Implantación de un sistema de gestión de la seguridad de la información y certificación ISO 27001 en la Administración Pública

TECNIMAP 2010

Manuel Cabrera Silva
José María Vinagre Bachiller
Paul Jabbour Padilla
Fernando Román Muñoz

Subdirección General de Tecnologías de la Información
Ministerio de Sanidad y Política Social

Palabras Clave

Análisis de riesgos, Esquema Nacional de Seguridad, MAGERIT, PDCA, PILAR, Seguridad, SGSI, 27001, 27002.

Resumen

Los sistemas de información están expuestos a un número cada vez mayor de amenazas que, aprovechando sus vulnerabilidades, constituyen riesgos sobre activos tan críticos como la información. Asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios es un deber ineludible. A esta necesidad pretenden dar respuesta la Ley 11/2007, de 22 de junio, y el recientemente publicado Real Decreto 3/2010, de 8 de enero. El nivel de seguridad que proporcionan los medios técnicos por sí mismos es insuficiente: la gestión de la seguridad de los sistemas de información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este trabajo describe las tareas que requiere el establecimiento de este sistema de gestión adoptando como referencia el enfoque propuesto por el estándar ISO/IEC 27001. Finalmente, se incluye un breve análisis de las diferencias que este enfoque presenta en relación con el Esquema Nacional de Seguridad.

Introducción

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos establece en su primer artículo la obligación de las Administraciones Públicas de utilizar las tecnologías de la información de forma que se aseguren la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Las referencias a la seguridad a lo largo de la mencionada ley son constantes. Y no puede ser de otra forma ya que, como recuerda el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, *la necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos*.

El objeto del Esquema Nacional de Seguridad, como requiere el artículo 42.2 de la Ley 11/2007, es precisamente establecer los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

La política de seguridad de una organización es la definición del marco general en el cual decide proteger los datos e informaciones que maneja y los servicios que presta. Contemplará, entre otras cuestiones, los objetivos de seguridad de la información de la organización, los requerimientos legales o contractuales relativos a la seguridad de la información o los criterios de evaluación y aceptación del riesgo.

Pero garantizar la seguridad de la información conforme al marco definido en la política de seguridad requiere un proceso sistemático, documentado y conocido por toda la organización, que es lo que conocemos como sistema de gestión de la seguridad de la información (en adelante, SGSI).

Cuando una organización decide implantar un SGSI debe elegir el camino para hacerlo, siendo el estándar internacional en este sentido el que definen la norma ISO/IEC 27001 y el conjunto de buenas prácticas ISO/IEC 27002 (anteriormente ISO/IEC 17799). Este trabajo describe el camino basado en estos estándares desde la experiencia del Ministerio de Sanidad y Política Social en la implantación de su SGSI.

El SGSI según la norma ISO/IEC 27001

La norma ISO/IEC 27001 fundamenta su modelo de SGSI en el modelo de mejora continua tradicional en los sistemas de gestión de la calidad: el llamado círculo (o mejor, espiral) de Deming o modelo PDCA (de las siglas en inglés: *plan*, *do*, *check*, *act*).

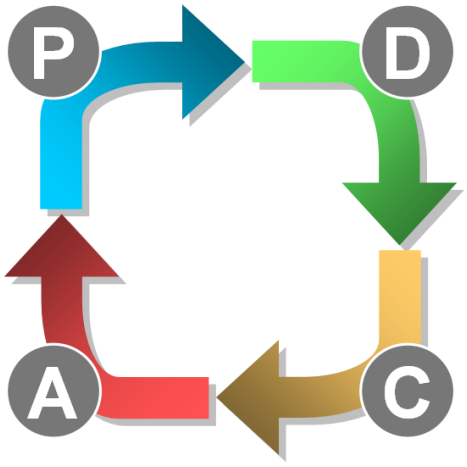

Figura 1. Ciclo de vida PDCA

El punto de partida es el planeamiento (*Plan*) del sistema de gestión. A continuación, ha de ejecutarse lo planeado (*Do*), lo que incluye tanto la implementación del sistema de gestión como su ejecución. Tras la puesta en marcha del sistema, se inician las actividades de monitorización y revisión del mismo (*Check*). Como resultado de ambas, se identificarán e implantarán mejoras en el sistema (*Act*).

