# ISO27001/ISO27002

## Una guía de bolsillo

Alan Calder

itgp™

# ISO27001/ISO27002

## Una guía de bolsillo

Alan Calder

itgp™

**ISO27001/ISO27002**

Una guía de bolsillo

# ISO27001/ISO27002

# Una guía de bolsillo

ALAN CALDER

IT Governance Publishing

IT Governance Publishing

IT Governance Limited

Unit 3, Clive Court, Bartholomew's Walk

Cambridgeshire Business Park

Ely, Cambridgeshire

CB7 4EA

Reino Unido

*www.itgovernance.co.uk*



Publicada por primera vez en el Reino Unido en 2008 por IT Governance Publishing.

ISBN 978-1-84928-918-4

# PRÓLOGO

La ISO/IEC 27001:2013 es la norma internacional para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Relacionada estrechamente con la ISO/IEC 27002:2013, esta norma (a veces llamada la norma del SGSI) puede ayudar a las organizaciones a alcanzar todos sus objetivos de cumplimiento reglamentario relacionados con la información y puede ayudarles a prepararse y posicionarse para la normativa nueva y emergente.

La información es el alma de la organización en la actualidad y, por tanto, asegurar que la información se protege y se pone a disposición simultáneamente para aquellos que la necesitan es fundamental en las operaciones comerciales modernas. Los sistemas de información no se diseñan normalmente desde el comienzo para ser seguros. Las medidas de seguridad técnica y las listas de verificación son limitadas en su capacidad para proteger un sistema de información completo. Los sistemas de gestión y los controles de procedimientos son componentes fundamentales de cualquier sistema de información verdaderamente seguro y, para ser eficaces, necesitan una planificación cuidadosa y atención a los detalles.

La ISO/IEC 27001 proporciona la especificación para un SGSI y, en el Código de Prácticas relacionado, la ISO/IEC 27002, recurre al conocimiento de un grupo de profesionales experimentados de la seguridad de la información en una amplia variedad de organizaciones importantes en más de 40 países para exponer las mejores prácticas en seguridad de la información. Un sistema conforme a la ISO 27001 proporcionará un enfoque sistemático para asegurar la disponibilidad, confidencialidad e integridad de la información corporativa. Los controles de la ISO 27001 se basan en identificar y combatir la gama entera de riesgos potenciales para los activos de información de la organización. Esta guía de bolsillo útil y práctica de la ISO27001/ISO27002 le da una visión de conjunto útil sobre estas dos normas importantes de la seguridad de la información.

# ACERCA DEL AUTOR

Alan Calder es un autor líder en normas de TI y cuestiones de la seguridad de la información. Es director ejecutivo de IT Governance Limited, la tienda integral para libros, herramientas, formación y consultoría sobre normas de TI, gestión del riesgo y cumplimiento.

Alan es una autoridad internacional en la gestión de la seguridad de la información y en la ISO 27001 (anteriormente BS7799), la norma de la seguridad internacional. Con el compañero Steve Watkins escribió la guía de cumplimiento definitiva, *Normas de TI: Una guía internacional para la seguridad de los datos y la ISO27001/ISO27002*, cuya quinta edición se publicó en 2012. Esta obra se basa en su experiencia de liderar la primera implementación con éxito del mundo de la BS7799 (la precursora de la ISO 27001) y es la base para el curso de posgrado de la Universidad Abierta sobre seguridad de la información.

Otros libros escritos por Alan incluyen *El Caso para ISO27001* y *Nueve pasos para el éxito: Una visión de conjunto de la implementación de la ISO27001:2013*, así como libros sobre gobernanza corporativa y normas de TI y varias guías de bolsillo es esta serie.

Alan es un comentarista frecuente en medios de comunicación sobre la seguridad de la información y las cuestiones de regulaciones de TI y ha contribuido con artículos y comentario especializado en un amplio abanico de medios informativos nacionales, por internet y de la industria.

# RECONOCIMIENTOS



Esta guía de bolsillo contiene muchas referencias, y resúmenes, del material que está disponible de modo más exhaustivo en las normas publicadas; tiene la intención de ser una herramienta útil de referencia que contiene en un solo sitio alguna de la información clave que aquellos que se ocupan de las normas y cuestiones relacionadas podrían necesitar. No contiene suficiente información para que cualquiera implemente, o audite la implementación, de un sistema de gestión basado en cualquiera de estas normas. Además, es una guía de bolsillo y no un manual completo[1] sobre la implementación de la ISO 27001.

---

[1] Si busca un manual completo sobre la implementación de la ISO 27001, hay uno disponible en *www.itgovernance.eu/shop/product/it-governance-an-international-guide-to-data-security-and-iso27001iso27002-sixth-edition*.

# ÍNDICE

# INTRODUCCIÓN

Es un tópico decir que la información es la moneda de la era de la información. La información es, en muchos casos, el activo más valioso que posee una organización, incluso si esa información no se ha sometido a una evaluación formal y exhaustiva.

El gobierno de TI es la disciplina que trata de las estructuras, normas y procesos que los consejos y los equipos de la gerencia aplican con el fin de gestionar, proteger y explotar de manera eficaz los activos de información de su organización.

La gestión de la seguridad de la información es el subconjunto del gobierno de TI que se centra en proteger y asegurar los activos de información de una organización.

## Riesgos para los activos de información

Un activo puede definirse como “cualquier cosa que tenga valor para una organización”. Los activos de información están sujetos a un amplio abanico de amenazas, tanto externas como internas, que van desde el azar hasta las muy específicas. Los riesgos incluyen casos fortuitos, fraude y otra actividad criminal, error del usuario y fallo del sistema.

## Sistema de gestión de la seguridad de la información

Un Sistema de Gestión de la Seguridad de la Información (SGSI) se define (en la ISO/IEC 27000) como "*parte del sistema de gestión general, basado en un enfoque de riesgo empresarial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. 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*".

# CAPÍTULO 1: LA FAMILIA DE NORMAS DE LA SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27000

La ISO 27001, la norma internacional sobre la gestión de la seguridad de la información, se publicó en 2005 y se actualizó en 2013. Se está volviendo muy conocida y seguida.

Ahora forma parte de una familia mucho más grande, de la cual la ISO/IEC 27000 es la raíz para toda una serie numerada de normas internacionales para la gestión de la seguridad de la información.

Desarrolladas por un subcomité de un comité técnico mixto (ISO/IEC JTC SC27) de la Organización Internacional de Normalización (ISO) en Ginebra y la Comisión Electrotécnica Internacional (IEC), estas normas proporcionan ahora un marco reconocido mundialmente para las mejores prácticas de gestión la seguridad de la información.

La designación correcta para la mayoría de estas normas incluye los prefijos ISO/IEC y todas ellas deben incluir un sufijo que es su fecha de publicación. La mayoría de estas normas, sin embargo, tienden a llamarse abreviadamente. ISO/IEC

27001:2013, por ejemplo, a menudo se le hace referencia a menudo simplemente como ISO 27001.

La primera de la serie ISO 27000 de las normas de seguridad de la información ya se ha publicado.

## ISO/IEC 27001:2013 (ISO 27001)

Esta es la versión actual de la especificación de la norma internacional para un sistema de gestión de la seguridad de la información. Es neutral respecto al vendedor e independiente de la tecnología. Se "pretende que sea aplicable a todas las organizaciones, independientemente del tipo, tamaño o naturaleza"[1] y en todos los sectores (p. ej. empresas comerciales, agencias gubernamentales y organizaciones sin ánimo de lucro) y en cualquier parte del mundo. Es un sistema de gestión y no una especificación de tecnología con el título formal de "Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos".

## ISO/IEC 27002:2013 (ISO 27002)

Esta norma se titula "Tecnología de la Información – Técnicas de seguridad – Código de prácticas para la gestión de la seguridad de la información". La primera edición se publicó en

julio de 2005, habiéndose numerado inicial y originalmente ISO/IEC 17799. La última edición se publicó en octubre de 2013.

## ISO/IEC 27003

Esta norma se titula “Tecnología de la Información – Técnicas de seguridad – Directriz sobre la implementación del sistema de gestión de la seguridad de la información”. Se publicó en enero de 2010.

## ISO/IEC 27004

La ISO/IEC 27004 se titula “Tecnología de la Información – Técnicas de seguridad – Gestión de la seguridad de la información – Medición”. Esta norma está diseñada para ayudar a las organizaciones a abordar más eficazmente el requisito, contenido en las cláusulas 9.1 a 9.3 de la ISO 27001, de medir la eficacia de los controles. Se publicó en diciembre de 2009.

## ISO/IEC 27005:2011

La gestión de los riesgos de la seguridad de la información (basada en e incorporando la ISO/IEC 13335 MICTS Parte 2) se publicó en junio de 2008, con una nueva edición publicada en 2011.

## ISO/IEC 27006:2011

Esta norma expone los requisitos para los organismos que ofrecen auditoría y certificación de los sistemas de gestión de la seguridad de la información.

## Definiciones

Se pretende que las definiciones empleadas en todas estas normas sean coherentes unas con otras y también con aquellas utilizadas en ISO/IEC Guía 73:2009. La ISO/IEC 27000:2016 también está disponible; se titula “Tecnología de la Información – Técnicas de seguridad – Sistema de gestión de la seguridad de la información – Visión de conjunto y vocabulario”.

_____

[1] ISO/IEC 27001:2013, Alcance 1.

