tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

179

IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA UNE 71502

Eloy Rafael Sanz Tapia
Asesor Técnico - Seguridad
Consejería de Educación - Junta de Andalucía

Juan Almorza Daza
Jefe de Sistemas de Información - Secretaría General Técnica
Consejería de Educación - Junta de Andalucía

Lourdes Benítez Sánchez-Cid
Jefa del Servicio de Informática - Secretaría General Técnica
Consejería de Educación - Junta de Andalucía

José Manuel Pavón Álvarez
Consultor - Seguridad
ISOTROL, S.A

Eloy Rafael Sanz Tapia
Juan Almorza Daza
Lourdes Benítez Sánchez-Cid
José Manuel Pavón Álvarez

Palabras clave

Seguridad de la información, sistemas de gestión, UNE 71502.

Resumen de su Comunicación

Esta comunicación describe la implantación, aún en curso, de un Sistema de Gestión de Seguridad (SGSI) de la Información conforme a la norma UNE71502 en la Consejería de Educación de la Junta de Andalucía. Se describe el estado actual de los sistemas de información de la Consejería, los objetivos del plan de implantación, las normas que están teniendo en cuenta, el modelo de datos deseado del sistema y las actuaciones que se están llevando a cabo. Por último se extraen conclusiones y se realizan algunas reflexiones sobre la experiencia que está suponiendo este proyecto.

Eloy Rafael Sanz Tapia
Juan Almorza Daza
Lourdes Benítez Sánchez-Cid
José Manuel Pavón Álvarez

IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA UNE 71502

1. Introducción

En los últimos años se ha producido un gran crecimiento en materia de sistemas de información y de tecnología en la Consejería de Educación de la Junta de Andalucía. Este crecimiento se debe a distintas causas, entre las cuales podemos destacar las siguientes:

• Los servicios electrónicos ofrecidos por la Consejería tanto a los padres y madres de alumnos (sistema PASEN) como al profesorado (sistema Séneca, proyecto Averroes y otros).

• La incorporación de centros educativos a la Red Corporativa de la Junta de Andalucía y su acceso cada vez más directo y frecuente a recursos internos de la Consejería.

• La implantación de los sucesivos programas de Centros TIC (incorporación de ordenadores al aula).

• La dependencia cada vez mayor de los sistemas de información para la tramitación y el proceso administrativo diario.

Este crecimiento lleva asociado, por supuesto, un incremento en el volumen y flujo de información tratados por los sistemas de la Consejería. Gran parte de esa información es de carácter personal, y en determinados casos de nivel alto según lo dictado por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD).

Se requiere un esfuerzo para mantener los niveles de seguridad de la información adecuados. Esta preocupación por la seguridad, ya presente desde el principio en la Consejería, está actualmente en proceso de formalización mediante la implantación de un Sistema de Gestión de Seguridad de la Información (en adelante SGSI) basado en la norma española UNE 71502.

Este documento describe el proceso de implantación de dicho sistema. En una primera sección se describirán los objetivos que se han marcado al inicio del proyecto, para describir su desarrollo en la siguiente sección. La tercera parte detallará las normas relacionadas con el SGSI así como su estructura, los productos utilizados y el futuro previsto del mismo. Por último se plantearán algunas conclusiones (no definitivas, puesto que el proyecto está aún en ejecución).

2. Objetivos

Los objetivos que se persiguen con el proyecto actualmente en curso son principalmente

• El mantenimiento y, en su caso, mejora de los niveles de seguridad en aplicaciones, sistemas, redes y equipos de escritorio, mediante técnicas de análisis de riesgos y aplicación de controles para la gestión de dichos riesgos.

• La creación de una estructura organizativa de consulta/iniciativa, decisión y seguimiento en materia de seguridad.

• La concienciación en materia de seguridad de todo el personal dependiente de la Consejería (personal técnico del Servicio de Informática, personal administrativo, altos cargos, profesorado...).

