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

Resumen Ejecutivo

Plan Director de Seguridad de la Información

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

2012

Índice

1. Plan Director de Seguridad

1.1 Descripción de la Organización de Estudio:

1.2 Actividad y Entorno:

La Organización de estudio del presente Trabajo Final de Máster para la Elaboración de un "Plan de Seguridad de la Información" será una 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.

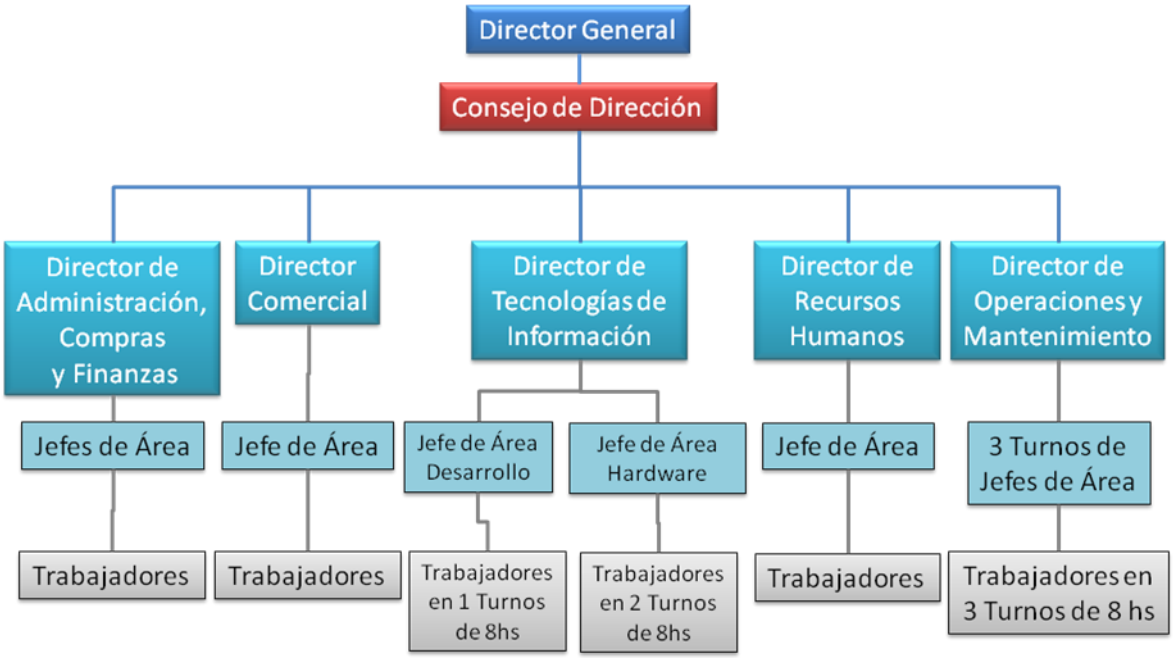
Posee una plantilla estable de 750 trabajadores, mayoritariamente operativos relacionados con las tareas de carga y descarga de los barcos atracados en la Terminal, divididos en tres turnos rotativos de 8 hs cada uno.

Los sectores administrativos como los de "Administración, Compras y Finanzas", "Comercial", "Tecnología de Información" y "Recursos Humanos" representan el 30 % de la plantilla de trabajadores de la terminal portuaria.

El personal del área de Tecnología de Información posee un área de help desk o mesa de ayuda divididos en dos turnos de 8 horas, un equipo de desarrolladores propio que provee las herramientas informáticas de toda la compañía en un turno de 8 horas, en ambos casos se realizan guardias pasivas nocturnas.

- **Objetivos de la Dirección:**
  - Satisfacer las necesidades y requerimientos de los clientes, cumpliendo con calidad y en términos lo pactado.
  - Garantizar la confidencialidad, integridad y disponibilidad en el manejo de la Información.
  - Garantizar la eficiencia y rentabilidad de los procesos y servicios de la compañía.
  - Capacitar al personal para asegurar la idoneidad en el desempeño de sus funciones.
  - Cumplimentar todos los requisitos legales aplicables, presentes y futuros.

A continuación se detalla el presente organigrama simplificado que muestra la estructura básica de las áreas de la organización, sin entrar en detalle de los departamentos internos de la organización que se irán detallando a medida que este trabajo avance y en la medida que sea necesario.



1.3 MOTIVACIÓN Y ENFOQUE:

Los riesgos inherentes a los servicios informáticos destinados a los clientes que posee la terminal y que son ofrecidos a través de internet con los riesgos y amenazas que este medio globalizado alberga, asi como las diferentes vulnerabilidades y problemas de seguridad que son reportados diariamente han motivado que el Consejo de Dirección se vea en la obligación de tomar medidas tendientes a mitigar, transferir o aceptar éstos y los futuros riesgos.

Se ha establecido realizar un "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), conocido como la triada "Confidencialidad, Integridad y Disponibilidad" que intenta asegurar y aplicarse en el diseño integral de la arquitectura de seguridad de la información sobre los activos en riesgo que serán identificados en etapas tempranas del proyecto y a medida que el plan avance; se intentarán proteger estos activos a lo largo del ciclo de vida del proyecto de acuerdo con las políticas definidas por el directorio.

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.

Del mismo modo, se plantea incluir en el proyecto los conceptos de "autenticidad, privacidad y trazabilidad" en los procesos críticos del sistema, para lo cual se planifica realizar un análisis de riesgos sobre los activos informáticos y todos los procesos relevantes para el funcionamiento de la terminal.

- **Objetivos de la Dirección:**
  - Crear una ventaja competitiva de negocio.
  - Gestionar las Amenazas y Vulnerabilidades en todos los Activos de la Organización y de los Servicios ofrecidos a través de Internet.
  - Fortalecer la relación de confianza entre el cliente y la organización.
  - Realizar un acercamiento progresivo a la norma Internacional UNE-ISO/IEC 27001:2007– Seguridad de la Información.
  - Realizar el "Plan Director de Seguridad de la Información".
  - Gestionar de manera adecuada los posibles incidentes de seguridad que puedan surgir.

1.4 ASPECTOS LEGALES:

La Dirección de la organización tiene la obligación legal de cumplimentar todos los requisitos legales aplicables presentes y futuros, por lo que deberá implementar las medidas necesarias y asignar los recursos económicos, técnicos y humanos suficientes para adoptar los mecanismos técnicos descriptas en las disposiciones legales, normativas y reglamentarias del país en función del ámbito comercial en el que opera la terminal, asi como las medidas para cumplimentar otras que afectan exclusivamente a su negocio y/o que son internacionales o regionales como las que dictamina la Unión Europea.

