Universitat Autònoma de Barcelona

Universitat Oberta de Catalunya

Universitat Rovira i Virgili

Implementación del SGSI en Mariscos S. A.

Presentación de resultados al Departamento de Gerencia

Descripción de la empresa

- Mariscos S. A. es una pequeña empresa con su sede en la ciudad de Cuenca – Ecuador.
- La empresa se dedica a la distribución de mariscos y carnes para toda la región sur del país.
- El negocio comprende además la atención de un micro comisariato en el que se realiza ventas al por menor no sólo de carnes y mariscos, sino de gran variedad de productos.
- Tiene una trayectoria de quince años de existencia.
- Es una empresa pionera en la ciudad en dar este servicio.

Descripción del problema

- Mariscos S. A. ha determinado que en 15 años su volumen de información se ha incrementado considerablemente, razón por la cuál se ha detectado varios problemas menores en la gestión de la seguridad de su información.

- A pesar de que aún no se ha experimentado pérdidas graves causadas por estos problemas, la empresa es consciente de que se debe actuar inmediatamente para evitar cualquier tipo de incidente que pueda causar daños de gran magnitud.

Antecedentes

- Mariscos S. A. ha definido a toda su información como el activo intangible más valioso que posee.

- Mariscos S. A. ha comprendido que la información merece protección igual que cualquier otro activo de la empresa.

Antecedentes

- Mariscos S. A. entiende que este activo puede verse comprometido por personas malintencionadas que pueden estar geográficamente en cualquier parte.

- Mariscos S. A. ha decidido implementar un Sistema de Gestión de Seguridad de la Información (SGSI) capaz de proteger adecuadamente la información.

Antecedentes

- Mariscos S. A. contrata los servicios del Ing. Miguel Arcos para que dirija el proyecto de diseño e implementación un SGSI en la empresa.

Requerimientos

- El SGSI que se ha de implementar en Mariscos S. A. debe cumplir con los requerimientos que lo hagan capaz de superar una auditoría de certificación de la norma ISO/IEC 27001:2013.

Introducción

- Toda la información presentada se encuentra ampliada en el documento *ArcosArgudoMiguel-TFM-SGSI-Memoria.pdf*, a no ser que se especifique lo contrario.

Introducción

- Un SGSI es un sistema que apoya a una organización en la protección adecuada de la información bajo determinados estándares internacionales establecidos precisamente para tales efectos.

- Para el caso de Mariscos S. A. se ha tomado como referencia el estándar internacional ISO/IEC 27001:2013.

Introducción

- La norma ISO/IEC 27001:2013 define una serie de requerimientos aprobados internacionalmente que apoyan a la correcta gestión de la seguridad de la información.
- Cuenta con el apoyo de la norma ISO/IEC 27002:2013 que contiene los controles técnicos que pueden ser implementados para cumplir con los requerimientos de la norma ISO/IEC 27001:2013.
- En Ecuador la empresa que otorga esta certificación es el Instituto Ecuatoriano de Normalización (INEN).

Introducción - Justificación

- Las razones que justifican la implementación de un SGSI en la empresa son:
  - Posee información acumulada en 15 años de existencia.
  - Almacena información confidencial tanto de clientes como de proveedores.
  - Ha ganado un prestigio de alto nivel en la Región Sur del Ecuador.
  - La información de toda su contabilidad debe ser de acceso restringido.
  - Se necesita protección tanto a nivel lógico como físico.

Introducción – Información Sensible

- La información de la empresa que se ha decidido proteger es la siguiente:
  - Datos de los clientes
  - Precios de compra
  - Precios de venta
  - Datos de proveedores
  - Estados financieros
  - Asuntos legales

Introducción – Estado inicial del SI

- La empresa cuenta con SI adquirido
- No existe documentación en materia de seguridad de la información
- El personal tiene un buen manejo de la información
- No existe una cultura de seguridad de la información

Alcance del Proyecto

- El SGSI abarcará todos los sistemas de información que dan soporte a todos los procesos del negocio de la empresa.

Alcance del Proyecto

- Respecto a los requisitos de la norma ISO/IEC 27001: 2013 y a los controles de la norma ISO/IEC 27002:2013 se ha verificado:
  - Requisitos y controles implementados correctamente
  - Requisitos y controles implementados incorrectamente
  - Requisitos y controles no implementados

Alcance del Proyecto

- Las áreas de la empresa que el SGSI cubre son:
  - Gerencia
  - Administración
  - Ventas
  - Bodega
  - Cobranzas
  - Contabilidad
  - Sistemas

Alcance del Proyecto

- Las áreas de la empresa que el SGSI no cubre son:
  - Transportistas
  - Proceso de mariscos
  - Proceso de cárnicos
  - Personal de limpieza

Objetivos de Seguridad

- Mejorar la seguridad de la aplicación adquirida por Mariscos S. A.
- Proteger de forma efectiva la información de los clientes depositada en la Organización.
- 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.
- Garantizar que los datos referentes a los productos como precio, stock, kardex, etc., mantengan su integridad.
- Garantizar que el personal de ventas pueda realizar su actividad de atención al cliente de manera ininterrumpida.

Análisis Diferencial

- El Análisis Diferencial permite determinar con gran exactitud el grado de cumplimiento que el SI inicialmente cumple con respecto a los requisitos de la norma ISO/IEC 27001:2013, y con respecto a la norma ISO/IEC 27002:2013.
- También se determina los requisitos o controles que no son aplicables, es decir aquellos que no necesitan ser implementados.
- El detalle de este análisis se encuentra en el archivo ***ArcosArgudoMiguel-TFM-SGSI-Análisis Diferencial.xlsx***.

Análisis Diferencial

- La siguiente tabla indica el grado de cumplimiento que cada control o requisito pueda tener:

