguridad de la información, este curso será impartido por el mismo personal que implementa el SGSI.
- La duración del curso será de dos semanas, en el que se impartirán clases de dos horas diarias de duración, de lunes a viernes.
- El presupuesto destinado a este curso $2000.00 USD.
- El horario del curso será después de la jornada laboral, es decir de 6:00 pm a 8:00 pm, razón por la cual el presupuesto del curso incluye un pequeño refrigerio durante un mini break (15 minutos) a las 7:00 pm.
- El lugar en el que se impartirá el curso será la Oficina del Departamento de Administración, la misma que será adecuada provisionalmente durante el tiempo que dura la capacitación.
- En la primera sesión se entregará a cada asistente una copia del documento de Políticas para la Seguridad de la Información de la empresa.
- Las horas de asistencia al curso será remunerado a cada asistente como horas extra, sin embargo, la falta no justificada de cualquier miembro del personal contará como falta no justificada a un día ordinario de labores.
- El personal que implementa el SGSI será libre de decidir si subcontrata una persona externa, especializada en materia de seguridad de la información, para que imparta el curso.
- El curso debe incluir clases de Proceso disciplinario.

Porcentaje esperado de reducción del riesgo: Se espera que, en este caso, el nivel de control del riesgo se incremente progresivamente, en un inicio se espera que el riesgo disminuya en un **35%**, y a corto plazo (2 meses) se espera llegar a un **75%**.

Monto de inversión estimado: $2000.00 USD

Indicadores para medir el control:

- Test individual sobre las políticas de seguridad de la información (anual).
- Simulacro de un incidente de seguridad (anual).

Frecuencia de evaluación del control: Cada año.

Responsable del control: Responsable de la seguridad de la información.

Fecha de inicio: enero 02 de 2015

Fecha de finalización: marzo 02 de 2015

7.3.2 Controles para MJ-003-A.8.1 Responsabilidad de los activos

Código del control: MJ-003-A.8.1

Riesgo que mitiga: Los usuarios no han aprendido aún el significado del término "activo de información", esto puede derivar en el uso inapropiado de los activos, razón por la cual se debe desarrollar un manual que detalle cuál debe ser el uso de cada activo según su naturaleza.

Procedimientos para implementar el control:

- El manual será desarrollado por el Departamento de Sistemas.
- El manual será aprobado por el Comité de Seguridad.
- El manual debe ser repartido a todo el personal que maneje activos de información.
- El manual debe ser redactado en el lapso de un mes con un mes de prórroga.
- El presupuesto para este proyecto será $500.00 USD.
- Al momento de la entrega del manual se recogerá la firma del receptor como constancia de que ha recibido el manual.
- Adjunto al manual se enviará una circular que indique el compromiso del receptor de auto-capacitarse mediante la lectura del manual y la prevención de una evaluación futura sobre el contenido del manual.
- El manual debe incluir los procedimientos necesarios para la correcta Devolución de activos.

Porcentaje esperado de reducción del riesgo: Se espera que, en este caso, el nivel de control del riesgo se incremente progresivamente, en un inicio se espera que el riesgo disminuya en un **35%**, y a corto plazo (2 meses) se espera llegar a un **75%**.

Monto de inversión estimado: $500.00 USD

Indicadores para medir el control:

- Prueba práctica aleatoria a los miembros del personal en el lugar de su trabajo (cada mes). Las personas evaluadas serán escogidas al azar.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Propietario del activo de información.

Fecha de inicio: enero 02 de 2015

Fecha de finalización: febrero 26 de 2015

7.3.3 Controles para MJ-004-A.8.2 Clasificación de la información

Código del Control: MJ-004-A.8.2

Riesgo que mitiga: La organización no tiene procedimientos documentados que den las directrices para que la información de la empresa sea clasificada de una manera adecuada. Actualmente la información es clasificada de una manera en la que se puede considerar que es organizada, sin embargo la falta de documentación provoca que en momentos críticos no se encuentre la información que se requiere.

Procedimientos para implementar el control:

Sobre la clasificación de la información

- Se deberá clasificar toda la información de la empresa en términos de requerimientos legales, valor, criticidad y sensibilidad.
- Los activos que no sean información también deben ser clasificados.
- Los propietarios de los activos serán los responsables de su clasificación.
- Los procedimientos de clasificación serán revisados cada año.
- Se debe analizar la información sobre cada dimensión de seguridad para definir su clasificación, según el apartado 5.2 del documento de Políticas para la seguridad de la Información.
- La clasificación de la información debe ser un procedimiento de rutina dentro de la empresa.
- Los resultados de la clasificación deben indicar el valor de los activos.
- En general:
    - Los activos con clasificación Superior serán de acceso permitido exclusivamente a la Gerencia.
    - Los activos con clasificación Alta podrán ser accedidos por la Administración y la Gerencia.
    - Los activos de clasificación Media podrán ser accedidos por los Jefes de cada departamento, la Administración y la Gerencia.
    - Los activos con clasificación Baja podrán ser accedidos por todo el personal de la empresa.

Sobre la manipulación de los activos

- La manipulación de los activos deberán ser definidos según la clasificación que tenga cada activo.
- Se deben definir niveles de restricción para el acceso a los diferentes niveles de la información.
- Se debe mantener un registro de toda persona que acceda a cada activo, sobre todo en los de clasificación Superior y Alta.
- Se debe otorgar protección a las copias de la información.
- Se debe respetar los manuales de los fabricantes para la manipulación de activos adquiridos.

Porcentaje esperado de reducción del riesgo: Se espera que el riesgo sea controlado a corto plazo (2 meses), y se reduzca en un 60%.

Monto de inversión estimado: $500.00 USD.

Indicadores para medir el control: Revisión mensual de la información clasificada dentro del mes.

Frecuencia de evaluación del control: Cada año.

Responsable del control: El propietario de cada activo.

Fecha de inicio: febrero 27 de 2015

Fecha de finalización: abril 23 de 2015

7.3.4 Control para MJ-006-A.9.2 Gestión de acceso al usuario

Código del Control: MJ-006-A.9.2

Riesgo que mitiga: La asignación de derechos privilegiados dentro del SGSI de la empresa no está bien gestionado, pues actualmente hasta los usuarios que le dan mantenimiento al sistema de información de manera cotidiana deben de pasar controles que se aplican a usuarios de baja jerarquía.

Procedimientos para implementar el control:

Sobre la Administración de derechos de acceso privilegiados

- Se debe identificar plenamente las necesidades que tiene la empresa sobre derechos de acceso privilegiado. Esto implica identificar los activos que necesiten este tipo de acceso.
- Se debe aplicar siempre la política de asignar el mínimo permiso necesario a cada usuario.
- La administración de la asignación de privilegios estará a cargo del Departamento de Sistemas.
- Se debe definir un tiempo en el que cada privilegio expire.

Sobre la Administración de información secreta de autentificación de usuarios

- Cada usuario deberá firmar un documento en el que se compromete a guardar la confidencialidad de la información de autenticación.
- Se debe implementar un sistema que obligue al usuario a cambiar su contraseña inicial, y luego que la cambie cada sesenta días. El usuario no podrá usar ninguna de las diez últimas contraseñas utilizadas.
- Las contraseñas iniciales serán entregadas a cada usuario de manera personal en sobre cerrado, el usuario firmará un acuse de recibo de su contraseña que servirá como constancia.
- Las contraseñas iniciales deberán ser únicas para cada usuario.