# CAPÍTULO 2: HISTORIA DE LAS NORMAS

La primerísima norma de seguridad de la información, la BS7799, se publicó originalmente en el Reino Unido en abril de 1999 como una norma con dos partes. Un código de prácticas anterior se había revisado y se convirtió en la parte 1 de la nueva norma (BS7799-1:1999) y se redactó y añadió una nueva Parte 2 (BS7799-2:1999).

Se creó un vínculo entre las dos normas en este punto:

La Parte 1 era un código de prácticas

La Parte 2 era una especificación para un SGSI que hacía uso de controles seleccionados del código de prácticas.

La Parte 2 original especificaba, en el cuerpo principal de la norma, el mismo conjunto de controles que se describían en mucho más detalle (concretamente en cuanto a la implementación) en la Parte 1. Estos controles se quitaron más tarde del cuerpo principal de la Parte 2 y se enumeraron en un anexo, el Anexo A.

Esta relación continúa hoy en día, entre la especificación para el SGSI que viene en una norma, y la directriz detallada sobre los controles de la seguridad de la información que se deben

considerar al desarrollar e implementar el SGSI que viene en la otra parte de la norma combinada.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC)[1] colaboraron entonces para adoptar e internacionalizar la BS7799-1 como ISO/IEC 17799:2000 en diciembre de 2000. La ISO 17799 era ampliamente usada por todo el mundo para proporcionar una directriz sobre las mejores prácticas de los controles de la seguridad de la información.

La ISO 17799 se revisó, mejoró y actualizó considerablemente cinco años más tarde (en 2005) y también se le cambió el número a la serie de la ISO27000.

## BS7799-2

La BS7799-2:1999 se revisó y volvió a publicar como BS7799-2:2002. Ocurrieron cambios importantes en este tiempo, incluido:

El alineamiento de la numeración de la cláusula en ambas partes de la norma.

La adición del modelo de PDCA (ver *Capítulo 15*) a la norma.

La adición de un requisito para mejorar continuamente el SGSI.

El alineamiento de la norma, y sus cláusulas detalladas, con la ISO 9001:2000 y la ISO 14001:1996, para facilitar el desarrollo de sistemas de gestión integrados.

## ISO 27001:2005

Aunque una serie de países adoptaron la BS7799-2, era todavía una norma británica en junio de 2005, cuando se iba a publicar la ISO/IEC 17799:2005. Se tomó la decisión, en aquel momento, de poner la BS7799-2 en la "vía rápida" para la internacionalización y se publicó el FDIS (Borrador final de la norma internacional) en junio de 2005. La BS7799-2:2005 (ISO/IEC 27001:2005) se publicó finalmente en octubre de 2005.

## ISO 27001:2013

Después de una consulta ampliada con las organizaciones miembros de la ISO/IEC, se publicó la última edición de la ISO 27001 en octubre de 2013. Se cambió la atención hacia crear un SGSI que complemente la organización y sus procesos, y una reducción de la redundancia en la especificación y los controles.

## Correspondencia entre la ISO 27001 y la ISO 27002

El Anexo A de la ISO/IEC 27001:2013 enumera los 114 controles que están en la ISO/IEC 27002:2013, sigue el mismo sistema de numeración y utiliza las mismas palabras para los controles y los objetivos del control.

El prefacio del anexo establece: “Los objetivos del control y los controles [a los que se hace referencia en esta edición] se derivan directamente y están alineados con aquellos enumerados en la ISO/IEC 27002:2013”. La ISO/IEC 27001 exige que la organización “determine todos los controles que sean necesarios para implementar la opción u opciones de tratamiento de los riesgos de la seguridad de la información elegidas”[2].

La ISO 27002 proporciona también una directriz de implementación considerable sobre cómo deben enfocarse los controles individuales. Cualquiera que implemente un SGSI de la ISO 27001 tendrá que adquirir y estudiar las copias de tanto la ISO 27001 y la ISO 27002.

Aunque la ISO 27001 en efecto manda el uso de la ISO 27002 como fuente de orientación sobre los controles, la selección de los controles y su implementación, no limita la elección de controles de la organización. La especificación establece: “Los objetivos del control y los controles enumerados en el Anexo A

no son exhaustivos y pueden ser necesarios objetivos del control y controles adicionales".[3]

## Uso de las normas

Ambas normas reconocen que la seguridad de la información no se puede lograr mediante medios tecnológicos solos, y nunca debe implementarse de manera que esté fuera de lugar con el enfoque de la organización para el riesgo, mine o cree dificultades para sus operaciones comerciales.

La seguridad de la información efectiva se define en la ISO 27000 como "la conservación de la confidencialidad, integridad y disponibilidad de la información".

---

[1] La IEC es "la organización global líder que prepara y publica las normas internacionales para todo los eléctrico, electrónico y tecnologías relacionadas". Su sitio web es *www.iec.ch*. La ISO y la IEC trabajan juntas, dentro del marco de la Organización Mundial del Comercio (OMC), para ofrecer apoyo técnico para el crecimiento de los mercados globales y para asegurar que los reglamentos técnicos, las normas voluntarias y los procedimientos de evaluación de la conformidad no crean

obstáculos innecesarios al comercio. El centro de información conjunto de la ISO/IEC tiene un sitio web en *www.standardsinfo.net*.

---

[2] ISO/IEC 27001:2013, 6.1.3 Tratamiento de los riesgos de la seguridad de la información.

---

[3] Ibídem.

# CAPÍTULO 3: ESPECIFICACIÓN FRENTE AL CÓDIGO DE PRÁCTICAS

La ISO/IEC 27001:2013 es una especificación para el sistema de gestión de la seguridad de la información. Utiliza palabras como "*debe*". Expone los requisitos. Es la especificación frente a la cual se pueden llevar a cabo las auditorías de primera, segunda y tercera parte.

La auditoría de primera parte es una auditoría de las prácticas propias de una organización que se llevan a cabo por esa organización. Una auditoría de segunda parte la realiza una organización asociada, normalmente conforme a una relación comercial de alguna descripción. Una auditoría de tercera parte es la que lleva a cabo un tercero independiente, tal como un organismo de certificación o un auditor externo.

Un código de prácticas o conjunto de directrices utilizan palabras como "*debe*" y "*puede*", que permiten que organizaciones individuales elijan qué elementos de la norma implementan y cuáles no. Este elemento incorporado de elección significa que la ISO 27002 no es capaz de ofrecer una norma firme frente a la cual se puede llevar a cabo una auditoría. Sin embargo, la ISO 27001 es preceptiva y ofrece dicha libertad.

Cualquier organización que implemente un SGSI que desee que la evalúen frente a la ISO 27001 tendrá que seguir la especificación que viene en esa norma.

Como regla general, las organizaciones que implementen un SGSI basándose en la ISO/IEC 27001:2013 harán bien en prestar mucha atención a la redacción de la norma misma y estar atentas a sus revisiones. No cumplir con cualquiera de las revisiones oficiales, que normalmente ocurren en un ciclo de 3 y cinco años, pondrán en peligro la certificación existente.

Un primer paso adecuado es obtener y leer una copia de la ISO/IEC 27001:2013. Se pueden comprar copias en el sitio web de la ISO, de organismos de normalización nacionales y de *www.itgovernance.eu/standards*. Debería haber una elección de copia en papel y versiones descargables para ajustarse a las necesidades individuales.

# CAPÍTULO 4: PROCESO DE CERTIFICACIÓN

La ISO 27001 proporciona una especificación frente a la cual el SGSI de una organización se puede auditar independientemente por un organismo de certificación acreditado. Si se observa que el SGSI está conforme con la especificación, se puede expedir a la organización un certificado formal confirmando esto.

## Organismos de certificación

La certificación la llevan a cabo organismos de certificación acreditados e independientes. Estos se llaman de manera diferente en distintos países, incluido “organismos de registro”, organismos de evaluación y registro”, “organismos de certificación/registro” y “registradores”. Comoquiera que se llamen, todos hacen lo mismo y están sujetos a los mismos requisitos.

Un organismo de certificación acreditado es uno que ha demostrado a un organismo de acreditación nacional (como, por ejemplo UKAS: Servicio de acreditación británico) que cumplió completamente las normas nacionales e internacionales establecidas para el funcionamiento de los

organismos de certificación. Estas normas normalmente restringen la capacidad de un organismo de certificación a prestar servicios de consultoría en relación con una norma para la cual también presta servicios de certificación.

Las organizaciones que buscan una certificación independiente de su SGSI siempre deben acudir a un organismo de certificación acreditado. Sus certificados normalmente válidos durante tres años y están sujetos a visitas de mantenimiento periódicas por el organismo de certificación; tienen credibilidad internacional y se expedirán en línea con un sistema aprobado para la expedición y mantenimiento de dichos certificados. Se puede utilizar una versión aprobada del símbolo de certificación del programa en el material de marketing de la organización.

Hay una lista de algunos organismos de certificación acreditados y otros organismos en las páginas de enlace de *www.itgovernance.eu/web_links*.

# CAPÍTULO 5: EL SGSI Y LA ISO 27001

## Definición de la seguridad de la información

La ISO 27000 define la seguridad de la información (en su sección de definiciones) como la "*conservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como la autenticidad, la responsabilidad, la irrefutabilidad y la fiabilidad pueden estar implicadas*.

Los riesgos de la información pueden afectar a uno o más de los tres atributos fundamentales de un activo de información: su

disponibilidad

confidencialidad

integridad.

