

Sistema de Gestión de la Seguridad de la Información UNE-ISO/IEC 27001



Aníbal Díaz
Comité de Entidades de
Certificación de la AEC



Introducción

La norma UNE-ISO/IEC 27001 está integrada por un "Sistema de Gestión de la Seguridad de la Información" y por un "Código de buenas prácticas de la gestión de la seguridad de la información" (anexo A), que establece las pautas a seguir para gestionar la seguridad de la información de forma adecuada y completa.

La norma ISO 27001 surgió de la integración de la norma BS7799-2, "Specifications for Information Security Management Systems", y de la norma UNE-ISO/IEC 17799, "Código de buenas prácticas de la gestión de la seguridad de la información", que se convirtió en el Anexo A.

La idea fundamental que se persigue es la gestión de la seguridad de la información para conseguir unos niveles de seguridad mínimos, y para ello es imprescindible contar con un Sistema de Gestión de la Seguridad de la Información (SGSI), mediante un proceso sistemático, documentado y conocido por toda la organización de forma similar a como se desarrollan los sistemas de gestión de la calidad basados en la norma ISO 9001/ISO 14001, etc.

La seguridad total no es posible al cien por cien, incluso en el caso de que se destinen recursos económicos y materiales, no se puede garantizar una seguridad total. La función que tiene un SGSI consiste en garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma

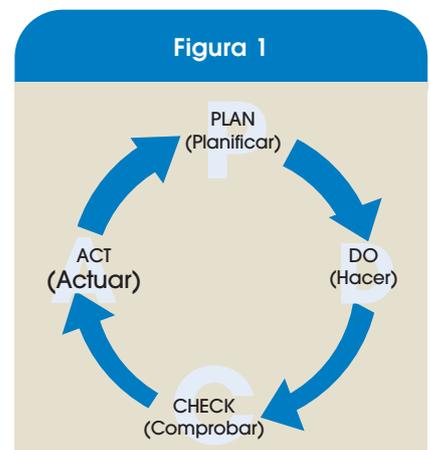
documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías, actualizándose constantemente y mejorando continuamente los sistemas y la gestión de la seguridad de la información.

Esquema general

Para establecer un SGSI, éste se desarrolla utilizando el ciclo de mejora continuo PDCA, que se aplica en todos los sistemas de gestión de calidad, medio ambiente, etc.

- *Plan* (planificar): establecer el SGSI.
- *Do* (hacer): implementar y utilizar el SGSI.
- *Check* (verificar): monitorizar y revisar el SGSI.
- *Act* (actuar): mantener y mejorar el SGSI.

El primer paso en el desarrollo de un SGSI, consiste en definir el alcance y los



límites del SGSI, en términos del negocio, tipo de organización, su ubicación, sus activos, tecnología y justificación de cualquier exclusión aplicable al SGSI.

El primer paso consiste en definir una política de seguridad que especifique el marco general, los objetivos generales que pretende alcanzar y el compromiso de la dirección con el SGSI.

Una vez definido el marco, se establecen las políticas específicas y una serie de procedimientos e instrucciones técnicas con el fin de desarrollar los conceptos aplicables al SGSI y utilizar los requisitos establecidos por la norma ISO 27001.

Una vez establecida la sistemática de trabajo, se deben generar los registros necesarios que sirvan como evidencia del funcionamiento del sistema. Estos registros van a ser el motor de la mayoría de los procesos de mejora, ya que si algo se ha hecho mal en los pasos anteriores o las acciones adoptadas no son suficientes, vamos a tener registros donde se pongan de manifiesto esas carencias y nos va a forzar a adoptar acciones correctivas con el fin de mejorar continuamente el sistema.

En la figura siguiente se muestra un posible ejemplo de la relación entre los distintos documentos que se crean en un SGSI.

Etapas de la implantación de un SGSI

Las etapas que debe cumplir el desarrollo de un SGSI se muestran a continuación, junto con la documentación que se genera (ver figura 3).

