Universitat Autònoma de Barcelona

UOC www.uoc.edu

Universitat Rovira i Virgili

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Plan Director de Seguridad de la Información

Alumno: Christian Daniel Ventura Ferreras.
Consultor: Antonio José Segovia Henares.

Contenido

1. Descripción de la Organización y Entorno
2. Motivación, Enfoque y Alcance
3. Requisitos del SGSI
4. Aspectos Organizativos y Participantes
5. Inventario y valoraciones de Dimensiones de Activos
6. Controles que no aplican
7. Plan de Tratamiento de Riesgos
8. Análisis de Riesgos del SGSI
9. Metodología y Evaluación de la Madurez
10. Resultados del Análisis del SGSI
11. Proyecto y Plan de Acción
12. Resultados del Proyecto en la Seguridad del SGSI
13. Conclusiones

1. Descripción de la Organización y Entorno

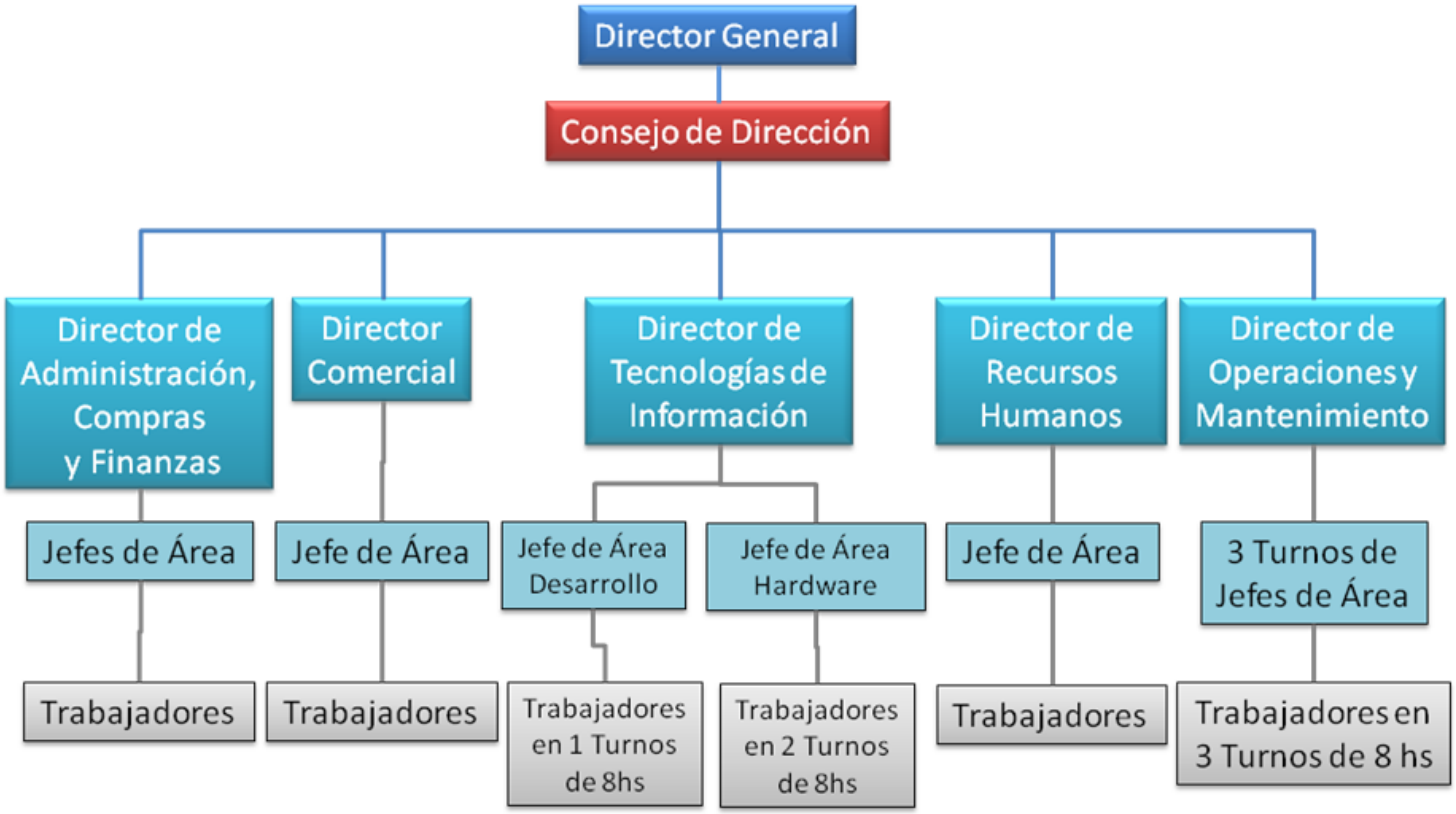
- Terminal Portuaria Multinacional de Carga y Descarga de Contenedores y Carga Suelta situada en Barcelona, España, miembro del mayor conglomerado mundial de operadores portuarios con base en Hong Kong.






1. Descripción de la Organización y Entorno

- A continuación se detalla el organigrama simplificado que muestra la estructura organizativa de las áreas de la terminal portuaria.
- El Consejo de Dirección es conformado por todos los Directores de Áreas.



2. Motivación, Enfoque y Alcance

El Consejo de Dirección establece para toda la organización:

- Motivación:
  - Crear una ventaja competitiva que posicione a la organización delante de sus competidores de mercado.
  - Que los servicios informáticos ofrecidos a través de Internet puedan ser gestionadas adecuadamente.
  - Fortalecer la relación de confianza entre el cliente, proveedores y la terminal.
  - Implementar los más altos estándares Internacionales en materia de Seguridad de la Información en todos los Procesos y Servicios que afecten a las operaciones portuarias.
  - Realizar una correcta gestión de los recursos técnicos, humanos, económicos y organizativos.
  - Minimizar el impacto de las posibles amenazas que la organización posee.
  - Garantizar la correcta gestión de la Continuidad del Negocio.
- Enfoque:

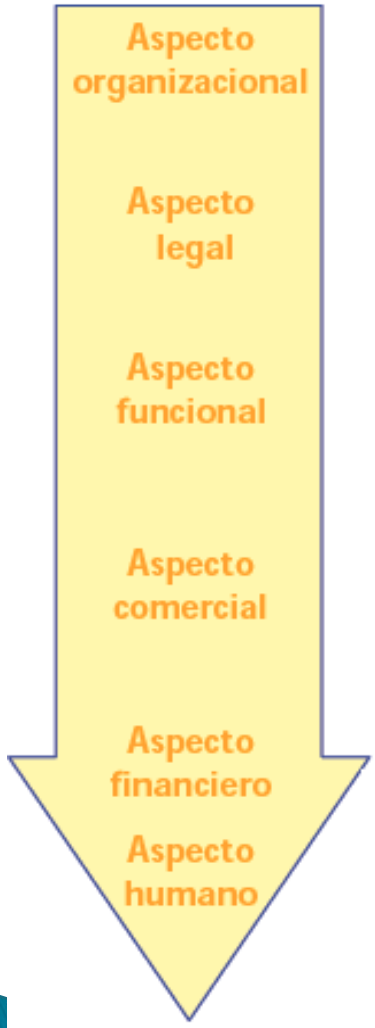
Se realizará un acercamiento progresivo y programado para lograr la implementación y posterior certificación de la norma internacional UNE-ISO/IEC 27001:2007– Seguridad de la Información (Organización Internacional de Normalización y Comisión Electrotécnica Internacional).

Se ha establecido realizar el “Plan Director de Seguridad de la Información” alineando los procedimientos y normativas internas al principio fundamental del “Sistema de Gestión de la Seguridad de la Información” (SGSI).

- Alcance:

El Consejo de Dirección plantea la aplicación de las normas y procedimientos abarcados en el Plan Director de Seguridad para que sean ejecutados por todo el Personal Interno y Externo de la Compañía y en todos los Sistemas de Información asociados a los procesos y servicios brindados a través de Internet que afecten a las operaciones portuarias.

3. Requisitos del SGSI



Compromiso: demostrar la eficacia y eficacia de los esfuerzos desarrollados para asegurar a la organización en todos sus niveles y probar la diligencia razonable de sus administradores.

Conformidad con **requisitos legales**: el registro permite demostrar que la organización observa todas las leyes y normativas aplicables al alcance.

Gestión de los **riesgos**: obtención de un mejor conocimiento de los sistemas de información, sus debilidades y los medios de protección. Garantiza una mejor disponibilidad de los materiales y datos.

Credibilidad y **confianza**: los socios, los accionistas y los clientes se tranquilizan al constatar la importancia que la organización concede a la protección de la información. Una certificación también puede brindar una diferenciación sobre la competencia y en el mercado.

Reducción de los **costes** vinculados a los incidentes y posibilidad de disminución de las primas de seguro.

Mejora la **sensibilización** del **personal** hacia la seguridad y a sus responsabilidades en la organización.

4. Aspectos Organizativos y Participantes

- Soporte de la Dirección:

  La Dirección de la Organización deberá velar por el cumplimiento del Plan Director de Seguridad de la Información, para lo cual requerirá realizar la asignación de recursos económicos, tecnológicos y humanos para la implementación del Plan asignando recursos económicos en el presupuesto anual, y por sobre todo brindando un claro apoyo al equipo de trabajo y haciendo participar a toda la organización en el proceso.

- Equipo del Proyecto:
  - Gestor del Proyecto:

    Será designado por la Dirección y el Comité de Seguridad de la Información, quien será un miembro de la organización cualificado con las siguientes características:
    - Visión global de la organización.
    - Capacidades de liderazgo y trabajo en equipo.
    - Conocimientos técnicos informáticos para liderar los equipos técnicos.
    - Desempeñará la función de nexo entre la dirección y los miembros del Comité, los Auditores, las áreas y departamentos de la organización en general.
  - Comité de Seguridad de la Información:

    El Comité de Seguridad de la Información, estará formado por miembros de la Dirección, Jefes de Área, Responsables de Departamentos, es decir todo el personal de la organización que tenga responsabilidad, poder de decisión sobre el negocio.

4. Aspectos Organizativos y Participantes

- Equipo del Proyecto:

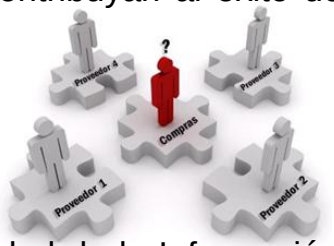

Comité Multidisciplinario de Seguimiento y Soporte del Plan Director

  - Comité Multidisciplinario de Seguimiento y Soporte del Plan Director:

    Se constituirá el Comité Multidisciplinario de Seguimiento y Soporte del Plan Director de Seguridad de la Información, quienes serán miembros clave de la organización que tendrán entre otras la responsabilidad de crear las Políticas, Normas, Procedimientos, Manuales y Otros documentos.

  - Suministradores:

    Las áreas como el departamento de Compras, Administración y Finanzas, serán los encargados de suministrar los productos, servicios en función de las necesidades que surjan durante el ciclo de vida del Plan, del mismo modo los Directores y Jefes de Áreas, desempeñaran la función de facilitadores que contribuyan al éxito del Plan Director de Seguridad de la Información.



  - Otros Actores:

    Las Empresas contratadas para brindar servicios relacionados al Plan Director de Seguridad de la Información, como los proveedores de Internet o ISP, aquellos que brindan suministros de Energía Eléctrica, serán identificadas, reguladas y monitorizadas dentro del alcance del Plan.

5. Inventario y valoraciones de Dimensiones de Activos

- La organización ha realizado una enumeración de los Bienes Relacionados Directa o Indirectamente con la actividad informática de la compañía, así como las Dependencias entre éstos, los mismos son divididos en las siguientes categorías:
  - Instalaciones: Que acogen equipos informáticos y de comunicaciones.
  - Hardware: Equipos Informáticos que permiten almacenar datos, aplicaciones y servicios.
  - Aplicación: Software que permite gestionar los datos almacenados en el hardware.
  - Datos: Elementos imprescindibles para el funcionamiento de la organización.
  - Red: Las Redes de Comunicaciones que permiten intercambiar los datos.
  - Servicios: Los servicios que gestionan los datos a través de las aplicaciones.
  - Equipamiento Auxiliar: El equipamiento que complementa y soporta el equipamiento informático.
  - Personal: El personal que manipula u opera todos los activos identificados.
  - Soporte de Información: Son los dispositivos de almacenamiento de información o datos.