Estos tres atributos se define en la ISO 27000 como sigue:

Disponibilidad: *"La propiedad de ser accesible y utilizable a su requerimiento por una entidad autorizada*", lo cual permite la posibilidad de que la información tenga que accederse por programas de software así como usuarios humanos.

Confidencialidad: *“La propiedad que la información no se pone a disposición ni divulga a personas, entidades ni procesos no autorizados”*.

Integridad: *“La propiedad de proteger la exactitud y la integridad de los activos”*.

## El SGSI

Un SGSI, que la norma es clara incluye “estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos”,[1] es un enfoque de gestión estructurado y coherente para la seguridad de la información, que está diseñado para asegurar la interacción eficaz de los componentes clave de la implementación de una política de seguridad de la información:

Proceso (o procedimiento)

Tecnología

Comportamiento del usuario.

El requisito de la norma es que el diseño y la implementación de un SGSI debe estar influido directamente por las “necesidades y objetivos, requisitos de seguridad, los procesos

organizativos utilizados y el tamaño y estructura de la organización" de cada organización.[2]

La ISO 27001 no es una solución única para todos, ni nunca se vio como una entidad fija y estática que interfiere con el crecimiento y el desarrollo de una empresa. La norma reconoce explícitamente que:

El SGSI "se hará a escala según las necesidades de la organización" y

"Se espera que el SGSI cambie con el tiempo".

---

[1] ISO/IEC 27000:2016, Términos y definiciones, 2.34, nota.

[2] ISO/IEC 27001:2013, Introducción general, 0.1.

# CAPÍTULO 6: VISIÓN DE CONJUNTO DE LA ISO/IEC 27001:2013

El título formal de esta norma es “Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos”. Desde octubre de 2013, reemplazó la edición anterior, la ISO/IEC 27001:2005.

Incluidas las partes finales, esta norma solo tiene 30 páginas. El núcleo de la norma está contenido en las nueve páginas que exponen las especificaciones para el diseño y la implementación de un sistema de seguridad de la información, y en las 13 páginas del Anexo A, que contienen los 114 controles individuales que deben considerarse, según la norma, para la aplicabilidad.

La especificación del SGSI está contenido en las cláusulas 4 a 10 de la ISO 27001.

Los contenidos de la norma (cláusulas principales y anexos) son:

0. Introducción

1. Alcance

# CAPÍTULO 7: VISIÓN DE CONJUNTO DE LA ISO/IEC 27002:2013

El título de esta norma es “Tecnología de la Información – Técnicas de seguridad – Código de prácticas para la gestión de la seguridad de la información”. Publicada en octubre de 2013, reemplazó la edición anterior, la ISO/IEC 27002:2005.

Es un código de prácticas y no una especificación. Utiliza palabras como “debería” y “puede”: Se *“puede”* considerar como un punto de partida para el desarrollo de las directrices específicas de la organización”.[1]

La ISO 27002 es más del doble de larga que la ISO 27001, con 90 páginas, 8 de las cuales son material introductorio. Unas 78 páginas tratan, en detalle, de los controles de la seguridad la información. Esta norma tiene 18 cláusulas, como se muestran a continuación:

Prólogo

. Introducción

. Alcance

. Referencias de la normativa

. Términos y definiciones

. Estructura de esta norma

. Políticas de seguridad de la información

. Organización de la seguridad de la información

. Seguridad de recursos humanos

. Gestión de los activos

. Control del acceso

. Criptografía

. Seguridad del entorno y física

. Seguridad de las operaciones

. Seguridad de las comunicaciones

. Adquisición del sistema, desarrollo y mantenimiento

. Relaciones con los proveedores

. Gestión de incidentes de seguridad de la información

. Aspectos de seguridad de la información de la gestión de la continuidad empresarial

. Cumplimiento

Bibliografía

Las 14 cláusulas numeradas del cinco al dieciocho contienen los controles que se especifican en el Anexo A de la ISO 27001. Estas cláusulas colectivamente contienen las 35 categorías de la seguridad. La numeración de los controles es exactamente la misma en ambas normas. El orden de las cláusulas no tiene importancia; “dependiendo de las circunstancias, los controles de seguridad de todas y cada una de las cláusulas podrían ser importantes”.[2]

## Las categorías de seguridad

Cada categoría de seguridad contiene:

Un objetivo de control, indicando qué tiene que lograr.

Uno o más controles que se pueden emplear para lograr ese objetivo indicado.

Cada control dentro de cada categoría de seguridad se expone exactamente de la misma manera. Hay:

Una exposición del control, que describe (en el contexto del objetivo de control) para qué es el control;

Una directriz de implementación, que es una orientación detallada que puede (o puede que no) ayudar a las organizaciones individuales a implementar el control;

Otra información que tenga que considerarse, incluida la referencia a otras normas.

---

[1] ISO/IEC 27002:2013, 0.4: Introducción, desarrollar sus propias directrices; énfasis añadido.

---

[2] ISO/IEC 27002:2013, Cláusula 4.1.

# CAPÍTULO 8: DOCUMENTACIÓN Y REGISTROS

Una de las razones clave para diseñar e implementar un sistema de gestión es posibilitar que la organización vaya más allá de lo conocido, en cuanto al modelo de capacidad, como organización "*ad hoc*". Una organización *ad hoc* es la que no cuenta con "procesos fijos, ni procedimientos y los resultados dependes muchísimo del rendimiento individual, y mucho tiempo de las personas se dedica a "apagar incendios", solucionar fallos de programación en el software y resolver incidentes".[1]

La ISO 9001:2008 es una garantía de calidad o sistema de gestión de procesos empresariales bien conocida e implementada. Si la organización no tiene ya un sistema existente de gestión certificado con la ISO 9001 y necesita asesoramiento sobre la documentación y el control de documentos cubiertos en la cláusula 7.5 de la ISO 27001, entonces debería obtener y utilizar la directriz en cualquier manual actual sobre la implementación de la ISO 9001.

Tenga en cuenta que las especificaciones de la ISO 27001 para el control de documentos (7.5.3) reflejan aquellas contenidas en la

ISO 9001:2008, cuando están numeradas 4.2.3 y 4.2.4 respectivamente.

## Requisitos del control de documentos

La ISO 27001 exige explícitamente que se documente el sistema de gestión. El control A.12.1.1 exige explícitamente que se documenten, conserven y estén disponibles los procedimientos de seguridad para todos los usuarios que los necesiten. Otros requisitos explícitos de documentación en el Anexo A incluyen:

A.5.1.1: políticas de seguridad de la información;

A.6.1.1: funciones y responsabilidades documentadas para la seguridad de recursos humanos;

A.8.1.3: uso aceptable de los activos;

A.9.1.1: política de control de acceso;

A.18.1.1: identificación de legislación aplicable.

Muchos de los demás controles exigen procedimientos “formales” o comunicación “clara”; aunque estos podrían lograrse técnicamente sin estar documentados, la expectativa es que todos los procesos y procedimientos lo serán.

## Contenidos de la documentación del SGSI

La documentación tiene que ser completa, extensa, en línea con los requisitos de la norma y personalizada para satisfacer las necesidades de las organizaciones individuales. El SGSI debe estar completamente documentado. La ISO 27001 describe la documentación mínima que se debe incluir en el SGSI.

No todas las organizaciones tienen que implementar una estructura de documentación igualmente compleja. La norma indica que "el alcance de la información documentada para un [SGSI] puede diferir de una organización a otra debido al [...] tamaño de la organización, su tipo de actividades y sus interacciones".[2]

Con la publicación de la ISO 27001:2013, ya no hay distinción entre documentos y registros, y ambos están sujetos a los mismos requisitos. En cualquier caso, a las organizaciones les puede parecer útil mantener esta distinción, especialmente si está implantada una ISO 9001 de sistema de gestión de calidad (SGC), ya que esta mantiene la distinción.

Hay registros específicos que las organizaciones tienen que conservar en el transcurso ordinario de su negocio y estos estarán sujetos a una variedad de periodos legislativos y de

retención reglamentaria. Los registros que proporcionan pruebas de la eficacia del SGSI son de naturaleza diferente a aquellos registros que el SGSI existe para proteger, pero, no obstante, estos registros mismos deben controlarse y deben mantenerse legibles, fácilmente identificables y recuperables.Esto significa que, concretamente para los registros electrónicos, un medio de acceso debe conservarse incluso después de que el hardware y el software se hayan mejorado.

## Anexo A controles de documentos

Hay más controles relacionados con los documentos en el Anexo A que deben incluirse en los aspectos de control de documentos del SGSI. Todos son controles importantes por derecho propio. Estos controles son:

A.8.2.1: clasificación de la información, que trata de los niveles de confidencialidad

A.8.2.2: etiquetado de la información, que trata de cómo los niveles de confidencialidad están marcados en la información y los medios de información

A.8.2.3: manejo de los activos, que trata de los procedimientos para manejar los activos de acuerdo con su clasificación

A.18.1.3: protección de registros, que trata de la retención de los documentos

A.18.1.4: privacidad y protección de la información identificable personalmente, que trata de la confidencialidad de la información personal.

---

[1] *IT Service CMM: Una guía de bolsillo*, Van Haren, 2004, página 24.

[2] ISO/IEC 27001:2013, 7.5.1, General, nota b.

# CAPÍTULO 9: RESPONSABILIDAD DE LA GESTIÓN

La implementación de un SGSI es algo que la ISO 27001 reconoce que afectará a toda la organización. Los requisitos acerca del alcance y la política de seguridad de la información son explícitos que tiene que haber una justificación documentada para cualquier exclusión del alcance, y que la política debe aplicarse en toda la organización.

