



## COMPARTIR



([https://twitter.com/intent/tweet?](https://twitter.com/intent/tweet?text=Standards%20for%20IT%20and%20cyber%20security&url=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/)

[text=Standards%20for%20IT%20and%20cyber%20security&url=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/](https://twitter.com/intent/tweet?text=Standards%20for%20IT%20and%20cyber%20security&url=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/))



(<https://www.linkedin.com/sharing/share-offsite/?url=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/>)



(<https://www.facebook.com/sharer/sharer.php?u=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/>)



(mailto:?subject=Standards%20for%20IT%20and%20cyber%20security&body=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/)

## Normas de seguridad informática y cibernética

Existe una amplia selección de normas británicas e internacionales con las que las pymes del Reino Unido (es decir, las pequeñas y medianas empresas) pueden trabajar para protegerse mejor de los riesgos relacionados con la TI y la ciberseguridad. También existen especificaciones disponibles al público (PAS), que son normas de aplicación rápida patrocinadas por las necesidades de las organizaciones clientes y desarrolladas de acuerdo con las directrices establecidas por BSI. BSI también publica una amplia gama de libros para pymes que explican las normas y sus beneficios.

Acceda a las siguientes secciones utilizando la siguiente lista:

- Normas BSI sobre TI y ciberseguridad (</en-IN/Cyber-Security/standards-for-it-and-cyber-security/#BSI-standards>)
- Especificaciones disponibles públicamente para TI y ciberseguridad (</en-IN/Cyber-Security/standards-for-it-and-cyber-security/#PAS-standards>)
- Libros de BSI sobre TI y ciberseguridad (</en-IN/Cyber-Security/standards-for-it-and-cyber-security/#BSI-books>)
- Libros ISO sobre TI y ciberseguridad (</en-IN/Cyber-Security/standards-for-it-and-cyber-security/#ISO-books>)
- Normas del Gobierno del Reino Unido sobre TI y ciberseguridad (</en-IN/Cyber-Security/standards-for-it-and-cyber-security/#Gov-standards>)

Número/nombre estándar	Descripción/Beneficios
BS 10012:2009, <i>Especificación para un sistema de gestión de información personal</i>	Estas normas proporcionan un marco para mantener y mejorar el cumplimiento de la legislación y las buenas prácticas en materia de protección de datos. Se han desarrollado para ayudar a las empresas a establecer y mantener un sistema de gestión de información personal de buenas prácticas que cumpla con la Ley de Protección de Datos de 1998.
BS ISO/IEC 18043:2006, <i>Selección, implementación y operación de sistemas de detección de intrusiones</i> ( <a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030068973">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030068973</a> )	Esta norma proporciona pautas para ayudar a las organizaciones a seleccionar, implementar y operar sistemas de detección de intrusiones (IDS). También proporciona información general sobre las tecnologías de IDS.
BS ISO 22301:2012, <i>Requisitos de los sistemas de gestión de la continuidad del negocio</i> ( <a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030207716">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030207716</a> )	Esta norma especifica los requisitos para establecer y gestionar un sistema eficaz de gestión de la continuidad del negocio para cualquier empresa, independientemente de su tipo o tamaño.
BS ISO 22313:2012, <i>Guía de sistemas de gestión de la continuidad del negocio</i> ( <a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030247741">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030247741</a> )	Esta norma es el documento de orientación para la norma BS ISO 22301. Proporciona un marco más intuitivo para quienes buscan las mejores prácticas de continuidad empresarial.

BS ISO/IEC 27000:2014, *Sistemas de gestión de seguridad de la información: descripción general y vocabulario*

(<https://shop.bsigroup.com/ProductDetail/?pid=000000000030284692>)

Esta norma proporciona una descripción general de los sistemas de gestión de seguridad de la información y de las distintas normas internacionales que se encuentran disponibles como parte de la serie ISO/IEC 27000. También define un vocabulario común de términos y definiciones que se utilizan en dichas normas.

BS ISO/IEC 27001:2013, *Sistemas de gestión de seguridad de la información – Requisitos*  
(<https://shop.bsigroup.com/ProductDetail/?pid=000000000030192065>)

Esta norma es la última versión de la norma líder mundial en materia de gestión de la seguridad de la información. Proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información. Su finalidad es que sea aplicable a empresas de todos los tamaños y tipos.