5. Inventario y valoraciones de Dimensiones de Activos

- La Terminal ha realizado una evaluación de cada activo identificado en función de la valoración propuesta en la metodología MAGERIT versión 2 en su libro 2 “Catalogo de Elementos” siendo el valor mas alto el 10 (Daño muy Grave) y el mas bajo 0 (Irrelevante), luego de valorarlos individualmente se ha obtenido un promedio de las dimensiones para conseguir el valor del activo en función de su criticidad, los mismos han sido divididos en las siguientes dimensiones:
  - **Confidencialidad**: Es la propiedad por la que sólo las personas autorizadas tienen acceso a la información sensible y/o privada.
  - **Integridad**: Es la propiedad que asegura que la información y sus métodos de procesamiento son exactos y completos, y no pueden ser manipulados sin autorización.
  - **Disponibilidad**: Es la propiedad de ser accesible y utilizable por una entidad autorizada.
  - **Autenticidad**: Es la garantía de la identidad de los usuarios o procesos que tratan la información, y de la autoría de una determinada acción.
  - **Trazabilidad**: Es la propiedad de reproducir un histórico o secuencia de acciones sobre un determinado proceso y determinar quién ha sido el autor de cada acción.
- **Valoración de Impacto Potencial en la Organización:**

  Planteando el impacto de la materialización de la amenaza de cada activo-amenaza en forma porcentual, con el objetivo de determinar un marco de priorización para establecer las medidas de salvaguardas a implementar en cada activo y en función de la importancia de éstos para la organización.

Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Valor del Activo
Sala de Servidores			10			**10**
Dto. de Tecnología de Información			6			**6**
Sala Eléctrica de UPS y Generador			10			**10**
svr-web	10	10	10	10	10	**10**
svr-email	10	9	9	10	8	**9,2**
svr-ssh	10	7	7	10	10	**8,8**

6. Controles que no aplican

El Comité de Seguridad de la Información conjuntamente con los responsables de las Áreas y miembros claves de la organización han establecido que los siguientes controles no aplican a la compañía.

- Controles que no Aplican a la Organización:

Los siguientes controles detallados a continuación corresponden a los controles de la Norma UNE-ISO/IEC 27002:2009, que agrupa un total de 133 controles o salvaguardas sobre las recomendaciones de buenas prácticas para la Gestión de la Seguridad de la Información organizado en un total de 11 áreas y 39 objetivos de control, identificación de los controles que no aplican en el sistema implementado por la organización.

Control - 10.8 Intercambio de Información:

No se realizan intercambios de información externos con ninguna entidad, salvo los canales normales, como el correo electrónico y los sistemas bancarios, por lo que se excluyen los controles:

- "10.8.1 Políticas y procedimiento de intercambio de información".
- "10.8.2 Acuerdos de Intercambio".
- "10.8.3 Soporte físicos en tránsito".
- "10.8.5 Sistemas de información empresariales".

Control – 10.9 Servicios de Comercio Electrónico:

La organización no realiza transacciones electrónicas de ninguna clase y en ningún formato, por lo que se excluyen los controles:

- "10.9.1 Comercio Electrónico".
- "10.9.2 Transacciones en Línea".

7. Análisis de Riesgos del SGSI

El Análisis de Riesgo es el proceso de identificación de los Riesgos o Amenazas que existen en los activos informáticos identificados para determinar el proceso, impacto en la organización, magnitud, frecuencia e identificar las áreas que requieren medidas de protección o salvaguardas, son agrupados en las categorías: Desastres naturales, De origen industrial, Errores y fallos no intencionados, Ataques intencionados.

Tipos de Análisis de Riesgos:

- **Riesgo intrínseco**: Es el estudio que se realiza sin tener en consideración las diferentes medidas de seguridad que se encuentran implantadas en una organización, la formula utilizada corresponde a: *[Valor activo * Vulnerabilidad * (impacto/100)].*

  El valor total del Riesgo Intrínseco calculado asciende a **€ 38.901,68**.- y corresponde a la sumatoria de todos los valores individuales del riesgo intrínseco por cada activo/amenaza.

- **Riesgo Residual**: Es el riesgo que queda tras la aplicación de las salvaguardas, siempre quedará un riesgo residual puesto que no es posible proteger a los activos un 100% y es el riesgo que la organización deberá asumir y vigilar.

- **Riesgo Efectivo**: Es el estudio que se realiza teniendo en consideración las diferentes medidas de seguridad que se encuentran implantadas en una organización.

  El Riesgo Efectivo establece una disminución de **€ 34.628,50**.- sobre el Riesgo Intrínseco, valorando el Riesgo Efectivo en un total de **€ 4.273,18**.-

AMENAZA	ACTIVO	IMPACTO POTENCIAL %	Valor del Activo	Frecuencia de Amenaza			Frecuencia Diaria de la Vulnerabilidad	Riesgo Intrínseco
				Día	Mes	Año		
[A.4] Manipulación de la configuración	svr-web	100	€ 2.000,00		1		0,033	€ 66,67
	svr-email	100	€ 1.500,00		1		0,033	€ 50,00
	svr-ssh	70	€ 1.000,00		2		0,067	€ 46,67
	svr-fw-dmz	90	€ 900,00		2		0,067	€ 54,00
	svr-fw-int	90	€ 900,00		3		0,100	€ 81,00
	svr-sql	90	€ 1.300,00		1		0,033	€ 39,00
	svr-antv	70	€ 1.100,00		1		0,033	€ 25,67
	svr-ids	90	€ 1.000,00		1		0,033	€ 30,00
	svr-bck	70	€ 1.100,00		1		0,033	€ 25,67
	Ordenadores	50	€ 700,00		2		0,067	€ 23,33
	Switch Comunicaciones	90	€ 1.300,00		1		0,033	€ 39,00
	Router Internet	90	€ 700,00			4	0,011	€ 6,90
	Central Telefónica	90	€ 2.500,00		1		0,033	€ 75,00
	Sistemas de Backup:	80	€ 600,00		1		0,033	€ 16,00
	Windows Servers 2003	90	€ 400,00		1		0,033	€ 12,00
	Linux Ubuntu Servers versión 11.10 (Oneiric Ocelot)	90	€ 300,00		1		0,033	€ 9,00

8. Plan de Tratamiento de Riesgos

El Comité de Seguridad de la Información conjuntamente con los responsables de las Áreas y miembros claves de la organización han establecido las medidas de protección, salvaguardas o contramedidas que se implementarán por cada activo/amenaza en función del impacto potencial porcentual que tiene la materialización de la amenaza si se materializara que ha sido detallado anteriormente, tomando como referencia la metodología MAGERIT en su Versión 2, la clasificación realizada corresponde a las siguientes categorías de amenazas:

- [N] Desastres naturales.
- [I] De origen industrial.
- [E] Errores y fallos no intencionados.
- [A] Ataques intencionados.

