21

EL PLAN DIRECTOR DE SEGURIDAD DE LA SUBDIRECCIÓN GENERAL DE INFORMÁTICA

Pedro Valcárcel
Jefe de Servicio de Políticas de Seguridad. Área de Seguridad. Centro de Calidad, Auditoría y Seguridad
SGI

RESUMEN
La Subdirección General de Informática de la Tesorería General de la Seguridad Social ha acometido un proyecto cuyo principal objetivo es realizar un análisis y diagnóstico de la seguridad de sus sistemas de información.

INTRODUCCIÓN

La Subdirección General de Informática (en adelante SGI) es el Servicio Común de la Seguridad Social, sin personalidad jurídica, que dirige, coordina y controla la creación, composición y actuación de los servicios de informática y de proceso de datos de las distintas Entidades Gestoras y Servicios Comunes de la Seguridad Social.

La SGI depende orgánicamente de la Tesorería General de la Seguridad Social y funcionalmente de cada Entidad Gestora de la Seguridad Social, de la Intervención General de la Seguridad Social y de la propia Tesorería General.

Entre sus funciones están las de proponer, implantar y coordinar los medios técnicos que garanticen la seguridad, integridad, calidad y confidencialidad de los sistemas de información de las Entidades Gestoras y Tesorería General de la Seguridad Social.

LA SEGURIDAD EN LA SGI

La información es un activo dentro de toda organización tan importante o más que cualquier otro, que dispone de un valor interno, y consecuentemente necesita ser salvaguardada adecuadamente de las amenazas que le afectan. La preocupación por la seguridad en el entorno de la SGI ha hecho que se implanten las medidas adecuadas para protegerla, asegurar una continuidad, minimizar los daños y maximizar las oportunidades de gestión administrativa.

Sin embargo, en el momento actual, la SGI ve esencial, para poder garantizar el nivel de protección adecuado a sus activos de información, identificar sus requerimientos de seguridad. Es por ello que ha tomado la decisión de llevar adelante un diagnóstico global de seguridad que le permita, tras la identificación del nivel de riesgo existente, llevar a cabo un plan de acción de mejora de la seguridad de los sistemas de información.

ALCANCE DEL PROYECTO

El ámbito del proyecto ha sido el sistema informático de la SGI y se ha basado en los requisitos de seguridad que han notificado las unidades de gestión. Para ello se ha centrado en cinco procesos de gestión considerados como críticos:

- Afiliación de trabajadores a la Seguridad Social e Inscripción de empresas y trabajadores.
- Recaudación de cuotas de la Seguridad Social (en período voluntario y ejecutivo).
- Gestión de las prestaciones concedidas y pago de las mismas.
- Control de la contabilidad de la Seguridad Social.
- Elaboración y seguimiento de los presupuestos de la Seguridad Social.

Esta selección previa ha sido esencial para la finalización en tiempo y forma del proyecto, pues la complejidad de los sistemas informáticos es tan alta que la haría inviable en un tiempo razonable.

También se ha aprovechado el esfuerzo empleado en el proyecto para estudiar el grado de conformidad de la organización con la norma internacional UNE-ISO/IEC 17799, de buenas prácticas para la Gestión de la Seguridad de la Información.