Un SGSI debe permitirnos conocer los riesgos a los que están sometidos nuestros datos, información y servicios, y asumirlos, minimizarlos, transferirlos o controlarlos mediante una operativa definida, documentada y conocida por toda la organización, que a su vez debe ser revisada y mejorada de forma continua.

Seguidamente, describiremos cada una de estas cuatro fases, pero comenzaremos revisando una serie de recomendaciones que se deberían tener en cuenta antes de iniciar el establecimiento del SGSI.

Recomendaciones previas

Antes de iniciar la puesta en marcha de un SGSI, es conveniente tener presente la necesidad, cuando no la obligación legal, de realizar ciertos planteamientos, disponer de ciertas herramientas y llevar a cabo determinadas actividades que son esenciales para garantizar la eficacia posterior del SGSI.

En primer lugar haremos referencia al compromiso de la Dirección. Como en cualquier otra iniciativa de este calado, el respaldo por parte de la Dirección es una condición necesaria para el éxito real de la misma. De hecho, este requerimiento se recoge en el estándar mismo y no se conforma con la mera declaración: se exige demostrar su implicación en el proceso. Es especialmente importante, a este respecto, la responsabilidad que tiene la Dirección de revisar en profundidad el SGSI (al menos una vez al año), como veremos más adelante.

Especial importancia tiene disponer de un sistema de gestión documental. La documentación es una actividad clave en cualquier SGSI. Los requisitos del sistema de gestión documental no deben ser demasiado elevados, pero como mínimo éste ha de permitir definir y gestionar los flujos de aprobación de los documentos y controlar el acceso y el tratamiento de los documentos definidos para cada rol contemplado en el modelo organizativo del SGSI.

También es imprescindible tener un inventario de activos actualizado y operativo. Se entiende por activo cualquier elemento que tenga valor para la organización (instalaciones, equipos, aplicaciones, servicios, etc.). Por ello, cualquier proyecto encaminado a disponer un sistema de inventario versátil y fácil de mantener e integrar con otros sistemas es una magnífica palanca para el éxito del SGSI.

Otra herramienta esencial para el establecimiento de un SGSI es un sistema de gestión de incidencias de seguridad. Es la herramienta habitual del servicio de atención a los usuarios (CAU), y debería bastar con adaptarlo a los flujos de gestión de incidencias de seguridad que definamos en nuestro SGSI. También aquí, la orientación hacia estándares de buenas prácticas en gestión de servicios, como por ejemplo ITIL, constituye una sinergia a tener en cuenta.

Cualquier SGSI debe incluir la adecuada gestión de la normativa legal que en cuestión de sistemas de información está obligada a cumplir la organización. En consecuencia, es recomendable tener en marcha el cumplimento de la normativa aplicable antes de poner en marcha el SGSI. A este respecto, es particularmente relevante el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, en particular, de las auditorías que exige.

En un nivel más táctico, es deseable disponer de una política de seguridad para la organización, si no explícitamente definida, al menos tácita. Con la publicación del

Esquema Nacional de Seguridad ha dejado de ser una recomendación para ser una obligación. Asimismo, será de gran ayuda la experiencia previa en análisis de riesgos. Existen muchas metodologías para realizar análisis de riesgos, pero en el ámbito de las Administraciones Públicas lo recomendable es utilizar MAGERIT y la herramienta de gestión asociada: PILAR.