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

Análisis Diferencial - Resultados

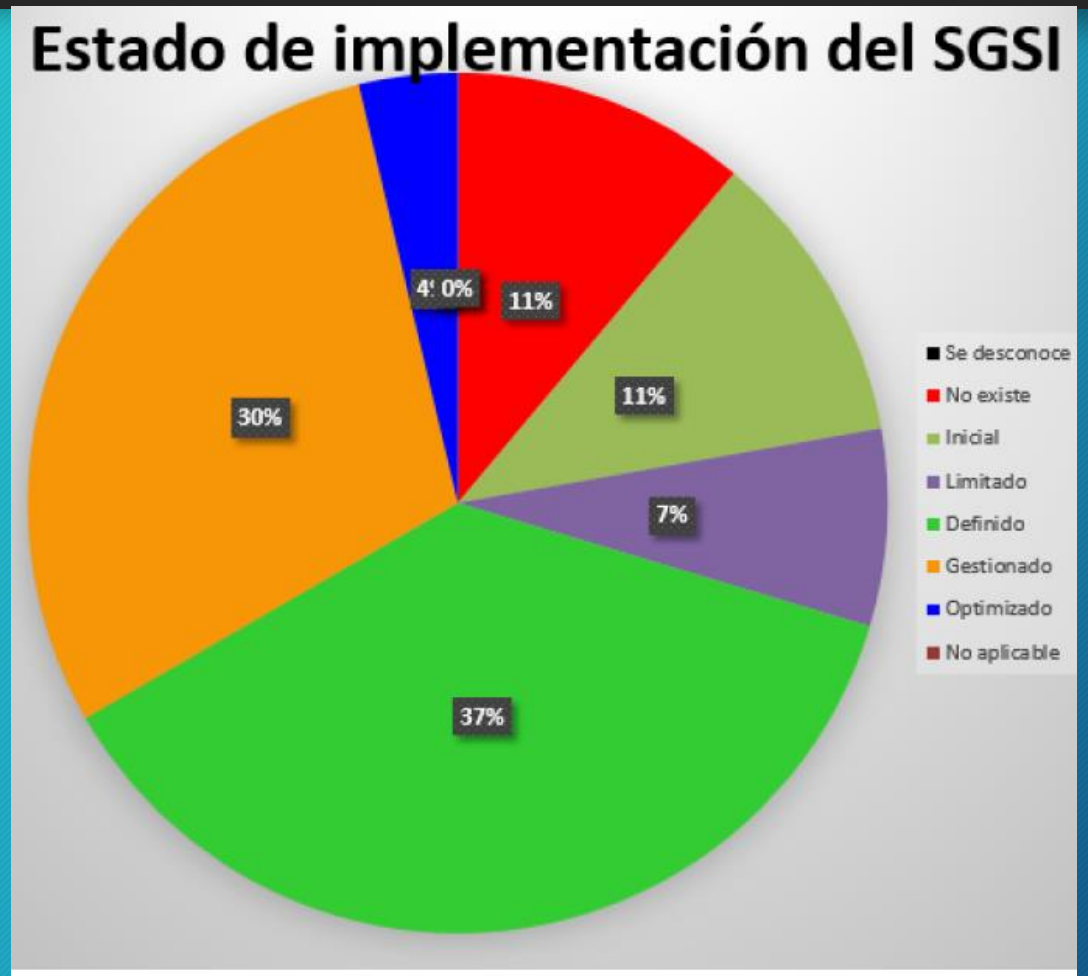


Figura 4.1: Cumplimiento de las exigencias de la norma ISO/IEC 27001:2013

Análisis Diferencial - Resultados

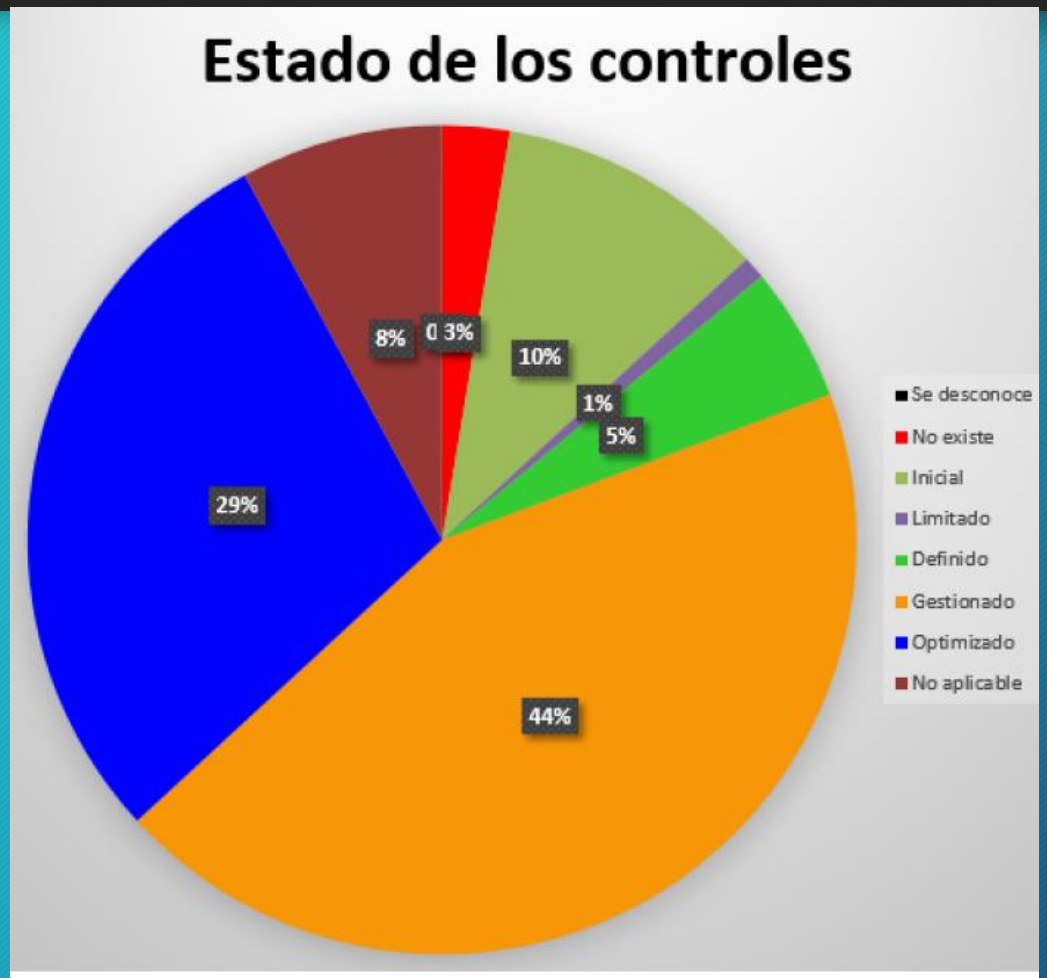


Figura 4.2: Cumplimiento de los controles de la norma ISO/IEC 27002

Esquema Documental

- Para la implementación del proyecto se ha redactado los siguientes documentos:
  - Políticas de seguridad de la información
  - Procedimiento de auditorías internas
  - Gestión de indicadores
  - Revisión por dirección
  - Gestión de roles y responsabilidades
  - Metodología de análisis de riesgos
  - Declaración de aplicabilidad

Esquema Documental – Políticas de Seguridad

- Documento que especifica los procedimientos para mantener la información de la empresa bajo una gestión de seguridad adecuada.
- Todo el personal de la empresa deberá acoger estas políticas sin excepción de persona.
- Será revisado anualmente.
- Debe ser comunicado a todo el personal de la empresa.
- Estará siempre disponible.

Esquema Documental – Procedimiento de Auditorías Internas

- Describe los procesos que se realizarán durante las etapas de comprobación del SGSI.
- Estas auditorías permitirán identificar las deficiencias todavía existentes en la implementación del SGSI.
- No son auditorías de certificación, son auditorías de revisión.
- Las auditorías internas se llevarán a cabo anualmente.