• El cumplimiento de la legislación vigente en materia de seguridad de la información y protección de datos de carácter personal.

• La documentación, formalización y registro de los procedimientos relacionados con la seguridad de la información.

3. Desarrollo del proyecto

En junio de 2004 la Consejería elaboró un Plan Director de Seguridad (PDS) con la finalidad de definir estrategias para la protección de la información y detectar medidas técnicas, organizativas y de control necesarias para garantizar su seguridad. Dicho plan incluía
• Una revisión del estado de la seguridad (sistemas existentes, estructuras organizativas relevantes, posibles campos de mejora...).

• Un modelo de seguridad enfocado a la construcción de un SGSI con indicación de los requisitos básicos, la estrategia de implantación y los controles organizativos y técnicos deseables.

• Un plan de proyectos a implementar, orientados a la consecución del modelo de seguridad descrito en el documento anterior.
Los proyectos principales que se han iniciado siguiendo este PDS están siendo desarrollados por personal de la Consejería con asistencia externa por parte de la empresa ISOTROL, S.A. Entre ellos cabe destacar:

• Implantación de herramientas y procedimientos para la gestión de la documentación del SGSI.

• Análisis de riesgos y selección de controles para la reducción de los riesgos detectados.

• Servicios de alerta temprana, análisis de vulnerabilidades, cumplimiento de la política de seguridad y monitorización y detección remota.

• Soporte y desarrollo de procedimientos de protección de redes.

• Elaboración de guías de configuración segura de sistemas. Desarrollo de procedimientos de configuración, endurecimiento y monitorización de sistemas.

• Formación y concienciación, tanto de los usuarios finales como del personal técnico, acerca de normativa aplicable y buenas prácticas en materia de seguridad.

4. El SGSI

Normativa relacionada

El Sistema de Gestión de Seguridad de la Información se ha diseñado siguiendo lo indicado por la norma española UNE 71502:2004 - Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Se ha seguido la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) versión 2.0, del Ministerio de Administraciones Públicas, para realizar el análisis de riesgos. Los controles para la reducción de los riesgos se han seleccionado de entre los descritos por la norma ISO/IEC 17799 (Information technology - Code of practice for information security management). Se han tenido en cuenta además normas nacionales (Criterios de seguridad, normalización y conservación, del MAP) y autonómicas (resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por

Eloy Rafael Sanz Tapia
Juan Almorza Daza
Lourdes Benítez Sánchez-Cid
José Manuel Pavón Álvarez