1.5 ESTADO INICIAL DE LA SEGURIDAD:

La situación actual en la que la organización está inmersa en cuanto a los servicios que brinda a través de internet, asi como los servicios internos amparados en ésta, y al manejo de información confidencial, por ejemplo en papel, como los contratos comerciales con las compañías marítimas; hacen que se planteen actualizar las políticas, procedimientos, reestructuración de tareas y funciones de algunas áreas por solapamientos y falta de independencia entre sus miembros.

La Direccion ha definido que se implementen los mecanismos de seguridad para todos los sistemas de información abarcados en el alcance, la infraestructura tanto de red como de comunicaciones para alcanzar los siguientes objetivos:

- Actualizar las políticas, procedimientos, reestructuración de tareas y funciones de algunas áreas.
- Implementar procesos de seguridad para el control en la infraestructura tanto de red como de comunicaciones, estableciendo contramedidas, mecanismos de monitoreo y gestión de incidentes.

- Crear mecanismos y procedimientos de Control de Calidad y Mejores Practicas en el desarrollo seguro de aplicaciones.
- Realizar una correcta gestión de privilegios para garantizar la Confidencialidad, Integridad, Disponibilidad, Autenticidad, Privacidad y Trazabilidad o No Repudio.
- Crear y gestionar una infraestructura tecnológica redundante para los servicios ofrecidos a través de internet que garanticen la calidad, disponibilidad e integridad de los mismos.

1.6 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS:

El Consejo de Dirección ha definido que realizará un acercamiento de sus procedimientos a la Norma Internacional UNE-ISO/IEC 27002:2009, desarrollando todos los puntos aplicables de la norma y haciendo énfasis en todos los controles aplicables al alcance definido, los mismos se encuentran enumerados desde el dominio 5 “Política de Seguridad” hasta el 15 “Cumplimiento”.

Dichos controles serán implementados y monitorizados durante todo el ciclo de vida del proyecto y sistema, se utilizará el modelo de mejora continua de Deming PDCA (Plan-Do-Check-Act) Planificar, hacer, verificar y actuar, que establece las cuatro fases indispensables para implantar un sistema de gestión a través de un ciclo iterativo, de forma que en cada iteración se mejoran los resultados del ciclo anterior y frecuentemente se amplía el alcance de la iteración anterior, lo que permite sentar las bases para un ciclo de mejora continua.

Requisitos para Implementar un 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.

La Seguridad de la Información no es un tema sólo del Área de Tecnología de la Información, sino de toda la Organización. Éste es quizás el factor de éxito más importante de un Plan de Seguridad; por lo que el Plan Director de Seguridad de la información (PDSI); tiene como objetivos identificar el “**Que**” es lo que hay que proteger y que interrelación o dependencia existe entre estos activos a proteger, “**Como**” se va a proteger, “**Cuando**” se va a proteger y bajo qué circunstancias, “**Donde**” se va a proteger, es decir en qué lugar geográfico dentro de la organización y por sobretodo “**Quién**” y de quién se van a proteger y finalmente “**Cuales**” son los aspectos legales aplicables.

La organización realizará la enumeración de los bienes relacionados directa o indirectamente con la actividad informática de la compañía como parte de su operatoria diaria, por lo que ha agrupado los activos informáticos involucrados en el alcance propuesto por la Dirección en nueve ámbitos de aplicación, al tiempo que se deberá identificar las dependencias de los activos para identificar la interrelación que existe entre ellos y se le asigne una prioridad en función de esta relacion, puesto que los requerimientos de seguridad de un activo superior deberán ser implementados en el activo inferior o dependiente, para poder cubrir las necesidades de seguridad del primero, los activos serán 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.

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.

El principal objetivo de un análisis de riesgos, es poner de manifiesto cuáles son los riesgos y amenazas a los que el negocio y los activos están expuestos, para que la Dirección de la Compañía pueda analizar y tomar decisiones al respecto, para cada uno de los riesgos identificados habrá que decidir y definir cuáles son las acciones a tomar, sin perder en ningún momento de vista el principio de proporcionalidad, ya que el coste de la implantación de una salvaguarda no deberá nunca superar el posible impacto de la materialización de una amenaza.

Esquematizacion del Analisis de Riesgos:

Tipos de Análisis de Riesgos:

- **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 calculado establece una disminución de **€ 34.628,50**.- sobre el Riesgo Intrínseco estimado, valorando el Riesgo Efectivo en un total de **€ 4.273,18**.-
- **Riesgo intrínseco**: Es el estudio que se realiza sin tener en consideración las diferentes medidas de seguridad que se encuentran implantadas en una organización.
    - 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.

Posteriormente a la obtención del Riesgo Residual se debe establecer el Nivel de Riesgo Aceptado por la Organización para cada activo/amenaza en función de los Objetivos fijados por la Dirección. Este nivel de riesgo es el que determinará el riesgo que la Compañía puede asumir o no y se utilizará como referencia para determinar qué controles aplicar y sobre qué activos.

Por otra parte, se estudiará la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT – versión 2, para la realización del Análisis de Riesgo, esta metodología permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos informáticos que desean ser protegidos, siguiendo los lineamientos de los objetivos, metas, estrategias y políticas que la organización fije.

Dentro del Plan Director se debe realizar una verificación de la Viabilidad Técnica, Económica y Operativa de las salvaguardas o contramedidas que surjan del Análisis de Riesgo, este análisis se realizará mediante la metodología MAGERIT.

El Comité de Seguridad de la Información conjuntamente con los responsables de las Áreas y miembros claves de la organización definirán una serie de amenazas sobre los activos identificados, por lo que ha realizado una categorización según la metodología MAGERIT versión 2 en su libro 2 "Catalogo de Elementos" en su apartado nro. 5 "Amenazas", en la misma se definirán frecuencias diarias, mensuales y anuales para dichas amenazas y se valorarán las dimensiones para asegurar la Confidencialidad, Integridad, Disponibilidad, Autenticidad, Privacidad y Trazabilidad o No Repudio, en forma porcentual por cada activo amenaza, la clasificación realizada corresponde a la siguiente:

- [N] Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
- [I] De origen industrial: Sucesos que pueden ocurrir en forma accidental, derivados de las actividades humanas de tipo industrial, pueden darse de forma accidental o deliberada.
- [E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas.
- [A] Ataques intencionados: Fallos deliberados causados por las personas.

La valoración del Impacto Potencial planteando el impacto de la materialización de la amenaza de cada activo-amenaza en forma porcentual, se realiza con el objetivo de:

- Determinar un marco de priorización.
- Establecer las medidas de salvaguardas a implementar en cada activo.
- Definir un plan de acción en función de la importancia para la organización.