Finalmente, en un ámbito más técnico, constituye un buen punto de partida toda experiencia relativa a la realización de auditorías técnicas de seguridad sobre sistemas, redes y aplicaciones (*hacking* ético), así como en la ejecución de proyectos de implantación de medidas de seguridad.

Fase de planeamiento (*plan*)

El primer paso de la fase de planeamiento para establecer un SGSI es definir el ámbito de aplicación del proyecto, su alcance. No tiene por qué ser todo o nada. De hecho, es recomendable empezar con pasos cortos. Hay que tener en cuenta que la definición del ámbito del SGSI es clave, ya que determina la complejidad inicial del proyecto. Si, por ejemplo, el ámbito no incluye usuarios finales, no será necesario analizar los riesgos existentes en activos tales como sus puestos de trabajo o las redes de acceso que utilizan. También es evidente que la definición del alcance afecta a la estimación de las necesidades de recursos que conllevará el proyecto de implantación del SGSI.

Se definirá explícitamente, si no existía ya, la política de seguridad que orientará a la organización en cuestión de fijación de objetivos y principios de actuación en todo lo relativo a seguridad de la información, en el tratamiento de los requerimientos legales o contractuales relativos a la seguridad de la información, y en el establecimiento de los criterios con los que se va a evaluar y tratar el riesgo. Es un documento clave y por ello debe ser aprobado por la dirección.

Es indispensable definir el modelo organizativo que soportará el funcionamiento del SGSI. Incluirá la definición del conjunto de roles, así como las funciones y responsabilidades correspondientes a cada rol. Un buen modelo buscará el compromiso entre responsabilidad y operatividad, de forma que las decisiones se tomen siempre al nivel más adecuado: la organización debe ser capaz de dar respuesta ante los incidentes de seguridad habituales en el día a día y reaccionar con eficacia ante incidentes de seguridad graves.

Figura 2. Ejemplo de Modelo Organizativo del SGSI

La figura más relevante del modelo organizativo será el Comité de Seguridad, máximo órgano decisor del SGSI, integrado por directivos de todas las áreas implicadas directamente en la seguridad. Son claros candidatos Tecnologías de la Información, Oficialía Mayor, Asesoría Legal y Recursos Humanos. También son parte esencial del

Comité de Seguridad el Responsable de Seguridad, encargado de la planificación, coordinación y ejecución de las actividades de seguridad de la información en toda la organización, y el Auditor Interno. Por supuesto, el modelo organizativo incluirá a los responsables de las diferentes áreas técnicas (Sistemas, Infraestructuras y Desarrollo), como responsables de la ejecución de las actividades de seguridad de la información en sus áreas respectivas.

La actividad más definitoria de esta fase es el análisis de riesgos. A fin de conocer con el mayor rigor posible los riesgos a los que están expuestos los activos que deseamos proteger, es necesario llevar a cabo un proceso sistemático de estimación de los riesgos a los que está expuesta nuestra organización. El análisis de riesgos un proceso en el que generalmente conviene contar con técnicos expertos.

