[ISO/IEC 27000](https://www.iso.org/standard/73906.html" \t "_blank)

Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012, una tercera edición de 14 de Enero de 2014 y una cuarta en Febrero de 2016. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español aunque hay que prestar atención a la versión descargada. [El original en inglés y su traducción al francés en su versión de 2018 puede descargarse gratuitamente](https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip).

[ISO/IEC 27001](https://www.iso.org/obp/ui/#!iso:std:54534:en)

Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013 segunda edición). Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.Desde el 12 de Noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014 y puede adquirirse online en [UNE](https://www.une.org/). En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015) y en Diciembre de 2015 una segunda modificación (ISO/IEC 27001:2013/Cor.2:2015) esta última matizando especificaciones en la declaración de aplicabilidad. Otros países donde también está publicada en español son, por ejemplo, [Colombia (NTC-ISO-IEC 27001)](https://tienda.icontec.org/), [Chile (NCh-ISO27001)](http://www.inn.cl/) o [Uruguay (UNIT-ISO/IEC 27001)](http://www.unit.org.uy/normalizacion/sistema/27000/). El original en inglés y la traducción al francés pueden adquirirse en iso.org.

Existe una reciente edición puesta a libre disposición pública por "Industria Conectada 4.0" de la versión [UNE-ISO/IEC 27001:2017](https://www.industriaconectada40.gob.es/difusion/Paginas/enlaces-interes.aspx) que es una edición consolidada de la traducción del 2013 y que incorpora las correcciones de 2015.

[ISO/IEC 27002](https://www.iso.org/obp/ui/#!iso:std:54533:en)

Publicada desde el 1 de Julio de 2007, renombra la norma ya publicada ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como [UNE-ISO/IEC 27002:2009](https://www.une.org/) desde el 9 de Diciembre de 2009 también está publicada en español por, entre otros, [Colombia (NTC-ISO-IEC 27002)](http://www.icontec.org/), [Venezuela (Fondonorma ISO/IEC 27002)](http://www.fondonorma.org.ve/), [Argentina (IRAM-ISO-IEC 27002)](https://www.iram.org.ar/), [Chile (NCh-ISO27002)](http://www.inn.cl/) o [Uruguay (UNIT-ISO/IEC 27002)](http://www.unit.org.uy/).La [última edición de 2013](https://www.une.org/) este estándar fue actualizada reestructurando el contenido en un total de 14 Dominios, 35 Objetivos de Control y 114 Controles.

Puede descargarse una [lista actualizada para la versión 2013](https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf) de todos los controles de esta norma en una práctica única página como mejor referencia.

Existe una reciente edición puesta a libre disposición pública por "Industria Conectada 4.0" de la versión [UNE-ISO/IEC 27002:2017](https://www.industriaconectada40.gob.es/difusion/Paginas/enlaces-interes.aspx) que es una edición consolidada de la traducción del 2013 y que incorpora las correcciones de 2015.

[ISO/IEC 27003](https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en)

Publicada el 01 de Febrero de 2010 y actualizada el 12 de Abril de 2017. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

[ISO/IEC 27004](https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-2:v1:en)

Publicada el 15 de Diciembre de 2009 y revisada en Diciembre de 2016. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

[ISO/IEC 27005](https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en)

Publicada la tercera edición en Julio de 2018 con actualizaciones respecto a requisitos de norma ISO/IEC 27001:2013. La segunda edición es de 1 de Junio de 2011 y la primera edición del 15 de Junio de 2008. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.

[ISO/IEC 27006](https://www.iso.org/obp/ui/#iso:std:iso-iec:27006:ed-3:v1:en)

Publicada en segunda edición el 1 de Diciembre de 2011 (primera edición del 1 de Marzo de 2007) y revisada el 30 de Septiembre de 2015 con una [adenda del 27 de Marzo de 2020](https://www.iso.org/standard/77722.html). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

[ISO/IEC 27007](https://www.iso.org/standard/77802.html)

Publicada el 14 de Noviembre de 2011, revisada el 09 de Octubre de 2017 y con una última versión de 21 de Enero de 2020. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

[ISO/IEC TS 27008](https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27008:ed-1:v1:en)

Publicada el 15 de Octubre de 2011 como ISO/IEC TR 27008 (Technical Report) es sustituido con una primera edición como "TS" (Technical Specification) desde el 14 de Enero de 2019. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

[ISO/IEC 27009](https://www.iso.org/obp/ui/#iso:std:iso-iec:27009:ed-1:v1:en)

Publicada inicialmente el 15 de Junio de 2016, revisada el 21 de Abril de 2020. No certificable. define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del Anexo A.

[ISO/IEC 27010](https://www.iso.org/obp/ui/#iso:std:iso-iec:27010:ed-2:v1:en)

Publicada el 20 de Octubre de 2012 y revisada el 10 de Noviembre de 2015. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones. Actualmente en proceso de revisión para su actualización.