Esquema Documental – Gestión de Indicadores

- Documento que da las directrices para definir los indicadores con los que se medirá el rendimiento de cada control de seguridad implementado.

Esquema Documental – Revisión por Dirección

- Documento que proporciona un marco referencial en el que el Departamento de Gerencia se puede apoyar para determinar el grado de convivencia del SGSI con el negocio de la empresa.

Esquema Documental – Gestión de Roles y Responsabilidades

- Son procedimientos con los que se definirá los roles de las personas que tengan algún grado de responsabilidad en la gestión de la seguridad de la información.

- Se encuentra incluido dentro del documento de Políticas de Seguridad.

Esquema Documental – Metodología de Análisis de Riesgos

- Documento que tiene las directrices para que la empresa gestione de manera adecuada los riesgos que amenazan a la seguridad de la información.

- Se detalla de manera muy completa el tratamiento que cada riesgo identificado recibirá para minimizarlo, eliminarlo, traspasarlo o asumirlo.

Esquema Documental – Declaración de aplicabilidad

- Documento que resume los controles de la norma ISO/IEC 27001:2013 que serán implementados en el SGSI de la empresa, y los controles que no son necesarios implementar.

Esquema Documental

- Todos los archivos del Esquema Documental se encuentra como documentos anexos, tal como muestra la siguiente tabla:

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

Análisis de Riesgos

- Esta fase permite determinar el nivel de cada riesgo que la seguridad de la información enfrenta.
- Se considera las salvaguardas implementadas y se trata de gestionar el riesgo residual.
- Ayuda también a determinar el umbral de riesgo que la empresa decide asumir.
- Para el caso de la empresa se ha decidido utilizar la metodología MAGERIT.

Análisis de Riesgos – Inventario de activos

- Listado de todos los activos de la empresa que tengan algún grado de relación con la manipulación de información, ya sean tangibles o intangibles.
- Cada activo es asignado a un grupo según la siguiente tabla:

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

Análisis de Riesgos – Inventario de activos

- Por ilustración se muestra un fragmento del inventario de activos:

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

Análisis de Riesgos – 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

Análisis de riesgos – Análisis de dependencias de activos

- Se diseña una especia de árbol que indica la dependencia que tienen los activos entre sí.
- Las dependencias se han establecido a nivel del tipo de activo.
- El activo más valioso se encuentra en el nodo superior, los activos menos valiosos son aquellos que se encuentran en los nodos inferiores.

Análisis de riesgos – Análisis de dependencias de activos

- El siguiente es el árbol de dependencias de activos determinado:

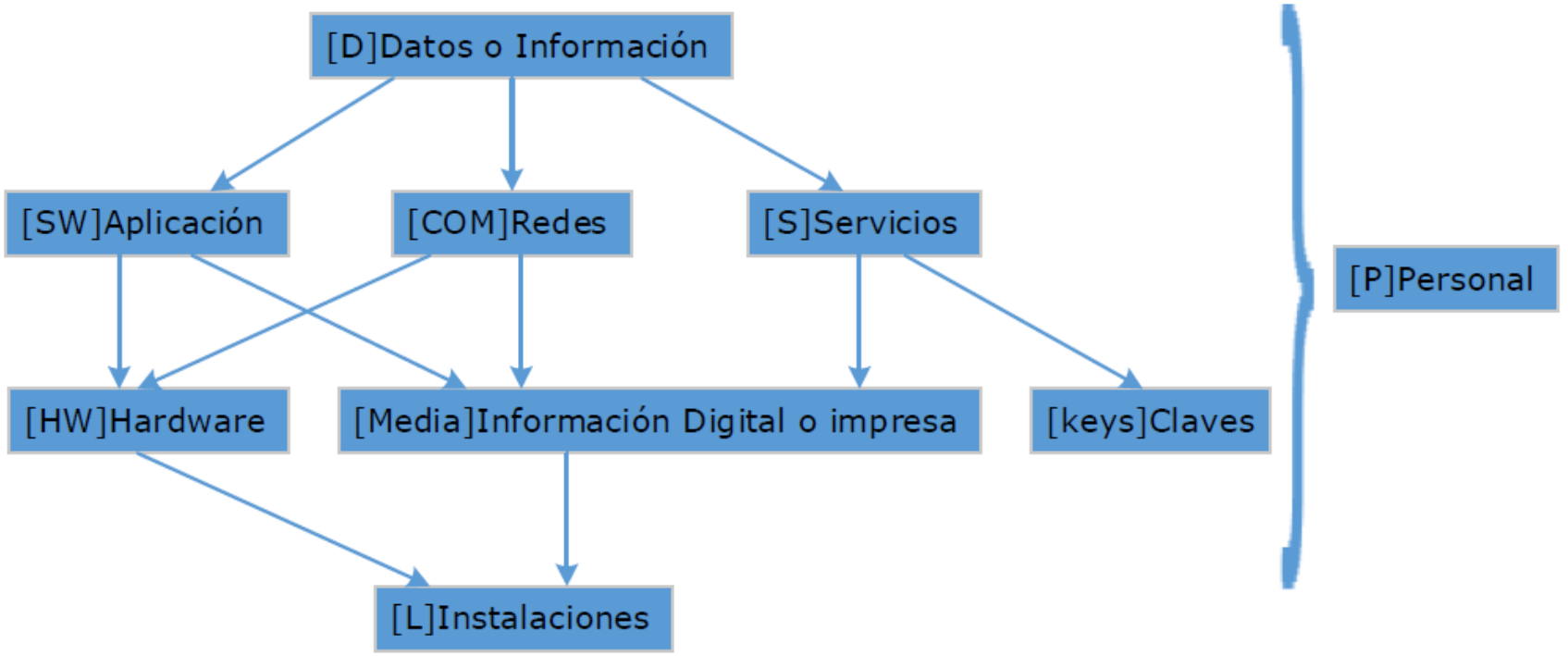


Figura 6.1: Árbol de dependencias de activos

Análisis de riesgos – Tabla de valoración de activos

- Del árbol de dependencia de activos se deriva que el activo más valioso de la empresa es la información, concretamente la información relativa a la Contabilidad de la organización.
- Es posible dar una valoración cuantitativa a cada activo, respetando los rangos de la siguiente tabla:

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

Análisis de riesgos – Tabla de valoración de activos

- A continuación se muestra un fragmento de la tabla de valoración de activos resultante:

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

Dimensiones de seguridad

- Cada activo posee (o puede poseer) cinco dimensiones de seguridad que pueden ser afectadas por ataques:
  - Autenticidad [A] – los datos deben ser auténticos
  - Confidencialidad [C] – los datos deben poder ser accedidos sólo por personal autorizado
  - Integridad [I] – los datos deben ser manipulados solamente por personal autorizado
  - Disponibilidad[D] – los datos deben estar disponibles cuando el personal autorizado lo requiera
  - Trazabilidad[T] – se debe poder determinar el usuario que hizo determinada acción sobre los datos

Dimensiones de seguridad

- El impacto que los activos puedan sufrir sobre cada una de sus dimensiones de seguridad serán evaluados cuantitativamente según la siguiente tabla:

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

- Impacto hace referencia al daño que sufre un activo luego de que se ha materializado una amenaza.