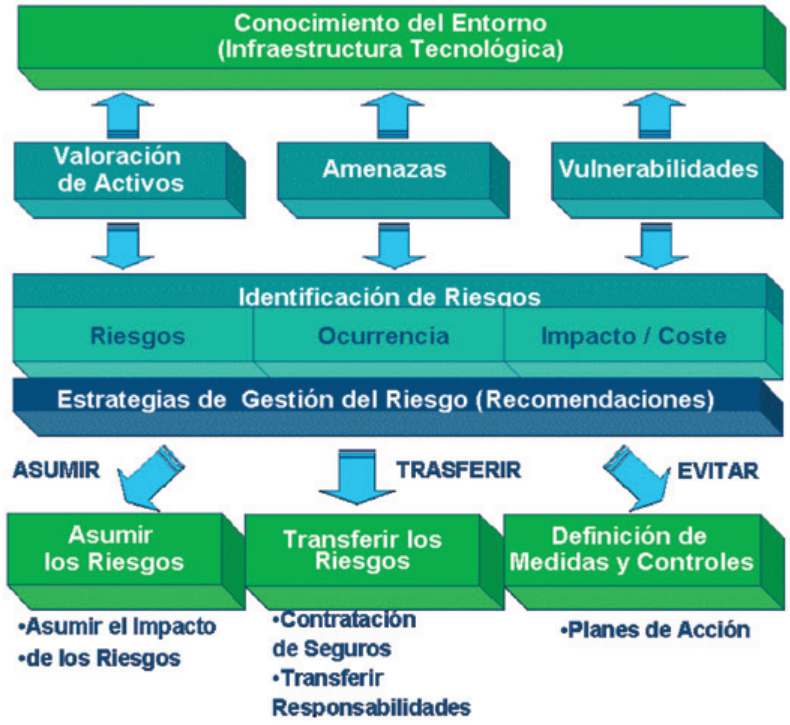
OBJETIVOS DEL PROYECTO

El principal objetivo es la realización de un análisis y diagnóstico de la seguridad de los sistema de información de la SGI. A partir del desarrollo de un análisis de riesgos, la meta es llegar a la definición de un plan director de seguridad, que permita reducir el riesgo global de la organización en sus sistemas informáticos.

Análisis y gestión del riesgo

Los sistemas de información están constantemente sometidos a amenazas, que pueden abarcar desde fallos técnicos y accidentes hasta acciones intencionadas, más o menos lucrativas, de curiosidad, espionaje, sabotaje, vandalismo, chantaje o fraude.

El análisis del riesgo estudia estas amenazas desde el punto de vista de la probabilidad de que ocurran y del impacto que producirían si ocurrieran. La gestión de riesgo consiste en asumir o eliminar los riesgos conocidos, por medio de un plan de contingencia o de seguridad, respectivamente.



Secuencia del análisis de riesgo

Visión conjunta de la seguridad

Frente a los planes parciales de mejora de la seguridad, una visión global de la seguridad tiene las siguientes ventajas:

- Se pueden descubrir las mayores vulnerabilidades. Un sistema informático es vulnerable justo en aquel componente que es más débil.

- Es posible tener una visión global del estado de la seguridad lo que no es sencillo en las grandes organizaciones.
- Es posible priorizar las acciones para minimizar la vulnerabilidad del sistema de información en conjunto. Al tener una relación de las acciones a realizar, junto con su facilidad de implantación, es posible comenzar por las más importantes o las que tienen menos coste.
- Se optimizan los esfuerzos de mejora de la seguridad, puesto que se pueden priorizar.
- Permite mostrar a la dirección de la organización los riesgos más importantes a los que está expuesto el sistema informático, puesto que se catalogan y para cada uno se estudia el impacto de la materialización de su amenaza. De esta manera , se dispone de un mecanismo objetivo para tomar decisiones sobre seguridad y en qué invertir recursos y esfuerzos para mejorar la situación.

Medidas de salvaguarda organizadas por proyectos

Las medidas de salvaguarda no se acometen por separado, sino que se organizan por proyectos. De esta forma se clasifican y coordinan en una serie de acciones con un objetivo conocido y con asignación de recursos y tiempo.

Dentro de una gran organización, el abordar las medidas de seguridad por proyectos tiene las ventajas descritas a continuación:

- Se controla de forma estándar el desarrollo de los proyectos de seguridad.
- Se perfila la estrategia de acción a medio y a largo plazo.
- Los proyectos se basan en un análisis coste / beneficio.
- Los proyectos se priorizan según los niveles de riesgo que cubre cada uno.
- Se agrupan las medidas para aprovechar sinergias, de forma que se aprovechen mutuamente unas de los beneficios de otras.

FASES DEL PROYECTO

El proyecto ha tenido una fase inicial de elaboración del mapa de activos y de valoración de las amenazas y vulnerabilidades. A continuación ha habido una fase de estimación del impacto y finalmente una de análisis y gestión de los riesgos de la organización. Con ellas se ha elaborado un plan director de seguridad.

La duración del proyecto ha sido de 7 meses, con un equipo de tres consultores, un jefe de proyecto por la empresa SIA y un jefe de proyecto por parte de la SGI.

De forma más detallada, las fases han sido:

Análisis de riesgo

Identificación y valoración de los activos

Durante esta tarea se identifican (por medio de entrevistas y accediendo a información de configuración de los sistemas de información de los sistemas de información) los activos necesarios para que el sistema informático funcione. Se clasifican en un mapa (que es una red estruc-

turada en niveles, donde los superiores representan el negocio en sí y los inferiores la infraestructura física, pasando por el software de base y de aplicación).