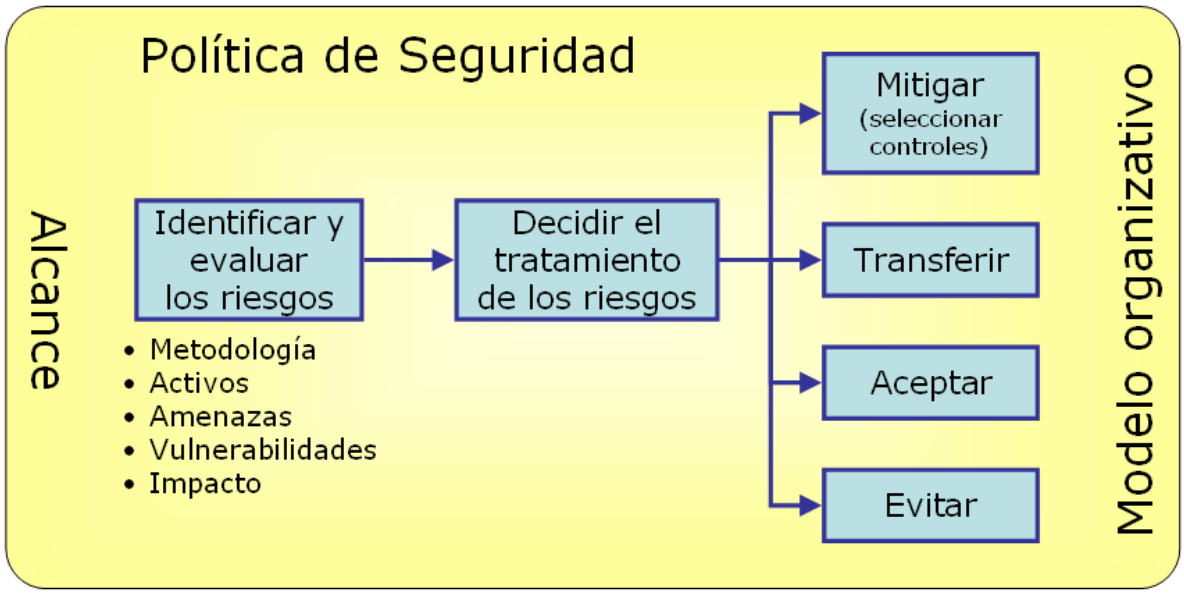

Figura 3. Análisis de Riesgos

El análisis de riesgos tendrá como resultado el tratamiento que la organización dará a cada uno de los diferentes riesgos, teniendo como referencia la política de seguridad y la normativa aplicable. Es lo que el estándar denomina selección de controles, y lleva asociada la identificación de indicadores de eficacia de las medidas de tratamiento de los riesgos. No se debe minimizar la importancia de esta última tarea, ya que está en la base del ciclo PDCA. Los indicadores aportarán información sobre la eficacia de nuestro SGSI y deben, de esta forma, ayudarnos a reorientarlo al final de cada ciclo.

En relación con la selección de controles, la norma ISO/IEC 27002 constituye un buen punto de partida a la hora de definir qué controles deseamos implantar. De hecho, la norma ISO/IEC 27001 (y también el Esquema Nacional de Seguridad) obliga a redactar un documento de aplicabilidad, en el cual se deben justificar la no aplicabilidad de aquellos controles que se decida no tener en consideración y la aplicabilidad de aquellos que es necesario tratar.

Este es también el momento de determinar si se desea obtener la certificación de nuestro SGSI. El proceso de certificación es un proceso relativamente dilatado, de ciclos de tres años. Por supuesto, tiene pros y contras. Entre los primeros, podemos mencionar que la obligación de someterse a auditorías anuales supone un acicate para mejorar la gestión del SGSI o también que permite obtener una acreditación nacional (con alcance internacional), contribuyendo positivamente a la imagen de la organización. En sentido opuesto, debe tenerse presente que requiere una dedicación adicional a las exigencias derivadas del propio SGSI y que supone un coste económico.

Por último, mencionaremos de nuevo la importancia del compromiso de la dirección en toda esta fase, ya que el tratamiento que se dará a los diferentes riesgos (que se plasmará en un plan de acción) supone o bien aportar los recursos necesarios para implantar las salvaguardas contempladas en dicho plan de acción o para transferir el riesgo a un tercero o bien asumir (aceptar explícitamente) la responsabilidad de los daños que podrían causar los riesgos residuales, aquellos para los que no se va a implantar salvaguarda alguna ni se van a transferir a terceros.

Fase de ejecución (*do*)

La ejecución del SGSI tiene dos vertientes claras: lo que podríamos llamar el día a día y la puesta en marcha de mejoras.