Sobre la Revisión de los derechos de acceso asignados

- Los privilegios a cada usuario deberán ser revisados de forma anual.
- La revisión de los accesos de un usuario particular se realizará cuando suceda cualquier cambio en la empresa relacionado con ese usuario.
- Se debe revisar de manera trimestral que cada usuario tenga solamente los privilegios asignados por el Departamento de Sistemas.

Porcentaje esperado de reducción del riesgo: Se esperan resultados a corto plazo (3 meses), reduciendo el riesgo en un 75%.

Monto de inversión estimado: $1000.00 USD.

Indicadores para medir el control: Revisión de accesos no autorizados al sistema. Revisión de que el cambio obligado de contraseñas funcione de manera óptima.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Departamento de Sistemas.

Fecha de inicio: marzo 03 de 2015

Fecha de finalización: junio 03 de 2015

7.3.5 Controles para MJ-007-A.9.4 Control de acceso a sistemas y aplicaciones

Código del Control: MJ-007-A.9.4

Riesgo que Mitiga: La restricción a la información de la empresa no está correctamente gestionada.

Procedimientos para implementar el control:

- Se debe implementar controles de software para guardar un registro de los usuarios que han leído, escrito o borrado información.
- Se debe implementar controles de software para guardar un registro de los usuarios que han ejecutado comandos o programas.
- Los demás controles necesarios para mitigar este riesgo se encuentran implementados.

Porcentaje esperado de reducción del riesgo: Se esperan resultados a corto plazo (un mes), reduciendo el riesgo en un 20%.

Monto: $1500.00 USD.

Indicadores para medir el control: Revisión de los registros requeridos.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Departamento de Sistemas.

Fecha de inicio: abril 24 de 2015

Fecha de finalización: mayo 22 de 2015

7.3.6 Controles para MJ-009-A.12.1 Responsabilidades y procedimientos de operación

Código del Control: MJ-009-A.12.1

Riesgo que mitiga: Los procedimientos operativos no están documentados, lo que evidencia una falta de una guía para el personal que los debe realizar.

Procedimientos para implementar el control:

- Se deberá documentar los procedimientos para:
    - Instalación y configuración de sistemas.
    - Procesamiento y manipulación de información tanto automatizada como manual.
    - Instrucciones para gestión de errores.
    - Outputs especiales e instrucciones de manipulación de media.
    - Reinicio de sistema y recuperación de procedimientos.
    - Monitoreo de procedimientos

Porcentaje esperado de reducción del riesgo: Se esperan resultados a corto plazo (6 meses), reduciendo el riesgo en un 65%.

Monto: $600.00 USD.

Indicadores para medir el control: Revisión de la documentación de los procesos.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Responsable de la seguridad de la información.

Fecha de inicio: enero 02 de 2015

Fecha de finalización: julio 02 de 2015

7.3.7 Controles para MJ-010-A.12.7 Consideraciones de las auditorías de los sistemas de información

Código del Control: MJ-010-A.12.7

Riesgo que mitiga: El sistema de información no está desarrollado pensado en los impactos que podrían causar la ejecución de auditorías.

Procedimientos para implementar el control:

- Los requerimientos de acceso a los sistemas deben ser gestionados por lo menos con 15 días de anticipación.
- Se debe acordar previamente el alcance de la auditoría.
- Las pruebas de auditoría deben restringirse a solamente lectura de los datos y software, a menos que se haga en sistemas aislados o sobre copias de datos.
- Las pruebas que puedan afectar a la estabilidad del sistema se deben hacer fuera del horario de trabajo.
- Todos los accesos deben ser monitoreados y registrados.

Porcentaje esperado de reducción del riesgo: Se esperan resultados a corto plazo (2 meses), reduciendo el riesgo en un 70%.

Monto: $100.00 USD.

Indicadores para medir el control: Simulación de pruebas de auditoría.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Departamento de Sistemas.

Fecha de inicio: enero 02 de 2015

Fecha de finalización: marzo 02 de 2015

7.3.8 Controles para MJ-012-A.14.2 Seguridad en los procesos de desarrollo y soporte

Código del Control: MJ-012-A.14.2

Riesgo que mitiga: La empresa no desarrollo software, contrata a una empresa proveedora, pero ésta no dispone políticas de desarrollo seguro de software, por lo que se les requerirá que implementen este control.

Procedimientos para implementar el control:

Se exigirá a la empresa proveedora de software:

- Desarrollar el software en un lugar seguro.
- Sobre el ciclo de vida del software:
    - Seguridad en la metodología del desarrollo del software.
    - Mantener directrices de programación seguras para cada lenguaje utilizado.
- Requerimientos de seguridad en la fase de diseño.
- Repositorios seguros.
- Seguridad en la versión de control.
- Conocimiento de seguridad en aplicaciones.
- Destreza en la búsqueda y reparación de vulnerabilidades.

Porcentaje esperado de reducción del riesgo: Se esperan resultados a corto plazo (8 meses), reduciendo el riesgo en un 50%.

Monto: $2000.00 USD.

Indicadores para medir el control: Solicitud de la documentación al proveedor de software.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Responsable de seguridad de la Información.

Fecha de inicio: enero 02 de 2015

Fecha de finalización: septiembre 02 de 2015

7.3.9 Controles para MJ-014-A.17.1 Continuidad de la seguridad de la información

Código del Control: MJ-014-A.17.1

Riesgo que mitiga: La empresa no tiene documentados los procesos y controles que garantizan la continuidad de la seguridad de la información.

Procedimientos para implementar el control:

Sobre el personal:

- La empresa debe de contar con personal experimentado y dotado de conocimientos en materia de seguridad de la información, y, en recuperación inmediata.
- La empresa debe contratar a personal de respuesta en caso de incidentes de seguridad, deben de tener autoridad y competencia para resolver los problemas.
- Se debe de tener documentados los procedimientos que el personal deba seguir en caso de que se produzca un incidente provocado por la materialización de una de las amenazas identificados.

Sobre la documentación:

- Debe haber documentación sobre los controles para la seguridad de la información.
- Debe haber documentación sobre los procesos, procedimientos e implementación de cambios que tengan que ver con el mantenimiento de la seguridad de la información durante una situación adversa.
- Debe haber documentación sobre los controles de compensación hacia los controles que se pueden mantener durante una incidencia.

Porcentaje esperado de reducción del riesgo: Se esperan resultados a corto plazo (2 meses), reduciendo el riesgo en un 60%.

Monto: $500.00 USD.

Indicadores para medir el control: Solicitud de la documentación requerida.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Responsable de seguridad de la Información.

Fecha de inicio: junio 04 de 2015

Fecha de finalización: agosto 04 de 2015

7.3.10 Controles para MJ-015-A.18.2 Revisiones de la seguridad de la información

Código del Control: MJ-015-A.18.1

Riesgo que mitiga: La empresa no tiene la costumbre de revisar periódicamente los procedimientos para la seguridad de la información.

Procedimientos para implementar el control:

Sobre el cumplimiento con las políticas de seguridad y los estándares:

- Se debe identificar las causas del no cumplimiento.
- Evaluar las necesidades para llegar al cumplimiento.
- Implementar las acciones correctivas apropiadas.
- Revisar las implementaciones realizadas y corregirlas si es necesario

Sobre la revisión de cumplimiento técnico:

- Se debe utilizar herramientas de examinación automáticas.
- Personal especializado debe revisar los manuales.
- Si se realiza pruebas de penetración se debe de tener la precaución de no comprometer la seguridad del sistema.
- Cada prueba debe ser previamente planeada, documentada y autorizada.