- **Objetivos de la Dirección**:

  - Adaptar los procedimientos y normativas internas para la implementación de la norma UNE-ISO/IEC 27002:2009 en toda la organización.
  - Desarrollar metodologías de control y monitoreo para los sistemas abarcados en el SGSI.
  - Generar métricas y mecanismos de auditorias para una retroalimentación del SGSI.
  - Realizar un seguimiento de los hallazgos encontrados en las auditorias y los posteriores planes de acción para subsanar las desviaciones.
  - Identificar los Activos en Riesgo.
  - Determinar las dependencias entre los activos.
  - Realizar un Análisis de Riesgos y Amenazas sobre los Activos identificados.
  - Comprobar los costes de degradación o pérdida cuantificando los activos en función de las amenazas y la frecuencia a las que están expuestos.
  - Analizar el Impacto Potencial dentro de la organización sobre las amenazas detectadas.
  - Especificar el nivel de riesgo aceptado por la organización para cada activo y amenaza.
  - Desarrollar contramedidas para mitigar las amenazas, reduciendo la frecuencia o limitando el daño, transferirlas a un tercero, aceptándolas o eliminándolas en función del impacto que provoquen en la organización.
  - Verificar la viabilidad técnica, económica y operativa de las salvaguardas desarrolladas realizando una estimación económica de la protección de los activos y accionando en consecuencia.
  - Realizar un plan de implementación para cada una de las contramedidas, especificando los participantes, los dominios abarcados y sus límites, las tareas y etapas en función de su prioridad, costes y dimensiones; asignando los recursos necesarios dentro del presupuesto anual.
  - Sistematizar los controles y monitoreos de la efectividad de las contramedidas en forma periódica, gestionando los cambios que sean requeridos.

1.7 Aspectos Organizativos y Participantes:

El Plan Director de Seguridad de la Información tiene como objetivo identificar "Quienes" son los participantes asociados y afectados a los objetivos y metas definidos por la alta Dirección para el Plan y "Qué" aspectos organizativos deberán tenerse en cuenta a la hora de implementarlo, los siguientes apartados describen los equipos de trabajos que serán creados para la implementación del Plan.

1.8 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 hacer participar a toda la organización en el proceso.

Su responsabilidad es dar el soporte del Sistema de Gestión de Seguridad de la Información, su implicancia en la implementación y posterior mantenimiento es vital para el éxito de la misma, ya que deberá tomar decisiones que afectarán a toda la organización.

1.9 Equipo del Proyecto:

El Plan Director de Seguridad plantea definir "Quienes" serán los encargados de ejecutar las tareas en el proyecto, es decir el equipo de trabajo encargado de hacer efectivo el plan.

1.10 Gestor del Proyecto:

La Dirección de la organización conjuntamente con el Comité de Seguridad de la Información, designará un miembro de la organización cualificado, con una visión global de la organización, capacidades de liderazgo, trabajo en equipo, conocimientos técnicos informáticos para liderar los equipos técnicos y que desempeñará la función de nexo entre la dirección y los miembros del Comité, los Auditores, las áreas y departamentos de la organización en general y será el máximo responsable de realizar la planificación de los recursos económicos, técnicos y humanos necesarios para llevar adelante el Plan de Seguridad.

1.11 Comité de Seguridad de la Información:

Se creará un Comité de Seguridad de la Información, estará formado por miembros de la Dirección, Jefes de Área, Responsables de Departamentos, es decir personal de la organización que tenga responsabilidad, poder de decisión sobre el negocio y esté implicado en el PDSI.

1.12 Comité Multidisciplinario de Seguimiento y Soporte del Plan Director:

Se creará 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.

1.13 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.

1.14 Otros Actores:

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

2. Auditoría de cumplimiento de la UNE-ISO/IEC 27002:2009

2.1 Metodología de Analisis del Mode lo de Madurez de la capacidad:

Se utilizará el Modelo de Madurez de la Capacidad (CMM) como metodología para el análisis del grado de madurez en la implementación del Sistema de Gestión de Seguridad de la Información o SGSI, el estándar Internacional correspondiente a 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.

2.2 PRESENTACIÓN DE RESULTADOS:

El presente apartado tiene como objetivo mostrar los resultados obtenidos luego de la auditoria documental realizada enfocando los mismos sobre las amenazas detectadas que afectan a los activos, con un impacto superior a ocho, los gráficos abajo detallados reflejarán por cada amenaza el grado de madurez del sistema especificado en la metodología CMM en función de cada control implementado de la norma UNE-ISO/IEC 27002:2009.

Como se detalla en el Gráfico 1, se ha detectado que los activos "Código Fuente Programas" y "Desarrollo Interno: Pagina Web, Formularios de Internet" en relación a la amenaza "[A.4] Manipulación de la configuración" poseen dificultades que deberán ser subsanadas, puesto que no existe una buena gestión de privilegios, restricción del acceso a la información y control de acceso al código fuente de los programas, no se establece un mecanismo que impida realizar el control de cambios de manera jerárquica y sistemática, siendo posible que cualquier desarrollador pueda implementar cambios en el sistema de producción.

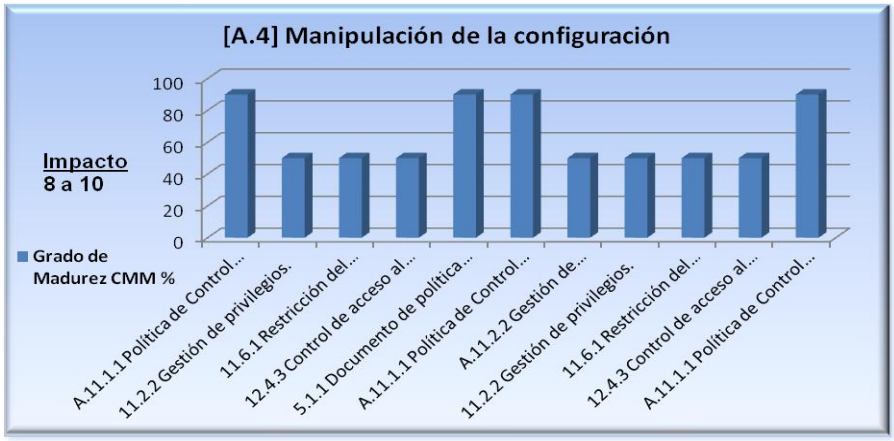


Gráfico 1

Como se ha comentado anteriormente, se deberán tomar medidas concernientes al control "12.4.3 Control de acceso al código fuente de los programas", por pate de los desarrolladores internos, ya que todos posee autorización y privilegios para realizar cambios en el servidor de producción, el Gráfico 2 muestra la falta de control 12.4.3 en cuanto a los activos "Código Fuente Programas" y "Desarrollo Interno: Pagina Web, Formularios de Internet" que han obtenido un valor de 50% en CMM.