El día a día lo ocupan las tareas de gestión de las operaciones del SGSI y de los recursos asignados al SGSI para el mantenimiento de la seguridad de la información. Corresponden al funcionamiento controlado de la maquinaria. Incluye la ejecución de los procedimientos y medidas previstos para la detección y respuesta de los incidentes de seguridad.

Entre los requerimientos menos aplaudidos a la hora de mantener vivo un SGSI se encuentra la obligación de mantener debidamente documentados los múltiples procedimientos operativos de gestión de la seguridad. Por ejemplo: cómo se gestionan los incidentes de seguridad, cómo se autorizan y revocan los privilegios de acceso, cómo se llevan a cabo las actualizaciones de software o cómo se bascula al centro de respaldo. Dado el esfuerzo requerido, es muy recomendable planificarlo también a corto, medio y largo plazo.

También forman parte del día a día el desarrollo de programas de formación y concienciación continua en relación con la seguridad de la información y dirigidos a todo el personal.

La otra cara de esta fase es la de la puesta en marcha de mejoras. Una vez que, tras el análisis de riesgos, se han identificado los principales riesgos a los que se hallan expuestos nuestros activos y seleccionado los controles a aplicar, ha de elaborarse un plan de acción. Este plan incluirá todos los proyectos que se consideran adecuados para implantar las salvaguardas seleccionadas. Es aconsejable distribuir los proyectos en el tiempo, agrupándolos en corto, medio y largo plazo, según criterios tales como su complejidad, urgencia y disponibilidad de recursos.

El plan de acción (o de tratamiento de riesgos) debe priorizar las acciones, incluir las necesidades de recursos y sus responsabilidades. Y, obviamente, debe contemplar la implementación de las métricas que permitan medir la eficacia de los controles seleccionados.

Fase de monitorización (*check*)

La necesidad de monitorizar el funcionamiento del SGSI está en su base. Algunas de las actividades de monitorización se realizan de forma continua y otras son puntuales. Deben ser continuas, por ejemplo, la detección de incidentes de seguridad, la supervisión de los recursos empleados en la gestión de la seguridad de la información o el registro de cualesquiera eventos que hayan supuesto o puedan suponer algún impacto sobre la efectividad del SGSI.

Pero muchas otras actividades de vigilancia se realizan de forma puntual y es por ello muy recomendable planificarlas. Destacaremos las siguientes:

- Medir con la periodicidad definida la efectividad de los controles para verificar que se cumple con los requisitos de seguridad. Es recomendable utilizar una

herramienta de seguimiento flexible en la generación de informes y orientada a integrarse con un cuadro de mando. Por supuesto, es importante automatizar las medidas cuando sea posible y eficiente hacerlo.

- Realizar auditorías internas a nuestro SGSI (la norma recoge la figura del Auditor Interno, como se mencionó al describir el modelo organizativo).
- Realizar las auditorías exigidas por la legislación aplicable. El caso más evidente es el de las auditorías exigidas por la Ley Orgánica de Protección de Datos de Carácter Personal.
- Si se ha optado por certificar nuestro SGSI, es obligatorio realizar también la auditoría externa y las revisiones que exige la empresa certificadora.
- Revisar los resultados de las anteriores auditorías de seguridad, incidentes de seguridad, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas por parte de la dirección para garantizar que el alcance definido al comienzo sigue siendo el óptimo, constatar la eficacia creciente del SGSI y validar las medidas correctoras.

Fase de mejora (*act*)

Corresponde a esta fase la puesta en marcha de las mejoras identificadas a partir de las actividades de verificación mencionadas anteriormente.

Estas mejoras pueden ser tanto acciones preventivas como correctivas, pero orientadas siempre hacia la solución definitiva del problema. En este sentido, juega un papel importante el análisis de la causa raíz, aquella que constituye la razón de fondo del incidente que queremos resolver.

Las mejoras introducidas son asimismo medidas de seguridad y debe, por tanto, verificarse que alcanzan los objetivos previstos. De la misma forma, deben ser adecuadamente documentadas y comunicadas a las partes interesadas.