La norma sigue la “estructura común de alto nivel y texto común idéntico” que adoptan todas las principales normas de sistemas de gestión. El Anexo A de BS ISO/IEC 27001:2013 contiene los objetivos y controles de control de seguridad de la información derivados de los enumerados en BS ISO/IEC 27002:2013, *Código de prácticas para controles de seguridad de la información* . Sin embargo, BS ISO/IEC 27001 se puede utilizar de forma independiente.

La norma ISO/IEC 27001 se utiliza en todo el mundo como criterio para indicar una gestión eficaz de la seguridad de la información. Es la única norma de certificación generalmente reconocida para la seguridad de la información y la ciberseguridad.

BS ISO/IEC 27002:2013, *Código de prácticas para controles de seguridad de la información*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030186138>)

Esta norma es la última versión de la norma líder mundial para la especificación de controles de seguridad de la información. Está diseñada para usarse como referencia al seleccionar controles durante la implementación de un sistema de gestión de seguridad de la información basado en ISO/IEC 27001. Sin embargo, se puede usar como guía al buscar información sobre controles de seguridad de la información comúnmente aceptados. También se puede usar como fuente de control al desarrollar pautas de gestión de seguridad de la información específicas de la industria u organización.

Aunque está estrechamente relacionada con la norma BS ISO/IEC 27001, *Sistemas de gestión de seguridad de la información: requisitos*, la norma BS ISO/IEC 27002 se puede utilizar de forma independiente. Proporciona un catálogo de posibles controles de seguridad de la información que se pueden utilizar para la evaluación comparativa, como especificaciones de requisitos o como parte de otras formas de sistema de gestión de la seguridad.

Para cada control sugerido, la norma BS ISO/IEC 27002 proporciona orientación sobre la implementación y otra información relevante, incluyendo, cuando corresponde, referencias a otras normas internacionales que contienen más detalles.

BS ISO/IEC 27003:2010, *Guía de implementación del sistema de gestión de seguridad de la información*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030133463>)

Esta norma ofrece recomendaciones básicas para el diseño de un sistema de gestión de la seguridad de la información (SGSI) en línea con la norma ISO/IEC 27001. Proporciona instrucciones claras para la planificación de un proyecto de SGSI en empresas de todos los tamaños y en todos los sectores. La versión actual de la norma ISO/IEC 27003 está alineada con la edición 2005 de la norma ISO/IEC 27001. Actualmente se está actualizando para alinearla con la nueva edición 2013.

BS ISO/IEC 27004:2009, *Medidas de gestión de la seguridad de la información*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030134765>)

Esta norma proporciona orientación sobre el desarrollo y uso de medidas y mediciones para evaluar la eficacia de un sistema de gestión de seguridad de la información (SGSI) implementado. Está diseñada para ser aplicable a organizaciones de todo tipo y tamaño. La versión actual de la norma ISO/IEC 27003 está alineada con la edición 2005 de la norma ISO/IEC 27001. Actualmente se está actualizando para alinearla con la nueva edición 2013.

BS ISO/IEC 27005:2011, *Gestión de riesgos de seguridad de la información*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030228522>)

Esta norma proporciona directrices para la gestión de riesgos de seguridad de la información. Respalda los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a implementar la seguridad de la información basándose en un enfoque de gestión de riesgos. Se está desarrollando una nueva versión que respaldará la versión 2013 de la norma BS ISO/IEC 27001. Sin embargo, el Anexo E de la edición 2011, que describe los enfoques de evaluación de riesgos, ya está alineado con la edición 2013 de la norma BS ISO/IEC 27001.

BS ISO/IEC 27006:2011, *Requisitos para organismos que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030246892>)

Esta norma especifica los requisitos y proporciona orientación para los organismos de certificación que prestan servicios de auditoría y certificación de sistemas de gestión de la seguridad de la información (SGSI). Para que sus certificados sean reconocidos internacionalmente, los organismos de certificación deben estar acreditados como conformes con la norma ISO/IEC 17021-1. Esta Norma Internacional establece los requisitos y la orientación adicionales necesarios para que puedan ofrecer la certificación ISO/IEC 27001. La versión actual de la norma ISO/IEC 27006 está alineada con la edición 2005 de la norma ISO/IEC 27001. Actualmente se está actualizando para alinearla con la nueva edición 2013.