La ISO 27001 también es clara que el SGSI debe diseñarse para satisfacer las necesidades de la organización, y debe implementarse y gestionarse de manera que satisfaga, y siga satisfaciendo, esas necesidades.

## Dirección de la gestión

La ISO 27001 contiene un requisito que la gestión debe "[comunicar] la importancia de la gestión eficaz de la seguridad de la información y en conformidad con los requisitos del sistema de gestión de la seguridad de la información".[1] Estos requisitos se han hecho más fuertes en las versiones sucesivas de la norma del SGSI ya que quedado incluso más claro que diseñar y establecer un SGSI es difícil sin dicha dirección y apoyo de gestión.

La naturaleza estratégica de un SGSI se reconoce explícitamente en la cláusula 4.4 de la norma, que indica el requisito que la organización “establecerá, implementará, conservará y mejorará continuamente el sistema de gestión de la seguridad de la información”. Esta postura estratégica se establece (en la cláusula 4.1) como basada en un entendimiento de la organización y su contexto.

La responsabilidad de la gestión es tan importante que la cláusula 5 se dedica a exponer en detalle los requisitos de gestión. Estos requisitos son que la gestión “demostrará el liderazgo y el compromiso con respecto al sistema de gestión de la seguridad de la información”, “establecerá una política de seguridad de la información” y “garantizará que las responsabilidades y autoridades para las funciones relevantes para la seguridad de la información están asignadas y comunicadas”.

## Controles relacionados con la gestión

Hay una serie de controles en el Anexo A que especifican la implicación de la gestión y están vinculados al apartado 5 de la ISO 27001. Estos, numerados como aparecen en el Anexo A, son como sigue:

A.5.1.1: políticas de seguridad de la información

A.6.1.2: segregación de los deberes

A.9.2.5: revisión de los derechos de acceso del usuario

A.18.2.2: cumplimiento con las políticas y normas.

## Requisito de revisión gerencial

Además de los requisitos de control, la norma ordena, en la cláusula 9.3 (revisión gerencial), que la gestión, en intervalos planificados, debe "revisar el SGSI de la organización [...] para garantizar su idoneidad continua, adecuación y eficacia".[2] Esta sección define claramente la contribución requerida para el proceso de revisión; incluye el resultado de la actividad de revisión y monitorización de la organización.

El resultado de la revisión gerencial debe documentarse y también debe implementarse; debe llevar a una mejora firme, en curso y continua del SGSI. Un SGSI certificado por la ISO 27001estará sujeto a revisiones regulares de certificación durante la aceptación del certificado; estas revisiones se centrarán en cómo la organización y su gestión han impulsado el proceso de mejora continua.

---

[1] ISO/IEC 27001:2013, 5.1.d.

---

[2] ISO/IEC 27001:2013.

# CAPÍTULO 10: ENFOQUE DEL PROCESO Y EL CICLO PDCA

El modelo o ciclo de PDCA es el ciclo de planifique–haga–compruebe–actúe que se originó en las década de 1950s por W. Edwards Deming. Indica que los procesos empresariales deben tratarse como si son un bucle de retroalimentación continua para que los gerentes puedan identificar y cambiar aquellas partes del proceso que necesiten una mejora. El proceso, o una mejora del proceso, debe planificarse primero, después implementarse y medir su rendimiento, después hay que comprobar las mediciones frente a la especificación planificada y cualquier desvío o mejora potencial identificada e informada a la gerencia para que tomen una decisión acerca de cómo actuar.

## PDCA e ISO 27001

En la edición anterior de la ISO 27001, la cláusula 0.2 claramente estipula que el proceso requerido para implementar un SGSI era el PDCA. Con la publicación de la ISO 27001:2013, sin embargo, este ya no era un rasgo obligatorio del SGSI. De hecho, la ISO 27001:2013 no ofrece ninguna directriz en cuanto al enfoque de mejora continua, aparte de especificar que es

necesaria, dejando que la organización identifique su mejor práctica para su SGSI.

A pesar de la eliminación del ciclo de PDCA de la especificación, sigue siendo un proceso válido y eficaz para implementar el SGSI. En ausencia de un proceso definido, es sensato aplicar un PDCA, lo cual ha sido un enfoque práctico durante muchos años.

La aplicación del ciclo PDCA a un enfoque de proceso significa que, siguiendo los principios básicos del diseño del proceso, tiene que haber contribuciones y resultados del proceso. Un SGSI recibe como contribución los requisitos y expectativas de seguridad de la información de las partes interesadas y, a través de los procesos y acciones necesarias, produce los resultados de seguridad de la información que cumplan esos requisitos y expectativas.[1]

## El ciclo PDCA y las cláusulas de la ISO 27001

La correspondencia entre el ciclo PDCA y las etapas identificadas en la norma para el desarrollo del SGSI son como se exponen a continuación.

Planifique (establezca el SGSI):

Defina la organización y su contexto (cláusula 4.1)

Defina el alcance del SGSI (cláusula 4.3)

Defina la política de seguridad de la información (cláusula 5.2)

Defina un enfoque sistemático para la evaluación del riesgo (cláusula 6.1.2)

Lleve a cabo una evaluación de riesgo para identificar, dentro del contexto de la política y el alcance del SGSI, los activos de información importantes de la organización y los riesgos para ellos (cláusula 8.2)

Evalúe los riesgos (cláusula 6.1.2.d)

Identifique y evalúe las opciones para el tratamiento de estos riesgos (cláusula 6.1.3)

Seleccione, para cada decisión de tratamiento de riesgos, los objetivos de control y los controles a implementarse (cláusula 6.1.3.b)

Prepare una declaración de aplicabilidad (SoA). (cláusula 6.1.3.d).

Haga (implemente y utilice el SGSI):

Formule el plan de tratamiento del riesgo y su documentación, incluidos los procesos planificados y los procedimientos detallados (cláusula 6.1.3.e)

Implemente el plan de tratamiento del riesgo y los controles planificados (cláusula 8.3)

Proporcione formación adecuada para el personal afectada, así como programas de sensibilización (cláusula 7.2)

Gestione operaciones y recursos en línea con el SGSI (cláusulas 7.2 y 8.1)

Implemente procedimientos que faciliten la pronta detección, y respuesta, de los incidentes de seguridad. (cláusula 8.1).

Compruebe (monitoree y revise el SGSI):

La etapa de “compruebe” tiene, fundamentalmente, solo un paso (o conjunto de pasos): monitorear, revisar, probar y auditar (cláusula 9)

Monitorear, revisar, probar y auditar es un proceso continuo que tiene que cubrir todo el sistema.

Actúe (mantener y mejorar el SGSI):

Probar y auditar los resultados debe ser revisado por la gerencia, al igual que el SGSI a la luz del entorno de riesgo cambiante, tecnología u otras circunstancias; las mejoras del SGSI deben identificarse, documentarse e implementarse (cláusula 9)

Después de eso, estará sujeto a una revisión continua, más pruebas e implementación de mejora, un proceso conocido como “mejora continua”. (cláusula 10).

---

[1] ISO/IEC 27001:2013, 4.2 y 4.3.

# CAPÍTULO 11: CONTEXTO, POLÍTICA Y ALCANCE

El primer paso de la planificación es el ejercicio del alcance.

El requisito del alcance está contenido en la cláusula 4.3 de la ISO 27001. El requisito es que la organización “determinará los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance [teniendo en consideración] problemas internos y externos, los requisitos [de las partes interesadas, e] interfaces y dependencias entre las actividades realizadas por la organización, y aquellas realizadas por otras organizaciones”.

Esto se basa en el entendimiento de la organización y su contexto, así como las expectativas de las partes interesadas. La cláusula 4.1 indica que la organización “determinará los problemas internos y externos que sean relevantes para su propósito y que afecten su capacidad para lograr el resultado o resultados previstos de su sistema de gestión de la seguridad de la información”. La cláusula 4.2 exige que la organización identifique las partes interesadas y sus requisitos en relación con el SGSI. Esto “puede incluir requisitos legales y obligatorios y obligaciones contractuales”.

## El ejercicio del alcance

El ejercicio del alcance debe determinar lo que queda dentro, y lo que queda fuera, del SGSI. El SGSI levantará, en efecto, una barrera entre todo lo que está dentro del perímetro y todo lo que está fuera de él. El desarrollo el SGSI exigirá cada punto en que haya contacto entre lo exterior y lo interior sea tratado como un punto de riesgo potencial, exigiendo el tratamiento específico y apropiado.

Los activos, como los procesos, no pueden estar mitad dentro y mitad fuera del SGSI; o están totalmente dentro o fuera.

## Marco legal y reglamentario

El marco legal y reglamentario (4.2) crea también una perspectiva específica sobre el alcance del SGSI. Claramente, la información y los procesos de gestión de la información que estén todos dentro del alcance de cualquier normativa única, u otro requisito legal, todos deben estar dentro del alcance del SGSI.

## Definición de la política

El segundo paso de planificación principal exigido por la ISO 27001 es la definición de la política.