Dimensiones de seguridad – Valoración de los impactos por activo

- A continuación se muestra un fragmento de la tabla de valoración de los impactos por activo resultante:

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

Análisis de amenazas

- Las amenazas analizadas son las sugeridas por la metodología MAGERIT en su libro 2 apartado 5, entre los cuales se encuentran:
  - Desastres naturales [N]
  - Desastres de origen Industrial [I]
  - Errores o fallos no intencionados [E]
  - Ataques intencionados [A]
- Ejemplo:

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%	

Impacto potencial de las amenazas por cada activo de información

- Se evaluará el impacto que cada activo de información sufriera si cada amenaza sugerida por MAGERIT se materializara en cada una de sus dimensiones de seguridad. Ejemplo:

Activos	Grupo	[D]					[D]				
	Código	AC-D-001					AC-D-002				
	Activo	Contabilidad					Base de Datos				
	Dimensiones	A	C	I	D	T	A	C	I	D	T
[E.1]	Errores de los usuarios		8	9	7			8	9	7	
[E.2]	Errores del administrador		6	7	8			6	7	8	
[E.3]	Errores de monitorización (log)			7					7		
[E.4]	Errores de configuración (conf)			6					6		
[E.7]	Deficiencias y fallos en la organización										
[E.8]	Difusión de software dañino										
[E.9]	Errores de [re-]encaminamiento										
[E.10]	Errores de secuencia										
[E.14]	Escapes de información		7					7			
[E.15]	Alteración accidental de información			8					8		
[E.18]	Destrucción de información				5					5	

Impacto potencial de las amenazas por cada activo de información

- El detalle de este análisis se encuentra en el archivo *ArcosArgudoMiguel-TFM-SGSI-Análisis de amenazas-Impacto de amenazas por activo.xlsx*

Cálculo de riesgo por activo

- El cálculo de riesgo por activo 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. Ejemplo:

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

Cálculo de riesgo por activo – Riesgo aceptable

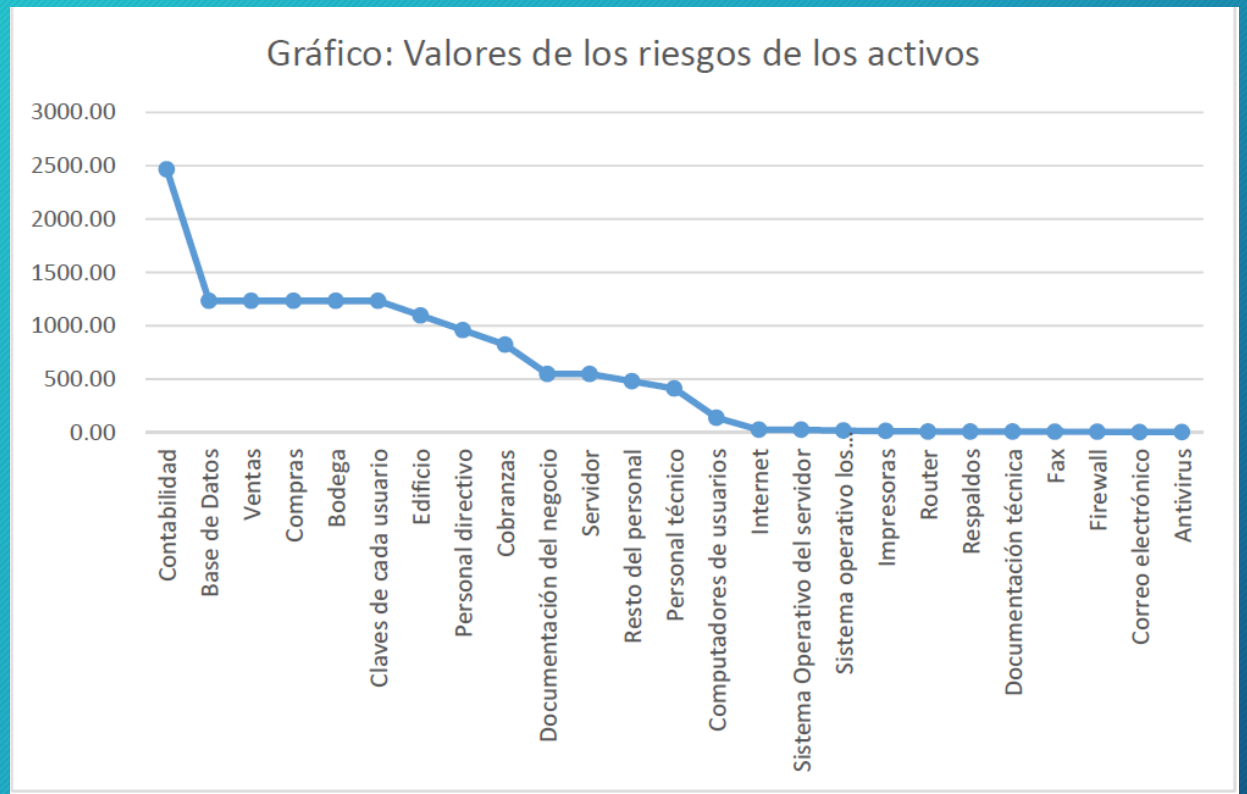
- Del cálculo del riesgo por activo se puede determinar el nivel de riesgo aceptable, ya sea por la poca probabilidad de que ocurra, o por que sería demasiado costosa la protección. Se toma como referencia la siguiente tabla:

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

Cálculo de riesgo por activo – Riesgo aceptable

- El siguiente gráfico muestra los valores de los riesgos para cada activo. En él se puede ver los riesgos que son asumidos por la empresa:



Cálculo de riesgo por activo – Riesgo aceptable

- 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.

Propuestas de mejoras para la seguridad de la información

- A continuación se proponen proyectos de mejora de la seguridad de la información que ayudarán a mitigar las amenazas que enfrenta la empresa y a reducir los riesgos que no serán asumidos por la misma.

- Estas propuestas deben estar en concordancia con la Declaración de Aplicabilidad que está en el archivo *ArcosArgudoMiguel-TFM-SGSI-Declaración de Aplicabilidad.xlsx*

Propuestas – Gestión de los controles a implementar

- Los controles de seguridad que serán implementados serán los sugeridos por la norma ISO/IEC 27002:2013

- A continuación se definirá los procedimientos con los que se gestionará estos controles.