Diagnóstico de vulnerabilidades.

Se identifican las amenazas presentes sobre los activos en base a los ficheros históricos de incidencias, documentación aportada y entrevistas.

Asignación de impactos

Se evalúa el daño que produce cada amenaza en el caso de que se materialice una vulnerabilidad sobre un activo. Se mide en términos de disminución de su nivel de seguridad o del valor del activo.

Estudio de los riesgos

Se definen los mecanismos de seguridad más adecuados a las necesidades de la organización desde el punto de vista de la capacidad tecnológica y de los procedimientos organizativos necesarios.

Se analiza el riesgo en los activos en función de la probabilidad y del impacto. Se determina el riesgo intrínseco (el calculado sin implantar medidas de seguridad), el efectivo (una vez tenidas en cuenta las medidas de seguridad) y el umbral (el que la organización está dispuesta a asumir).

Plan de acción

Consiste en la elaboración del Plan Director de Seguridad, que es el que debe acometer la SGI para disminuir los riesgos identificados en las fases anteriores. Incluye un plan de proyectos valorados que ha permitido a la SGI planificar sus actividades de seguridad de la información a corto, medio y largo plazo.

Formación

En esta fase se realiza la transferencia de conocimiento por parte de la empresa colaboradora, junto con la formación necesaria para el mantenimiento de las métricas de seguridad.

Finalización

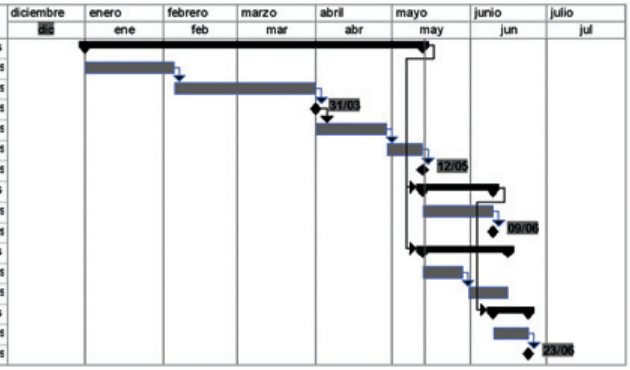
En esta fase se realiza el cierre formal del proyecto, mediante la elaboración y aprobación de un documento ejecutivo para el visto bueno de la SGI.

Esquema de las fases.

En el diagrama de Gantt adjunto se representa la duración de las tareas y sus dependencias para el caso de un proyecto que comience el 1 de Enero de 2.004.

La descripción de las tareas y la duración de las mismas son las mismas que se han producido en el proyecto de la SGI.

Id	Nombre de tarea	Duración
1	**Análisis de Riesgos**	**95 días**
2	Identificación y valoración activos	25 días
3	Diagnóstico de vulnerabilidades	40 días
4	Validación de activos por la SGI	0 días
5	Asignación de impactos	20 días
6	Estudio de los riesgos	10 días
7	Entrega del documento de análisis de riesgos	0 días
8	**Plan de acción**	**20 días**
9	Elaboración del Plan Director de Seguridad	20 días
10	Entrega del Plan Director de Seguridad	0 días
11	**Formación**	**24 días**
12	Transferencia conocimiento y metodología	12 días
13	Cuadro de Mando	12 días
14	**Finalización**	**10 días**
15	Elaboracion y preparación del documento ejecutivo	10 días
16	Presentación del documento ejecutivo	0 días