<p>BS ISO/IEC 27007:2011, <i>Directrices para la auditoría de sistemas de gestión de seguridad de la información</i></p>	<p>Esta norma proporciona orientación sobre la gestión de un programa de auditoría de sistemas de gestión de la seguridad de la información (SGSI), sobre la realización de auditorías de SGSI y sobre las competencias requeridas a los auditores de SGSI. Se basa en la orientación general sobre auditoría de sistemas de gestión contenida en la norma ISO 19011.</p>
<p>PD ISO/IEC TR 27008:2011, <i>Directrices para auditores sobre controles de seguridad de la información</i> (<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030204591">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030204591</a>)</p>	<p>Esta norma proporciona orientación a los auditores sobre la revisión de la implementación y el funcionamiento de los controles de seguridad, como los definidos en la norma ISO/IEC 27002. No proporciona orientación sobre la auditoría de los aspectos de los sistemas de gestión de la seguridad de la información.</p>
<p>BS ISO/IEC 27031:2011, <i>Directrices para la preparación de tecnologías de la información y la comunicación para la continuidad del negocio</i> (<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030168355">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030168355</a>)</p>	<p>Esta norma proporciona pautas de mejores prácticas para preparar los sistemas de tecnología de la información y la comunicación para cumplir con los requisitos de continuidad del negocio y proporciona un marco de métodos y procesos para evaluar y mejorar esa capacidad.</p>



BS ISO/IEC 27032:2012, *Directrices para la ciberseguridad*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030168517>)

Esta norma es una norma internacional que proporciona orientación para mejorar la seguridad cibernética; en particular, proporciona orientación técnica para abordar los riesgos comunes de seguridad cibernética. La norma contiene orientación dirigida a diferentes partes interesadas en la seguridad cibernética, incluidos los consumidores, los proveedores de servicios y los administradores de riesgos. También identifica diferentes formas de amenazas a la seguridad cibernética. Sin embargo, no aborda cuestiones cibernéticas no relacionadas con el uso de Internet.

BS ISO/IEC 27033-1:2009, *Seguridad de la red - Parte 1: Descripción general y conceptos*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030168527>)

Esta norma proporciona detalles significativos sobre la mayoría de los problemas de seguridad de la red y responde preguntas que la mayoría de los propietarios y gerentes de pequeñas empresas probablemente tengan sobre la estrategia y las tecnologías de seguridad de la red.

BS ISO/IEC 27033-2:2012, *Seguridad de red - Parte 2: Directrices para el diseño e implementación de la seguridad de red*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030168530>)

Esta norma identifica de forma precisa los requisitos de seguridad de la red. También incluye una plantilla de documentación como anexo, que proporciona una lista de verificación para garantizar que el diseño de la red cubra todo lo que necesita. Contiene muy poca información sobre el diseño y la implementación de redes, por lo que es más adecuada para aquellas personas que gestionan el diseño y la adquisición de redes, en lugar de los diseñadores de redes propiamente dichos.

<p>BS ISO/IEC 27033-3:2010, <i>Seguridad de redes - Parte 3: Escenarios de redes de referencia. Amenazas, técnicas de diseño y problemas de control</i> (<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030192104">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030192104</a>)</p>	<p>Esta norma forma parte de la serie 27033 de normas que tratan sobre el diseño de redes seguras. Describe numerosos escenarios de uso en los que se emplean redes y, a continuación, identifica las amenazas, las técnicas de diseño y los problemas de control asociados a cada uno de ellos.</p>
<p>BS ISO/IEC 27033-4:2014, <i>Tecnología de la información. Técnicas de seguridad. Seguridad de redes. Protección de las comunicaciones entre redes mediante pasarelas de seguridad</i> (<a href="https://shop.bsigroup.com/ProductDetail/?pid=000000000030192107">https://shop.bsigroup.com/ProductDetail/?pid=000000000030192107</a>)</p>	<p>Esta parte de la norma ISO/IEC 27033 proporciona orientación técnica detallada para proteger las comunicaciones entre redes mediante puertas de enlace de seguridad. Describe diferentes tipos de cortafuegos y otros dispositivos de seguridad de puerta de enlace, como enrutadores y sistemas de protección contra intrusiones.</p>
<p>BS ISO/IEC 27033-5:2013, <i>Tecnología de la información. Técnicas de seguridad. Seguridad de redes. Protección de las comunicaciones entre redes mediante redes privadas virtuales (VPN)</i> (<a href="https://shop.bsigroup.com/ProductDetail/?pid=000000000030192110">https://shop.bsigroup.com/ProductDetail/?pid=000000000030192110</a>)</p>	<p>Esta parte de ISO/IEC 27033 proporciona orientación técnica detallada para proteger las interconexiones de red y conectar usuarios remotos a redes mediante el uso de redes privadas virtuales.</p>