Propuestas – Gestión de los controles a implementar

- Análisis del estado inicial
  - Recopilar información existente
  - Documentar controles implementados

Propuestas – Gestión de los controles a implementar

- Gestión de recursos para la implementación de controles
  - Se define el personal que implementará el control
    - Personal interno
    - Personal externo
    - Personal por contratar
  - Se debe contar con la aprobación del Departamento de Gerencia para gestionar los recursos
  - Se debe tener claro el propósito del control

Propuestas – Gestión de los controles a implementar

- Desarrollo de los controles a implementar
  - El personal que implementa el SGSI capacitará a los empleados involucrados en materia de seguridad en tema de normalización, redacción y documentación de controles.

Propuestas – Gestión de los controles a implementar

- Cada documentación deberá contener por lo menos los siguientes aspectos:
  - Código del control
  - Riesgo que mitiga
  - Procedimientos para implementar el control
  - Porcentaje esperado de reducción de riesgo
  - Monto de inversión estimado
  - Indicadores para medir el control
  - Frecuencia de evaluación del control
  - Responsable del control
  - Fecha de inicio
  - Fecha de finalización

Mejoras implementadas

- Las siguientes mejoras han sido implementadas:
  - **MJ-001-A.5.1 Política de seguridad de la información**
  - **MJ-002-A.7.2 Durante el empleo**
  - **MJ-003-A.8.1 Responsabilidad de los activos**
  - **MJ-004-A.8.2 Clasificación de la información**
  - **MJ-005-A.9.1 Requisitos del negocio para el control de accesos**
  - **MJ-006-A.9.2 Gestión de acceso al usuario**
  - **MJ-007-A.9.4 Control de acceso a sistemas y aplicaciones**

Mejoras implementadas

- MJ-008-A.11.2 Seguridad en los equipos
- MJ-009-A.12.1 Responsabilidades y procedimientos de operación
- MJ-010-A.12.7 Consideraciones de las auditorías de los sistemas de información
- MJ-011-A.13.2 Transferencia de información
- MJ-012-A.14.2 Seguridad en los procesos de desarrollo y soporte
- MJ-013-A.16.1 Gestión de incidentes de seguridad de la información y mejoras
- MJ-014-A.17.1 Continuidad de la seguridad de la información
- MJ-015-A.18.2 Revisiones de la seguridad de la información

Mejoras implementadas

- De estas mejoras, las siguientes ya han sido implementadas en la fase de Gestión Documental:
  - **MJ-001-A.5.1 Política de seguridad de la información**
  - **MJ-005-A.9.1 Requisitos del negocio para el control de accesos**
  - **MJ-008-A.11.2 Seguridad en los equipos**
  - **MJ-011-A.13.2 Transferencia de información**
  - **MJ-013-A.16.1 Gestión de incidentes de seguridad de la información y mejoras**

Mejoras implementadas

- **Controles para el apartado: MJ-002-A.7.2 Durante el empleo**
  - Capacitar y concientizar a todo el personal en materia de seguridad de la información
  - Duración 2 semanas
  - Presupuesto $2.000
  - Reducción del riesgo hasta un 75%
  - Evaluación del control anual

Mejoras implementadas

- **Controles para MJ-003-A.8.1 Responsabilidad de los activos**
  - Redactar un manual de usos de activos de información
  - Desarrollado por el Departamento de Sistemas
  - Presupuesto $500
  - Guardar una constancia de recepción
  - Fomentar la costumbre de lectura del manual
  - Reducción del riesgo en 75%
  - Evaluación anual

Mejoras implementadas

- **Controles para MJ-004-A.8.2 Clasificación de la información**
  - Implementar directrices para una organizada clasificación de los activos de información
  - Cada activo será clasificado por su propietario
  - La clasificación se realizará luego de analizar cada dimensión de seguridad de cada activo
  - La clasificación debe determinar el valor de cada activo
  - De la clasificación dependerá también la manipulación del activo
  - La clasificación podrá ser: Baja, Media, Alta o Superior
  - Presupuesto $500
  - Reducción del riesgo 60%
  - Evaluación anual del control

Mejoras implementadas

- **Control para MJ-006-A.9.2 Gestión de acceso al usuario**
  - Identificar plenamente las necesidades de la empresa sobre este aspecto
  - Aplicar siempre la política de asignar el mínimo permiso necesario
  - Control a cargo del Departamento de Sistemas
  - Cada privilegio debe tener fecha de expiración
  - Debe haber un compromiso de parte del usuario de mantener el secreto
  - Los privilegios deberán ser revisados de forma anual
  - Reducción del riesgo en 75%
  - Presupuesto $1.000
  - Evaluación anual del control

Mejoras implementadas

- **Controles para MJ-007-A.9.4 Control de acceso a sistemas y aplicaciones**
  - Implementar controles para guardar un registro de la información a la que cada usuario ha tenido acceso.
  - Implementar controles para guardar un registro de los comandos o programas que han ejecutado los usuarios.
  - Reducción del riesgo 20%
  - Presupuesto $1.500
  - Evaluación anual del control

Mejoras implementadas

- **Controles para MJ-009-A.12.1 Responsabilidades y procedimientos de operación**
  - Documentar todos los procedimientos operativos
    - Instalación y configuración de sistemas
    - Procesamiento y manipulación de información
    - Instrucciones para gestión de errores
    - Outputs especiales
    - Monitoreo de procedimientos
  - Reducción del riesgo 65%
  - Presupuesto $600
  - Evaluación anual del control

Mejoras implementadas

- **Controles para MJ-010-A.12.7 Consideraciones de las auditorías de los sistemas de información**
  - Se debe anticipar con por lo menos 15 días la realización de auditorías
  - Se debe predefinir el alcance de la auditoría
  - En la medida de lo posible solamente debería realizarse lectura de datos
  - Se debe determinar las pruebas que se deban realizar fuera del horario de trabajo
  - Reducción del riesgo 70%
  - Presupuesto $100
  - Evaluación anual del contro

Mejoras implementadas

- **Controles para MJ-012-A.14.2 Seguridad en los procesos de desarrollo y soporte**
  - La empresa proveedora del SI deberá desarrollarlo en un lugar seguro
  - Debe garantizar metodologías seguras de desarrollo de software
  - Debe garantizar repositorios seguros
  - Debe tener destreza en la búsqueda y reparación de vulnerabilidades
  - Reducción del riesgo 50%
  - Presupuesto $2.000
  - Evaluación anual del control

Mejoras implementadas

- **Controles para MJ-014-A.17.1 Continuidad de la seguridad de la información**
  - La empresa debe dotarse de personal con experiencia en materia de seguridad de la información y en recuperación inmediata.
  - Debe haber personal con la competencia para tomar decisiones en momentos del suceso de un incidente.
  - Debe existir documentación de los procesos a seguir en caso de emergencias.
  - Debe haber documentación de los controles implementados.
  - Reducción del riesgo 60%
  - Presupuesto $500
  - Evaluación anual del control