9. Metodología y Evaluación de la Madurez

- Metodología de Análisis del Estado de Madurez del SGSI:

  La metodología utilizada para el análisis de Madurez del Sistema de Gestión de Seguridad de la Información o SGSI corresponde al Modelo de Madurez de la Capacidad (CMM) en el que se utiliza una escala de 0 a 100, en donde el 0% corresponde a la Inexistencia de madurez y el 100% a la Optimización de los procesos maduros.

- Evaluación de la Madurez:

  La evaluación se ha realizado tomando como referencia el estándar Internacional de la Norma UNE-ISO/IEC 27001:2007, que agrupa un total de 133 controles o salvaguardas sobre las recomendaciones de buenas prácticas para la Gestión de la Seguridad de la Información organizado en un total de 11 áreas y 39 objetivos de control, así como los controles descriptos en la norma UNE-ISO/IEC 27002:2009.

  La estimación fue efectuada tomando como fuente de información y evidencia los documentos mas relevantes de los procesos de negocio y el relevamiento in-situ realizado en las oficinas de la organización, la clasificación realizada corresponde a las siguientes categorías de amenazas:

  - [N] Desastres naturales.
  - [I] De origen industrial.
  - [E] Errores y fallos no intencionados.
  - [A] Ataques intencionados.

AMENAZA	ACTIVO	IMPACTO POTENCIAL	Salvaguarda o Contramedida	Objetivos de Control norma UNE-ISO/IEC 27002:2009	Grado de Madurez CMM %
[A.4] Manipulación de la configuración	svr-web	10	Se restringirá el uso de la cuenta de Administrador de los servidores a solo algunas cuentas de usuarios autorizados del Dto. de TI. Se realizarán Auditorías Periódicas para el control de los procedimientos implementados. Se realizarán Auditorías Periódicas para el control de los procedimientos implementados.	A.11.1.1 Política de Control de Acceso	90
	svr-email	10			
	svr-ssh	7			
	svr-fw-dmz	9		A.11.2.2 Gestión de Privilegios	70
	svr-fw-int	9			
	svr-sql	9	No se utilizará la cuenta de Administrador, se les asignarán el rol a los usuarios autorizados.	5.1.1 Documento de política de seguridad de la información	90
	svr-antv	7			
	svr-ids	9	Los Empleados del Dto. de Tecnología de Información firmaran una Política de TI, en la que se especificará que se realizará un las tareas administrativas según las mejores prácticas de los estándares internacionales y se dará buen	7.1.3 Uso aceptable de los activos	90
	svr-bck	7			
	Ordenadores Escritorio/Portátiles y Teléfonos Móviles	5	Los usuarios no poseerán privilegios que le permita realizar modificaciones en las configuraciones o sistemas, esta tarea será reservada exclusivamente a los Administradores del dto. de TI.	11.2.2 Gestión de privilegios	70
	Switch Comunicaciones	9	Se restringirá el uso de la cuenta de Administrador de los equipos de Comunicaciones solo algunas cuentas de usuarios autorizados del Dto. de TI.	A.11.1.1 Política de Control de Acceso	90
	Router Internet	9			
	Central Telefónica	9			
			Se restringirá el uso de la cuenta de Administrador de los servidores a solo algunas	A.11.1.1 Política de Control de Acceso	90

10. Resultados del Análisis del SGSI

- Resultados de la Evaluación de Madurez del SGSI:

  Los resultados obtenidos de la evaluación de la madurez del Sistema de Gestión de Seguridad de la Información han sido alcanzados luego de la auditoria documental y presencial realizada el 28 de Diciembre de 2012, enfocando los mismos sobre las amenazas detectadas que afectan a los activos, el análisis se ha realizado con la metodología del Modelo de Madurez de la Capacidad (CMM) en función de cada control implementado de la norma UNE-ISO/IEC 27002:2009.

- Hallazgos Observados:
  - Los activos "**Código Fuente Programas**" y "**Desarrollo Interno: Pagina Web, Formularios de Internet**" para la amenaza **"[A.4] Manipulación de la configuración**":
    - No existe una buena **Gestión de Privilegios**.
    - No se realiza **Restricción de Acceso** a la información para Desarrolladores.
    - No se efectúa un **Control de Acceso al Código Fuente** de los Programas ni el **Control de Cambios**.
  - El control "**12.4.3 Control de acceso al código fuente de los programas**", de los activos "**Código Fuente Programas**" y "**Desarrollo Interno: Pagina Web, Formularios de Internet**":
    - Los Desarrolladores internos posee **Privilegios** para efectuar **Cambios en el Servidor de Producción**.
  - Los controles "**12.2.2 Control del procesamiento interno**", en la amenaza "**[E.18] Destrucción de la información**" y en el control "**10.1.3 Segregación de tareas**":
    - El personal del área de Desarrollo, posee **Privilegios** sobre los **Servidores Principales** que les permiten realizar **Modificaciones y Cambios de Versiones** sobre las aplicaciones de Internet y en el código fuente.
    - Riesgo de **destrucción de la información**.
    - No se realiza una correcta **separación de funciones** y tareas del personal de Desarrollo.
  - Los activos "**Red de Datos: Ethernet**", "**Red de Telefonía fija: PABX**", "**Fibra Óptica - Internet**".
    - No existe un **proveedor alternativo** ante la caída del servicio de **Internet o Telefonía Fija**, siendo estos servicios esenciales para el normal funcionamiento de la terminal portuaria

