Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes

Ana Andrés
Luis Gómez

AENOR ediciones

Título: *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*

Autores: Ana Andrés y Luis Gómez

ISBN: 978-84-8143-602-0

Depósito Legal: M-15480-2009

Impreso en España - *Printed in Spain*

Edita: AENOR

Maqueta y diseño de cubierta: AENOR

Imprime: AENOR

Nota: AENOR no se hace responsable de las opiniones expresadas por los autores en esta obra.

AENOR **Asociación Española de Normalización y Certificación**

Génova, 6. 28004 Madrid • Tel.: 902 102 201 • Fax: 913 103 695
comercial@aenor.es • www.aenor.es

Índice

Introducción

La información es el principal activo de muchas organizaciones y precisa ser protegida adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio.

En la actualidad, las empresas de cualquier tipo o sector de actividad se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de contingencias, las cuales pueden dañar considerablemente tanto los sistemas de información como la información procesada y almacenada.

Ante estas circunstancias, las organizaciones han de establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio, primando la protección de la información.

Para proteger la información de una manera coherente y eficaz es necesario implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema es una parte del sistema global de gestión, basado en un análisis de los riesgos del negocio, que permite asegurar la información frente a la pérdida de:

- Confidencialidad: sólo accederá a la información quien se encuentre autorizado.
- Integridad: la información será exacta y completa.
- Disponibilidad: los usuarios autorizados tendrán acceso a la información cuando lo requieran.

La seguridad total es inalcanzable, pero mediante el proceso de mejora continua del sistema de seguridad se puede conseguir un nivel de seguridad altamente satisfactorio, que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si efectivamente se produjeran.

Objeto de esta guía

El objeto de esta guía es facilitar la comprensión de los diversos conceptos involucrados en un sistema de gestión normalizado y contemplar recomendaciones generales para la implementación de un SGSI en una pyme. La aplicación de la Norma UNE-ISO/IEC 27001 facilita la mejora en seguridad, pero puede resultar de difícil aplicación para quien no se encuentre familiarizado con dichos conceptos.

Esta guía no pretende ser preceptiva (existen infinidad de formas de implementar correctamente la norma), sino informativa, proporcionando explicaciones básicas de los requisitos de la norma y orientando respecto a la manera en que se pueden cumplir esos requisitos.

Generalmente, una primera aproximación a la norma puede infundir desconfianza en cuanto a la capacidad de la empresa para poder llevar a cabo todos los requerimientos que expresa. Muchos términos no se utilizan en la actividad cotidiana de una pyme, tales como riesgos, amenazas, vulnerabilidades. Además, exige una serie de tareas desconocidas en la operativa habitual, tales como la realización de un análisis de riesgos y la selección de controles. Para complicar más las cosas, se hace referencia a la Norma PNE-ISO/IEC 27002, que especifica una amplia gama de controles de seguridad a implementar, en numerosos casos, con una gran carga de contenido técnico. Los objetivos, controles e indicaciones contenidos en la Norma PNE-ISO/IEC 27002 pueden llegar a ser muy difíciles de valorar por un gestor que no cuente con la información o la formación adecuada, hecho que le impediría decidir cabalmente sobre cuál es su relevancia para la empresa y las consecuencias de la implementación o no de un determinado control en ella.

Esta guía pretende suplir semejantes carencias, proporcionando información detallada sobre el significado práctico de los requisitos de la norma y explicando con ejemplos cómo se pueden realizar, teniendo siempre en cuenta la situación inicial,

los requisitos de seguridad de la empresa y, por supuesto, los recursos disponibles, ya que sin contar con esto ningún sistema de gestión se hallará bien diseñado y, por lo tanto, estará condenado al fracaso.

Para una mejor comprensión de las implicaciones de los diversos requisitos de la norma, esta guía incluye un ejemplo práctico, basado en una empresa ficticia, con la documentación básica que debe incluir un SGSI e indicaciones sobre la información que debe recoger cada documento.