Mejoras implementadas

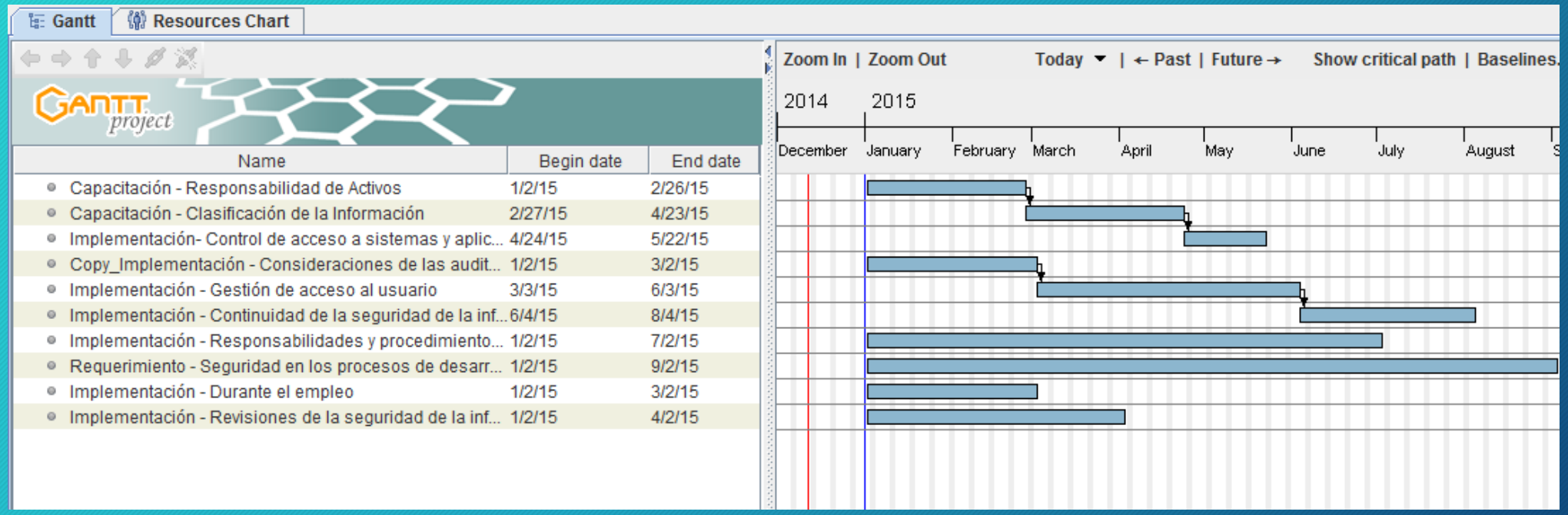
- **Controles para MJ-015-A.18.2 Revisiones de la seguridad de la información**
  - La empresa debe buscar las causas del no cumplimiento
  - Evaluar las necesidades de llegar al cumplimiento
  - Implementar las acciones correctivas apropiadas
  - Utilizar herramientas de examinación automáticas para el cumplimiento técnico
  - Reducción del riesgo 60%
  - Presupuesto $900
  - Evaluación anual del control

Mejoras implementadas

- Una relación entre los activos de información y las propuestas de mejoras se encuentra en el archivo ***ArcosArgudoMiguel-TFM-SGSI-Relacion-Activos-Proyectos.xlsx***, a continuación se muestra un fragmento como ejemplo:

Proyectos	Código	MJ-001-A.5.1	MJ-002-A.7.2	MJ-003-A.8.1	MJ-004-A.8.2	MJ-005-A.9.1	MJ-006-A.9.2	MJ-007-A.9.4	MJ-008-A.11.2
	Nombre	Política de seguridad de la información	Durante el empleo	Responsabilidad de los activos	Clasificación de la información	Requisitos del negocio para el control de accesos	Gestión de acceso al usuario	Control de acceso a sistemas y aplicaciones	Seguridad en los equipos
Activos de la información									
Código	Nombre								
AC-D-001	Contabilidad	X		X	X	X	X		
AC-D-002	Base de Datos	X		X	X	X	X		
AC-D-003	Cobranzas	X		X	X	X	X		
AC-D-004	Ventas	X		X	X	X	X		
AC-D-005	Compras	X		X	X	X	X		
AC-COM-006	Internet	X		X	X	X	X		
AC-D-007	Bodega	X		X	X	X	X		
AC-S-008	Correo electrónico	X		X	X	X	X	X	
AC-Media-09	Documentación del negocio	X		X	X	X	X		
AC-HW-010	Servidor			X	X	X	X		X
AC-HW-011	Computadores de usuarios			X	X				X

Mejoras implementadas – Diagrama de Gantt



Auditoría de Cumplimiento

- En esta fase se ha probado todos los requerimientos y controles implementados en el SGSI de la empresa.
- No existen datos de auditorías anteriores para que sean tomados en cuenta en esta auditoría.
- Se trata de evaluar la madurez que el SGSI de la empresa ha experimentado después de haber implementado el proyecto.
- El informe de esta auditoría se encuentra en el archivo ***ArcosArgudoMiguel-TFM-SGSI-Procedimientos de Auditorías Internas.pdf***

Evaluación de la madurez de la seguridad de la información

- Se ha evaluado cada requerimiento de la norma ISO/IEC 27001:2013 y cada control de la norma ISO/IEC 27002:2013, según la tabla siguiente:

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

Evaluación de la madurez de la seguridad de la información

- A continuación se muestra un fragmento de la evaluación de los controles de la norma ISO/IEC 27002:2013 implementados:

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%**	

Evaluación de la madurez de la seguridad de la información

- Los resultados detallados de la evaluación se encuentran en el archivo ***ArcosArgudoMiguel-TFM-SGSI-Evaluaciónde Controles en la Auditoría de Cumplimiento.xlsx***