Política de seguridad

La política de seguridad, básicamente, tiene que reflejar qué es lo que la organización quiere hacer con respecto a la seguridad de la información, los objetivos que se pretenden conseguir, contemplando los requisitos legales y reglamentarios aplicables y el compromiso de la dirección para conseguirlo.

Alcance del SGSI

Al igual que otros sistemas de gestión, el SGSI se aplica a un alcance determinado. Es necesario definir los servicios, procesos, actividades, departamentos, etc., a los que aplica el SGSI, con especial importancia a las oficinas o instalaciones a las que se aplica, el entorno tecnológico y las características del negocio.

Se tiene que tener en cuenta, a la hora de definir el alcance de un SGSI, que se debe poder acreditar la confianza otorgada a terceros externos a la organización, es decir, a los clientes.

Análisis de riesgos

Es imprescindible definir una metodología de evaluación de los riesgos apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptables. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles.

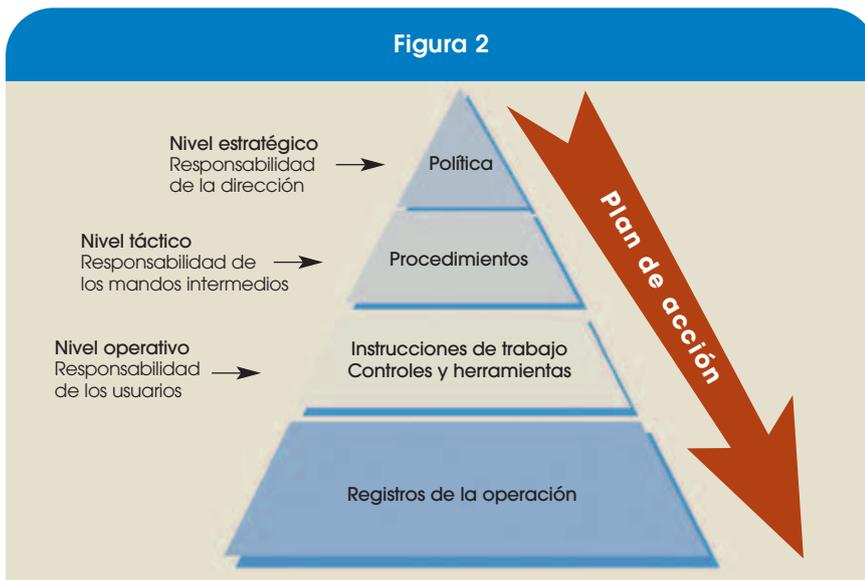
El análisis de riesgos se entiende como un proceso global de estimación y evaluación del riesgo que nos va a permitir conocer los activos, su importancia para la organización y una valoración de los mismos para tener algo consistente en que basarnos a la hora de seleccionar los controles de seguridad que necesitamos.

Existen muchas herramientas y metodologías para abordar un análisis de riesgos, pero la norma no especifica cuál debe aplicarse, tan solo que debe asegurarse que sean las adecuadas y permitir abordar un plan de gestión de riesgos y una selección de los controles necesarios.

Los diferentes hitos de un análisis de riesgos son:

- Identificar los riesgos:
 - identificar los activos que están dentro del alcance del SGSI y a sus responsables directos;
 - identificar las amenazas en relación a los activos;
 - identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
 - identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos identificados por la organización.
- Analizar y evaluar los riesgos:
 - evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;

Figura 2



- evaluar, de forma realista, la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
- estimar los niveles de riesgo;
- determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