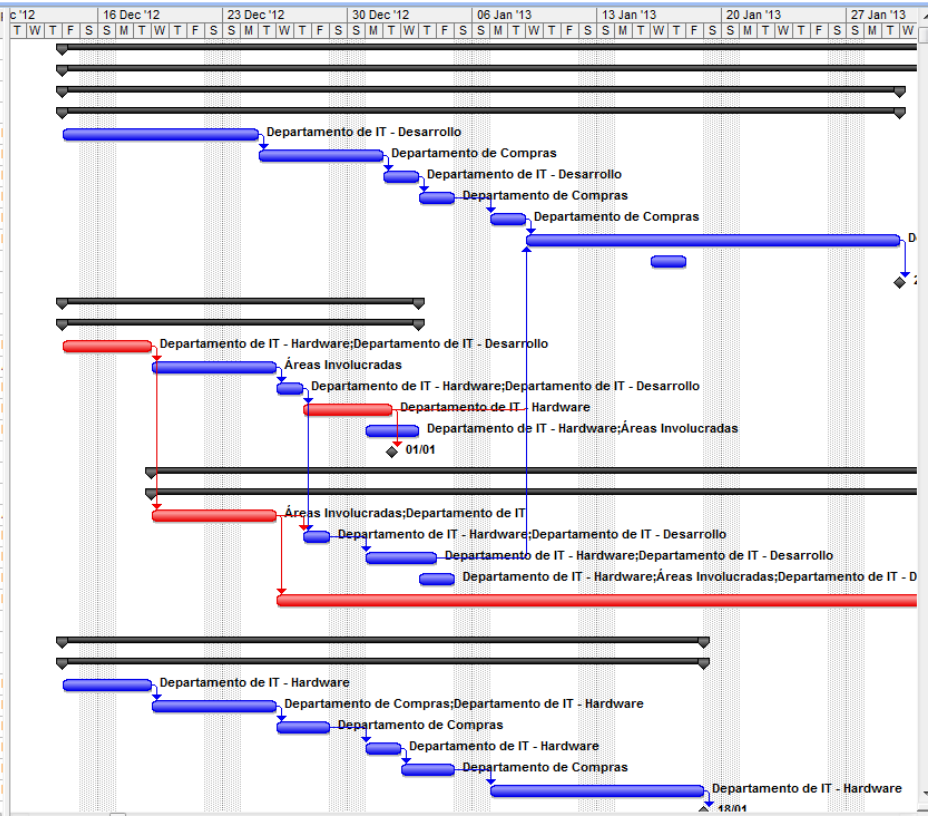
11. Proyecto y Plan de Acción

- El presente proyecto SGSI tiene una estimación de **35 días duración**, iniciando el viernes 14 de diciembre y finalizando el 05 de Febrero de 2013, con un costo total de **€ 17.944,00** en horas de trabajo por parte del personal de las áreas involucradas, siendo necesario agregar a este importe a los productos y/o servicios contratados, así como los posibles contratos de mantenimiento y asistencia técnica o nivel de servicios.

- Las fases propuestas son cuatro y están divididas en las siguientes etapas:
  - Fase 1 – Workflow para el Control de Cambios de Código Fuente
  - Fase 2 – Gestión de Privilegios
  - Fase 3 – Segregación de Tareas
  - Fase 4 – Proveedores Alternativos para los servicios de Internet y la PABX

F1 - Workflow Control Cambios Cód. Fuente

	Task Name	Duration	Start	Finish	Predeces	Cost
1	**Proyecto SGSI**	**38 days**	**Fri 14/12/12**	**Tue 05/02/13**		**$17.944,00**
2	**Inicio Proyecto**	**38 days**	**Fri 14/12/12**	**Tue 05/02/13**		**$17.944,00**
3	**F1 - Workflow Control Cambios Cód. Fuente**	**33 days**	**Fri 14/12/12**	**Tue 29/01/13**		**$3.384,00**
4	**F1 - Inicio**	**33 days**	**Fri 14/12/12**	**Tue 29/01/13**		**$3.384,00**
5	Búsqueda de Herramientas de Control de Cambio	7 days	Fri 14/12/12	Mon 24/12/12		$672,00
6	Solicitud de Presupuestos	5 days	Tue 25/12/12	Mon 31/12/12	5	$400,00
7	Selección del Producto	2 days	Tue 01/01/13	Wed 02/01/13	6	$192,00
8	Realización del pedido de Compras	2 days	Thu 03/01/13	Fri 04/01/13	7	$160,00
9	Compra del Producto	2 days	Mon 07/01/13	Tue 08/01/13	8	$160,00
10	Implementación del Producto	15 days	Wed 09/01/13	Tue 29/01/13	9;18;25	$1.800,00
11	Control de Implementación del Producto	2 days	Wed 16/01/13	Thu 17/01/13		$0,00
12	F1 - Fin	0 days	Tue 29/01/13	Tue 29/01/13	10	$0,00
13	**F2 - Gestión Privilegios**	**14 days**	**Fri 14/12/12**	**Wed 02/01/13**		**$2.400,00**
14	**F2 - Inicio**	**14 days**	**Fri 14/12/12**	**Wed 02/01/13**		**$2.400,00**
15	Relevamiento de Usuarios/Privilegios	3 days	Fri 14/12/12	Tue 18/12/12		$576,00
16	Solicitud de Requerimiento de Servicios y Privilegios a las Áre	5 days	Wed 19/12/12	Tue 25/12/12	15	$600,00
17	Creación de Roles y Asignación de Privilegios	1,5 days	Wed 26/12/12	Thu 27/12/12	16	$288,00
18	Implementación de Requerimientos de Servicios y Privilegios	3 days	Thu 27/12/12	Tue 01/01/13	17	$288,00
19	Control de Implementación de Req. de Serv. Y Priv.	3 days	Mon 31/12/12	Wed 02/01/13		$648,00
20	F2 - Fin	0 days	Tue 01/01/13	Tue 01/01/13	18	$0,00
21	**F3 - Segregación de Tareas**	**35 days**	**Wed 19/12/12**	**Tue 05/02/13**		**$9.360,00**
22	**F3 - Inicio**	**35 days**	**Wed 19/12/12**	**Tue 05/02/13**		**$9.360,00**
23	Solicitud de Requerimiento de Puesto/Función	5 days	Wed 19/12/12	Tue 25/12/12	15	$1.200,00
24	Creación de Roles y Responsabilidades	1,5 days	Thu 27/12/12	Fri 28/12/12	23;17	$288,00
25	Implementación de Restricciones por Puesto	4 days	Mon 31/12/12	Thu 03/01/13	24	$768,00
26	Control de Restricciones por Puesto	2 days	Thu 03/01/13	Fri 04/01/13		$624,00
27	Formación y Capacitación	30 days	Wed 26/12/12	Tue 05/02/13	23	$6.480,00
28	F3 - Fin	0 days	Tue 05/02/13	Tue 05/02/13	27	$0,00
29	**F4 - Proveedores Alternativos Internet/PABX**	**26 days**	**Fri 14/12/12**	**Fri 18/01/13**		**$2.800,00**
30	**F4 - Inicio**	**26 days**	**Fri 14/12/12**	**Fri 18/01/13**		**$2.800,00**
31	Especificaciones Técnicas de los Servicios	3 days	Fri 14/12/12	Tue 18/12/12		$288,00
32	Relevamiento de Proveedores Alternativos	5 days	Wed 19/12/12	Tue 25/12/12	31	$880,00
33	Solicitud de Presupuestos	3 days	Wed 26/12/12	Fri 28/12/12	32	$240,00
34	Selección de Proveedores	2 days	Mon 31/12/12	Tue 01/01/13	33	$192,00
35	Contratación del Servicio	3 days	Wed 02/01/13	Fri 04/01/13	34	$240,00
36	Implementación y puesta a punto	10 days	Mon 07/01/13	Fri 18/01/13	35	$960,00
37	F4 - Fin	0 days	Fri 18/01/13	Fri 18/01/13	36	$0,00