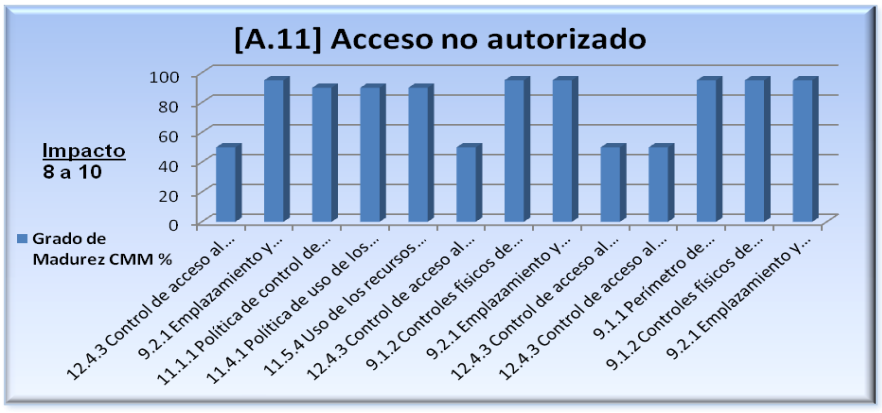


Gráfico 2

Asimismo, se ha detectado que el personal del área de Desarrollo, posee privilegios sobre los servidores que permiten realizar cambios de versiones sobre las aplicaciones de Internet y en el código fuente, haciendo posible una destrucción de la información en los controles "12.2.2 Control del procesamiento interno", que han obtenido una valoración CMM 50%, algo similar sucede en la amenaza "[E.18] Destrucción de la información" en el control "10.1.3 Segregación de tareas" que ha obtenido un valor idéntico, por no realizar una correcta segregación de funciones administrativas y tareas del personal de desarrollo.

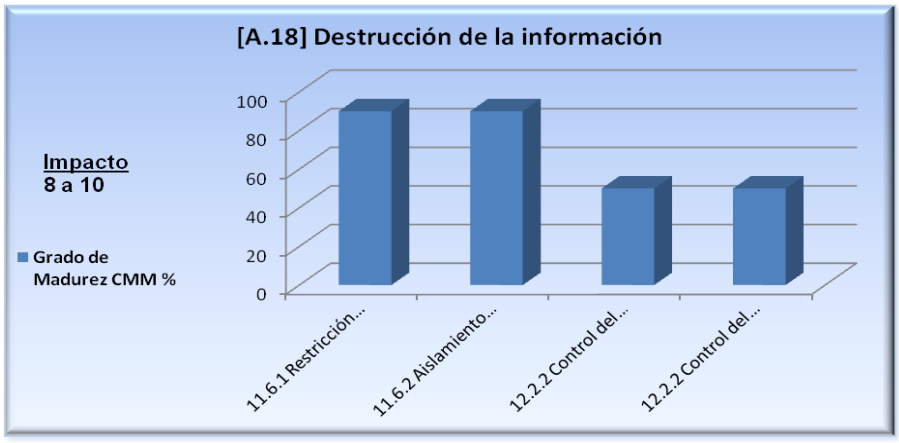


Gráfico 3

Se ha relevado los proveedores del servicio de comunicaciones de Internet y 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”.

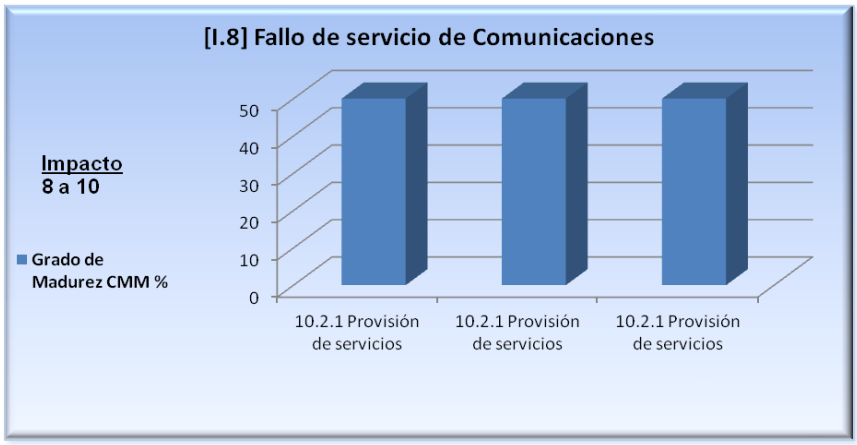


Gráfico 4

Por otra parte, el Gráfico 5 muestra el estado de madurez de los objetivos que no alcanzan un valor superior al 70% comparados con el objetivo estipulado por la organización, se deberán tomar medidas a corto, mediano y largo plazo para subsanar las diferencias encontradas.

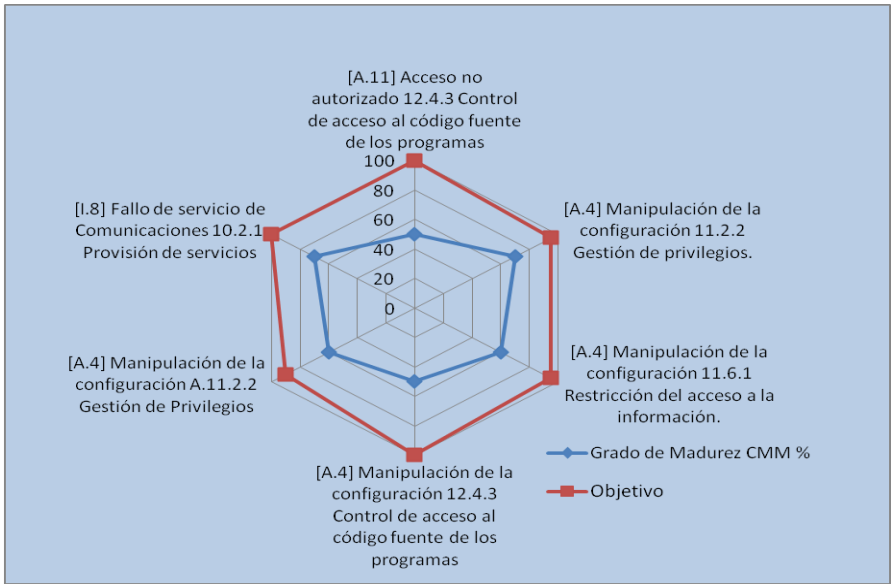


Gráfico 5

3. PROPUESTAS DE PROYECTOS

3.1 PROPUESTAS:

El presente apartado tiene como objetivo detallar los proyectos a llevarse a cabo luego de la realización del Análisis de Riesgo en donde se han identificado una serie de salvaguardas a implementar para las amenazas que no alcanzan el objetivo del 90% según la valoración de la metodología CMM.