1 Introducción a los Sistemas de Gestión de Seguridad de la Información *(SGSI)*

1.1. Definición de un SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Nos permitirá conocer mejor nuestra organización, cómo funciona y qué podemos hacer para que la situación mejore.

La norma especifica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Es decir, tanto la documentación de soporte como las tareas que se realizan. Los sistemas de gestión que definen las normas ISO siempre están documentados, ya que, por un lado, es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar, cosa que no sucedería si se confía en un traspaso de información verbal informal.

La norma es compatible con el resto de las normas ISO para sistemas de gestión (UNE-EN ISO 9001 y UNE-EN ISO 14001) y poseen idéntica estructura y requisitos comunes, por lo que se recomienda integrar el SGSI con el resto de los sistemas de gestión que existan en la empresa para no duplicar esfuerzos.

Incluso cuando no exista un sistema de gestión formal, el amplio conocimiento actual de estos sistemas hace que las principales características de la norma sean comprensibles para la mayoría de la gente, y que para explicarla en detalle sea suficiente con

incidir en las diferencias fundamentales, a saber, que con un SGSI lo que tratamos es de gestionar la seguridad de la información de nuestra organización.

1.2. El ciclo de mejora continua

Para establecer y gestionar un sistema de gestión de la seguridad de la información se utiliza el ciclo PDCA (conocido también como ciclo Deming), tradicional en los sistemas de gestión de la calidad (véase la figura 1.1). El ciclo PDCA es un concepto ideado originalmente por Shewhart, pero adaptado a lo largo del tiempo por algunos de los más sobresalientes personajes del mundo de la calidad. Esta metodología ha demostrado su aplicabilidad y ha permitido establecer la mejora continua en organizaciones de todas clases.

El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (*Plan-Do-Check-Act*, de sus siglas en inglés), tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización:

- *Plan*. Esta fase se corresponde con establecer el SGSI. Se planifica y diseña el programa, sistematizando las políticas a aplicar en la organización, cuáles son los fines a alcanzar y en qué ayudarán a lograr los objetivos de negocio, qué medios se utilizarán para ello, los procesos de negocio y los activos que los soportan, cómo se enfocará el análisis de riesgos y los criterios que se seguirán para gestionar las contingencias de modo coherente con las políticas y objetivos de seguridad.
- *Do*. Es la fase en la que se implementa y pone en funcionamiento el SGSI. Las políticas y los controles escogidos para cumplirlas se implementan mediante recursos técnicos, procedimientos o ambas cosas a la vez, y se asignan responsables a cada tarea para comenzar a ejecutarlas según las instrucciones.
- *Check*. Esta fase es la de monitorización y revisión del SGSI. Hay que controlar que los procesos se ejecutan como se ha establecido, de manera eficaz y eficiente, alcanzando los objetivos definidos para ellos. Además, hay que verificar el grado de cumplimiento de las políticas y procedimientos, identificando los fallos que pudieran existir y, hasta donde sea posible, su origen, mediante revisiones y auditorías.
- *Act*. Es la fase en la que se mantiene y mejora el SGSI, decidiendo y efectuando las acciones preventivas y correctivas necesarias para rectificar los fallos, detectados en las auditorías internas y revisiones del SGSI, o cualquier otra información relevante para permitir la mejora permanente del SGSI.

La mejora continua es un proceso en sí mismo. Debe entenderse como la mejora progresiva de los niveles de eficiencia y eficacia de una organización en un proceso continuo de aprendizaje, tanto de sus actividades como de los resultados propios.

Dado que la norma se encuentra enfocada hacia la mejora continua, es un esfuerzo innecesario tratar de implementar un SGSI perfecto en un primer proyecto de este tipo. El objetivo debería ser diseñar un SGSI que se ajuste lo más posible a la realidad de la organización, que contemple las medidas de seguridad mínimas e imprescindibles para proteger la información y cumplir con la norma, pero que consuma pocos recursos e introduzca el menor número de cambios posibles. De esta manera, el SGSI se podrá integrar de una forma no traumática en la operativa habitual de la organización, dotándola de herramientas con las que hasta entonces no contaba que puedan demostrar su eficacia a corto plazo.