La cláusula 5.2 exige que la organización defina una política de seguridad de la información. Este requisito también está contenido en el primer control del Anexo A, control número 5.1.1. Esta es la primera de muchas cláusulas en la ISO 27001 que están respaldadas por la directriz y mejor práctica de la ISO 27002. La cláusula 5.1.1 de la ISO 27002 se expande en el requisito con número similar en el Anexo A y coincide con la especificación contenida en la cláusula 5.2 de la ISO 27001. El objetivo de control cumplido con la expedición de un documento de política es que proporciona "dirección y apoyo de gestión para la seguridad de la información de acuerdo con los requisitos empresariales y la normativa y leyes pertinentes".[1]

## Política y objetivos empresariales

La cláusula 5.1.1 continúa indicando que el documento de la política debe exponer el "enfoque de la organización para gestionar sus objetivos de seguridad de la información". La perspectiva de la norma es que un SGSI útil y con éxito será el que no mine ni bloquee la actividad empresarial. El riesgo significativo al implementar los sistemas que bloqueen la actividad empresarial, que no estén en línea con los objetivos empresariales, es que las personas en la empresa ignorarán o evitarán los controles del SGSI.

La política de la seguridad de la información debe suscribirse por la alta gerencia y estar disponible según sea apropiado para cualquiera que la necesite.

_____

[1] ISO/IEC 27002:2013, 5.1.

# CAPÍTULO 12: EVALUACIÓN DEL RIESGO

El paso siguiente de planificación es la evaluación del riesgo de la seguridad. La evaluación del riesgo se trata en las cláusulas 6.1.2 y 8.2 de la ISO 27001, respaldadas por la directriz de la ISO 27002 cláusula 0.2.

Más que ser inmediatamente complementaria, la ISO 27002 reconoce el valor de los marcos de gestión y control adicionales. La directriz de evaluación del riesgo ofrecida en la ISO 27002, por tanto, es necesariamente breve ya que anima a la organización a que elija el enfoque que sea más aplicable a su sector, complejidad y entorno de riesgo.

## Vínculo con ISO/IEC 27005

La ISO 27005 es un código de prácticas y proporciona una directiva extensa y detallada sobre cómo implementar los requisitos ordenados por la ISO 27001. Aunque la evaluación del riesgo debe llevarse a cabo en línea con los requisitos de la ISO 27001, la directriz de la ISO 27005 se puede utilizar al desarrollar la metodología de la evaluación del riesgo detallada.

## Objetivos del tratamiento del riesgo

Los planes del tratamiento del riesgo tienen cuatro objetivos vinculados. Estos son para

eliminar riesgos (ponerles fin),

reducir aquellos que no se pueden eliminar hasta niveles “aceptables” (tratarlos),

tolerarlos, ejercer cuidadosamente los controles para mantenerlos “aceptables”, o

transferirlos, por medio de un contrato o seguro, a alguna organización.

La ISO 27001 exige que la organización (en la cláusula 6.1.2) defina los criterios de aceptación del riesgo y los criterios para realizar las evaluaciones del riesgo de la seguridad de la información. El proceso adoptado por la gerencia para tomar decisiones debe ser “a medida según las necesidades de la organización”.[1] Además, cualquiera que sea el proceso de evaluación del riesgo que la organización elija implementar, debe ser capaz de “producir resultados sistemáticos, válidos y comparables”.[2]

Un plan de tratamiento del riesgo solo se puede elaborar una vez que se hayan identificado, analizado y evaluado los riesgos,

El proceso de evaluación del riesgo debe diseñarse para funcionar dentro del marco de tratamiento del riesgo general de la organización (si existe) y debe seguir los requisitos específicos de la ISO 27001.

## Requisitos contractuales, reglamentarios y legales

La ISO 27001 exige que la organización implemente cualquier control que podría ser necesario para cumplir sus obligaciones contractuales, reglamentarios y legales. Una vez que estos controles se han seleccionado e implementado, la organización puede proceder a llevar a cabo la evaluación del riesgo para identificar qué controles adicionales podrían ser necesarios para que este gestione los riesgos dentro del nivel de tolerancia de riesgos.

## Proceso de evaluación del riesgo

La ISO 27001 expone siete pasos que deben seguirse al llevar a cabo una evaluación del riesgo:

Identificar los riesgos asociados con la pérdida de confidencialidad, disponibilidad e integridad de la información dentro del alcance del SGSI;

Identificar los responsables del riesgo;

Evaluar las consecuencias que pueden resultar si un riesgo identificado se materializa;

Evaluar la probabilidad de que ocurra el riesgo;

Determinar los niveles del riesgo;

Comparar los resultados del análisis frente a los criterios del riesgo;

Priorizar los riesgos para el tratamiento.

## Identificar los riesgos (6.1.2.c.1)

Los riesgos de seguridad de la información son “el potencial de que las *amenazas* explotarán las *vulnerabilidades* de un activo o grupo de activos de información y así dañan una organización”.[3]

## Amenazas

Las amenazas son algo que puede ir mal o que puede “atacar” los activos identificados. Pueden ser internas o externas. La ISO 27001 exige que el SGSI se base en un fundamento de una identificación detallada y la evaluación de las amenazas para cada activo de información individual que esté dentro del

alcance. Las amenazas variarán según el sector y el alcance del SGSI.

## Vulnerabilidades

Estas dejan un sistema abierto al ataque por algo que se clasifica como una amenaza, o dejan que un ataque tenga éxito o un impacto mayor. Una vulnerabilidad puede ser explotada por una amenaza. Identifique, para cada activo identificado y para cada una de las amenazas enumeradas junto a cada uno de los activos, las vulnerabilidades que cada amenaza podría explotar.

## Identificar los responsables de los riesgos (6.1.2.c.2)

Además de los responsables de los riesgos que deben identificarse en el registro de activos antes de la evaluación del riesgo, cada riesgo identificado se asigna a un responsable. Es importante reconocer la distinción en funciones entre el propietario del activo y el responsable del riesgo. Aunque el propietario del activo es responsable de asegurar que el activo esté inventariado, clasificado y protegido, controlado y tratado adecuadamente[4], el responsable del riesgo no tiene responsabilidades específicas hacia el activo, pero es responsable de gestionar el riesgo y aceptar los riesgos de seguridad de la información residuales. Es importante también

tener en cuenta que un solo riesgo puede afectar a varios activos.

## Evaluar las consecuencias del riesgo (6.1.2.d.1)

La explotación con éxito de una vulnerabilidad por una amenaza tendrá un impacto en la disponibilidad, confidencialidad e integridad del activo. Se deben identificar todos estos impactos y, cuando sea posible, se les asignará un valor. La ISO 27001 es clara en que estos impactos se deben evaluar bajo cada uno de estos tres apartados; una sola amenaza, por tanto, podría explotar más que una vulnerabilidad y cada explotación podría tener más de un tipo de impacto.

El requisito de la norma es evaluar el alcance de la posible pérdida para la empresa para cada impacto potencial. Un objeto de este ejercicio es priorizar el tratamiento (controles) y para hacerlo así en el contexto del umbral de riesgo aceptable de la organización; es aceptable clasificar la pérdida posible más que intentar calcularla exactamente.

## Probabilidad (6.1.2.d.2)

Debe haber una evaluación de la probabilidad del impacto identificado que ocurre realmente. Las probabilidades podrían

ir desde “no muy probable” (p. ej. un terremoto importante en el sur de Inglaterra que destruya instalaciones principales y de copia de seguridad) hasta “casi diariamente” (p. ej. varios miles de ataques de piratas y malware automático contra la red).

### Niveles de riesgo (6.1.2.d.3)

Evalúe el nivel de riesgo para cada impacto como una combinación de las consecuencias y la probabilidad. Cada organización tiene que decidir por sí misma qué quiere establecer como umbrales para clasificar cada impacto potencial.

## Comparar el análisis del riesgo con los criterios del riesgo (6.1.2.e.1)

Coja los niveles de riesgo establecidos durante el análisis y compárelos con los criterios del riesgo establecidos al principio del proceso. Esto aporta una visión de conjunto más amplia del nivel del riesgo general que la organización afronta basándose en riesgo por riesgo y activo por activo, y proporciona la base del resto del SGSI.

## Priorizar los riesgos (6.1.2.e.2)

Cuanto más se desvíe un riesgo de los criterios de aceptación del riesgo, mayor es la prioridad. Incluso en el caso de que un riesgo esté dentro de los criterios de aceptación, puede ser valioso asignarle una prioridad para el tratamiento final o se puede predecir que el riesgo aumentará en circunstancias específicas.

## Plan del tratamiento del riesgo

La cláusula 6.1.3 de la ISO 27001 exige que la organización formule un plan de tratamiento del riesgo. Este debe identificar la acción de gestión adecuada, las responsabilidades y las prioridades para gestionar los riesgos de la seguridad de la información. El plan de tratamiento del riesgo se debe documentar. Debe establecerse dentro del contexto de la política de seguridad de la información de la organización y debe identificar claramente el enfoque de la organización para el riesgo y sus criterios para aceptar el riesgo. Estos criterios deben, cuando ya exista un marco de tratamiento del riesgo, ser coherente con los requisitos de la ISO 27001.

---

[1] ISO/IEC 27001:2013, 1.

[2] ISO/IEC 27001:2013, 6.1.2.b.

[3] ISO/IEC 27000, 2.61, Nota 6; énfasis añadido.

[4] ISO/IEC 27002, 8.1.2.

# CAPÍTULO 13: LA DECLARACIÓN DE APLICABILIDAD (SOA)

Aunque la declaración de aplicabilidad es fundamental para un SGSI y para la certificación acreditada del SGSI (es el documento desde el cual un auditor empezará el proceso de confirmar si se implantaron los controles adecuados o no y si son efectivos o no), solo puede prepararse verdaderamente una vez que se ha completado la evaluación del riesgo y se ha documentado el plan de tratamiento del riesgo.