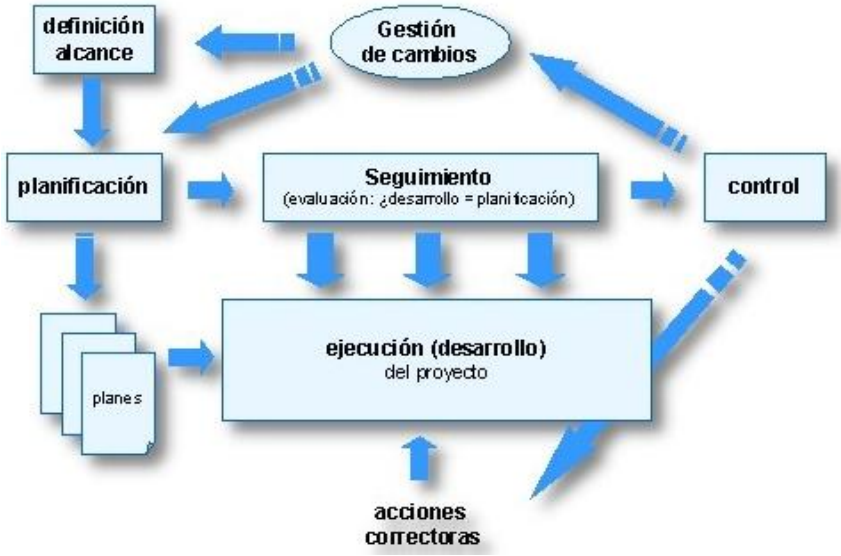


11. Proyecto y Plan de Acción

- Hallazgos Observados:
  - Se ha detectado que los activos "**Código Fuente Programas**" y "**Desarrollo Interno: Pagina Web, Formularios de Internet**" para la amenaza **"[A.4] Manipulación de la configuración**" que no existe una buena gestión de privilegios, así como restricción del acceso a la información y un buen control de acceso al código fuente de los programas, ya que no se establece un mecanismo que impida realizar el control de cambios de manera jerárquica y sistemática.
  - **Fase 1 – Workflow para el Control de Cambios de Código Fuente**:

    Esta fase tiene una estimación de treinta y tres días de duración, iniciando el viernes 14 de diciembre y finalizando el 29 de Enero de 2013, con un costo total de **€ 3.384,00** en horas de trabajo por parte del personal de las áreas involucradas, siendo necesario agregar a este importe el/los producto/s comprado/s.

- Áreas Involucradas:
  - Departamento de IT – Desarrollo.
  - Departamento de Compras.
- Tareas:
  - Búsqueda de Herramientas de Control de Cambio.
  - Solicitud de Presupuestos
  - Selección del Producto
  - Realización del pedido de Compras
  - Compra del Producto
  - Implementación del Producto
  - Control de Implementación del Producto



11. Proyecto y Plan de Acción

○ Fase 1 – Workflow para el Control de Cambios de Código Fuente:

- Alcance:

La presente fase del proyecto plantea un alcance abarcado en el Departamento de Tecnología de Información, específicamente para el área de Desarrollo con soporte del Área de Hardware.

- Objetivos:

Implementar de un Software que permita realizar el Control de Cambios del Código Fuente, con las siguientes características:

- Realizar un correcto control de cambios.
- Realizar un flujograma de autorización jerárquico de manera centralizada.
- Visualizado históricamente.
- Saber todos y cada uno de los cambios realizados.
- Conocer la persona autorizada para realizar el cambio, otorgando una “trazabilidad” que en la actualidad no existe.
- Mejor control de las nuevas versiones y una optimización de recursos técnicos y humanos
- Proporcionar “Integridad”, “Disponibilidad”, “Confidencialidad”, “Autenticación” y “Trazabilidad” en cada nueva versión.
- Permitir realizar Auditorias y servir como evidencia ante auditorías externas.
- Se podrían generar indicadores de evolución que permitan ver los progresos que se han obtenido al implementar la misma.

11. Proyecto y Plan de Acción

- Hallazgos Observados:
  - Se ha observado que para el control "**12.4.3 Control de acceso al código fuente de los programas**", los desarrolladores internos de la organización posee autorización y privilegios para efectuar cambios en el servidor de producción sobre los activos "**Código Fuente Programas**" y "**Desarrollo Interno: Pagina Web, Formularios de Internet**".

- **Fase 2 – Gestión de Privilegios:**

La fase tiene una estimación de catorce días de duración, iniciando el viernes 14 de diciembre y finalizando el 02 de Enero de 2013, con un costo total de **€ 2.400,00** en horas de trabajo por parte del personal de las áreas involucradas.

- Áreas Involucradas:
  - Departamento de IT – Desarrollo y Hardware.
  - Todas las Áreas y Departamentos de la Organización.

- Tareas:
  - Relevamiento de Usuarios/Privilegios.
  - Solicitud de Requerimiento de Servicios y Privilegios a las Áreas.
  - Creación de Roles y Asignación de Privilegios.
  - Implementación de Requerimientos de Servicios y Privilegios.
  - Control de Implementación de Requerimientos de Servicios y Privilegios.

11. Proyecto y Plan de Acción

○ Fase 2 – Gestión de Privilegios:

- Alcance:

Esta fase plantea la necesidad de gestionar adecuadamente los privilegios de todos los sistemas de información de la organización en forma centralizada de todos los usuarios involucrados en el alcance.