Proyecto SGSI:

El presente proyecto SGSI tiene una estimación de treinta y cinco 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 SLA.

3.1.1 FASE 1 – WORKFLOW PARA EL CONTROL DE CAMBIOS DE CÓDIGO FUENTE:

La fase 1 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.

La implementación de un producto para realizar el Control de Cambios del Código Fuente permitirá realizar un flujograma de autorización jerárquico que podrá ser visualizado históricamente, permitiendo con esto saber todos y cada uno de los cambios realizados, así como la persona autorizada para tal acción, otorgando una "trazabilidad" que en la actualidad no existe dentro de la organización.

Del mismo modo, la implementación de dicha herramienta permitirá un mejor control de las nuevas versiones y una optimización de recursos técnicos y humanos, al focalizar las nuevas versiones y poder administrarlas de una manera centralizada y segura.

- 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:

  - Control de Versionado y cambios del Código Fuente.
  - Flujograma de Autorización Jerárquico.
  - Administración Centralizada de Cambios.
  - Visualización de Cambios Históricos y Auditorias.
  - Verificación del personal que realizó la Aprobación de Cambios y Versionados.

- 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

3.1.2 FASE 2 – GESTIÓN DE PRIVILEGIOS:

La fase 2 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.

La correcta gestión de privilegios en todos los sistemas de información permitirá asegurar a la organización la centralización y correcta administración de los privilegios que cada usuario posee, esto permite entre otras cosas que solo los usuarios autorizados puedan acceder, modificar o borrar cierta información, lo que nos permite asegurar la "confidencialidad" de la misma.

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 tener cada usuario en el sistema, debiendo ser revisada al menos una vez al año o cuando el usuario cambie de tarea o deje de pertenecer a la organización.

Del mismo modo, 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.

- 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 Operativos de la Terminal.
  - Sistemas de Desarrollo y Código Fuente.
  - Acceso a la lectora de CD/DVD/USB.
  - Carpetas Publicas/Privadas/Confidenciales.

- 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.

3.1.3 FASE 3 – SEGREGACIÓN DE TAREAS:

La fase 3 tiene una estimación de treinta y dos días de duración, 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.

La segregación de tareas permitirá una correcta gestión de los recursos humanos, técnicos y organizativos dentro de la organización, al eliminar los solapamientos de tareas y funciones, al mismo tiempo que permitirá detectar errores o fraudes voluntarios o involuntarios, mejorando el control interno de los desarrollos, tareas y funciones.

Del mismo modo, la confección de perfiles de puestos y funciones permitirá realizar un plan de formación anual para cada puesto que requiera conocimientos o habilidades específicas, siendo una evidencia clara de evolución del sistema, permitiendo una retroalimentación del mismo.

- 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, al eliminar los solapamientos de tareas y funciones, al mismo tiempo que permitirá detectar errores o fraudes voluntarios o involuntarios, mejorando el control interno de los desarrollos, tareas y funciones.

- 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.
  - Detectar las necesidades de habilidades técnicas, humanas u operativas.
  - Realizar un Plan de Formación y Capacitación.

- 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.

3.1.4 FASE 4 – PROVEEDORES ALTERNATIVOS PARA LOS SERVICIOS DE INTERNET Y LA PABX:

La fase 4 tiene una estimación de veintiséis días de duración, 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.

La búsqueda de proveedores alternativos para los servicios de Internet y telefonía fija, asegurará la correcta gestión de la continuidad del negocio, puesto que hoy en día la organización tienen una clara dependencia de estas tecnologías, la 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.

- 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:

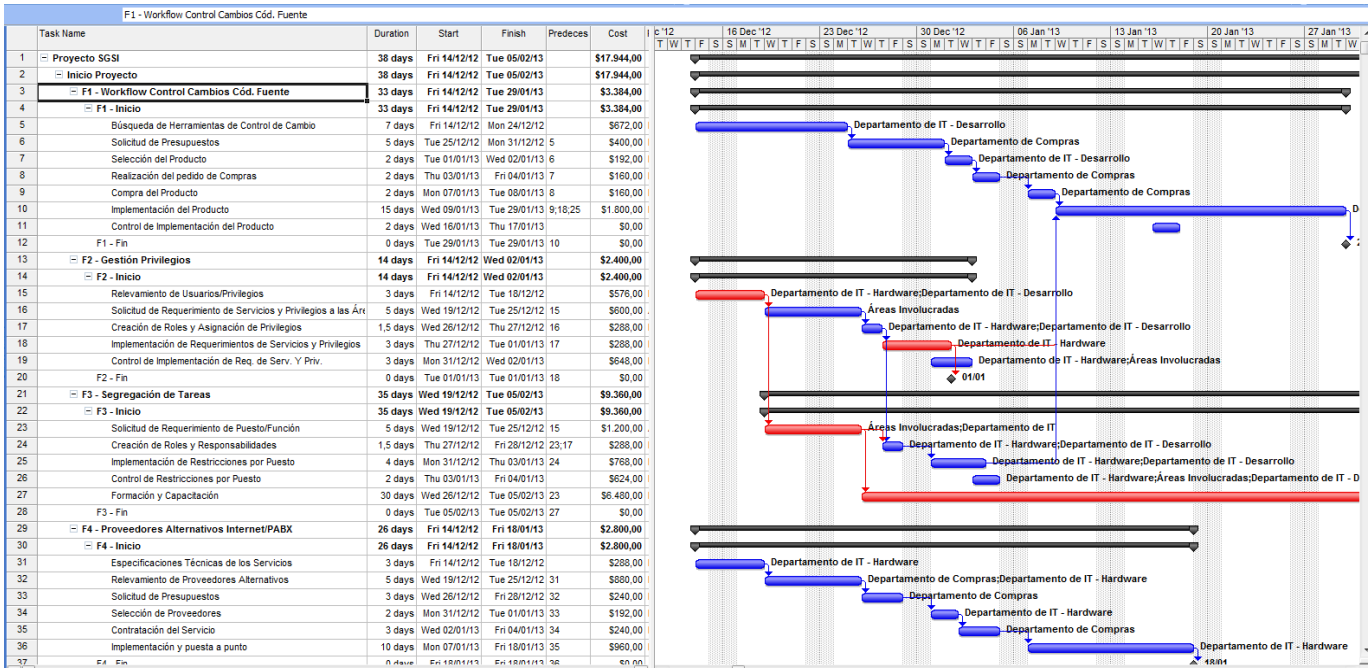
  - Gestionar el Plan de Contingencia y Continuidad de Negocio.
  - Implementar sistemas redundantes para telefonía fija e Internet.
  - Garantizar los servicios ante fallas, roturas o destrucción.
  - Gestionar los Costos de la Telefonía Fija al realizar ruteos en función del costo de la llamada y el destino.