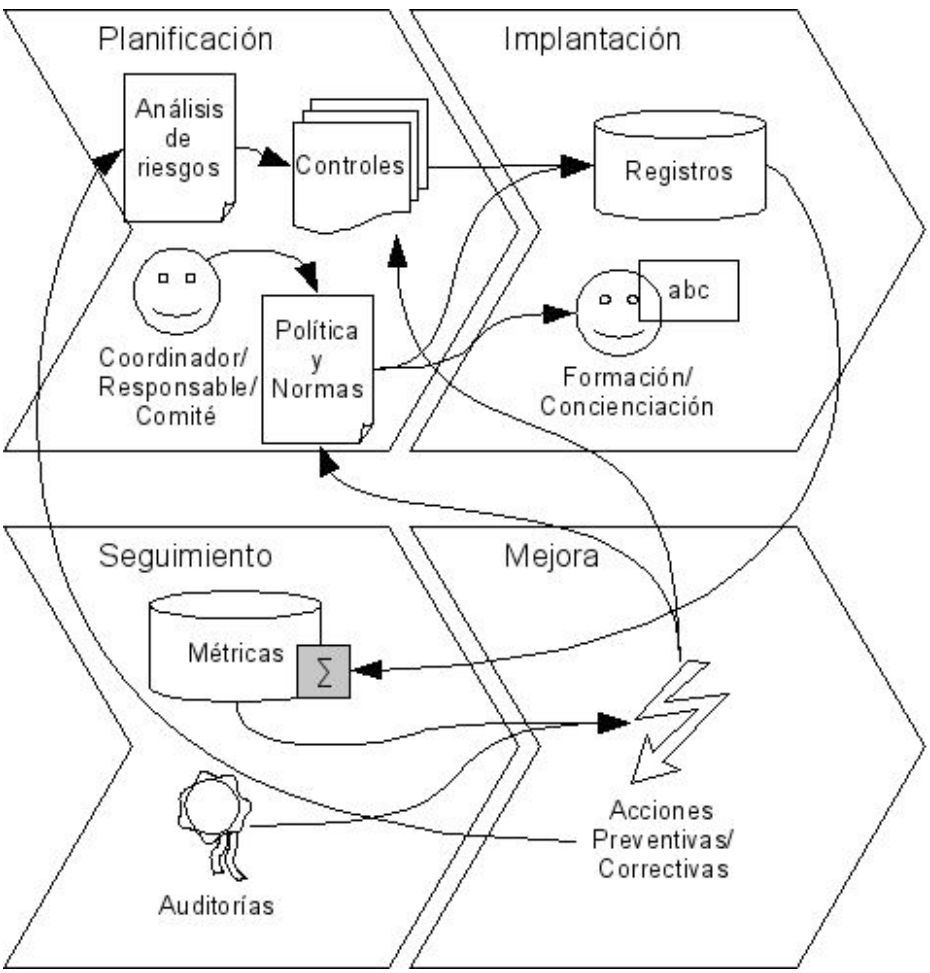

Fig.1: Esquema del SGSI

la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía).

Estructura

La figura 1 muestra gráficamente y de forma concisa la estructura del SGSI y las relaciones entre sus elementos. Se está siguiendo el ciclo iterativo PDCA (plan-do-check-act, planificación-implantación-seguimiento-mejora) propugnado por la norma 71502.

En la fase de planificación se ha realizado un análisis de riesgos sobre el ámbito del SGSI: se han detectado los activos de información, se han descrito las amenazas a que están sometidos y se ha calculado el impacto de la materialización de dichas amenazas y, en función de la frecuencia probable de dicha materialización, el riesgo que soportan. En base a ese análisis de riesgos se han seleccionado controles de entre los que define el estándar 17799. En esta fase también se ha iniciado la definición de la estructura organizativa, incluyendo el Comité de Seguridad y el Responsable o Coordinador de Seguridad. Por último, se han escrito la Política y las Normas (nivel medio) de Seguridad y se han documentado los Procedimientos de Seguridad (ver tabla 1). Cada procedimiento de seguridad indica su objeto y alcance, los documentos de referencia, los responsables de realizarlo, la operativa a desarrollar y los registros que deben quedar de la ejecución del mismo.

En la fase de implantación (actualmente en avanzado desarrollo) se pondrán en marcha los controles y se comenzarán a seguir de manera formal los Procedimientos de Seguridad. De unos y otros se extraerán registros que describan el funcionamiento normal del SGSI (solicitudes de nuevas reglas de cortafuegos, incidentes detectados por las sondas de detección de intrusiones, revisiones periódicas de listados de usuarios y privilegios de acceso...). También se iniciará un plan de formación y concienciación sobre la normativa del SGSI y la legislación aplicable en materia de seguridad de la información.

La fase de seguimiento evaluará el funcionamiento del SGSI principalmente de dos formas: mediante la generación de métricas asociadas a los registros y mediante auditorías, tanto internas como externas.
Esa evaluación se traducirá posiblemente en modificaciones preventivas y/o correctivas del SGSI, persiguiendo la mejora continua del sistema. Las modificaciones se producirán principalmente (aunque no necesariamente) sobre la documentación, el análisis de riesgos y los controles.