Porcentaje esperado de reducción del riesgo: Se esperan resultados a corto plazo (3 meses), reduciendo el riesgo en un 60%.

Monto: $900.00 USD.

Indicadores para medir el control: Pruebas de cumplimiento.

Frecuencia de evaluación del control: Cada año.

Responsable del control: Responsable de seguridad de la Información.

Fecha de inicio: enero 02 de 2015

Fecha de finalización: abril 02 de 2015

7.4 Relación de los activos de la información con los proyectos propuestos

Cada activo de la información debe tener una relación con cada proyecto que intentará protegerlo, caso contrario, si un proyecto no tiene relación con ningún activo, sería un proyecto que no tuviera sentido de implementación. Esta relación se establece en el archivo adjunto **ArcosArgudoMiguel-TFM-SGSI-Relacion-Activos-Proyectos.xlsx**.

A continuación se muestra un diagrama de Gantt (figura 7.1) sobre el cronograma de los proyectos propuestos para la mejora de la seguridad de la información.

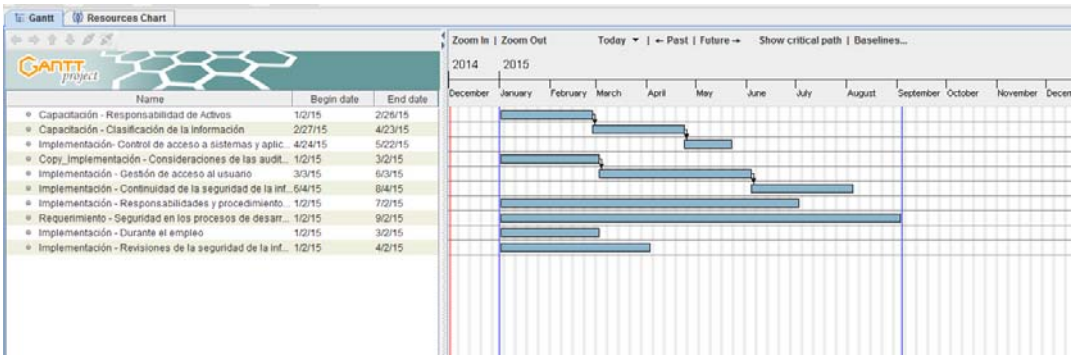

Figura 7.1: Diagrama de Gantt de la propuesta de Proyectos

8. Auditoría de Cumplimiento

Una vez ya implementadas, probadas y corregidas las propuestas de mejoras para la seguridad de la información, se procede a realizar una primera auditoría de cumplimento del SGSI, cabe recordar que anteriormente nunca había existido una auditoría externa ni interna por lo que no hay datos preexistentes de auditoría para tomarlos en cuenta. El objetivo de este apartado es valorar objetivamente la madurez que ha experimentado el SGSI y el funcionamiento de los controles de seguridad de la norma ISO/IEC 27002:2013 implementados.

8.1 Metodología para la Auditoría de Cumplimiento

La metodología de auditoría aplicada es la definida en el documento *ArcosArgudoMiguel-TFM-SGSI-Procedimientos de Auditorías Internas.pdf*.

8.1.1 Evaluación de la madurez de la seguridad de la información

A continuación se muestra los resultados de la evaluación de cada control implementado para la gestión de la seguridad de la información.

La efectividad de cada control se ha evaluado según la tabla 8.1:

Efectividad	CMM	Estado	Descripción
S/D	-	**Se desconoce**	Se desconoce si existe
L0	0%	**No existe**	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
L1	10%	**Inicial**	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal.
L2	50%	**Reproducible**	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea.
L3	90%	**Definido**	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
L4	95%	**Gestionado**	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se tienen 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.
NA	N/A	**No aplicable**	El control no es aplicable

Tabla 8.1: Tabla para evaluación de efectividad de controles implementados

El informe de la auditoría se encuentra en el documento adjunto *ArcosArgudoMiguel-TFM-SGSI-Informe de Auditoria Interna.pdf*, los resultados de la evaluación de la madurez los controles se muestra en la tabla 8.2, dichos resultados también se puede observar con más detalle en el archivo adjunto ArcosArgudoMiguel-TFM-SGSI-Evaluación de Controles en la Auditoría de Cumplimiento.xlsx.

Evaluación de Controles en la Auditoría de Cumplimiento			
Sección	**Control de la seguridad de la información**	**CMM**	**Observaciones**
A5	**Política de seguridad**	**90%**	
A5.1	**Política de seguridad de la información**	**90%**	
A5.1.1	Documento de política de seguridad de la información	**L3**	El documentos de Políticas está definido y comunicado a todo el personal
A5.1.2	Revisión de la política de seguridad de la información	**L3**	Existe un proceso definido para la revisión del documento de políticas
A6	**Aspectos Organizativos de la seguridad de la información**	**91%**	
A6.1	**Organización Interna**	**91%**	
A6.1.1	Asignación de responsabilidades para la seguridad de la información	**L3**	Control bien implementado
A6.1.2	Segregación de tareas	**L3**	Control bien implementado
A6.1.3	Contacto con las autoridades	**L4**	Control bien implementado
A6.1.4	Contacto con grupos de interés especial	**L3**	Control bien implementado
A6.1.5	Seguridad de la información en la gestión de proyectos	**L3**	Control bien implementado
A6.2	**Dispositivos para movilidad y teletrabajo.**		
A6.2.1	Política de uso de dispositivos para movilidad	**NA**	Control no aplicable
A6.2.2	Teletrabajo	**NA**	Control no aplicable
A7	**Seguridad ligada a los recursos humanos**	**81.39%**	
A7.1	**Antes de la contratación**	**72.50%**	
A7.1.1	Investigación de antecedentes	**L3**	Control bien implementado
A7.1.2	Términos y condiciones de contratación	**L4**	Control bien implementado
A7.2	**Durante el empleo**	**76.66%**	
A7.2.1	Responsabilidades de gestión	**L3**	Control bien implementado

A7.2.2	Concienciación, educación y capacitación en seguridad de la información	**L2**	Las capacitaciones de han impartido pero los resultados aún no son los aceptables
A7.2.3	Proceso disciplinario	**L3**	Control bien implementado
A7.3	**Terminación o cambio de puesto de trabajo**	**95%**	
A7.3.1	Cese o cambio de puesto de trabajo	**L4**	Este control se aplica bajo parámetros legales
A8	**Gestión de activos**	**92.08%**	
A8.1	**Responsabilidad sobre los activos**	**92.50%**	
A8.1.1	Inventario de activos	**L3**	Control bien implementado
A8.1.2	Propiedad de los activos	**L3**	Control bien implementado
A8.1.3	Uso aceptable de los activos	**L4**	Control bien implementado
A8.1.4	Devolución de activos	**L4**	Control bien implementado
A8.2	**Clasificación de la información**	**91.66%**	
A8.2.1	Directrices de clasificación	**L3**	Control bien implementado
A8.2.2	Etiquetado y manipulado de la información	**L4**	Control bien implementado
A8.2.3	Manipulación de activos	**L3**	Control bien implementado
A8.3	**Manejo de los soportes de almacenamiento extraíbles**		
A8.3.1	Gestión de soportes extraíbles	**NA**	Control no aplicable
A8.3.2	Eliminación de soportes	**NA**	Control no aplicable
A8.3.3	Soportes físicos en tránsito	**NA**	Control no aplicable
A9	**Gestión de acceso**	**93.25%**	
A9.1	**Requisitos de negocio para el control de accesos**	**92.50%**	
A9.1.1	Política de control de accesos	**L4**	Control bien implementado
A9.1.2	Control de acceso a las redes y servicios asociados	**L3**	Control bien implementado
A9.2	**Gestión de acceso de usuario**	**92.50%**	
A9.2.1	Gestión de altas/bajas en el registro de usuarios	**L4**	Control bien implementado
A9.2.2	Gestión de los derechos de acceso asignados a usuarios	**L4**	Control bien implementado
A9.2.3	Gestión de los derechos de acceso con privilegios especiales	**L3**	Control bien implementado
A9.2.4	Gestión de información confidencial de autenticación de usuarios	**L3**	Control bien implementado
A9.2.5	Revisión de los derechos de acceso de los usuarios	**L3**	Control bien implementado