La aceptación de este primer SGSI es un factor de éxito fundamental. Permitirá a la organización ir mejorando su seguridad paulatinamente y con escaso esfuerzo.

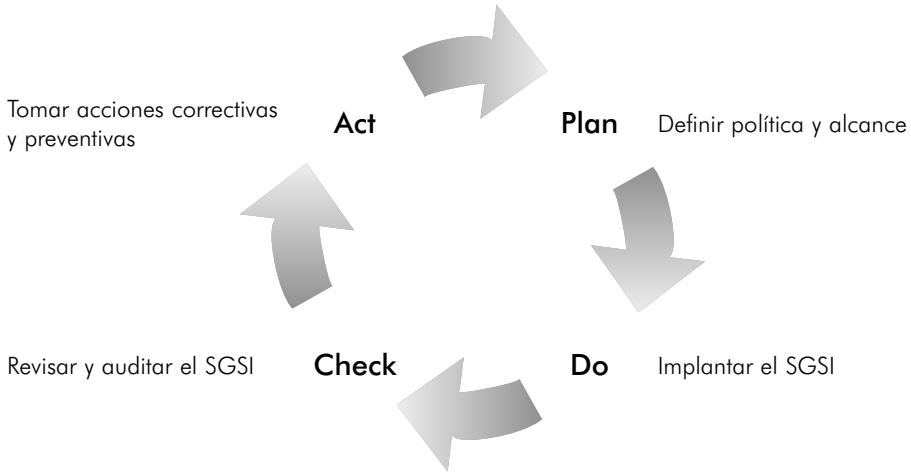

Figura 1.1. **Ciclo PDCA**

1.3. La Norma UNE-ISO/IEC 27001

1.3.1. Origen de la norma

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en

el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo.

En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1 (*Joint Technical Committee* 1). Los borradores de estas normas internacionales, adoptadas por la unión de este comité técnico, son enviados a los organismos de las diferentes naciones para su votación. La publicación como norma internacional requiere la aprobación de, por lo menos, el 75% de los organismos nacionales que emiten su voto.

La Norma Internacional ISO/IEC 27002 fue preparada inicialmente por el Instituto de Normas Británico (como BS 7799), y adoptada bajo la supervisión del subcomité de técnicos de seguridad del comité técnico ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales miembros de ISO e IEC.

La Norma ISO/IEC 27001 es la nueva norma oficial. También fue preparada por este JTC 1 y en el subcomité SC 27 *Técnicas de seguridad*. La versión que se considerará en este texto es la primera edición, de fecha 15 de octubre de 2005.

Como se ha comentado anteriormente, este estándar internacional adopta también el modelo *Plan-Do-Check-Act* (PDCA), es decir, se basa en un ciclo de mejora continua que consiste en planificar, desarrollar, comprobar y actuar en consecuencia con lo que se haya detectado al efectuar las comprobaciones. De esta manera se conseguirá ir refinando la gestión, haciéndola más eficaz y efectiva.

1.3.2. Objeto y campo de aplicación de la norma

La Norma UNE-ISO/IEC 27001, como el resto de las normas aplicables a los sistemas de gestión, está pensada para que se emplee en todo tipo de organizaciones (empresas privadas y públicas, entidades sin ánimo de lucro, etc.), sin importar el tamaño o la actividad.

Esta norma especifica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Por ejemplo, uno de los principales requisitos es la realización de un análisis de riesgos con unas determinadas características de objetividad y precisión, pero no aporta indicaciones de cuál es la mejor manera de llevar a cabo dicho análisis. Puede ejecutarse con una herramienta

comercial, con una aplicación diseñada expresamente para la empresa, mediante reuniones, entrevistas, tablas o cualquier otro método que se estime oportuno. Todos estos recursos servirán para cumplir la norma, siempre y cuando se observen los requisitos de objetividad del método, los resultados sean repetibles y la metodología se documente.