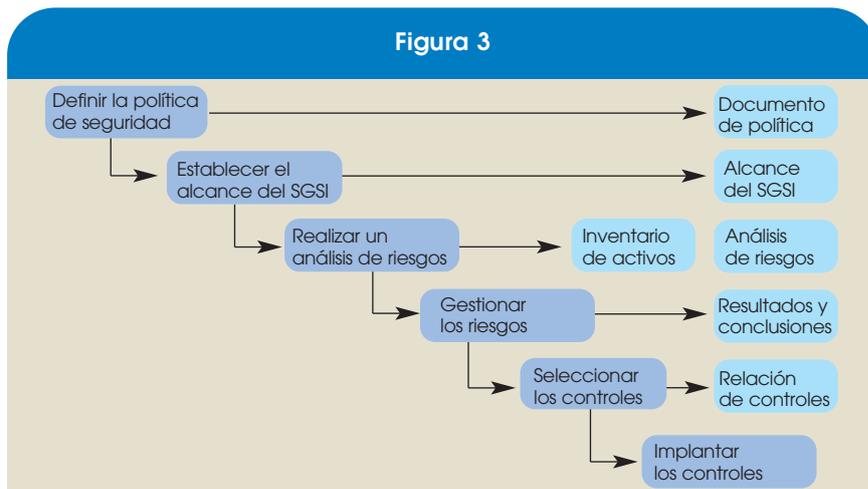
- aplicar controles adecuados;
- aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- evitar el riesgo, por ejemplo, mediante el cese de las actividades que lo originan;
- transferir el riesgo a terceros, por ejemplo, compañías aseguradoras o proveedores de *outsourcing*.

Plan de gestión de riesgos

Después de realizar el análisis de riesgo, la organización debe tomar decisiones sobre qué hacer con cada uno de ellos y plasmarlo en un plan de gestión de riesgos, teniendo en cuenta que de cada riesgo se derivan requisitos o necesidades de seguridad.

Con cada riesgo identificado se pueden adoptar varias posturas:

1. Aceptarlo y no tomar ninguna acción al respecto.
2. Eliminar la causa, cambiando el nivel de disponibilidad o cancelando el contrato con el cliente.
3. Transferirlo, contratando un servicio externo, mediante la firma de un SLA (*Service Level Agreement*).
4. Reducirlo, implantando una serie de controles que garanticen los niveles mínimos de seguridad que se deben cumplir.



Selección de objetivos y controles

Una vez definido el plan de tratamiento de riesgos que identifica las acciones que vamos a implementar, se seleccionan los controles para cubrir los requisitos de seguridad.

Los controles elegidos se seleccionan del Anexo A de la norma ISO 27001, aunque se pueden elegir otros controles que no se encuentran en esta norma y que complementen los controles seleccionados.

Con el fin de comprobar la eficacia de los controles seleccionados y su implantación, se definen una serie de métricas que nos permiten comprobar la eficacia de los controles seleccionados.

Declaración de aplicabilidad e implantación

La selección de los controles aplicables se plasma en un documento que se denomina "Declaración de Aplicabilidad", donde se recoge para cada objetivo y cada control de la norma las razones de su selección o exclusión del SGSI con respecto a la organización, es muy importante plasmar cuales son los controles aplicables a la organización, teniendo en cuenta el tipo de negocio, organización, personal, infraestructuras, etc.

La norma tiene 133 controles de seguridad, algunos de ellos bastante selectivos, por lo que algunas organizaciones prefieren excluir del sistema varios

controles y dejar un SGSI más sencillo de implantar, mantener y controlar, pero esas exclusiones deben estar perfectamente justificadas y argumentadas.

Se trata de un documento fundamental dentro del SGSI, y tendrá que estar disponible para los auditores que vayan a certificar el sistema, ya que es aquí donde van a comprobar qué controles se han implantado y las razones de su implantación, pero, sobre todo, cuáles no se han implantado y por qué.

Revisión y mejora continua

El SGSI se debe de revisar regularmente atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas, tener en cuenta que no se termina con la implantación del sistema y la certificación, sino que el sistema se debe de mejorar continuamente.

Cualquier sistema de gestión lleva consigo un proceso de revisión y mejora continua, puesto que entre otras cosas se espera de él que vaya aprendiendo de los errores y adoptando las medidas necesarias para que no se repitan los mismos problemas.

De ellos se derivan una serie de acciones correctivas y preventivas cuya finalidad es la de ir perfeccionando y mejorando el SGSI continuamente. ■