A9.2.6	Retirada o adaptación de los derechos de acceso	**L4**	Control bien implementado
A9.3	**Responsabilidades del usuario**	**95%**	
A9.3.1	Uso de información confidencial para la autenticación	**L4**	Control bien implementado
A9.4	**Control de acceso a sistemas y aplicaciones**	**93%**	
A9.4.1	Restricción del acceso a la información	**L3**	Control bien implementado
A9.4.2	Procedimientos seguros de inicio de sesión	**L3**	Control bien implementado
A9.4.3	Gestión de contraseñas de usuario	**L4**	Control bien implementado
A9.4.4	Uso de herramientas de administración de sistemas	**L4**	Control bien implementado
A9.4.5	Control de acceso al código fuente de los programas	**L4**	Control bien implementado
A10	**Criptografía**	**90%**	
A10.1	**Controles criptográficos**	**90%**	
A10.1.1	Política de uso de los controles criptográficos	**L3**	Control bien implementado
A10.1.2	Gestión de contraseñas	**L3**	Control bien implementado
A11	**Seguridad física y ambiental**	**91.94%**	
A11.1	**Áreas seguras**	**91.66%**	
A11.1.1	Perímetro de seguridad física	**L3**	Control bien implementado
A11.1.2	Controles físicos de entrada	**L4**	Control bien implementado
A11.1.3	Seguridad de oficinas, despachos y recursos	**L4**	Control bien implementado
A11.1.4	Protección contra las amenazas externas y ambientales	**L3**	Control bien implementado
A11.1.5	El trabajo en áreas seguras	**L3**	Control bien implementado
A11.1.6	Áreas de acceso público, carga y descarga	**L3**	Control bien implementado
A11.2	**Seguridad de los equipos**	**92.22%**	
A11.2.1	Emplazamiento y protección de equipos	**L3**	Control bien implementado
A11.2.2	Instalaciones de suministro	**L4**	Control bien implementado
A11.2.3	Seguridad del cableado	**L4**	Control bien implementado
A11.2.4	Mantenimiento de los equipos	**L4**	Control bien implementado
A11.2.5	Salida de activos fuera de las dependencias de la empresa	**L3**	Control bien implementado
A11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	**L3**	Control bien implementado

A11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	**L3**	Control bien implementado
A11.2.8	Equipo informático de usuario desatendido	**L4**	Control bien implementado
A11.2.9	Política de puesto de trabajo despejado y pantallas limpias	**L3**	Control bien implementado
A12	**Seguridad de operaciones**	**92.14%**	
A12.1	**Responsabilidades y procedimientos de operación**	**90%**	
A12.1.1	Documentación de procedimientos de operación	**L3**	Control bien implementado
A12.1.2	Gestión de cambio	**L3**	Control bien implementado
A12.1.3	Gestión de capacidades	**L3**	Control bien implementado
A12.1.4	Separación de entornos de desarrollo, prueba y producción	**L3**	Control bien implementado
A12.2	**Protección contra código malicioso**	**95%**	
A12.2.1	Controles contra el código malicioso	**L4**	Control bien implementado
A12.3	**Respaldos de seguridad**	**95%**	
A12.3.1	Respaldos de seguridad de la información	**L4**	Control bien implementado
A12.4	**Registro de actividad y supervisión**	**92.50%**	
A12.4.1	Registro y gestión de eventos de actividad	**L4**	Control bien implementado
A12.4.2	Protección de los registros de información	**L3**	Control bien implementado
A12.4.3	Registros de actividad del administrador y operador del sistema	**L4**	Control bien implementado
A12.4.4	Sincronización de relojes	**L3**	Control bien implementado
A12.5	**Control del software en producción**	**90%**	
A12.5.1	Instalación del software en sistemas en producción	**L3**	Control bien implementado
A12.6	**Gestión de la vulnerabilidad técnica**	**92.50%**	
A12.6.1	Gestión de las vulnerabilidades técnicas	**L4**	Control bien implementado
A12.6.2	Restricciones en la instalación de software	**L3**	Control bien implementado
A12.7	**Consideraciones de las auditorías de los sistemas de información**	**90%**	
A12.7.1	Consideraciones de las auditorías de los sistemas de información	**L3**	Control bien implementado
A13	**Seguridad de telecomunicaciones**	**92.50%**	

A13.1	**Gestión de la seguridad en las redes**	**95%**	
A13.1.1	Controles de red	**L4**	Control bien implementado
A13.1.2	Mecanismos de seguridad asociados a servicios en red	**L4**	Control bien implementado
A13.1.3	Segregación de redes	**L4**	Control bien implementado
A13.2	**Transferencia de información**	**90%**	
A13.2.1	Políticas y procedimientos de intercambio de información	**L3**	Control bien implementado
A13.2.2	Acuerdos de intercambio	**L3**	Control bien implementado
A13.2.3	Mensajería electrónica	**L3**	Control bien implementado
A13.2.4	Acuerdos de confidencialidad y secreto	**L3**	Control bien implementado
A14	**Adquisición, desarrollo y mantenimiento de los Sistemas de Información**	**89.26%**	
A14.1	**Requisitos de seguridad de los sistemas de información**	**90%**	
A14.1.1	Análisis y especificación de los requisitos de seguridad	**L3**	Control bien implementado
A14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	**L3**	Control bien implementado
A14.1.3	Protección de las transacciones por redes telemáticas	**L3**	Control bien implementado
A14.2	**Seguridad en los procesos de desarrollo y soporte**	**82.77%**	
A14.2.1	Política de desarrollo seguro de software	**L2**	Documento requerido a la empresa proveedora de software pero aún no recibido
A14.2.2	Procedimientos de control de cambios en los sistemas	**L3**	Control bien implementado
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	**L4**	Control bien implementado
A14.2.4	Restricciones a los cambios en los paquetes de software	**L3**	Control bien implementado
A14.2.5	Uso de principios de ingeniería en protección de sistemas	**L3**	Control bien implementado
A14.2.6	Seguridad en entornos de desarrollo	**L2**	Solicitud requerida a la empresa proveedora de software pero aún no recibida
A14.2.7	Externalización del desarrollo de software	**L3**	Control bien implementado
A14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	**L4**	Control bien implementado
A14.2.9	Pruebas de aceptación	**L4**	Control bien implementado