1.4. La Norma ISO 27002

1.4.1. Origen

La Norma ISO/IEC 27002 *Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información*, ha sido elaborada por el AEN/CTN 71/SC 27 *Técnicas de seguridad* que pertenece al comité técnico conjunto ISO/IEC JTC 1/SC 27 *Tecnología de la información*. En ambas normas el contenido es idéntico, diferenciándose únicamente en la numeración, que ha sido modificada en el marco de la creación de la familia de normas ISO 27000.

Esta norma se está desarrollando dentro de una familia de normas internacionales sobre Sistemas de Gestión de la Seguridad de la Información (SGSI). Tal familia incluye normas internacionales sobre requisitos, gestión del riesgo, métricas y mediciones, así como una guía de implementación de los sistemas de gestión de la seguridad de la información. Dicha familia de normas tiene un esquema de numeración que utilizará los números de la serie 27000.

1.4.2. Objeto y campo de aplicación

La Norma ISO/IEC 27002 establece las directrices y principios generales para el comienzo, la implementación, el mantenimiento y la mejora de la gestión de la seguridad de la información en una organización. Es un catálogo de buenas prácticas, obtenido a partir de la experiencia y colaboración de numerosos participantes, los cuales han alcanzado un consenso acerca de los objetivos comúnmente aceptados para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma internacional tienen como fin servir de guía para el desarrollo de pautas de seguridad internas y prácticas efectivas de gestión de la seguridad. Por ello, la elección de los controles permanece sujeta a lo detectado en un análisis de riesgos previo, y el grado de implementación de cada uno de los controles se llevará a cabo de acuerdo a los requisitos de seguridad identificados y a los recursos disponibles de la organización para alcanzar así un balance razonable entre seguridad y coste.

1.5. Términos y definiciones

Para cumplir con las intenciones de este documento, conviene aclarar el significado de ciertos términos y definiciones:

- Activo

  Cualquier bien que tiene valor para la organización.

  [ISO/IEC 13335-1:2004]

- Disponibilidad

  La propiedad de ser accesible y utilizable por una entidad autorizada.

  [ISO/IEC 13335-1:2004]

- Confidencialidad

  La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

  [ISO/IEC 13335-1:2004]

- Seguridad de la información

  La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

  [ISO/IEC 17799:2005]

- Evento de seguridad de la información

  La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

  [ISO/IEC TR 18044:2004]

- Incidente de seguridad de la información

  Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

  [ISO/IEC TR 18044:2004]

- Sistema de Gestión de la Seguridad de la Información (SGSI) [*Information Security Management System*, ISMS]

  La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

  Nota: el sistema de gestión incluye la estructura organizativa. las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

- Integridad

  La propiedad de salvaguardar la exactitud y completitud de los activos.

  [ISO/IEC 13335-1:2004]

- Riesgo residual

  Riesgo remanente que existe después de que se hayan tornado las medidas de seguridad.

  [ISO/IEC Guide 73:2002]

- Aceptación del riesgo

  La decisión de aceptar un riesgo.

  [ISO/IEC Guide 73:2002]

- Análisis de riesgos

  Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

  [ISO/IEC Guide 73:2002]

- Evaluación de riesgos

  El proceso general de análisis y estimación de los riesgos.

  [ISO/IEC Guide 73:2002]

- Estimación de riesgos

  El proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.

  [ISO/IEC Guide 73:2002]

- Gestión de riesgos

  Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

  [ISO/IEC Guide 73:2002]

- Tratamiento de riesgos

  El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.

  [ISO/IEC Guide 73:2002].

  Nota: en esta norma internacional, el término "control" se utiliza como sinónimo de "medida de seguridad."

- Declaración de aplicabilidad

  Declaración documentada que describe los objetivos de control y los controles que son relevantes para el SGSI de la organización y aplicables al mismo.

  Nota: los objetivos de control y los controles se basan en los resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, en los requisitos legales o reglamentarios, en las obligaciones contractuales y en las necesidades empresariales de la organización en materia de seguridad de la información.