La declaración de aplicabilidad es una declaración en cuanto a qué controles identificados en el Anexo A de la ISO 27001 son aplicables para la organización y cuáles no lo son. También puede contener controles adicionales seleccionados desde otras fuentes.

## La declaración de aplicabilidad y las partes externas

La declaración de aplicabilidad se debe revisar de manera regular y definida. Es el documento que se usa para demostrar a terceros el grado de seguridad que se ha implementado y al que se hace referencia normalmente, con su estado de expedición, en el certificado de cumplimiento expedido por los organismos terceros de certificación.

## Controles y Anexo A

La cláusula 6.1.3.b exige que la organización determine todos los controles necesarios para implementar el plan de tratamiento del riesgo. De manera significativa, esto se completa *antes* de consultar el Anexo A.

La cláusula 6.1.3.c de la ISO 27001 exige que la organización seleccione los objetivos de control y los controles adecuados entre aquellos especificados en el Anexo A para que coincidan con los controles seleccionados en 6.1.3.b. Sin embargo, indica que los controles adicionales también se pueden seleccionar desde otras fuentes. Como parte de escribir la declaración de aplicabilidad en 6.1.3.d, se exige a la organización que justifique la selección (y exclusión) de los controles.

La ISO 27002 proporciona buenas prácticas sobre el propósito y la implementación de cada uno de los controles enumerados en el Anexo A. Sin embargo, hay algunas áreas en las que las organizaciones pueden necesitar ir más lejos de lo que se especifica en la ISO 27002; el alcance hasta dónde puede ser necesario está impulsado por el grado al que se hayan desarrollado la tecnología y las amenazas desde la finalización de la ISO 27002.

## Controles (6.1.3.b)

Los controles son las contramedidas para las vulnerabilidades. La definición formal de la ISO 27000 de un control es un “medio de gestionar el riesgo, incluidas las políticas, los procedimientos, las directrices, prácticas o estructuras organizativas, que pueden ser de naturaleza administrativa, técnica, legales o de gestión. El control también se utiliza como sinónimo de dispositivo de seguridad o contramedida”.[1]

Aparte de aceptar intencionadamente los riesgos que estén dentro de cualquier criterio de aceptabilidad la organización ha adoptado en su plan de tratamiento del riesgo, o transferir el riesgo (a través de un contrato o seguro), la organización puede decidir implementar un control para reducir el riesgo.

## Riesgos residuales

No es posible ni práctico ofrecer una seguridad total contra cada uno de los riesgos, pero es posible proporcionar una seguridad eficaz contra la mayoría de los riesgos controlándolos hasta un nivel en el que el riesgo residual sea aceptable para la gerencia. El responsable del riesgo debe aceptar formalmente el riesgo residual (cláusula 6.1.3.f).

Los riesgos pueden y de hecho cambian, sin embargo, por tanto el proceso de revisar y evaluar los riesgos y los controles es

esencial y continuo (cláusula 8.2).

## Objetivos de control

Los controles se seleccionan a la luz de un objetivo de control. Un objetivo de control es una declaración de la intención de una organización para controlar alguna parte de sus procesos o activos y lo que pretende lograr mediante la aplicación del control. Un objetivo de control puede ser cumplido por una serie de controles.

El Anexo A de la ISO 27001 identifica los objetivos de control adecuados y enumera los controles para cada uno de ellos, que cumplen estos objetivos como mínimo. La organización debe seleccionar sus objetivos de control del Anexo A a la luz de su evaluación del riesgo y entonces garantiza que los controles que elija implementar (ya sea del Anexo o de fuentes adicionales) permitirán que logren el objetivo identificado.

## Planificar los incidentes de seguridad

Es importante que, al considerar los controles, los incidentes de seguridad probables que puede que haya que detectar se identifiquen, consideren y planifiquen. El proceso de seleccionar los controles individuales entre aquellos enumerados en el Anexo A de la norma deben incluir una

consideración de qué pruebas se necesitarán y qué mediciones de eficacia (6.1.1.e.2) ser harán para demostrar:

que los controles se han implementado y están funcionando eficazmente.

que cada riesgo se ha reducido, de ese modo, a un nivel aceptable, como exige la cláusula 6.1.2.a.1 de la norma. Los controles deben crearse de tal manera que cualquier error, fallo durante la ejecución, sea capaz de una detección rápida y que esa acción correctiva planificada, ya sea automática o manual, sea eficaz reduciendo a un nivel aceptable de riesgo de lo que pueda pasar después.

---

[1] ISO/IEC 27000, 2.16.

# CAPÍTULO 14: IMPLEMENTACIÓN

La implementación del SGSI implica las siguientes cinco tareas:

Implemente el plan de tratamiento del riesgo y los controles identificados en la declaración de aplicabilidad (8.3).

Defina cómo medir y evaluar la eficacia de todos los controles (9.1.b).

Implementar la formación y los programas de sensibilización (7.2 y 7.3), que se vinculan con el Control A.7.2.2 – sensibilización, educación y formación de la seguridad de la información.

Gestionar el SGSI (8.1). Todos los controles y procesos de interbloqueo deben seguir funcionando y las nuevas amenazas identificadas, evaluadas y, si es necesario, neutralizadas. Se debe contratar y formar gente, supervisar su rendimiento y desarrollar sus destrezas desarrolladas en línea con las necesidades cambiantes del negocio.

Implemente un procedimiento de respuesta y detección (10.1), que se vincule con la cláusula 16 del Anexo A, gestión de incidentes de seguridad de la información. Esta cláusula

contiene siete controles que diferencien entre un evento y un incidente y defina cómo se debe gestionar la respuesta.

# CAPÍTULO 15: VERIFICAR Y ACTUAR

La cláusula 9 de la norma trata completamente de la monitorización y la revisión. Contiene el requisito para que se implique la gestión activamente en la gestión a largo plazo del SGSI al tiempo que se reconoce la realidad de que el entorno de la amenaza de la seguridad de la información cambia incluso más rápidamente que el entorno empresarial. Esta cláusula trata, en líneas generales, de tres tipos de actividad: monitorización, auditoría y revisión.

## Monitorización

El propósito de la actividad de monitorización es principalmente detectar los errores de procesamiento y los eventos de la seguridad de la información rápidamente para llevar a cabo una acción correctiva inmediata. La monitorización debe ser formal, sistemática y generalizada. La categoría de la seguridad A.12.4 (inicio de sesión y monitorización) contiene controles que están relacionados específicamente con la actividad de TI y estos están vinculados a esta parte de la ISO 27001. El área de control A.16, gestión del incidente de seguridad de la información, también reconoce que la organización debe monitorear las desviaciones y los incidentes, responden ante ellos y aprende de estos.

## Auditoría

Las auditorías deben planificarse para garantizar que los controles documentados en la declaración de aplicabilidad sean eficaces y para identificar las no conformidades y las oportunidades de mejora. Los objetivos de control A.18.1 (cumplimiento con los requisitos legales y contractuales) y A.18.2 (revisiones de la seguridad de la información) se ocupan específicamente de este problema y ordenan revisiones de cumplimiento regulares y planificadas tanto a nivel de proceso como técnico. El objetivo de control A.12.7 (consideraciones de la auditoría de sistemas de información) trata los requisitos de seguridad para las herramientas de auditoría. El requisito de auditoría se describe en más profundidad en la cláusula 9.2 de la ISO 27001, que expone dos aspectos importantes del proceso:

La organización “planificará, establecerá, implementará y mantendrá un programa o programas de auditoría, incluida la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la generación de informes”.[1]

El programa de auditoría “tendrá en consideración la importancia de los procesos concernientes y los resultados de las auditorías previas”.[2]

La gestión en todos los niveles de la organización tiene un papel que jugar en la implementación eficaz, el mantenimiento y la mejora del SGSI. Esto se debe tener en cuenta en las descripciones del trabajo gerencial y de supervisión, los contratos de empleo, la inducción y otra formación y las revisiones de rendimiento.

## Revisión

Las revisiones de políticas de auditoría interna y externa, los informes de rendimiento, los informes de excepción, los informes de la evaluación del riesgo y todas las políticas y procedimientos asociados se llevan a cabo para asegurar que el SGSI continúa siendo eficaz en este contexto cambiante.

Los controles del Anexo A que sean relevantes directamente para este etapa del ciclo PDCA del SGSI son:

A.5.1.2: revisión de las políticas de seguridad de la información

A.9.2.5: revisión de los derechos de acceso del usuario

A.12.4: “inicio de sesión y monitorización” mismo como un objetivo de control que está relacionado, obviamente con el inicio de sesión y la monitorización, y que contiene cuatro controles

A.14.1: requisitos de seguridad de los sistemas de información, un objetivo de control que en efecto trata del uso de la aplicación de monitorización y el tratamiento de los datos

A.15.2.1: monitorización y revisión de los servicios del proveedor

A.16.1.6: aprendizaje de los incidentes de la seguridad de la información

A.17.1.3: verificación, revisión y evaluación de la continuidad de la seguridad de la información.

A.18.2.1: revisión independiente de la seguridad de la información.

Todos estos controles deben abordarse en esta tercera fase del desarrollo e implementación del SGSI. Los hallazgos y resultados de las actividades de monitorización y generación de informes se debe traducir en una acción correctiva y de mejora y, para los fines del SGSI, el registro de auditoría que demuestra que el proceso de la toma de decisiones y la implementación de esas decisiones debe conservarse en los registros del SGSI.