- 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.

A continuación, se detallan los diferentes proyectos descriptos mediante un diagrama de Gantt, que será anexado a la documentación suministrada.



3.2 REALIMENTACIÓN DE RESULTADOS:

El siguiente apartado corresponde al análisis de los resultados pre y post implementación de las cuatro fases del proyecto SGSI mencionado anteriormente.

El presente gráfico 6, 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.

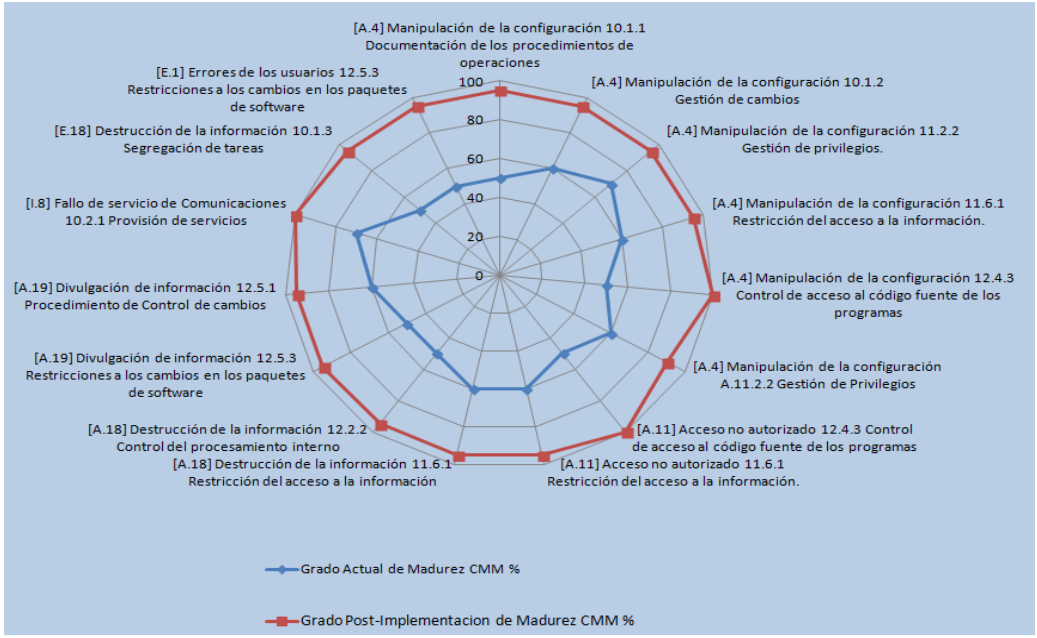


Gráfico 6

Como se puede visualizar en el gráfico 6, 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 para futuras auditorías internas y externas, 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 los objetivos de la organización.

4. RESUMEN DE HALLAZGOS DE AUDITORIA:

El alcance de la auditoría ha sido realizado tomando en consideración lo dispuesto en la Norma UNE-ISO/IEC 27001:2007, según la documentación suministrada como evidencia y fuente de información, abarcados en todos los Sistemas de Información asociados a los procesos y servicios brindados a través de Internet que afecten a las Operaciones Portuarias.

Se ha comprobado que se realizan reuniones por parte de la Dirección de la Terminal en forma trimestral en las que se revisan todos los puntos del SGSI, los eventos de seguridad y los hallazgos encontrados en las auditorías internas.

Se ha visto plasmado en el presupuesto anual del corriente año las partidas económicas para solventar los requerimientos técnicos, operativos y humanos del Sistema de Gestión de Seguridad de la información.

Hemos observado el conocimiento de las políticas, normas y procedimientos por parte del personal relevado, así como el personal del área de Tecnología de Información que fuera auditado oportunamente.

Se han visualizado registros de incidentes de seguridad, así como los procedimientos de notificaciones llevados a cabo, los procesos de recopilación de información y posterior almacenamiento en forma segura.

Se han constatado los registros de formación realizados por el personal de Desarrollo del Dto. de TI, así como las planillas de Puestos y Funciones relevantes a las tareas y funciones que prestan los mismos.

Se ha chequeado la existencia de las planillas de “Servicios y Privilegios” por parte del personal de Hardware del Dto. De TI, asi como los privilegios que los mismos poseen en el sistema.

Se ha auditado las políticas de contraseñas de los sistemas de información de la organización, siendo consistentes con las mejores prácticas de seguridad y fortaleza de las mismas, ya que las mismas están compuesta por letras, números y caracteres especiales.

Se ha comprobado el Sistema de Control de Acceso de la Sala de Servidores, constatando que los mismos se realizan a través de la apertura por huella dactilar y un PIN personal de 6 dígitos.

Se ha chequeado la sala que aloja los Sistemas de Alimentación Ininterrumpida (SAI/UPS), Generadores Eléctricos, Equipos de Climatización y Equipos de Control de Temperatura y Humedad, los mismos se encontraban con los registros de mantenimiento actualizados y en funcionamiento.

Se constató en la Sala de Servidores, la correcta instalación y etiquetado el Cableado Estructurado de Red, así como el cableado de Fibra Óptica de comunicaciones y la separación con el cableado Eléctrico.

Se constataron los registros de mantenimiento de los servidores “svr-web”, “svr-ids”, “svr-email”, comprobando que en todos los casos los contratos se encuentran vigentes y no se detectan errores en los mismos.