A14.3	**Datos para pruebas**	**95%**	
A14.3.1	Protección de los datos de prueba	**L4**	Control bien implementado
A15	**Relaciones con proveedores**	**92.50%**	
A15.1	**Seguridad de la información en las relaciones con proveedores**	**90%**	
A15.1.1	Política de seguridad de la información para proveedores	**L3**	Control bien implementado
A15.1.2	Tratamiento del riesgo dentro de acuerdos de proveedores	**L3**	Control bien implementado
A15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	**L3**	Control bien implementado
A15.2	**Gestión de la prestación del servicio por suministradores**	**95%**	
A15.2.1	Supervisión y revisión de los servicios prestados por terceros	**L4**	Control bien implementado
A15.2.2	Gestión de cambios en los servicios prestados por terceros	**L4**	Control bien implementado
A16	**Gestión de los incidentes de seguridad de la información**	**91.43%**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	**91.43%**	
A16.1.1	Responsabilidades y procedimientos	**L4**	Control bien implementado
A16.1.2	Notificación de los eventos de seguridad de la información	**L3**	Control bien implementado
A16.1.3	Notificación de puntos débiles de la seguridad	**L3**	Control bien implementado
A16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	**L4**	Control bien implementado
A16.1.5	Respuesta a los incidentes de seguridad	**L3**	Control bien implementado
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	**L3**	Control bien implementado
A16.1.7	Recopilación de evidencias	**L3**	Control bien implementado
A17	**Aspectos de seguridad de la información en la Gestión de la Continuidad del Negocio**	**84.17%**	
A17.1	**Continuidad de la seguridad de la información**	**78.33%**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	**L3**	Control bien implementado
A17.1.2	Implantación de la continuidad de la seguridad de la información	**L2**	Aún no hay los resultados esperados de este control

A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**L4**	Control bien implementado
A17.2	**Redundancias**	**90%**	
A17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	**L3**	Control bien implementado
A18	**Cumplimiento**	**91%**	
A18.1	**Cumplimiento de los requisitos legales y contractuales**	**92%**	
A18.1.1	Identificación de la legislación aplicable	**L3**	Control bien implementado
A18.1.2	Derechos de propiedad intelectual	**L4**	Control bien implementado
A18.1.3	Protección de los registros de la organización	**L4**	Control bien implementado
A18.1.4	Protección de datos y privacidad de la información personal	**L3**	Control bien implementado
A18.1.5	Regulación de los controles criptográficos	**L3**	Control bien implementado
A18.2	**Revisiones de la seguridad de la información**	**90%**	
A18.2.1	Revisión independiente de la seguridad de la información	**L3**	Control bien implementado
A18.2.2	Cumplimiento de las políticas y normas de seguridad	**L3**	Control bien implementado
A18.2.3	Comprobación del cumplimiento	**L3**	Control bien implementado

Tabla 8.2: Evaluación de los controles de seguridad implementados

A continuación se presenta también se muestra los resultados del cumplimiento de los requerimientos de la norma ISO/IEC 27001 en la tabla 8.3:

Estado de la implementación de la norma ISO/IEC 27001			
Sección	**Requerimiento de la norma ISO/IEC 27001**	**CMM**	**Observaciones**
4	**Contexto de la Organización**	**93%**	
4.1	**Contexto Organizacional**	**95%**	
4.1	Determinar los objetivos del SGSI de la Organización y cualquier cuestión que pueda afectar su efectividad	**L4**	Requerimiento cumpliendo aceptablemente
4.2	**Partes interesadas**	**90%**	
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	**L3**	Requerimiento cumpliendo aceptablemente
4.2 (b)	Determinar sus requerimientos de seguridad de información relevante y obligaciones	**L3**	Requerimiento cumpliendo aceptablemente
4.3	**Alcance del SGSI**	**95%**	

4.3	Determinar y documentar el alcance del SGSI	**L4**	Requerimiento cumpliendo aceptablemente
4.4	**SGSI**	**90%**	
4.4	Establecer, implementar, mantener y mejorar continuamente el SGSI acorde al standard.	**L3**	Requerimiento cumpliendo aceptablemente
5	**Liderazgo**	**91.66%**	
5.1	**Liderazgo y compromiso**	**95%**	
5.1	Liderazgo y compromiso mostrado por la alta dirección con el SGSI	**L4**	Requerimiento cumpliendo aceptablemente
5.2	**Política**	**90%**	
5.2	Documentar la información de las políticas de seguridad	**L3**	Requerimiento cumpliendo aceptablemente
5.3	**Roles de la Organización, responsabilidades y autoridades**	**90.00%**	
5.3	Asignar y comunicar roles de la seguridad de la información y responsabilidades	**L3**	Requerimiento cumpliendo aceptablemente
6	**Planificación**	**90.00%**	
6.1	**Acciones para enfrentar riesgos y oportunidades**	**90.00%**	
6.1.1	Diseño/planificación del SGSI para satisfacer los requerimientos , hacer frente a los riesgos y responsabilidades	**L3**	Requerimiento cumpliendo aceptablemente
6.1.2	Definir y aplicar un proceso de gestión de riesgos de seguridad de la información	**L3**	Requerimiento cumpliendo aceptablemente
6.1.3	Documentar y aplicar un proceso de gestión de riesgos de seguridad de la información	**L3**	Requerimiento cumpliendo aceptablemente
6.2	**Objetivos y estudios de la seguridad de la información**	**95%**	
6.2	Establecer y documentar los objetivos y estudios de la seguridad de la información	**L3**	Requerimiento cumpliendo aceptablemente
7	**Soporte**	**82.00%**	
7.1	**Recursos**	**90.00%**	
7.1	Determinar y asignar los recursos necesarios para el SGSI	**L3**	Requerimiento cumpliendo aceptablemente
7.2	**Competencia**	**90%**	
7.2	Determinar, documentar y hacer las competencias necesarias disponibles	**L3**	Requerimiento cumpliendo aceptablemente
7.3	**Concientización**	**50%**	

7.3	Establecer un programa de concientización de la seguridad	**L2**	Falta una nueva capacitación al personal
7.4	**Comunicación**	**90%**	
7.4	Determinar las necesidades de las comunicaciones internas y externas para el SGSI	**L3**	Requerimiento cumpliendo aceptablemente
7.5	**Información Documentada**	**90%**	
7.5.1	Proporcionar la documentación requerida por el estándar más que la requerida por la organización	**L3**	Requerimiento cumpliendo aceptablemente
7.5.2	Proporcionar títulos de documentos, autores, etc., dar un formato consistente, revisarlos y aprobarlos	**L3**	Requerimiento cumpliendo aceptablemente
7.5.3	Control adecuado de la documentación	**L3**	Requerimiento cumpliendo aceptablemente
8	**Operación**	**90.00%**	
8.1	**Planificación y control operativo**	**90%**	
8.1	Planificar, implementar, controlar y documentar los procesos del SGSI para gestionar los riesgos	**L3**	Requerimiento cumpliendo aceptablemente
8.2	**Gestión de los riesgos de la seguridad de la información**	**90%**	
8.2	Evaluar y documentar regularmente los riesgos de la seguridad de la información y sus cambios	**L3**	Requerimiento cumpliendo aceptablemente
8.3	**Información del tratamiento de los riesgos e la información**	**90%**	
8.3	Implementar el plan de tratamiento de riesgos y documentar los resultados	**L3**	Requerimiento cumpliendo aceptablemente
9	**Evaluación del desempeño**	**91.66%**	
9.1	**Monitoreo, medición, análisis y evaluación**	**90%**	
9.1	Monitorear, medir, analizar y evaluar el SGSI y sus controles	**L3**	Requerimiento cumpliendo aceptablemente
9.2	**Auditoría interna**	**90%**	
9.2	Planificar y ejecutar auditorías internas del SGSI	**L3**	Requerimiento cumpliendo aceptablemente
9.3	**Revisión de la dirección**	**95%**	
9.3	Revisiones regulares del SGSI por parte de la dirección	**L4**	Requerimiento cumpliendo aceptablemente
10	**Mejoras**	**90.00%**	

10.1	**No conformidad y acciones correctivas**	**90%**	
10.1	Identificar, corregir y tomar medidas para prevenir la recurrencia de las no conformidades, documentación de las acciones	**L3**	Requerimiento cumpliendo aceptablemente
10.2	**Mejora Continua**	**90%**	
10.2	Mejorar continuamente el SGSI	**L3**	Requerimiento cumpliendo aceptablemente

Tabla 8.3: Resultados de cumplimiento de requerimientos de la norma ISO/IEC 27001

8.1.2 Presentación de resultados

La tabla 8.2 muestra los resultados de la madurez de los controles de seguridad implementados en el SGSI uno por uno, es decir muy detalladamente, sin embargo podemos resumir esta información de forma gráfica como se muestra en la figura 8.1.