BS ISO/IEC 27035:2011, *Gestión de incidentes de seguridad de la información*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030184433>)

Esta norma describe un enfoque estructurado y planificado para gestionar incidentes de seguridad de la información. Aunque está dirigida a organizaciones de mayor tamaño, las PYME pueden utilizarla para extraer un conjunto más básico de documentos y procedimientos adecuados a sus necesidades. La norma BS ISO/IEC 27035 se publicó anteriormente como PD ISO/IEC TR 18044:2004 y actualmente se está revisando. La nueva versión será una norma de varias partes, con partes separadas para diferentes aspectos de la gestión de incidentes.

BS ISO/IEC 27036-1:2014, *Tecnología de la información. Técnicas de seguridad. Seguridad de la información para las relaciones con los proveedores. Descripción general y conceptos*  
(<https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030249456>)

Esta parte de la norma ISO/IEC 27036 describe los conceptos clave para asegurar las relaciones con los proveedores desde el punto de vista tanto de los compradores como de los proveedores. También proporciona una introducción a las otras partes de la norma ISO/IEC 27036. Tenga en cuenta que la norma 27036-2 (requisitos fundamentales) estará disponible en breve y que la norma 27036-4 (relaciones con los proveedores en la nube) todavía está en desarrollo.

<p>BS ISO/IEC 27036-3:2013, <i>Tecnología de la información. Técnicas de seguridad. Seguridad de la información para las relaciones con los proveedores. Directrices para la seguridad de la cadena de suministro de tecnología de la información y la comunicación</i> (<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030250179">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030250179</a>)</p>	<p>Esta parte de la norma ISO/IEC 27036 proporciona orientación sobre la gestión de los riesgos de seguridad de la información causados por cadenas de suministro de TIC físicamente dispersas y de múltiples capas; la respuesta a los riesgos de seguridad de la información de las cadenas de suministro de TIC globales; y la integración de procesos y prácticas para respaldar los controles de seguridad de la información en procesos más amplios del ciclo de vida del sistema y del software.</p>
<p>BS ISO/IEC 27037:2012, <i>Directrices para la identificación, recopilación, adquisición y conservación de evidencia digital</i> (<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030207800">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030207800</a>)</p>	<p>Esta norma proporciona directrices para el manejo de pruebas digitales. Se aplica a todo tipo de dispositivos digitales, no solo a las computadoras. Además de principios generales que son de interés principalmente para los tribunales y los jueces, contiene consejos sumamente prácticos, como cuándo utilizar cinta adhesiva para evitar que las máquinas se reinicien accidentalmente.</p>
<p>BS ISO 28000:2007, <i>Especificación para sistemas de gestión de seguridad para la cadena de suministro</i> (<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030155502">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030155502</a>)</p>	<p>Esta norma aborda la gestión de las actividades que afectan a la seguridad de la cadena de suministro de una manera coherente con otras normas de sistemas de gestión. La norma BS ISO/IEC 28000 está respaldada por otras normas internacionales de la serie 28000 que definen cómo se pueden auditar y certificar las organizaciones según la norma ISO/IEC 28000.</p>

## Especificaciones disponibles públicamente para TI y ciberseguridad

Número/nombre estándar	Descripción/Beneficios
PAS 555:2013, <i>Riesgo de ciberseguridad - Gobernanza y gestión - Especificación</i> ( <a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030261972">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030261972</a> )	Esta norma PAS detalla un marco para la gobernanza y la gestión del riesgo de ciberseguridad. Los requisitos de esta norma PAS (especificación disponible públicamente) definen los resultados de una ciberseguridad eficaz e incluyen medidas técnicas, físicas, culturales y de comportamiento, junto con un liderazgo y una gobernanza eficaces. Está diseñada para ser escalable y, por lo tanto, es adecuada para empresas de todos los tamaños.