## Actúe, mantener y mejorar el SGSI

Esta es una sección breve y refleja la brevedad relativa de los requisitos del apartado 6.1.1.c de la ISO 27001. Esta cláusula expone el requisito de que la organización planea lograr la mejora continua del SGSI. Además, vincula el apartado 10 de la norma, cuyas dos cláusulas (10.1, no conformidad y acción correctora; y 10.2, mejora continua) especifican la naturaleza y el propósito de la actividad que debe ser una parte integrante de las acciones diarias de todos los que participan en la gestión cotidiana del SGSI.

---

[1] ISO/IEC 27001:2013, Cláusula 9.2.c.

[2] Ibídem.

# CAPÍTULO 16: REVISIÓN GERENCIAL

Cláusula 9.3 de la ISO 27001 (y objetivo de control A.18.2), que trata de la revisión gerencial del SGSI, enfatiza que la revisión gerencial debe tener en cuenta la "retroalimentación sobre el rendimiento de la seguridad de la información, incluidas las tendencias en [...] no conformidades y acciones correctoras",[1] así como cualquier cambio en cualquier parte o cualquier cosa que pudiera afectar al SGSI y las recomendaciones para la mejora.

Debe tenerse en cuenta que la acción correctora y preventiva debe priorizarse basándose en la evaluación del riesgo.[2]

La ISO 27001 exige, en el control A.18.2.1, una "revisión independiente de la seguridad de la información", la cual debe tener lugar a intervalos planificados (o cuando quiera que haya habido cambios importantes) y debe ser exhaustiva ("objetivos de control, controles, políticas, procesos y procedimientos"). La certificación de terceros cumpliría este requisito de control.

Evaluar y calcular los riesgos es una competencia principal que se exige a una organización que sea seria acerca de lograr y mantener una certificación acreditada de la ISO 27001. Es útil recordad el punto de que la prevención de las no

conformidades es a menudo más rentable que la acción correctora, que resume el enfoque de sentido común, rentable y basado en los riesgos de la norma.

---

[1] ISO/IEC 27001:2013, 9.3.c.1.

[2] ISO/IEC 27001:2013, 6.1.2.e.2.

# CAPÍTULO 17: ISO 27001 ANEXO A

El Anexo A de la ISO/IEC 27001:2013 tiene 14 cláusulas principales o áreas de control numeradas de A.5 a A.18, cada una de las cuales identifica uno o más objetivos de control. Cada objetivo de control está atendido por uno o más controles. Cada control está numerado secuencialmente.

Hay, en total, 114 subcláusulas, cada una de las cuales tiene un número de claúsula alfanumérico.

El Anexo A está alineado con la ISO 27002; esto significa que se utiliza precisamente los mismos objetivos de control, controles, numeración de la cláusula y redacción en tanto el Anexo A como en la ISO 27002. Tenga en cuenta que la afirmación clara de que “los objetivos del control y los controles enumerados en el Anexo A no son exhaustivos y pueden ser necesarios objetivos del control y controles adicionales”.[1] Las 14 cláusulas de control del Anexo A (no tiene las cláusulas del 1 al 4) todas empiezan con una A y se enumeran a continuación.

A5: Políticas de seguridad de la información

A6: Organización de la seguridad de la información

A7: Seguridad de recursos humanos

A8: Gestión de los activos

A9: Control del acceso

A10: Criptografía

A11: Seguridad del entorno y física

A12: Seguridad de las operaciones

A13: Seguridad de las comunicaciones

A14: Adquisición del sistema, desarrollo y mantenimiento

A15: Relaciones con los proveedores

A16: Gestión de incidentes de seguridad de la información

A17: Aspectos de seguridad de la información de la gestión de la continuidad empresarial

A18: Cumplimiento.

## Anexo A áreas de control y controles

Cada una de las cláusulas del Anexo A trata de una o más categorías de seguridad, y cada categoría de seguridad tiene un objetivo de control y uno o más controles que servirán para

asegurar ese objetivo. Las cláusulas, las categorías de control, los objetivos de control y los nombres de control se exponen a continuación; los requisitos de control detallados están contenidos en la norma, y esta se debe adquirir y estudiar.

## Cláusula A5: Políticas de seguridad de la información

**Dirección gerencial para seguridad de la seguridad:** proporcionar dirección gerencial y apoyo a la seguridad de acuerdo con los requisitos empresariales, las leyes y las regulaciones pertinentes.

Políticas para la seguridad de la información

Revisión de las políticas de la seguridad de la información

## Cláusula A6: Definición de la seguridad de la organización

**Organización interna:** para establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

Funciones y responsabilidades de la seguridad de la información

Segregación de los deberes

Contacto con las autoridades

Contacto con grupos de interés especiales

Seguridad de la información en gestión de proyectos

**Dispositivos móviles y teletrabajo:** para garantizar la seguridad del teletrabajo y el uso de dispositivos móviles

Política de dispositivos móviles

Teletrabajo

## Cláusula A7: Seguridad del recurso humano

**Antes del empleo:** para asegurar que los empleados y los contratistas entienden sus responsabilidades y son idóneos para las funciones para las que se les considera

Investigación

Términos y condiciones del empleo

**Durante el empleo:** para asegurar que los empleados y contratistas conocen y cumplen sus responsabilidades de la seguridad de la información

Responsabilidades de la gerencia

Sensibilización, educación y formación en seguridad de la información

Proceso disciplinario

**Terminación y cambio de empleo:** para proteger los intereses de la organización como parte del proceso de cambiar o terminar el empleo.

Terminación o cambio de las responsabilidades del empleo

## Cláusula A8: Gestión de los activos

**Responsabilidad por los activos:** para identificar los activos organizativos y definir las responsabilidades de protección adecuadas

Inventario de activos

Propiedad de los activos

Uso aceptable de los activos

Rendimiento de los activos

**Clasificación de la información:** para asegurar que la información recibe un nivel adecuado de protección de acuerdo

con su importancia para la organización

Clasificación de la información

Etiquetado de la información

Manejo de los activos

**Manejo de los medios:** para evitar la divulgación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios

Gestión de los medios extraíbles

Eliminación de los medios

Transferencia de los medios físicos

## Cláusula A9: Control del acceso

**Requisitos empresariales de control de acceso:** para limitar el acceso a la información y las instalaciones de procesamiento de la información

Política de control de acceso

Acceso a redes y servicios de establecimiento de contactos

**Gestión del acceso del usuario:** para asegurar el acceso del usuario autorizado y para prevenir el acceso no autorizado a los sistemas y servicios

Registro del usuario y cancelación del registro

Provisión del acceso del usuario

Gestión de los derechos de acceso privilegiado

Gestión de la información de autenticación secreta de los usuarios

Revisión de los derechos de acceso del usuario

Eliminación o ajuste de los derechos de acceso

**Responsabilidades del usuario:** para asegurarse de que los usuarios son responsables de salvaguardar su información de autenticación

Uso de la información de autenticación secreta

**Control del acceso a la aplicación y al sistema:** para prevenir el acceso no autorizado a los sistemas y las aplicaciones

Restricción al acceso de la información

Procesos de inicio de sesión seguros

Sistema de gestión de la contraseña

Uso de programas de utilidades privilegiadas

Control de acceso al código de la fuente del programa

## Cláusula A10: Criptografía

**Controles criptográficos:** para asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información

Política sobre el uso de controles criptográficos

Gestión clave

## Cláusula A11: Seguridad del entorno y física

**Áreas seguras:** para prevenir el acceso físico no autorizado, los daños y la interferencia en la información de la organización y las instalaciones de procesamiento de la información

Perímetro de seguridad física

Controles de entrada física

Seguridad de oficinas, cuartos e instalaciones

Protección frente a amenazas externas y del entorno

Trabajo en áreas seguras

Áreas de entrega y descarga

**Equipo:** para prevenir la pérdida, los daños, el robo o el compromiso de activos y la interrupción en las operaciones de la organización

Ubicación y protección del equipo

Utilidades de apoyo

Seguridad del cableado

Mantenimiento del equipo

Eliminación de activos

Seguridad del equipo y los activos fuera de las instalaciones

Eliminación segura y reutilización del equipo

Equipo del usuario sin atender

Política de escritorio despejado y pantalla despejada

## Cláusula A12: Seguridad de las operaciones

**Procedimientos operativos y responsabilidades:** para asegurar operaciones correctas y seguras de las instalaciones de procesamiento de la información

Procedimientos operativos documentados

Gestión del cambio

Gestión de la capacidad

Separación de desarrollo, prueba y entornos operativos

**Protección frente al malware:** para asegurar que la información y las instalaciones de procesamiento de la información estén protegidas frente al malware

Controles frente al malware

**Copia de seguridad:** para proteger frente a la pérdida de datos

Copia de seguridad de la información

**Inicio de sesión y monitorización:** para registrar eventos y generar pruebas

Inicio de sesión de eventos

Protección de la información de la sesión

Sesiones del administrador y del operador

Sincronización del reloj

**Control del software operativo:** para asegurar la integridad del software operativo

Instalación de software en los sistemas operativos

**Gestión de la vulnerabilidad técnica:** para evitar la explotación de vulnerabilidades técnicas

Gestión de vulnerabilidades técnicas

Restricciones en la instalación de software

**Consideraciones de la auditoría de los sistemas de información:** para minimizar el impacto de las actividades de auditoría en los sistemas operativos

Controles de auditoría de los sistemas de información

## Cláusula A13: Seguridad de las comunicaciones

**Gestión de la seguridad de la red:** para asegurar que la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo

Controles de redes

Seguridad de los servicios de redes

Segregación en redes

**Transferencia de la información:** para mantener la seguridad de la información transferida dentro de una organización y con una entidad externa