De la misma forma podemos resumir la información de la tabla 8.2 en un gráfico radial, como lo muestra la figura 8.2 y 8.3. En este caso se muestra el grado de cumplimiento de los controles de seguridad implementados en el SGSI pero por cada capítulo de la norma ISO/IEC 27002:2013, es decir des el capítulo 5 hasta el capítulo 18, en este gráfico se compara el estado actual de los controles contra el estado objetivo de los mismos. El gráfico 8.2 muestra el grado de cumplimiento antes de la implementación del SGSI, mientras que el gráfico 8.3 muestra el grado de cumplimientos actual del SGSI.

De estos dos gráficos se puede deducir que el nivel de seguridad del SGSI ha experimentado un cambio positivo muy significativo en comparación con el estado inicial que se evaluó antes de realizar la implementación de todas las fases descritas en el presente documento.

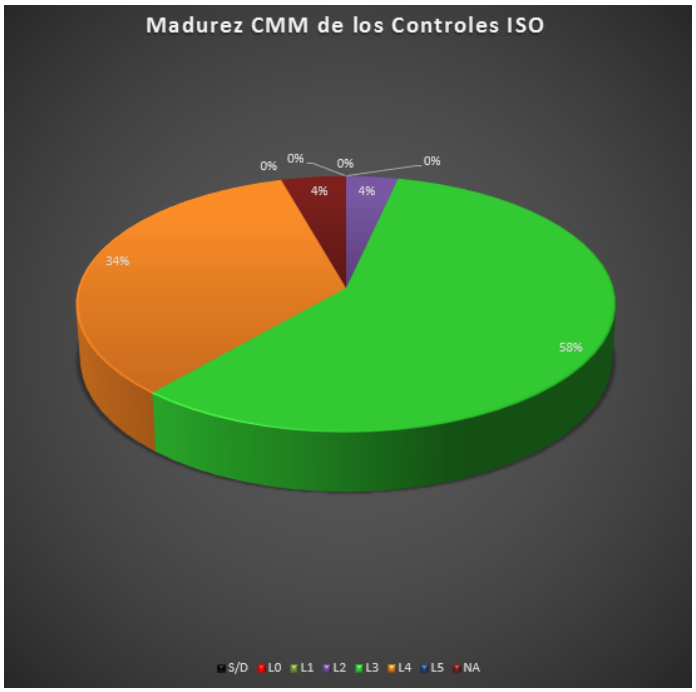

Figura 8.1: Gráfico de los resultados de la evaluación de los controles (Pastel)

Figura 8.2: Gráfico comparativo del estado inicial de los controles por capítulo de la norma ISO/IEC 27002:2013 (Radial)

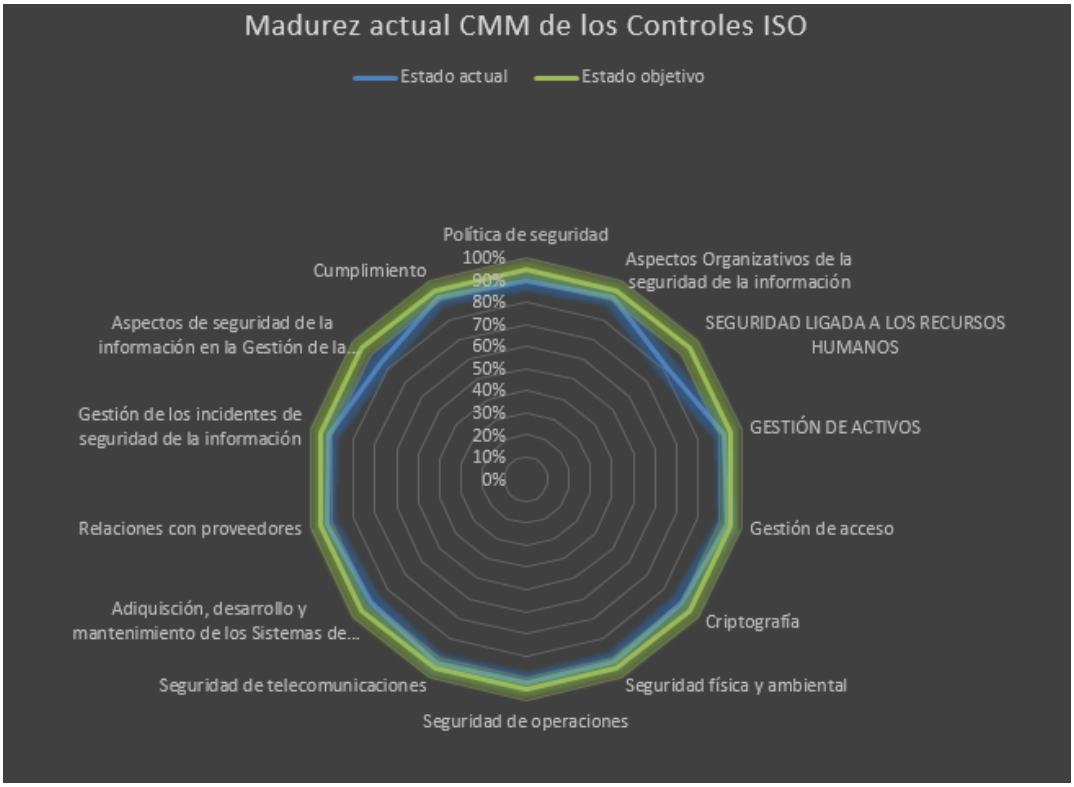

Figura 8.3: Gráfico comparativo del estado actual de los controles por capítulo de la norma ISO/IEC 27002:2013 (Radial)

Análogamente podemos resumir los resultados del cumplimiento de la norma ISO/IEC 27001 en las siguientes figuras:

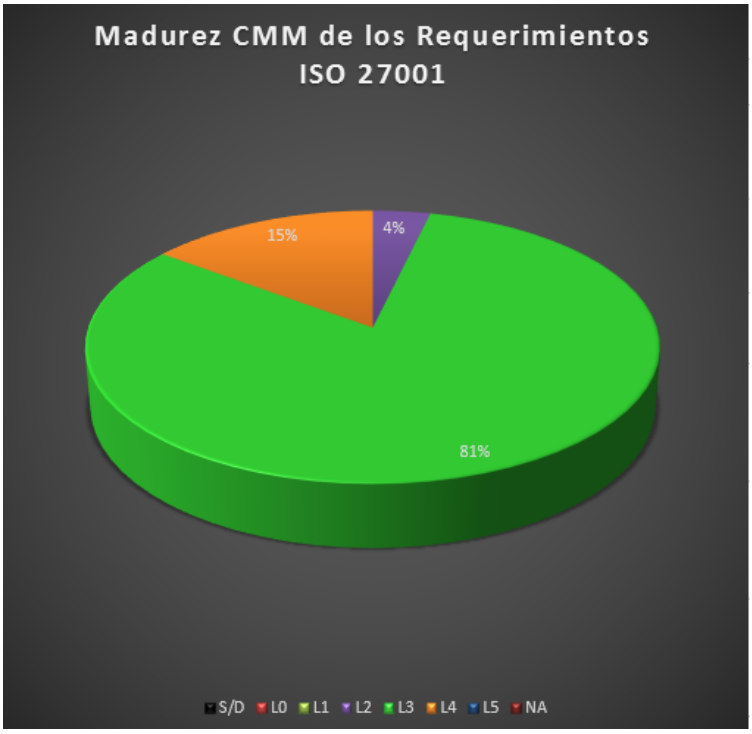

Figura 8.4: Gráfico de los resultados de la evaluación de los requerimientos de la norma ISO/IEC 27001 (Pastel)

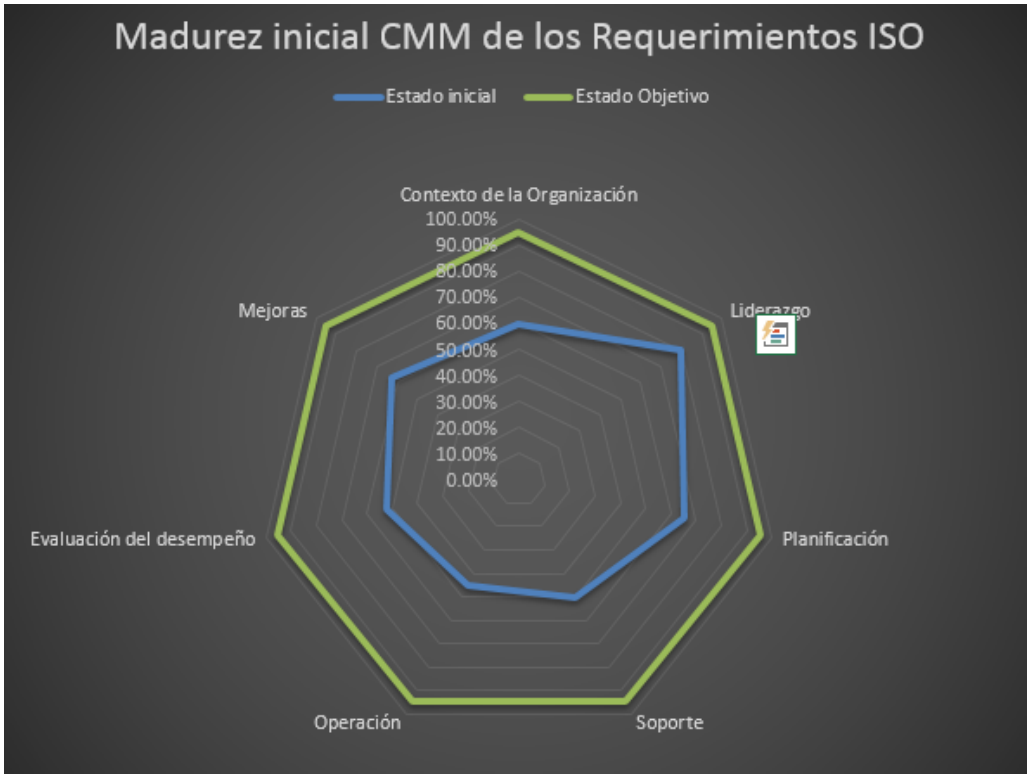

Figura 8.5: Gráfico radial del estado inicial del cumplimiento de los requerimientos de la norma ISO/IEC 27001 (Radial)

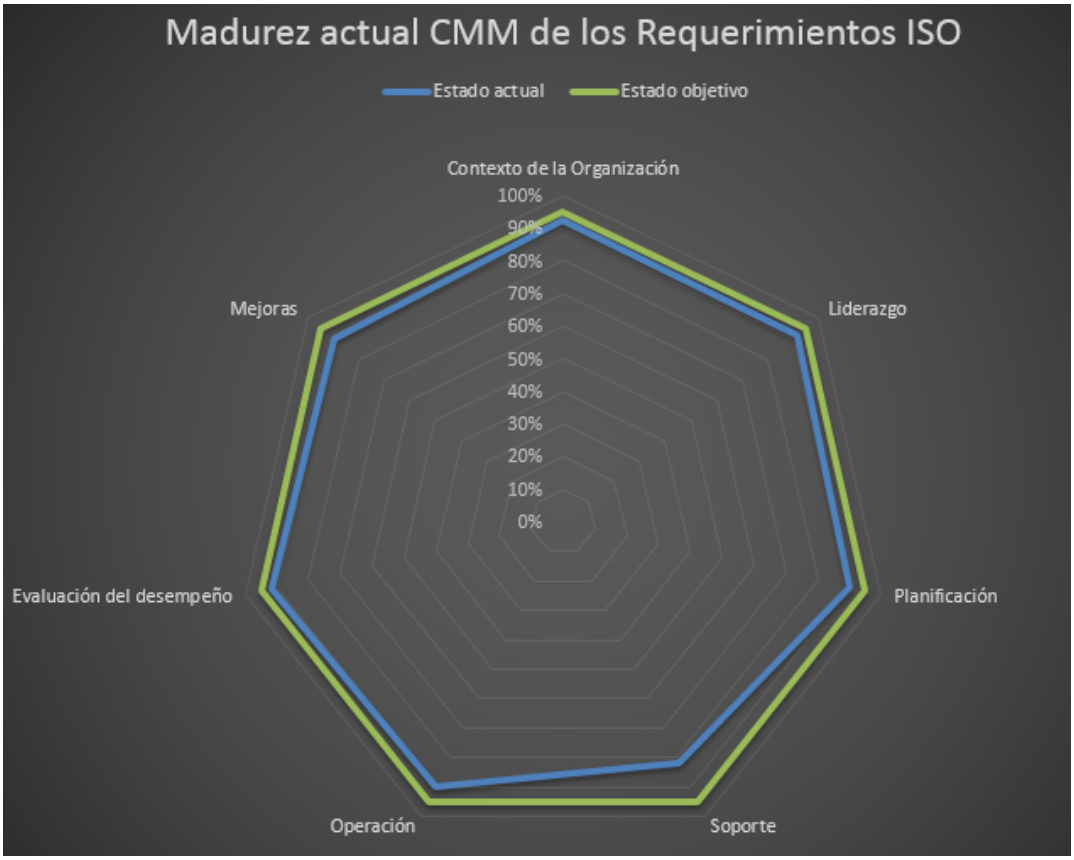

Figura 8.6: Gráfico Radial del cumplimiento actual de los requerimientos de la norma ISO/IEC 27001 (Radial)

9. Resumen Ejecutivo

El presente trabajo ha consistido en el estudio e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una pequeña empresa ubicada en Ecuador, concretamente en la ciudad de Cuenca, basado en la norma ISO/IEC 27001:2013.

La empresa disponía de un sistema de información y contaba con varios controles de seguridad, sin embargo era muy inmaduro en cuanto a la documentación y la concientización del personal sobre la importancia de la seguridad de la información.