- Objetivos:

Realizar la confección y revisión anual de la planilla de “Servicios y Privilegios” para toda la terminal, especificando el Rol y Privilegios del usuario, si posee acceso, permiso de modificación, escritura, lectura y borrado a los siguientes Ítems:

- Correo Electrónico.
- Acceso a Internet por Proxy/NAT.
- Sistemas Operativo de la Terminal.
- Sistemas de Desarrollo y Código Fuente.
- Acceso a la lectora de CD/DVD/USB.
- Carpetas Publicas/Privadas/Confidenciales.
- Gestionar de forma centralizada y correcta la administración de los privilegios que cada usuario posee.
- Solo los usuarios autorizados puedan acceder, modificar o borrar cierta información.
- Permite asegurar la “Integridad”, “Disponibilidad”, “Confidencialidad” y “Autenticación” de la información.

La confección de la planilla de “Servicios y Privilegios” permitirá:

- Que los jefes de área especifiquen de una forma clara y precisa que permisos deberían poseer cada usuario a su cargo en el sistema.
- Permitirá ser revisada al menos una vez al año o cuando el usuario cambie de tarea o deje de pertenecer a la organización.
- Las planillas servirán como evidencia ante posibles incidentes o ante auditorías internas o externas, para demostrar que existe una correcta gestión de privilegios y permisos en el sistema.

11. Proyecto y Plan de Acción

- Hallazgos Observados:
  - Se ha constatado que el personal del área de Desarrollo, posee privilegios sobre los servidores principales que les permiten realizar modificaciones y cambios de versiones sobre las aplicaciones de Internet y en el código fuente, haciendo posible la destrucción de la información que afecta a los controles "**12.2.2 Control del procesamiento interno**", algo similar sucede en la amenaza "**[E.18] Destrucción de la información**" en el control "**10.1.3 Segregación de tareas**"; ya que no se realiza una apropiada separación de funciones y tareas del personal de desarrollo.

- **Fase 3 – Segregación de Tareas:**

  Esta fase está estimada con una duración de treinta y dos días, iniciando el miércoles 19 de diciembre y finalizando el 05 de Febrero de 2013, con un costo total de **€ 9.360,00** en horas de trabajo por parte del personal de las áreas involucradas, incluyendo las horas de formación que deberán recibir el personal de cada área, sin incluir a ésta el costo del curso si fuese el caso de formación por parte de empresas externas.

- Áreas Involucradas:
  - Departamento de IT – Desarrollo y Hardware.
  - Todas las Áreas y Departamentos de la Organización.

- Tareas:
  - Solicitud de Requerimiento de Puesto/Función a las áreas.
  - Creación de Roles y Responsabilidades.
  - Implementación de Restricciones por Puesto.
  - Control de Restricciones por Puesto.
  - Formación y Capacitación.

11. Proyecto y Plan de Acción

○ Fase 3 – Segregación de Tareas:

- Alcance:

Realización de la segregación de tareas y funciones que permitirá una correcta gestión de los recursos humanos, técnicos y organizativos dentro de toda la organización.

- Objetivos:

Realizar la confección de la planilla de “Puestos y Funciones”, para alcanzar una correcta separación de Funciones y Tareas de toda la Terminal, buscando alcanzar los siguientes objetivos:

- Eliminar el solapamiento de tareas y funciones.
- Detectar errores o fraude, voluntario o involuntario.
- Desarrollar perfiles de Puestos y Funciones específicos para cada tarea.
- Detectar las necesidades de habilidades técnicas, humanas u operativas, identificando las necesidades de formación.
- Realizar proyecciones anuales para que puedan ser incluidas en el presupuesto anual.
- Realizar la correcta gestión de los recursos humanos, técnicos y organizativos dentro de la organización.
- Mejorar el control interno de los desarrollos, tareas y funciones de todo el personal.
- La identificación de las necesidades permitirá la contrastación de las mismas con los perfiles existentes en la organización; ya que si se diera una vacante en algún puesto, el perfil puede ser contrastado con los existentes.
- Realizar búsquedas internas que cubran las necesidades, brindando posibilidades de progreso en las carreras profesionales de los empleados, o de lo contrario realizar búsquedas externas ya con un perfil claramente definido.
- Podrán ser utilizadas como evidencia ante auditorias, así como los planes de formación y capacitación al poder ser contrastados con las necesidades de los puestos y funciones.

11. Proyecto y Plan de Acción

- Hallazgos Observados:
  - Se ha relevado los proveedores del servicio de comunicaciones de Internet, telefonía fija y se ha detectado que no posee un proveedor alternativo ante la caída del servicio, siendo estos servicios esenciales para el normal funcionamiento de la organización, los activos afectados son "**Red de Datos: Ethernet**", "**Red de Telefonía fija: PABX**", "**Fibra Óptica - Internet**".

- **Fase 4 – Proveedores Alternativos para los servicios de Internet y la PABX:**

  La fase fue estimada con una duración de veintiséis días, iniciando el viernes 14 de diciembre y finalizando el 18 de Enero de 2013, con un costo total de **€ 2.800,00** en horas de trabajo por parte del personal de las áreas involucradas, siendo necesario agregar a este importe a los productos y/o servicios contratados, así como los posibles contratos de mantenimiento y asistencia técnica o SLA.

- Áreas Involucradas:
  - Departamento de IT – Hardware.
  - Departamentos de Compras.

- Tareas:
  - Especificaciones Técnicas de los Servicios.
  - Relevamiento de Proveedores Alternativos.
  - Solicitud de Presupuestos.
  - Selección de Proveedores.
  - Contratación del Servicio.
  - Implementación y puesta a punto.

11. Proyecto y Plan de Acción

○ Fase 4 – Proveedores Alternativos para los servicios de Internet y la PABX:

- Alcance:

La búsqueda de proveedores alternativos para los servicios de Internet y telefonía fija, que asegurarán la correcta gestión de la continuidad del negocio y contingencia, ya que la organización posee una clara dependencia de estas tecnologías, la utilización de medios electrónicos de comunicación, el teléfono o el fax, al mismo tiempo que brinda servicios a sus clientes a través de Internet .