De especial relevancia para el éxito del ciclo de mejora es la óptima ejecución de la revisión por la Dirección (recogida en el apartado 7 de la ISO/IEC 27001). Consiste en una revisión periódica en la que se presentan a la Dirección una foto suficientemente completa del SGSI y propuestas de mejora, de forma que la Dirección tome las decisiones que considere oportunas sobre análisis de riesgos, cambios en procedimientos y controles de seguridad, recursos necesarios o indicadores de eficacia. El conjunto de decisiones adoptadas es la entrada fundamental para la fase de planeamiento que abrirá el ciclo PDCA siguiente.

Adecuación al Esquema Nacional de Seguridad

El real decreto del Esquema Nacional de Seguridad recientemente publicado ha venido a establecer los principios básicos y requisitos mínimos de una política de seguridad en la utilización de medios electrónicos que permitan la adecuada protección de la información y los servicios, mediante un marco normativo común para las Administraciones Públicas.

Al tratarse de un enfoque distinto al que hemos descrito en este trabajo, se plantea inmediatamente la cuestión de en qué medida es satisfecho el Esquema Nacional de Seguridad por una organización que ya dispone de un SGSI conforme con la recomendación ISO/IEC 27001. Como resumen orientativo, la tabla siguiente recoge algunas de las diferencias entre las dos aproximaciones a la gestión de la seguridad de la información.

GESTIÓN SEGÚN ISO/IEC 27000	GESTIÓN SEGÚN ESQUEMA NACIONAL DE SEGURIDAD
Su objetivo es la gestión de la seguridad de la información	Regula los principios básicos y establece los requisitos mínimos
Deja libertad para elegir el alcance del SGSI	Se refiere a los medios electrónicos utilizados por los ciudadanos en su relación con las Administraciones Públicas
Se enfoca hacia los recursos en general, no limitándose a los sistemas de información	Se enfoca en el sistema de información (como conjunto organizado de recursos)
El análisis de riesgos siempre es obligatorio	El análisis de riesgos sólo es real para sistemas de categoría media y alta (en materia de seguridad)
No obliga a implantar medidas de seguridad concretas, aunque requiere justificar su no aplicación	Obliga a implantar un conjunto determinado de medidas de seguridad (según la categoría del sistema)
Exige la realización de auditorías periódicas sobre el alcance del SGSI	Exige una auditoría bienal de conformidad con el ENS para los sistemas de categoría media y alta (en materia de seguridad)

Conclusiones

La gestión de la seguridad de los sistemas de información debe realizarse mediante un enfoque sistemático. El SGSI propuesto por el estándar ISO/IEC 27001 ofrece numerosas ventajas:

- La toma de decisiones sobre la seguridad de los activos críticos de información se basa en información a priori (análisis de riesgos) y a posteriori (auditorías e indicadores).
- Se orienta a la mejora continua, a través de la gestión de acciones correctivas y preventivas.
- Integra directamente en la gestión de la seguridad a todos los actores necesarios.
- Incluye el cumplimiento de la normativa legal aplicable.
- Si se decide obtener la certificación ISO/IEC 27001 del sistema, mejora la imagen del organismo y se contribuye a generar confianza entre los ciudadanos y empresas.
- Sitúa a la Administración Pública en una posición privilegiada para cumplir el Esquema Nacional de Seguridad.
- Las normas ISO/IEC 27001 y 27002 están razonablemente elaboradas, sirviendo de guía clara en el proceso.

Por supuesto, también supone un mayor nivel de exigencia:

- Requiere un esfuerzo suplementario de gestión, mayor en las etapas iniciales del proyecto.
- La formalización inherente al estándar supone el riesgo de perder de vista el objetivo básico, que no es otro que la seguridad de los sistemas de información. Por ello, es importante valorar continuamente si la utilidad que aporta cada elemento del SGSI es mayor que su coste.