

# Sistema de Gestión de la Seguridad de la Información

1

## Contenidos

1. ¿Qué es un SGSI?
2. ¿Para qué sirve un SGSI?
3. ¿Qué incluye un SGSI?
4. ¿Cómo se implementa un SGSI?
5. ¿Qué tareas tiene la Gerencia en un SGSI?
6. ¿Se integra un SGSI con otros sistemas de gestión?

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

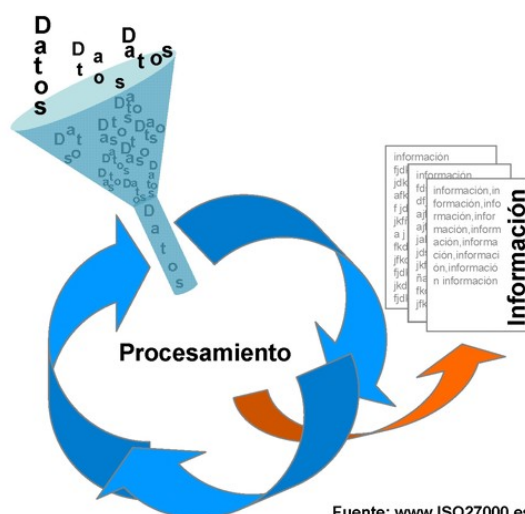
Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, 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.

En las siguientes secciones, se desarrollarán los conceptos fundamentales de un SGSI según la norma ISO 27001.

## 1. ¿Qué es un SGSI?

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System*.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.



La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

## 2. ¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.



El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

### 3. ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:



## Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

## Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

## Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

## Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como *output* que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables .
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de

seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- Declaración de aplicabilidad: (SOA -*Statement of Applicability*-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

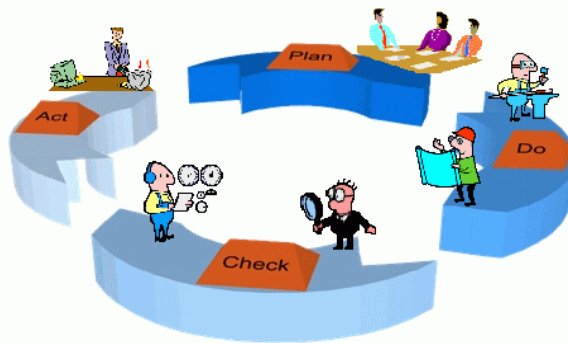
### **Control de la documentación**

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

## **4. ¿Cómo se implementa un SGSI?**

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.



- **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.

### **Plan: Establecer el SGSI**

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:
  - incluya el marco general y los objetivos de seguridad de la información de la organización;
  - considere requerimientos legales o contractuales relativos a la seguridad de la información;
  - esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
  - establezca los criterios con los que se va a evaluar el riesgo;
  - esté aprobada por la dirección.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- Identificar los riesgos:
  - identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;

- 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.
- 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;
  - 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, p. ej., mediante el cese de las actividades que lo originan;
  - transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de *outsourcing*.





- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya:
  - los objetivos de control y controles seleccionados y los motivos para su elección;
  - los objetivos de control y controles que actualmente ya están implantados;
  - los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene [133 controles](#), según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de “documento indispensable para la aplicación de este documento” y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

### ***Do: Implementar y utilizar el SGSI***

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

## Check: Monitorizar y revisar el SGSI

---

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
  - detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
  - identificar brechas e incidentes de seguridad;
  - ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
  - detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
  - determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, 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.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

## Act: Mantener y mejorar el SGSI

---

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de *Act* lleva de nuevo a la fase de *Plan* para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

## 5. ¿Qué tareas tiene la Gerencia en un SGSI?

Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (recuérdese que el alcance no tiene por qué ser toda la organización).

Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos:

### Compromiso de la dirección

---

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información.

- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI, como se detalla más adelante.

### **Asignación de recursos**

---

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario.

### **Formación y concienciación**

---

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado. Se deberá:

- Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.
- Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.

- Evaluar la eficacia de las acciones realizadas.
- Mantener registros de estudios, formación, habilidades, experiencia y cualificación.

Además, la dirección debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

## Revisión del SGSI

---

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

## 6. ¿Se integra un SGSI con otros sistemas de gestión?

Un SGSI es, en primera instancia, un sistema de gestión, es decir, una herramienta de la que dispone la gerencia para dirigir y controlar un determinado ámbito, en este caso, la seguridad de la información.

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, el impacto medio-ambiental según ISO 14001 o la prevención de riesgos laborales según OHSAS 18001. Ahora, se añade ISO 27001 como estándar de gestión de seguridad de la información.

Las empresas tienen la posibilidad de implantar un número variable de estos sistemas de gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

El objetivo último debería ser llegar a un único sistema de gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA de mejora continua común a todos estos estándares. Las facilidades para la integración de las normas ISO son evidentes mediante la consulta de sus anexos.

ISO 27001 detalla en su Anexo C, punto por punto, la correspondencia entre esta norma y la ISO 9001 e ISO 14001. Ahí se observa la alta correlación existente y se puede intuir la posibilidad de integrar el sistema de gestión de seguridad de la información en los sistemas de gestión existentes ya en la organización. Algunos puntos que suponen una novedad en ISO 27001 frente a otros estándares son la evaluación de riesgos y el establecimiento de una declaración de aplicabilidad (SOA), aunque ya se plantea incorporar éstos al resto de normas en un futuro.

En nuestras secciones de [Fags](#) y de [Artículos](#), podrá encontrar más informaciones acerca de la integración del SGSI con otros sistemas de gestión.