4.1 RESUMEN DE HALLAZGOS DE LA AUDITORIA:

Fecha	Punto de la Norma UNE-ISO/IEC 27001:2007	Grado Cumpl.	Aplica	Hallazgos / Cumplimientos Descripción
28-11-12	**3 Términos y Definiciones**	**SFI**	**A**	La Seguridad Física y Ambiental, no detalla los términos y definiciones tales como "SAI (Sistema de Alimentación Ininterrumpida), UPS (Uninterrumpible Power Supply)".
28-11-12	**4 Sistema de Gestión de Seguridad de la Información**			
28-11-12	4.2.2 Implementación y Operaciones del SGSI	**SFI**	**A**	Se recomienda definir y realizar una evaluación periódica, al menos una vez al año, de los riesgos que amenazan los activos y una posterior modificación del Plan de Tratamiento de los Riesgos en función de las nuevas amenazas detectadas.
28-11-12	**5 Responsabilidades de la Dirección**			
28-11-12	5.2.2 Concienciación, formación y competencia	**RC**	**A**	La presente Política de Seguridad de la Información no menciona la formación, competencias, las evaluaciones periódicas de las mismas, ni los registros pertinentes.
28-11-12	**6 Auditorías Internas del SGSI**	**SFI**	**A**	Se recomienda realizar un relevamiento posterior de la realización de las auditorías internas con fecha 03-06-2012, para asegurarse que se llevan a cabo los planes y acciones para mitigar los hallazgos encontrados en el procedimiento de "Organización de la Seguridad de la Información", ya que no se realiza una correcta segregación de funciones en el área de desarrollo.
28-11-12	**7 Revisión del SGSI por la Dirección**			
28-11-12	7.3 Resultados de la Revisión	**SFI**	**A**	Se han identificado los hallazgos de la última auditoría con fecha 03-06-2012, pero no se han registrado las conclusiones ni el plan de acción sobre los mismos.
28-11-12	**8 Mejora del SGSI**			
28-11-12	8.1 Mejora Continua	**RC**	**A**	En la Política de Seguridad de la Información, se evidencia una alineación con los objetivos de la organización, en donde se establecen revisiones periódicas, alineando los términos a la estrategia de la compañía, en la búsqueda de la excelencia, brindando garantía en la prestación de los servicios y aportando valor para los clientes y optimizando los costes en el proceso. No se especifican los Indicadores de mejora, ni la metodología utilizada para realizar la misma, ej: PDCA, por lo que se recomienda en posteriores auditorias relevar la existencia de los mismos, en los procedimientos, informes y normativas detalladas en la PSI.
28-11-12	8.2 Acciones Correctivas	**RC**	**A**	Se detalla la existencia de una "Política de Revisión y Mejora", no se especifican la metodología utilizada para realizar la misma, por lo que se recomienda en posteriores auditorias relevar la existencia de los mismos.
28-11-12	8.3 Acciones Preventivas	**RC**	**A**	Se enumera la existencia de una "Política de Revisión y Mejora", no se especifican la metodología utilizada para realizar la misma, por lo que se recomienda en posteriores auditorias relevar la existencia de los mismos.
Fecha	**Controles de la Norma UNE-ISO/IEC 27002:2009**	**Grado Cumpl.**	**Aplica**	**Hallazgos / Cumplimientos** **Descripción**
28-11-12	**A.5 Política de Seguridad**			
28-11-12	A.5.1 Política de seguridad de la información.	**SFI**	**A**	Se evidencia la implantación de la "Política de Seguridad de la Información", la dirección se compromete a su difusión en toda la organización, se recomienda buscar evidencia de formación y difusión de la misma en posteriores auditorias, a pesar de que se ha comprobado el conocimiento de la misma por parte de los empleados.
28-11-12	**A.6 Aspectos Organizativos de la seguridad de la información**			
28-11-12	A.6.1 Organización interna	**RC**	**A**	Se detalla en la PSI la presencia de la "Política de Personal", en la misma no se detalla la existencia de documentos en donde se detallen los roles y responsabilidades abarcados en la Organización de la Seguridad de la información de cada puesto y función dentro de la misma.
28-11-12	**A.10 Gestión de Comunicaciones y Operaciones**			
28-11-12	***A.10.1 Responsabilidades y procedimientos de operación***			

	A.10.1.1 Documentación de los procedimientos de operaciones	**RC**	**A**	Los "Procedimientos de Operaciones Normales" se encuentran documentados, actualizados y correctamente versionados, pero se ha detectado que no existe una correcta asignación de perfiles de usuario en función de sus tareas dentro de la organización, se recomienda realizar un documento que especifique los privilegios de cada usuario en función de sus tareas.
	A10.1.2 Gestión de Cambios	**NC - Menor**	**A**	No se visualiza una correcta gestión de cambio en el área de desarrollo y en relación con la generación de código fuente de las aplicaciones web.
	A.10.1.3 Segregación de Tareas	**NC - Menor**	**A**	Se comprueba una incorrecta gestión de segregación de funciones en lo referente al área de desarrollo y la posibilidad de realizar actualizaciones del código fuente por parte de los desarrolladores, se recomienda realizar un documento que detalle las funciones y privilegios que cada puesto dentro de la organización debe poseer.
28-11-12	***A.10.2 Gestión de la provisión de servicios por terceros.***			
	A.10.2.1 Provisión de Servicios	**SFI**	**A**	Se ha constatado la existencia de un proveedor único para los servicios de telefonía fija e internet, ambos servicios utilizan el mismo cableado de Fibra Óptica, por lo que la caída del vinculo supone una Incomunicación total de la organización tanto de Internet como de la Telefonía Fija, Se recomienda la contratación de uno o más proveedores alternativos para éstos servicios, o la asunción de las posibles consecuencias y el impacto que tendría la materialización de la amenaza "I.8 Fallo de Servicio de Comunicaciones" según la metodología MAGERIT Versión 2.
28-11-12	***A.10.4 Protección contra el código malicioso y descargable***			
	10.4.1 Controles contra el código malicioso	**SFI**	**A**	La organización cuenta con sistemas de detección de intruso, firewall y antivirus, pero se ha detectado que los desarrolladores poseen privilegios de administrador sobre algunos servidores, lo cual posibilita la difusión de software malicioso.
28-11-12	***A.11.2 Gestión de acceso de usuario***			
	A.11.2.2 Gestión de Privilegios	**NC – Menor**	**A**	Se ha constatado que los desarrolladores poseen privilegios de "administrador" en el servidor "svr-web" que les permite realizar cualquier acción en el mismo, así como la actualización, eliminación y modificación de las versiones del código fuente existente y que es brindado como servicio a los clientes de la organización, por lo que se recomienda realizar un documento que detalle los privilegios y permisos que deben poseer cada empleado dentro de la organización autorizado por el personal jerárquico correspondiente al área en cuestión.
28-11-12	***A.11.6 Control de acceso a las aplicaciones y a la información***			
	A.11.6.1 Restricción del Acceso a la Información	**RC**	**A**	Se ha verificado que los desarrolladores poseen privilegios de "administrador" en el servidor "svr-web" que les permite realizar cualquier acción en el mismo, se recomienda la implementación de un "Sistema de Control de Cambios" que implemente una metodología de Flujograma jerárquico que permita una visualización histórica.
28-11-12	***A.12.2 Tratamiento correcto de las aplicaciones***			
	12.2.1 Validación de los datos de entrada.	**RC**	**A**	Se ha constatado que la aplicación de "Información de Buques" es susceptible a ataques del tipo "Blind SQL Injection", se recomienda la corrección del formulario web, realizando una correcta gestión de validación de los datos de entrada.
	A.12.2.2 Control del Procesamiento Interno	**RC**	**A**	Se ha constatado que la aplicación de "Información de Buques" es susceptible a ataques del tipo "Blind SQL Injection", se recomienda la corrección del formulario web, realizando una correcta gestión de validación de los datos de entrada.
28-11-12	***A.12.4 Seguridad de los archivos de sistema.***			
	A.12.4.3 Control de acceso al código fuente de los programas.	**NC - Menor**	**A**	Se ha constatado que los desarrolladores poseen privilegios de "Administrador" en el servidor "svr-web" que les permite realizar modificaciones y actualizaciones del código fuente, utilizando una cuenta única de "Administrador", por lo que no puede ser rastreado quien ha realizado dicha modificación.
28-11-12	***A.12.5 Seguridad en los procesos de desarrollo y soporte***			
	A.12.5.1 Procedimiento de Control de Cambios	**NC - Menor**	**A**	Se ha constatado que no se realiza una correcta gestión de cambios en relación al código fuente de las aplicaciones web, ya que los desarrolladores poseen privilegios de "Administrador" en el servidor "svr-web" que les permite realizar modificaciones y actualizaciones del código fuente, utilizando una cuenta única de "Administrador", por lo que no puede ser rastreado quien ha realizado dicha modificación.
	A.12.5.3 Restricciones a	**NC -**	**A**	No se realiza una correcta gestión de cambios en relación al código