- Objetivos:

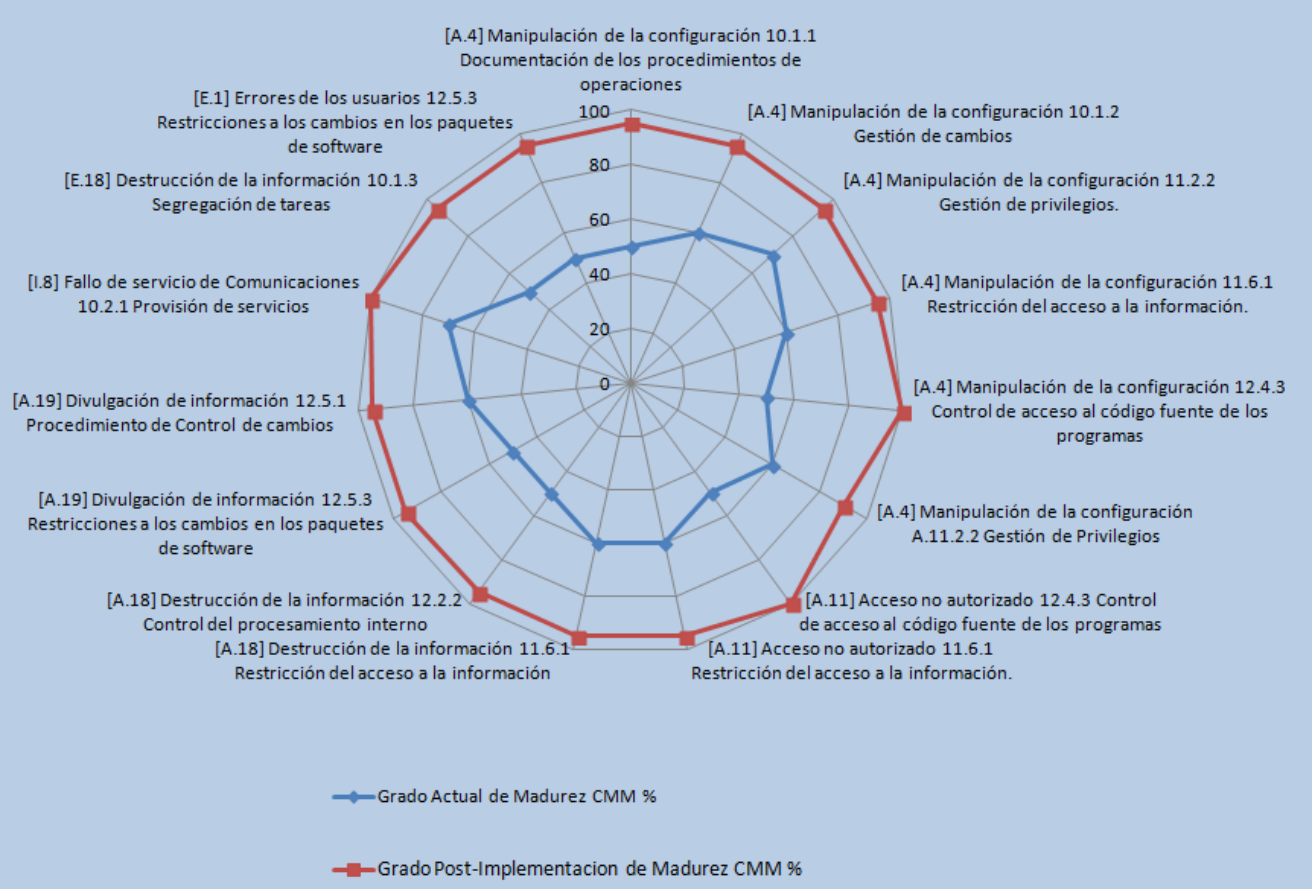
Realizar la implementación de sistemas redundantes para la telefonía fija e Internet, buscando alcanzar los siguientes objetivos:

- Gestionar el Plan de Contingencia y Continuidad de Negocio para minimizar el impacto potencial de la falta de estos servicios, y garantizar que la organización pueda estar conectada con sus clientes y proveedores en forma permanente.
- Implementar sistemas redundantes para telefonía fija e Internet.
- Garantizar los servicios ante fallas, roturas o destrucción.
- Gestionar los Costos de la Telefonía Fija al realizar ruteos en función del costo de la llamada y el destino.
- Cubrir las necesidades de utilización de medios electrónicos de comunicación como el correo electrónico son fundamentales a la hora de establecer acuerdos comerciales, así como los tradicionales sistemas de comunicaciones como el teléfono o el fax.
- La implementación de sistemas redundantes y al mismo tiempo por caminos diferentes o tecnologías diferentes, en el caso de sistemas inalámbricos, por ejemplo, permite garantizar que si existiera una falla, rotura, o destrucción de uno de los sistemas la empresa podría seguir funcionando realizando unos pequeños cambios en forma semiautomática o automática.
- Realizar una correcta gestión de costos de las llamadas, al poder implementar sistemas múltiples de enrutamiento, permitiendo elegir en forma automática o no el proveedor más económico o de mejor calidad.

12. Resultados del Proyecto en la Seguridad del SGSI

- Resultados Observados:

  El presente gráfico, corresponde a la representación gráfica de la evolución en el grado de madurez luego de la implementación de cada fase del proyecto SGSI, que está alineada con el análisis de impacto y los objetivos de madurez de la seguridad requeridos por la organización.



13. Conclusiones

- Generales:

La implementación de estas mejoras en el Sistema de Gestión de Seguridad de la Información permitirá alcanzar los niveles de madurez fijados por la organización, al mismo tiempo que permitirá un mayor acercamiento para realizar la Certificación del SGSI mediante la norma UNE-ISO/IEC 27001:2007.

Por otra parte, las medidas de seguridad propuestas facilitarán y mejorarán los resultados de las auditorias internas y externas, ya sean técnicas, documentales u operacionales, al contar con evidencias claras de una correcta gestión de la seguridad.

Asimismo, como se puede visualizar en el gráfico antes mostrado, luego de la implementación de los planes de mejoras se han alcanzado niveles de madurez óptimos permitiendo una evolución del sistema y su seguridad, demostrando el progreso que permite minimizar el riesgo y el impacto de la materialización de las amenazas encontradas durante el análisis de riesgos.

Esta evolución permitirá una retroalimentación del sistema en el ciclo de “Deming” y su seguridad que podrá ser analizada para identificar el nivel de cumplimiento de los diferentes dominios de control de la norma UNE-ISO/IEC 27002:2009, como parte de un ciclo iterativo, este análisis de la evolución deberá repetirse en forma periódica y sistemática para asegurar que los controles o salvaguardas siguen siendo efectivos y no se producen desviaciones, nuevas amenazas o cambios en el contexto o en los objetivos de la organización.

La implementación de los planes y las medidas de seguridad permitirán una reducción de costos al contar con sistemas mas seguros que impidan la materialización de las amenazas optimizando los recursos y evitando solapamientos de funciones, así como el fortalecimiento de la relación con el cliente, los accionistas y proveedores.

13. Conclusiones