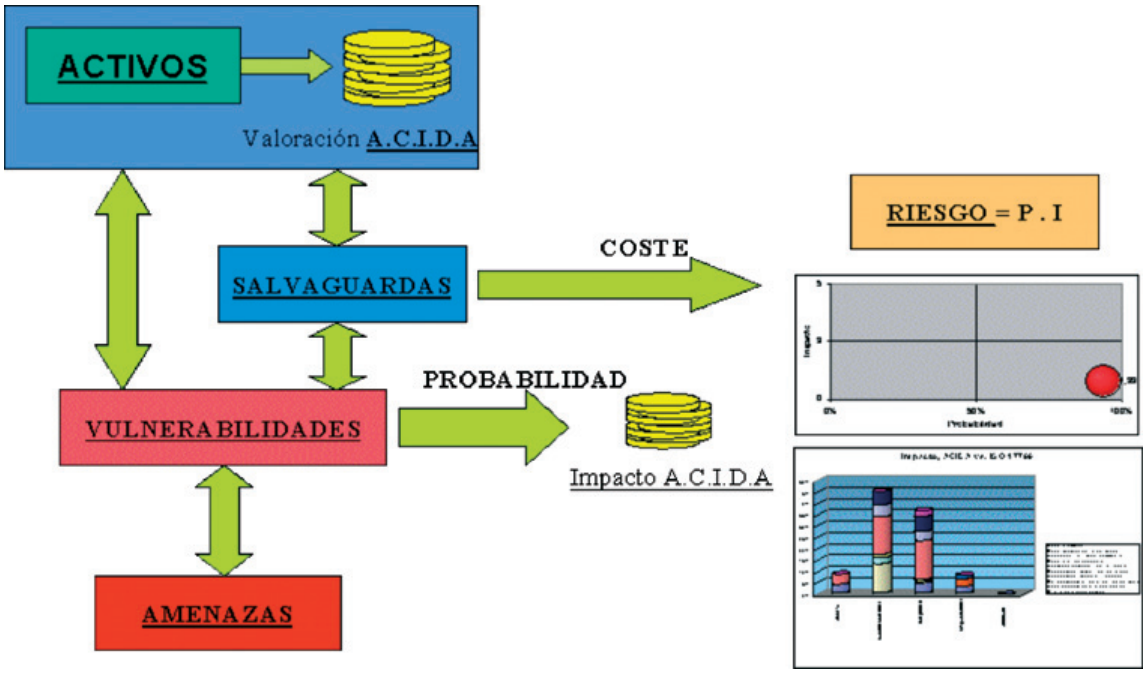
2.7 Metodología y estándares

El proyecto se ha realizado con la metodología de la empresa colaboradora, SIA, que tiene un desarrollo propio basado en los estándares definidos en la metodología MAGERIT (del Ministerio de Administraciones Públicas), que sirve como base para las definiciones, conceptos y la planificación de tareas a realizar. Es una metodología clara y de referencia en el ámbito nacional.

Por otra parte, el grado de madurez de la organización en cuanto a la seguridad se fundamenta en la norma UNE-ISO/IEC 17799 "Guía de Buenas Prácticas para la Gestión de la Seguridad de la Información". A partir de ésta se ha medido el estado de la seguridad en nuestra organización.

El cálculo del valor de los activos y del riesgo asociado se realiza basándose en cinco criterios de seguridad:

- Autenticación, que establece la identidad del usuario y asegura que sea quien dice ser.
- Confidencialidad, que previene contra la divulgación no autorizada de información.
- Integridad, que protege contra la modificación o destrucción no autorizadas de información.
- Disponibilidad, que evita que la información no esté accesible en el momento y de la forma adecuada.
- Auditoría, que asegura que se mantienen evidencias de las acciones realizadas sobre la información.