Políticas y procedimientos de transferencia de la información

Acuerdos sobre la transferencia de la información

Envío de mensajes electrónicos

Acuerdos de confidencialidad o no divulgación

## Cláusula A14: Adquisición del sistema, desarrollo y mantenimiento

**Requisitos de seguridad de los sistemas de información:** para asegurar que la seguridad de la información sea una parte

integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de la información que prestan servicios en redes públicas

Análisis y especificación de los requisitos de seguridad de la información

Seguridad de los servicios de aplicación en las redes públicas

Protección de las transacciones de los servicios de aplicación

**Seguridad en los procesos de desarrollo y apoyo:** para asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida del desarrollo de los sistemas de información

Política de desarrollo seguro

Procedimientos de control del cambio del sistema

Revisión técnica de las aplicaciones después de los cambios de la plataforma operativa

Restricciones en los cambios en los paquetes de software

Principios de ingeniería de sistemas seguros

Entorno de desarrollo seguro

Desarrollo subcontratado

Prueba del sistema de seguridad

Prueba de aceptación del sistema

**Datos de la prueba:** para asegurar la protección de los datos utilizados para la prueba

Protección de los datos de la prueba

## Cláusula A15: Relaciones con los proveedores

**Seguridad de la información en las relaciones con los proveedores:** para asegurar la protección de los activos de la organización que sea accesible por los proveedores

Política de seguridad de la información para las relaciones con los proveedores

Abordar la seguridad dentro de los acuerdos con los proveedores

Cadena de suministro de la tecnología de la comunicación y la información

**Gestión de la entrega del servicio del proveedor:** para mantener un nivel de seguridad de la información acordado y una entrega del servicio en línea con los acuerdos con el proveedor

Monitorización y revisión de los servicios del proveedor

Gestión de los cambios en los servicios del proveedor

## Cláusula A16: Gestión de incidentes de seguridad de la información

**Gestión de las mejoras y los incidentes de la seguridad de la información:** para asegurar un enfoque coherente y eficaz en la gestión de los incidentes de la seguridad de la información, incluida la comunicación sobre las debilidades y los eventos de seguridad

Responsabilidades y procedimientos

Generación de informes de eventos de seguridad de la información

Generación de informes de las debilidades de la seguridad de la información

Evaluación y decisión sobre los eventos de seguridad de la información

Respuesta a los incidentes de la seguridad de la información

Aprendizaje de los incidentes de seguridad de la información

Recopilación de pruebas

## Cláusula A17: Aspectos de seguridad de la información de la gestión de la continuidad empresarial

**Continuidad de la seguridad de la información:** la continuidad de la seguridad de la información estará integrada en los sistemas de gestión de la continuidad empresarial de la organización

Planificación de la continuidad de la seguridad de la información

Implementación de la continuidad de la seguridad de la información

Verificación, revisión y evaluación de la continuidad de la seguridad de la información

**Redundancias:** para asegurar la disponibilidad de las instalaciones de procesamiento de la información

Disponibilidad de las instalaciones de procesamiento de la información

## Cláusula A18: Cumplimiento

**Cumplimiento con los requisitos legales y contractuales:** para evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de cualquier requisito de la seguridad

Identificación de la legislación aplicable y los requisitos contractuales

Derechos de propiedad intelectual

Protección de los registros

Privacidad y protección de información identificable personalmente

Regulación de controles criptográficos

**Revisiones de la seguridad de la información:** para asegurar que la seguridad de la información se implementaba y utilizaba de conformidad con los procedimientos y políticas organizativos

Revisión independiente de la seguridad de la información

Cumplimiento con las políticas y normas

Revisión de cumplimiento técnica

_____

[1] ISO/IEC 27001:2013, 6.1.3.c, Nota 2.

# RECURSOS DE ITG

IT Governance Ltd consigue, crea y entrega productos y servicios para satisfacer las necesidades de regulación de TI del mundo real en constante cambio de las organizaciones, directores, gerentes y profesionales de la actualidad.

El sitio web de ITG (*www.itgovernance.eu*) es la tienda integral internacional para información, asesoramiento, orientación, libros, herramientas, formación y consultoría de regulaciones corporativas y de TI.

*www.itgovernance.eu/iso27001* es la página de información en nuestro sitio web para los recursos de la seguridad de la información.

## Otros sitios web

Los libros y herramientas publicados por IT Governance Publishing (ITGP) están disponibles en todos los vendedores de libros empresariales y también están disponibles inmediatamente en los siguientes sitios web:

*www.itgovernance.co.uk*

*www.itgovernanceusa.com*

*www.itgovernance.asia*

www.itgovernancesa.co.za

## Herramientas

La gama única de herramientas de ITG incluye la herramienta del marco de gobierno de TI, que contiene todas las herramientas y orientación que necesitará con el fin de desarrollar e implementar un marco de gobierno de TI para su organización.

Para recibir un documento gratuito sobre cómo utilizar el Marco de gobierno de TI patentado, y para una versión gratuita de las herramientas, consulte *www.itgovernance.eu/free_trial*.

Hay además una amplia gama de herramientas para simplificar la implementación de los sistemas de gestión, tales como un SGSI de la ISO/IEC 27001 o un BCMS de la ISO/IEC 22301, y estas se pueden ver y comprar en *www.itgovernance.eu*.

## Servicios de formación

IT Governance ofrece una cartera extensa de cursos de formación diseñados para formar en seguridad de la información, gobierno de TI, gestión del riesgo y profesionales

del cumplimiento. Nuestra aula y programas de formación por internet le ayudarán a desarrollar las habilidades necesarias para ofrecer las mejores prácticas y el cumplimiento en su organización. Además, mejorarán su carrera proporcionándole las certificaciones estándar de la industria y un aumento en el reconocimiento de sus pares. Nuestra gama de cursos ofrecen una ruta de aprendizaje estructurada desde el nivel básico al avanzado en los temas clave de seguridad de la información, gobierno de TI, continuidad empresarial y gestión del servicio.

ISO/IEC 27001:2013 es la norma de gestión internacional que ayuda a las empresas y organizaciones en todo el mundo a desarrollar el mejor sistema de gestión de la seguridad de la información en su clase. Se considera fundamental el conocimiento y la experiencia en implementar y mantener el cumplimiento de la ISO 27001 para establecer una carrera con éxito en la seguridad de la información. Tenemos el primer programa del mundo de formación en ISO 27001 certificado con cursos de formación Básico, Implementador líder, Gestión del riesgo y Auditor líder Cada curso está diseñado para proporcionar a los delegados conocimiento y habilidades pertinentes y una cualificación reconocida en el sector galardonada por el International Board for IT Governance Qualifications (IBITGQ).

Los detalles completos de todos los cursos de formación de IT Governance se pueden encontrar en *www.itgovernance.eu/training*.

## Consultoría y servicios profesionales

Su misión para cubrir las diferencias de seguridad crítica recibirá una enorme ayuda de los consultores de IT Governance, que han asesorado a cientos de gerentes de seguridad de la información en la adopción de los Sistemas de Gestión de la Seguridad dela Información (SGSI) de la ISO 27001.

Los activos, la seguridad y los sistemas de datos de la organización, sin mencionar la reputación, están en sus manos. Un violación de la seguridad importante podría provocar un desastre. Un asesoramiento y apoyo oportunos de los especialistas en gobierno de TI le permitirá identificar las amenazas, evaluar los riesgos e implantar los controles necesarios antes de que haya un incidente.

En IT Governance, entendemos que la información, la seguridad de la información y la tecnología de la información siempre son cuestiones empresariales y no solo informáticas. Nuestros servicios de consultoría le ayudan a gestionar las

estrategias de seguridad de la información en armonía con las metas empresariales, transmitiendo los mensajes correctos a sus compañeros para apoyarles en la toma de decisiones.

Para obtener más información acerca de la consultoría de IT Governance vea: *www.itgovernance.eu/consulting*.

## Servicios de publicaciones

IT Governance Publishing (ITGP) es la impresión de publicaciones líder del mundo en gestión de cumplimiento, riesgos y normas de TI que es de propiedad exclusiva de IT Governance Ltd.

Con libros y herramientas que cubren todos los marcos de cumplimiento, riesgos y normas de TI, somos la editorial de elección para autores y distribuidores por igual, produciendo publicaciones únicas y prácticas de la calidad más alta, en los últimos formatos disponibles, que los lectores encuentran inestimables.

*www.itgovernancepublishing.co.uk* es el sitio web dedicado a ITGP que facilitar el acceso a más información para autores, distribuidores, lectores y otras partes interesadas tanto actuales como futuros. Esto permite a los visitantes del sitio web de ITGP mantenerse al día con las últimas noticias y publicaciones.

## Boletín

El gobierno de TI es uno de los temas más candentes en el negocio en la actualidad, y no menos porque también es el que está en constante cambio.

Puede estar al día con las últimas novedades en todo el espectro de las materias sobre normas de TI, incluida: la gestión del riesgo, seguridad de información, Biblioteca de Infraestructura de Tecnologías de Información (ITIL) y gestión de servicios de TI, gestión de proyectos, cumplimiento y mucho más, suscribiéndose a las publicaciones principales de ITG y los correos electrónicos de las alertas del tema.

Simplemente visite nuestro centro de suscripciones y seleccione sus preferencias: *www.itgovernance.eu/daily-sentinel*.