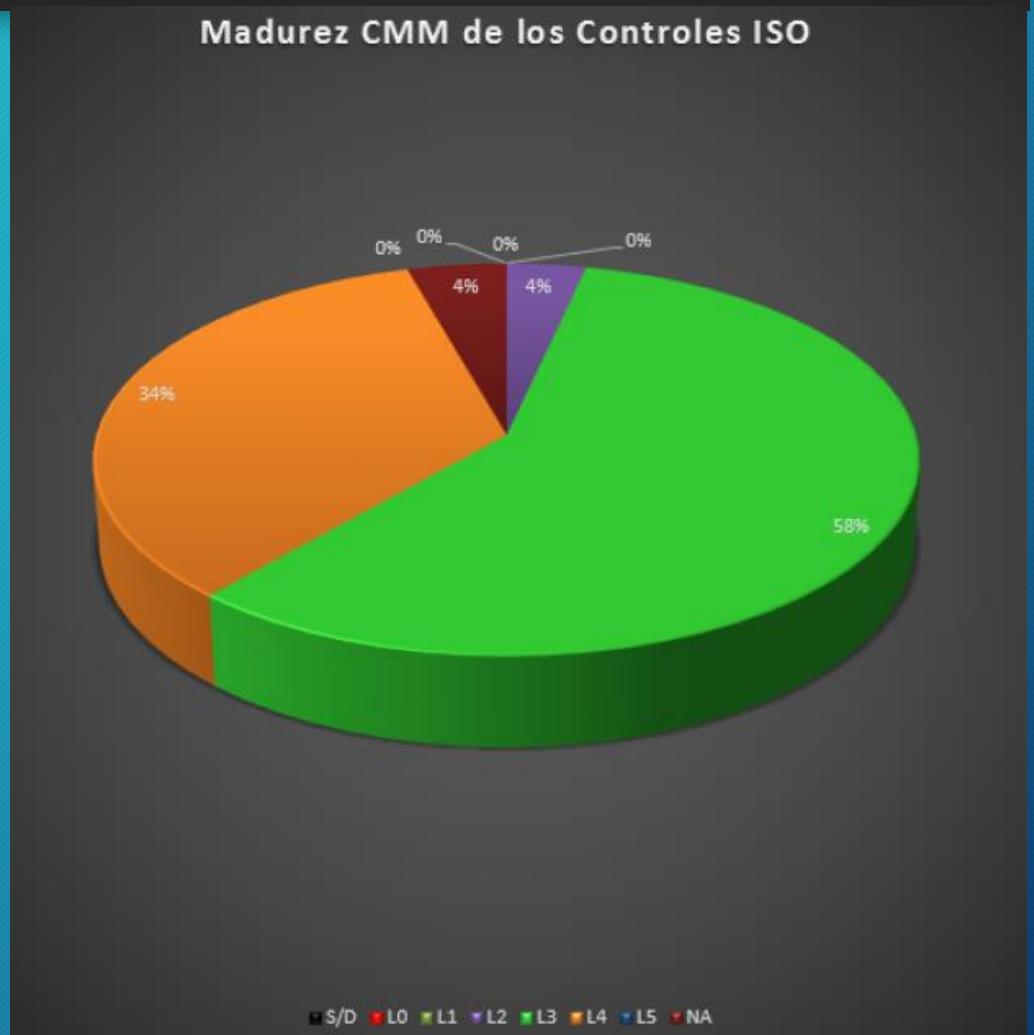
Evaluación de la madurez de la seguridad de la información

- A continuación se muestra un fragmento de la evaluación de la madurez de los requerimientos de la norma ISO/IEC 27001:2013 implementados:

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%**	

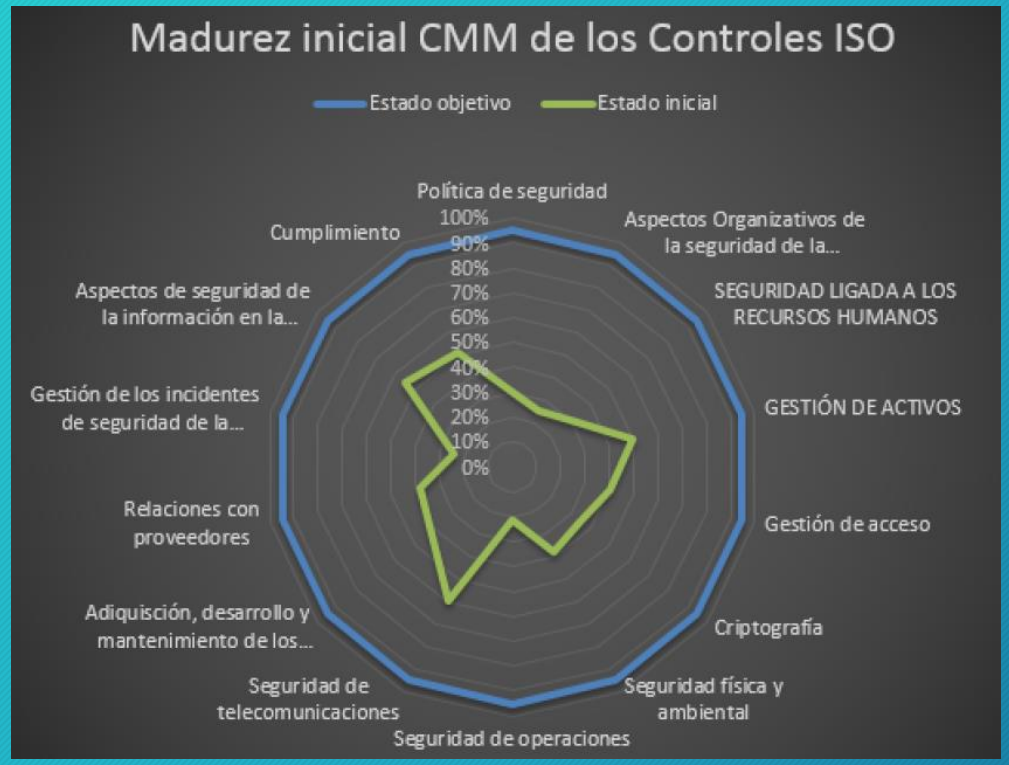
Presentación de resultados

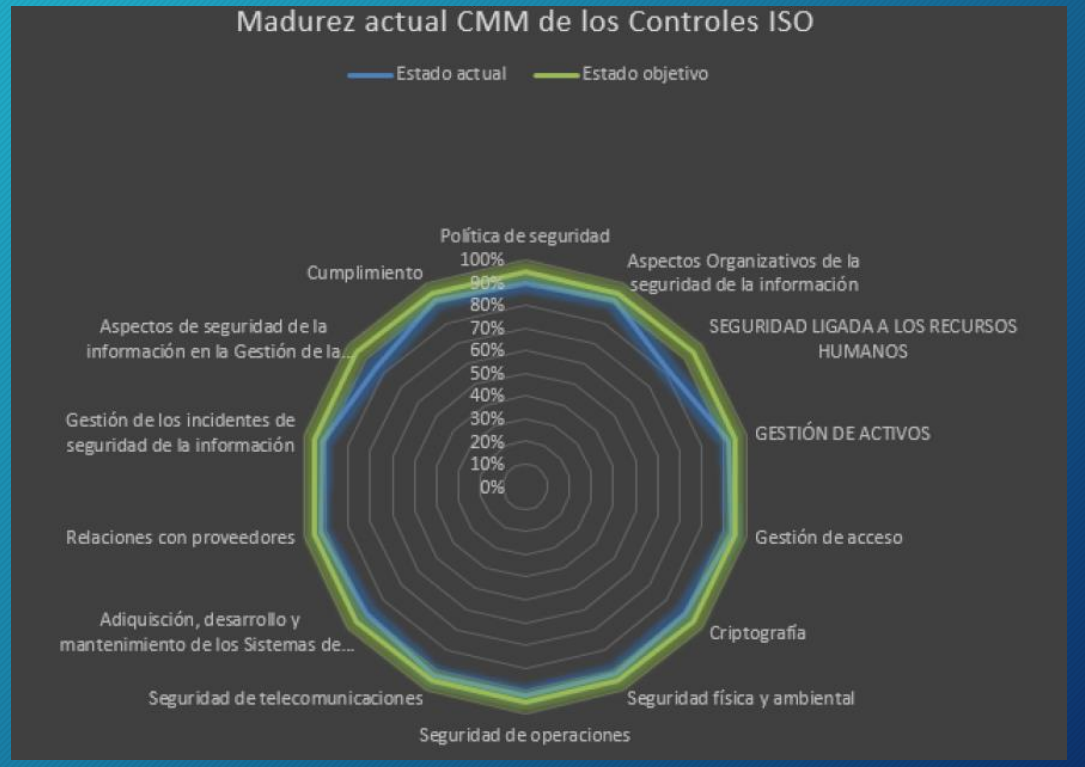
- De forma gráfica podemos presentar los resultados de la evaluación de la madurez de los controles de la norma ISO/IEC 27002:2013