Esquema de los conceptos de la metodología

RESULTADOS DEL PROYECTO

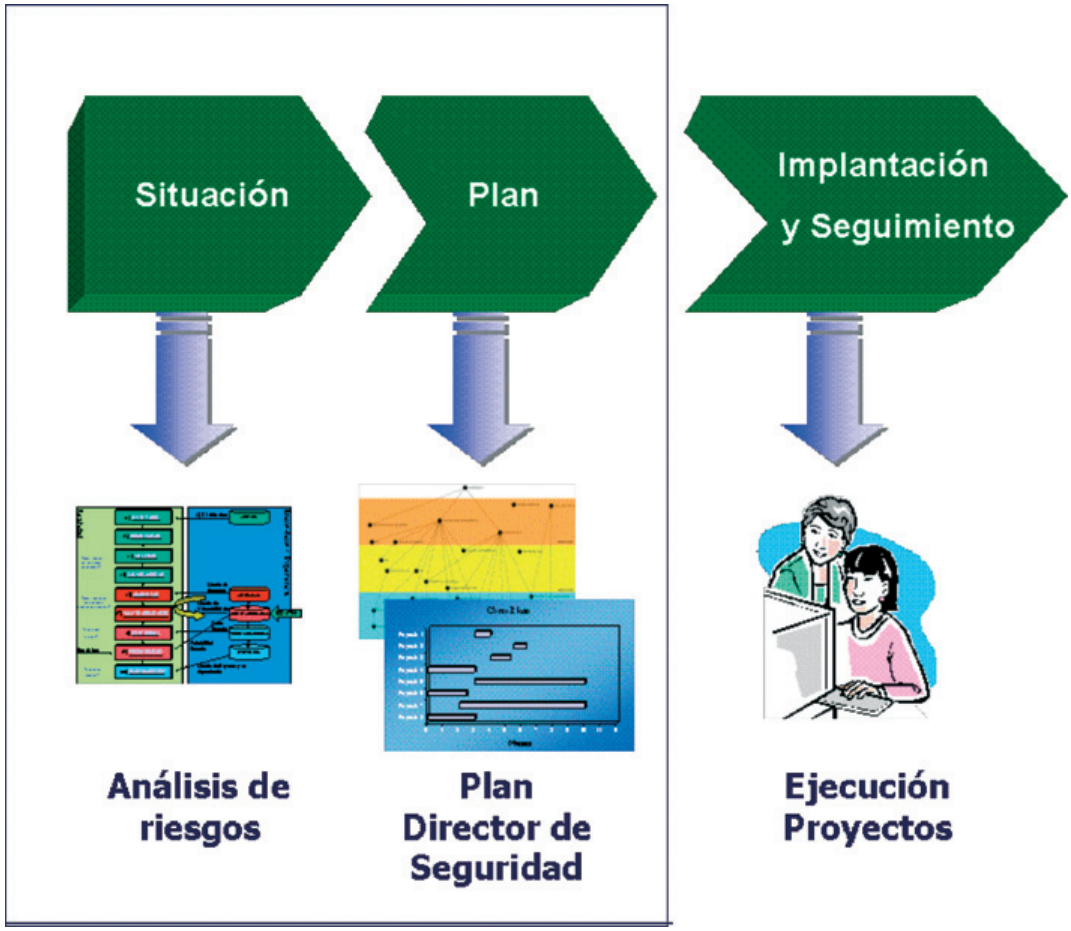
Plan Director de Seguridad

Es el documento más importante del proyecto. Se trata del plan de proyectos definidos a corto, medio o largo plazo, cuyo objetivo es reducir los niveles de riesgo de la organización.

Con cada uno de los proyectos hay una estimación del esfuerzo a realizar en términos de horas – hombre o monetarios, junto con un análisis coste / beneficio.

El ámbito de estos proyectos es multidisciplinar, pues comprende medidas de seguridad:

- Físicas (como restricción de acceso a los edificios, equipos humanos de seguridad, etc.).
- Organizativas (por ejemplo las políticas, prácticas y procedimientos de seguridad).
- Legales (como la inscripción de ficheros en los registros administrativos correspondientes).
- Técnicas (adaptación de aplicaciones, adopción de mecanismos de cifrado de datos, etc.)



Estrategia de Seguridad

Adecuación a la norma UNE-ISO/IEC 17799

Por medio de una serie de trabajos de investigación se han llegado a estudiar las vulnerabilidades referidas en la norma internacional, clasificadas en sus diez capítulos:

- Política de seguridad.
- Organización de la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Seguridad física y del entorno.
- Comunicaciones y explotación.
- Control de accesos.
- Desarrollo y mantenimiento.
- Continuidad de la actividad.
- Conformidad.

El resultado de los mismos se refleja en un documento en el que se cuantifica el número de recomendaciones de la norma que se están cumpliendo. Estos datos forman el llamado "cuadro

de mando de seguridad", que sirve a la dirección de la organización para ver el grado de adecuación en el momento actual y compararlo con situaciones futuras.

PRESENTE Y FUTURO DE LA SEGURIDAD DE LA SGI

El Plan Director de Seguridad ha supuesto el conocer el mapa de riesgos de la SGI y tener un plan estratégico basado en la seguridad.

De esta forma, se han conseguido definir las medidas correctoras para reducir el número y el impacto de los incidentes de seguridad, proporcionar una visión global de la seguridad, estructurando los planes para mejorarla en estrategias de acción a corto, medio y a largo plazo.

Todo ello ha permitido a la dirección de la SGI conocer la situación actual y planificar la situación futura en cuanto a la seguridad de la información, para reducir los niveles de riesgo, lo que redundará en un mejor servicio a la gestión de la Seguridad Social.