El objetivo de este trabajo fue estudiar el estado actual de la seguridad de la información, determinar sus falencias e implementar los controles y salvaguardas necesarios para mejorar el nivel de seguridad, a tal punto de que sea capaz de superar una auditoría de certificación ISO/IEC 27001:2013. El proceso que se ha realizado se puede resumir de la siguiente manera:

1. Se realizó el Análisis Diferencial, es un estudio en el que se analiza cada aspecto de seguridad de la información inicial del sistema de la empresa, en comparación con los requerimientos de la norma ISO/IEC 27001:2013, y de los controles de la norma ISO/IEC 27002:2013. También se determina los controles que son aplicables y los que no lo son.
2. Se definió el alcance del SGSI, de tal forma que se ha definido lo que amerita protección, por ejemplo la documentación sobre contabilidad, y lo que no lo amerita, por ejemplo el departamento de limpieza.
3. Se redactó todos los documentos requeridos para la implementación del SGSI (Gestión Documental), estos son:
   - Declaración de aplicabilidad: Se establece los controles de la norma ISO/IEC 27002:2013 que se implementarán y los que no se implementarán, siempre con una justificación.
   - Gestión de indicadores: Se define los métodos por los que se evaluarán los controles de seguridad que se implementen.
   - Metodología del análisis de riesgos: Se define la forma en que se evaluarán los riesgos a los que se enfrenta el SGSI, en este caso se utilizó la metodología MAGERIT.
   - Políticas para la seguridad de la información: Documento que reúne las directrices y procedimientos que se deberán seguir por parte de todo el personal de la empresa, sin excepción. Este documento está aprobado por la Gerencia de la empresa y comunicado a todo el personal.
   - Procedimientos de auditorías internas: Se detalla el proceso que deberán seguir las auditorías internas.
   - Revisión por dirección: Se detalla el proceso que la Gerencia deberá seguir para aprobar los procesos que le competa.
4. Se realizó el inventario de activos de información, en los que se asignó sus propietarios y su valoración cuantitativa. Se definió también las dimensiones de seguridad en las que cada activo necesitaba protección.
5. Se realizó el análisis de amenazas sobre cada activo, el impacto potencial que cada uno podría sufrir, es decir, se aplicó la metodología MAGERIT, que también contempla definir un nivel de riesgo aceptable y riesgo residual.
6. Se realizó la propuesta de una serie de proyectos que luego fueron implementados, y que contribuyen a mejorar la seguridad de la información.

7. Se realizó una auditoría para verificar el actual cumplimiento y madurez de los controles implementados en el SGSI con relación a los controles de la norma ISO/IEC 27002:2013.

Una vez realizados todos estos procesos se presenta este documento y todos sus anexos al Departamento de Gerencia con los resultados obtenidos, y, a pesar de que la auditoría de cumplimiento mostró que hay aspectos que corregir, demuestran que la seguridad de la información de la organización ha madurado muy considerablemente, lo que muestra el éxito del trabajo.

10. Conclusiones

Al término del presente proyecto podemos concluir principalmente que la información de una empresa puede llegar a ser invaluable, ya que su correcta gestión de seguridad pudiera marcar la diferencia entre el éxito y el fracaso. Desde este punto de vista un Sistema de Gestión de Seguridad de la Información (SGSI) puede llegar a ser un apoyo muy importante que ayudaría a organizar los procesos, controles y salvaguardas con los que se mantendría la información bajo medidas de seguridad que garanticen su integridad, confidencialidad y autenticidad.

Para asegurarse de que se mantiene un SGSI adecuado, se lo ha implementado con la intención de que supere una auditoría de certificación bajo la norma ISO/IEC 27001:2013, la misma que cuenta con la aceptación a nivel internacional, esta norma impone a un SGSI que implemente una serie de requisitos antes de ser sometido a dicha auditoría. Para poder cumplir con estos requerimientos se ha recurrido a la norma ISO/IEC 27002:2013 que facilita una serie de controles que pueden ser implementados nivel técnico. Estas dos norma juntas nos ha facilitado el trabajo de la implementación del SGSI, pues marca un camino a seguir y permite visualizar el estado objetivo al que se debe llevar el sistema de gestión de seguridad de la información.

Las propuestas de mejoras a implementar para elevar el nivel de la seguridad de la información han sido presentadas en concordancia con la declaración de aplicabilidad, y siempre pensando en que sus presupuestos estén al alcance de la empresa.

Finalmente la auditoría de cumplimiento nos permitido palpar objetivamente el grado de madurez que ha experimentados el SGSI, pues todos los controles y salvaguardas implementadas apoyan al cumplimiento de las exigencias de la norma ISO/IEC 27001:2013.

11. Resumen de anexos

A continuación se muestra la tabla 10.1 que muestra el resumen de los documentos anexos que componen este trabajo:

Nombre de Documento	Descripción
ArcosArgudoMiguel-TFM-SGSI-Análisis de amenazas-Impacto de amenazas por activo.xlsx	Análisis de amenazas e Impacto de amenazas por activo
ArcosArgudoMiguel-TFM-SGSI-Análisis Diferencial.xlsx	Análisis diferencial
ArcosArgudoMiguel-TFM-SGSI-Declaración de Aplicabilidad.xlsx	Declaración de Aplicabilidad
ArcosArgudoMiguel-TFM-SGSI-Evaluación de Controles en la Auditoría de Cumplimiento.xlsx	Resultados de auditoría de cumplimiento respecto a los controles implementados
ArcosArgudoMiguel-TFM-SGSI-Gestión de Indicadores.pdf	Gestión de Indicadores
ArcosArgudoMiguel-TFM-SGSI-Informe de Auditoria Interna.pdf	Informe de auditoría interna
ArcosArgudoMiguel-TFM-SGSI-Justificación Análisis Diferencial.pdf	Justificación del análisis diferencial
ArcosArgudoMiguel-TFM-SGSI-Metodología de Análisis de Riesgos.pdf	Metodología de análisis de riesgos
ArcosArgudoMiguel-TFM-SGSI-Políticas de Seguridad de Información para la Empresa Mariscos SA .pdf	Documento de políticas para la seguridad de la información
ArcosArgudoMiguel-TFM-SGSI-Procedimientos de Auditorías Internas.pdf	Procedimientos de auditorías internas
ArcosArgudoMiguel-TFM-SGSI-Relacion-Activos-Proyectos.xlsx	Relación entre activos y proyectos propuestos
ArcosArgudoMiguel-TFM-SGSI-Revisión por dirección.pdf	Revisión por dirección

Tabla 10.1: Listado de documentos anexos

12. Referencias Bibliográficas

[1] International Standard ISO/IEC 27001:2013

[2] International Standard ISO/IEC 27002:2013

[3] International Standard ISO 17799

[4] International Standard ISO 31000:2009

[5] http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

[6]www.iso27001security.com/ISO27k_ISMS_and_controls_status_wtth_SoA_and_gaps.xlsx

[7]www.isotools.org/2013/11/28/auditorias-de-los-controles-del-sistema-de-seguridad-segun-iso-27000/

[8] http://seguinfo.wordpress.com/2006/08/02/iso-9001-indicadores-de-gestion/

[9] http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf

[10]http://www.qualypedia.org/ISO%2027001.S-7-REVISION-POR-LA-DIRECCION.ashx

[11] http://administracionelectronica.gob.es/

[12] http://www.pmg-ssi.com/2013/12/iso27001-origen/

[13] www.normalizacion.gob.ec