---

## Libros de BSI sobre TI y ciberseguridad

Título	Descripción
Directrices sobre requisitos y preparación para la certificación de SGSI según la norma ISO/IEC 27001 Segunda Edición (BIP 0071) ( <a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030282637">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030282637</a> )	Este libro proporciona orientación sobre los requisitos especificados en la norma ISO/IEC 27001:2013 (/en-IN/ISOIEC-27001-Information-Security/ISOIEC-27001-revision/) y las mejores prácticas descritas en ISO/IEC 27002:2013 para respaldar el uso adecuado de estas normas. Ofrece orientación sobre el “ciclo de vida” completo de los procesos y actividades del SGSI (sistema de gestión de seguridad de la información) necesarios para establecer, implementar, monitorear y mejorar continuamente un conjunto de controles y procesos de gestión para lograr una seguridad de la información eficaz.

<p>¿Está preparado para una auditoría de SGSI basada en la norma ISO/IEC 27001? Segunda edición (BIP 0072)</p> <p>(<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030282638">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030282638</a>)</p>	<p>Este libro ofrece orientación al usuario sobre cómo prepararse para una auditoría de certificación de SGSI basada en la norma ISO/IEC 27001:2013. Es una lectura esencial para aquellas organizaciones que están a punto de embarcarse en una certificación de terceros.</p>
<p>Guía para la implementación y auditoría de controles SGSI basados en la norma ISO/IEC 27001 Segunda Edición (BIP 0073)</p> <p>(<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030282631">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030282631</a>)</p>	<p>Este libro proporciona orientación sobre la implementación de los requisitos de control del SGSI para auditar las implementaciones de control existentes, con el fin de ayudar a las organizaciones a prepararse para la certificación de acuerdo con los requisitos especificados en la norma ISO/IEC 27001:2013. Proporciona orientación sobre la implementación, verificación y auditoría de los controles.</p>
<p>Gestión de riesgos de seguridad de la información (BIP 0076)</p> <p>(<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030172860">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030172860</a>)</p>	<p>La norma ISO/IEC 27005 es una norma de gestión de riesgos de SGSI que respalda la implementación de la norma ISO/IEC 27001. Este libro es un manual práctico para el uso y la aplicación de la norma ISO/IEC 27005. Proporciona orientación y asesoramiento para respaldar específicamente la implementación de los requisitos especificados en la norma ISO/IEC 27001:2005 que se relacionan con los procesos de gestión de riesgos y las actividades asociadas. Aunque este manual se basa en una versión reemplazada de la norma ISO/IEC 27001, la mayor parte de su contenido es independiente de la versión y sigue siendo válido.</p>

<p>Gestión de la seguridad en entornos externalizados y deslocalizados (BIP 0116)</p> <p>(<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030207795">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030207795</a>)</p>	<p>Se establecen pautas, prácticas recomendadas y factores críticos de éxito para la gestión de la seguridad en entornos subcontractados. Cuando corresponde, se abordan cuestiones de ciberseguridad. Un capítulo aborda la computación en la nube.</p>
<p>Computación en la nube: una introducción práctica a los aspectos legales (BIP 0117)</p> <p>(<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030215581">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030215581</a>)</p>	<p>Proporciona asesoramiento sobre los aspectos legales asociados a la computación en la nube. Para ello, proporciona una descripción técnica de las diferentes modalidades de computación en la nube y sus problemas asociados de seguridad de la información y protección de datos.</p>
<p>Introducción a la norma ISO 27001:2013 (BIP 0139)</p> <p>(<a href="https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030279462">https://shop.bsigroup.com/en/ProductDetail/?pid=000000000030279462</a>)</p>	<p>Este libro sirve como introducción básica a la norma ISO/IEC 27001:2013 y como guía sencilla para su implementación. No se presupone ningún conocimiento previo de la norma ISO/IEC 27001 ni de los sistemas de gestión. La guía es aplicable a una amplia gama de implementaciones de SGSI adecuadas para pequeñas empresas y organizaciones de mayor tamaño. El libro también incluye un método práctico y fácil de usar para la evaluación y el tratamiento de riesgos que ofrece resultados expresados directamente en términos comerciales significativos.</p>