Presentación de resultados

- El gráfico siguiente muestra la evolución de la madurez de los controles desde el estado inicial hasta el estado actual:



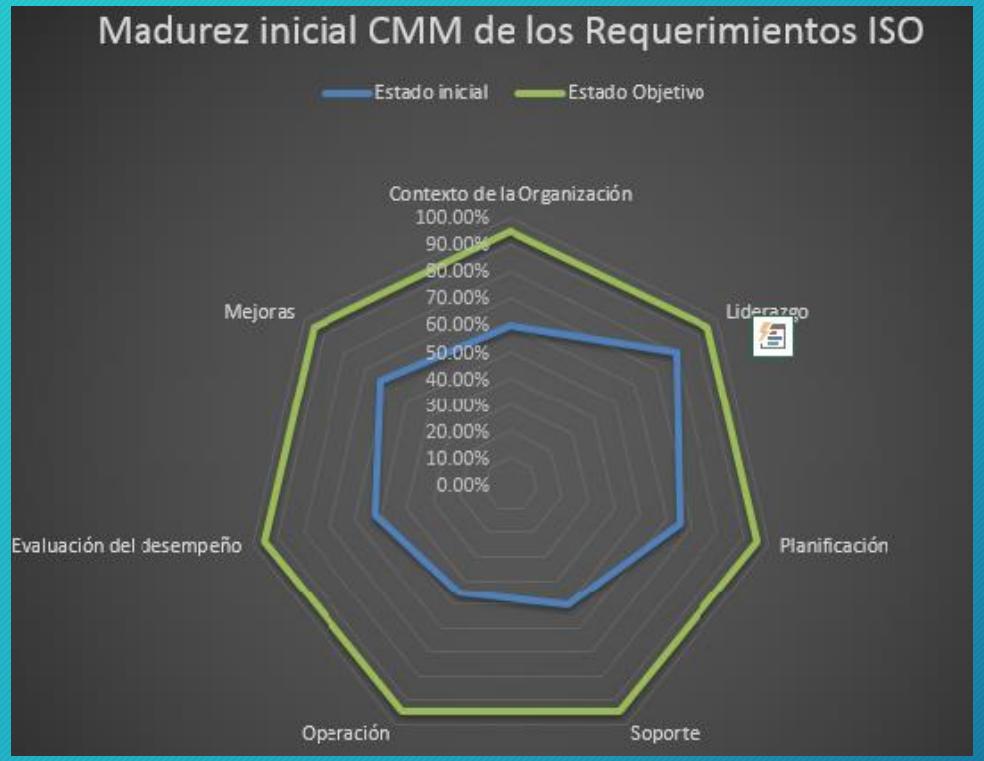


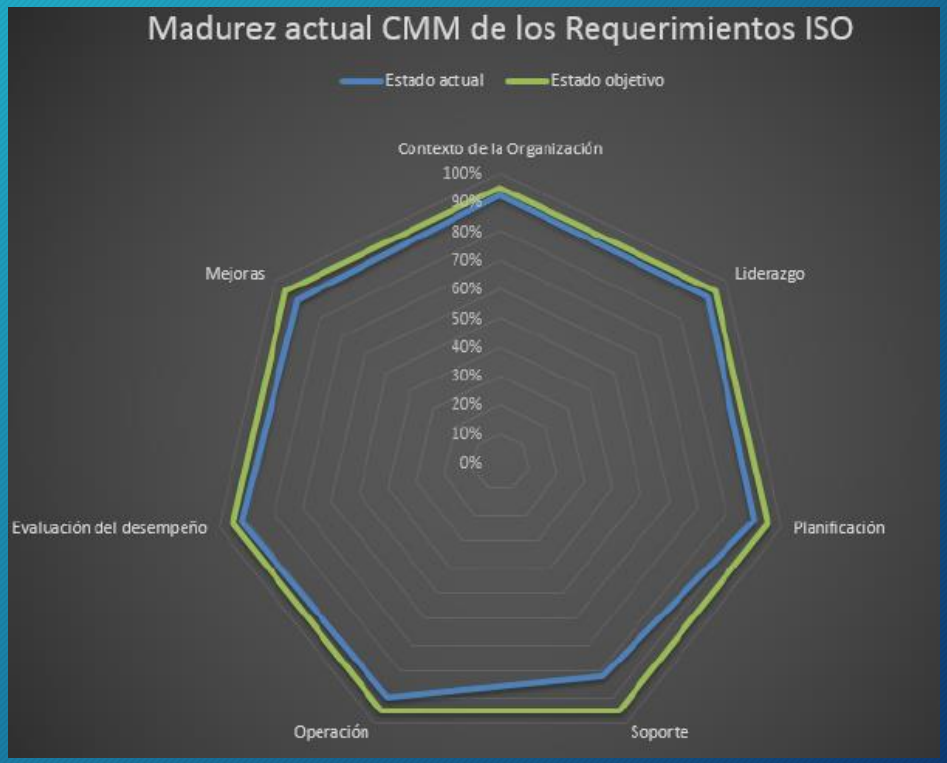
Presentación de resultados

- De forma gráfica podemos presentar los resultados de la evaluación de la madurez de los requerimientos de la norma ISO/IEC 27001:2013

Presentación de resultados

- El gráfico siguiente muestra la evolución de la madurez de los requerimientos desde el estado inicial hasta el estado actual:





Resumen de anexos

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

Conclusiones

- Mariscos S. A. requería necesariamente de la implementación de un SGSI para solventar sus deficiencias de seguridad de la información.
- El SGSI se ha implementado con gran éxito, los resultados obtenidos demuestran que la seguridad ha levantado muy considerablemente su nivel.
- El SGSI estaría listo para superar una auditoría de certificación ISO/IEC 27001:2013 dentro de aproximadamente 6 meses, tiempo en el que el personal empezará a acostumbrarse a cumplir con las medidas de seguridad de forma rutinaria.

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-deseguridad-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-LADIRECCION.ashx
- [11] http://administracionelectronica.gob.es/
- [12] http://www.pmg-ssi.com/2013/12/iso27001-origen/
- [13] www.normalizacion.gob.ec

Gracias