Productos utilizados y obtenidos

Para la implantación de los controles técnicos se ha utilizado una mezcla de productos libres y propietarios. Nmap para detección de servicios ofrecidos, Cacti y Nagios para monitorización de servidores, DocMGR como gestor documental, OpenOffice.org como soporte ofimático, OpenDocument y PDF como formatos de documentación, Nessus para análisis de vulnerabilidades, Symantec ESM para control de cumplimiento de política, Checkpoint FW1 y Proventia ISS para protección perimetral, servicios de seguridad gestionada (MSS) y de alerta temprana (DeepSight) de Symantec...

También se está desarrollando un modelo de datos y una aplicación para la gestión de servidores y dispositivos, incluyendo actuaciones sobre los mismos, aplicaciones servidas, presencia en subredes, vulnerabilidades detectadas...

Futuro

A corto plazo se desea certificar el SGSI implantado según la norma UNE 71502 ante AENOR, lo que implicará una auditoría externa por una empresa de acreditación y revisiones periódicas del sistema.
La aparición en octubre de 2005 del estándar internacional ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) inicia una familia de estándares (ISO27000) sobre Gestión de Seguridad de la Información. En un futuro próximo será interesante seguir su evolución y, en su caso, adaptar el SGSI a esta norma y certificarlo.

5. Conclusiones

La implantación del SGSI en la Consejería de Educación está teniendo muchas ramificaciones y efectos secundarios, aparte del deseado incremento de la seguridad. Todos los implicados están aprendiendo y comprendiendo partes del funcionamiento de los sistemas de información de la Consejería que les dan mejor visión de conjunto.

Hay algunas dificultades, como no podía ser menos en un proyecto de esta envergadura. La implantación de algunas medidas técnicas puede ocasionar molestias a los usuarios finales o trabajo adicional al personal del Servicio de Informática.

La formalización de los procesos, muchos de los cuales ya se realizan correctamente pero de manera no documentada, ha sido bien aceptada al proporcionar una asignación de responsabilidades y un valioso apoyo de la dirección. Por ejemplo, el proceso de gestión de reglas de cortafuegos incluye una solicitud formal y no técnica del acceso, indicando organismo, motivo y duración. El responsable del proceso tiene capacidad de decidir la mejor combinación de reglas para atender dicha solicitud, así como la caducidad

de dichas reglas.

La recogida de registros de actividad pudiera parecer tediosa y, de hecho, suele criticarse en los sistemas de gestión de calidad (71502, al igual que ISO 9000, es en cierto modo un sistema de gestión de calidad). La ventaja de aplicar el sistema en un entorno ya de por sí tecnológico, con personal muy cualificado y acostumbrado a manejar sistemas complejos, facilita que la toma de registros se haga de manera automática. Por ejemplo: se está pensando en modificar (o "envolver") las herramientas de parcheo más comunes de los sistemas Solaris y Linux (probablemente también de los sistemas Windows) para que quede constancia de forma automática de la instalación de nuevos parches de seguridad. Dicho registro será recibido también por la empresa que proporciona los servicios de seguridad gestionada (ISOTROL, S.A.) para que sea tenido en cuenta en los sucesivos análisis de vulnerabilidades e informes de alerta temprana.

La documentación del SGSI se almacena de forma versionada y con acceso limitado en función de su clasificación (público/interno/confidencial) en un sistema de gestión documental basado en software libre (DocMGR). El uso de este sistema se ha extendido al área de Sistemas y Redes del Servicio de Informática con gran aceptación.

La necesidad de mantener un inventario de servidores ha llevado al desarrollo de una aplicación específica que incluye información no relacionada directamente con la seguridad de la información, pero que es de gran interés para el servicio. Es sólo una idea aún, pero el uso intensivo de dicha aplicación y su ampliación en funcionalidad puede cubrir algunos de los procesos y funciones de Soporte y Entrega de Servicios del marco ITIL (Information Technology Infrastructure Library). Pero sobre ITIL se puede hablar mucho... En otro artículo.