## Libros ISO sobre TI y ciberseguridad

Título	Descripción
--------	-------------

<p>ISO/IEC 27001 para pequeñas empresas: consejos prácticos (<a href="https://www.iso.org/iso/home/store/publications_and_products/publication_item.htm?pid=PUB100255">https://www.iso.org/iso/home/store/publications_and_products/publication_item.htm?pid=PUB100255</a>)</p>	<p>Este manual pretende desmitificar la seguridad de la información y presenta un enfoque práctico, claramente explicado y paso a paso para que las PYME implementen un SGSI de información basado en la norma ISO/IEC 27001:2005. Utiliza un enfoque de lista de verificación con cuestionario. Este manual está disponible únicamente en papel. Lo publican ISO e IEC y se puede obtener en la tienda web de ISO (<a href="https://www.iso.org/iso/home/store.htm">https://www.iso.org/iso/home/store.htm</a>). No está disponible en BSI.</p>
---	--

## Normas del Gobierno del Reino Unido sobre TI y ciberseguridad

Nombre/número estándar	Descripción
<b>Esquema de elementos esenciales cibernéticos, <i>resumen</i> (BIS/14/696) (PDF)</b>	Este folleto proporciona un resumen del Plan Cyber Essentials, junto con información de fondo sobre su uso previsto y sus beneficios.
<b>Esquema de elementos esenciales para la seguridad cibernética, <i>Esquema de elementos esenciales para la seguridad cibernética: Requisitos para la protección técnica básica contra ataques cibernéticos</i> (BIS/14/696) (PDF)</b>	En este documento se describen los cinco tipos de controles técnicos que sustentan el plan Cyber Essentials y se los vincula con la norma ISO/IEC 27002 y otras normas.



**Esquema de elementos esenciales cibernéticos, *marco de garantía* (BIS/14/697) (PDF)**

Este documento describe el marco de certificación que respalda Cyber Essentials. Define la filosofía de garantía y las pruebas obligatorias. Incluye información sobre qué sistemas y servicios pueden y no pueden estar dentro del alcance del Esquema.

Norma IA n.º 1 de HMG, *Evaluación de riesgos técnicos* (PDF)

([http://www.cesg.gov.uk/publications/Documents/is1\\_risk\\_assessment.pdf](http://www.cesg.gov.uk/publications/Documents/is1_risk_assessment.pdf))

Esta norma es una norma de garantía de la información (IA) para los administradores de riesgos y los profesionales de la IA responsables de identificar, evaluar y tratar los riesgos técnicos de los sistemas y servicios cibernéticos que manejan información del gobierno del Reino Unido. El uso de esta norma es un requisito obligatorio para todos los sistemas cibernéticos que manejan, almacenan y procesan información del gobierno marcada de manera protectora o datos críticos para el negocio, o que están interconectados con redes o servicios intergubernamentales. La versión completa de este documento no es de dominio público.

COMPARTIR



(<https://twitter.com/intent/tweet?text=Standards%20for%20IT%20and%20cyber%20security%20and%20cyber%20security&url=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/>)



(<https://www.linkedin.com/sharing/share-offsite/?url=https://www.bsigroup.com/en-IN/Cyber-Security/standards-for-it-and-cyber-security/>)





La imparcialidad es el principio rector de la forma en que BSI proporciona sus servicios. La imparcialidad significa actuar de manera justa y equitativa en sus relaciones con las personas y en todas las operaciones comerciales. Significa que las decisiones se toman sin ningún tipo de influencia que pueda afectar la objetividad de la toma de decisiones.

Como organismo de certificación acreditado, BSI Assurance no puede ofrecer certificación a clientes que también hayan recibido consultoría de otra parte del Grupo BSI para el mismo sistema de gestión. Del mismo modo, no ofrecemos consultoría a clientes que también buscan la certificación para el mismo sistema de gestión.

La British Standards Institution (BSI, una empresa incorporada por Royal Charter), realiza la actividad de National Standards Body (NSB) en el Reino Unido. BSI, junto con sus empresas del grupo, también ofrece una amplia cartera de soluciones comerciales distintas de la actividad de NSB que ayudan a las empresas de todo el mundo a mejorar los resultados a través de las mejores prácticas basadas en estándares (como certificación, herramienta de autoevaluación, software, pruebas de productos, productos de información y capacitación).