	los cambios en los paquetes de software	**Menor**		fuente de las aplicaciones web, ya que los desarrolladores poseen privilegios de "Administrador" en el servidor "svr-web" que les permite realizar modificaciones y actualizaciones del código fuente. No se especifica una clausula de derechos de autor en la "Política de Personal", por lo que los desarrolladores podrían reutilizar el código para uso personal, se recomienda la incorporación de la misma en la política.
28-11-12	**A.15. Cumplimiento**			
28-11-12	***A.15.1 Cumplimiento de los requisitos legales***			
	15.1.1 Identificación de la legislación aplicable.	**SFI**	**A**	Se evidencia un compromiso en la Política de seguridad de la información por parte de la dirección para el cumplimiento estricto de los requisitos legales que le afecten, se recomienda realizar un relevamiento posterior de los procedimientos realizados para llevar a cabo el cumplimiento, así como la periodicidad y el plan de acción de los mismos.

4.2 GRADO DE CUMPLIMIENTO:

C = Cumplido.
NC Mayor = No Conformidad Mayor - Incumplimiento de un apartado completo de la norma.
NC Menor = No Conformidad Menor - Incumplimiento de un punto de la norma.
RC = Requiere Corrección/Observación - No existe incumplimiento pero se requiere corrección; ya que si no se corrige en una futura auditoría se puede llegar a convertir en No conformidad.
SFI = Scope for Improvement (Posibilidad de Mejora) - Es una recomendación del equipo de auditoría basada en la experiencia, no existe un incumplimiento a la norma.
PF = Punto Fuerte – Reconocimiento del esfuerzo por parte de la organización que ha realizado para gestionar uno o más elemento en su Sistema de Gestión de Seguridad de la Información (SGSI).

Aplicabilidad:

A = Aplica.
NA = No Aplica.

5. CONCLUSIONES:

- **Generales**:

  La implementación del "Plan Director de Seguridad" en los Sistemas de Información de la compañía conformará un mecanismo de optimización de recursos, ahorro de costos y mejora continua que permitirá a la Organización alcanzar los objetivos y metas planteados, al mismo tiempo que podrá afianzar los lazos de confianza con los clientes mientras le brinda a la compañía una ventaja competitiva que los posicionará en el mercado mundial.

  La mejoras en el Sistema de Gestión de Seguridad de la Información posibilitará 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, asi como los resultados de las auditorias internas y externas para la certificación, al obtener evidencias concretas de una correcta y evolucionada gestión de la 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.

- **Metodología de análisis y gestión:**

  La utilización de la Norma Internacional UNE-ISO/IEC 27001:2007– Seguridad de la Información y la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT en su versión nro. 2", que ha sido bastamente utilizado por empresas de todo el mundo, le permitirá a la organización contar con un soporte técnico, organizativo y humano que le aportarán una nueva visión del mercado, a la vez que le agrega una ventaja competivita para su negocio y fortalece la visión de la compañía para sus competidores, proveedores y clientes.

- **Análisis y Gestión de Riesgos:**

  El análisis y la gestión de riesgos ha permitido la correcta identificación de los activos en riesgo, determinando sus dependencias y el impacto potencial de la materialización de las amenazas, desarrollando y cuantificando las medidas de protección, ya sean operativas, técnicas y humanas que permitirán mitigar, aceptar o transferir los riesgos a la vez que las contramedidas serán monitorizadas y adaptadas cuando sean necesarias.

  Este análisis deberá ser repetido al menos una vez al año o cuando se realice algún cambio significativo en el sistema o en el contexto en que opera la organización.

- **Conformación del Equipo de Trabajo:**

  La conformación de un equipo multidisciplinario le otorgará una macro visión que permitirá abarcar todos los aspectos relevantes y en detalle del Sistema de Gestión de la Seguridad de la Información, asi como la unión, integración y espíritu de equipo de todos los miembros de la terminal para garantizar el éxito del Plan de Seguridad de la Informacion.

- **Inventario y valoraciones de Dimensiones y Amenazas de los Activos:**

  Se recomienda realizar periódicamente o al menos una vez al año, una revisión del Inventario de la compañía, así como la valoración de las dimensiones sobre los nuevos y los existentes, para determinar las desviaciones o modificaciones que existan en los procesos de negocio.

  La valoracion de los activos de hoy puede ser insuficiente para el futuro, por lo que habrá que constatar el Analisis de Riesgo y sus amenazas cada vez que se realice un cambio relevante para el SGSI o cada vez que la organización lo considere oportuno, por cambios de contexto o incorporación de nuevos activos, servicios o amenazas, para determinar si las medidas de salvaguardas o contramedidas continúan siendo efectivas y en su defecto estudiar las acciones que sean necesarias para subsanar las desviaciones.

- **Controles que no aplican:**

  Se aconseja revisar anualmente, los 133 controles de la norma UNE-ISO/IEC 27002:2009, ya que los cambios de contexto o nuevos procesos y servicios de negocios de la organización podrían afectar al Sistema de Gestión de Seguridad de la Información.

  Al mismo tiempo se debería verificar regularmente las disposiciones regulatorias, legales y normativas que la organización está obligada a cumplimentar, puesto que las legislaciones van adaptándose en torno a los cambios de contextos nacionales e internacionales.