[ISO/IEC 27011](https://www.iso.org/obp/ui/#iso:std:iso-iec:27011:ed-2:v1:en)

Publicada el 15 de Diciembre de 2008 y revisada en Diciembre de 2016. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-T X.1051.

[ISO/IEC 27013](https://www.iso.org/obp/ui/#iso:std:iso-iec:27013:ed-2:v1:en)

Publicada el 15 de Octubre de 2012 y actualizada el 24 de Noviembre de 2015. Es una guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

[ISO/IEC 27014](https://webstore.iec.ch/preview/info_isoiec27014%7Bed2.0%7Den.pdf)

Publicada el 23 de Abril de 2013 y actualizada en segunda edición en Diciembre 2020 consiste en una guía de gobierno corporativo de la seguridad de la información, la ciberseguridad y privacidad.

[ISO/IEC TR 27015](https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27015:ed-1:v1:en)

Publicada el 23 de Noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005. Desde 24 de Julio, de 2017 se anuncia que no será actualizada en relación a las novedades de la norma ISO/IEC 27002:2013 aunque sigue disponible para su adquisición por parte de los interesados.

[ISO/IEC TR 27016](https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27016:ed-1:v1:en)

Publicada el 20 de Febrero de 2014. Es una guía de valoración de los aspectos financieros de la seguridad de la información.

[ISO/IEC 27017](https://www.iso.org/obp/ui/#iso:std:iso-iec:27017:ed-1:v1:en)

Publicada el 15 de Diciembre de 2015. Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube. Es posible la certificación en esta norma en conjunto con la implantación de un SGSI en base a los requisitos indicados en ISO/IEC 27001.

[ISO/IEC 27018](https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-2:v1:en)

Publicada el 29 de Julio de 2014 y revisada el 15 de Enero de 2019, es un código de buenas prácticas en controles de protección de datos para aquellos proveedores de servicios de computación en cloud computing. Es posible la certificación en esta norma en conjunto con la implantación de un SGSI en base a los requisitos indicados en ISO/IEC 27001.

[ISO/IEC TR 27019](https://www.iso.org/obp/ui/#iso:std:iso-iec:27019:ed-1:v2:en)

Publicada el 17 de Julio de 2013. Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía. Actualizada como ISO/IEC 27019:2017 en Octubre de 2017 para su alineación con ISO/IEC 27002:2013, además de la aplicación a los sistemas de control de procesos (p.ej. PLCs) utilizados por la industria de la energía para controlar y monitorear la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo y calor y para el control de los procesos de soporte asociados, también incluye un requisito para adaptar los procesos de evaluación y tratamiento de riesgos descritos en ISO/IEC 27001:2013 a la orientación específica del sector de servicios de energía.

[ISO/IEC 27021](https://www.iso.org/obp/ui/#iso:std:iso-iec:27021:ed-1:v1:en)

Publicada el 31 de Octubre de 2017 especifica los requisitos de competencia para aquellos profesionales que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del sistema de gestión de seguridad de la información (SGSI) que cumplan con ISO/IEC 27001.

[ISO/IEC 27022](https://www.iso.org/standard/61004.html)

Publicada el 11 de Marzo de 2021, define un modelo de referencia de procesos para el dominio de la gestión de seguridad de la información con el objetivo de guiar a los usuarios de ISO/IEC 27001 a incorporar el enfoque de proceso tal y como se describe en ISO/IEC 27000:2018 (4.3 - SGSI) y de modo alineado con otras normas de la familia ISO/IEC 27000 desde la perspectiva de la operación de los procesos SGSI. Este documento complementa la perspectiva orientada a los requisitos de ISO/IEC 27003 con un punto de vista operativo y orientado a procesos.

[ISO/IEC TR 27023](https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27023:ed-1:v1:en)

Publicada el 02 de Julio de 2015. No certificable. Es una guía de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005.

[ISO/IEC 27030](https://www.iso.org/standard/44373.html)

En fase de desarrollo cubrirá la seguridad y privacidad en principios, riesgos y controles aplicables al Internet de las Cosas (IoT - Internet of Things).

[ISO/IEC 27031](https://www.iso.org/obp/ui/#!iso:std:44374:en)

Publicada el 01 de Marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.

[ISO/IEC 27032](https://www.iso.org/obp/ui/#!iso:std:44375:en)

Publicada el 16 de Julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

[ISO/IEC 27033](https://www.iso.org/obp/ui/#iso:std:iso-iec:27033:-1:ed-2:v1:en)

Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 6 partes: [27033-1](https://www.iso.org/obp/ui/#iso:std:iso-iec:27033:-1:ed-2:v1:en), conceptos generales (Publicada el 15 de Diciembre de 2009 y revisada el 10 de Octubre de 2015); [27033-2](https://www.iso.org/obp/ui/#!iso:std:51581:en), directrices de diseño e implementación de seguridad en redes (Publicada el 27 de Julio de 2012); [27033-3](https://www.iso.org/obp/ui/#!iso:std:51582:en), escenarios de referencia de redes (Publicada el 3 de Diciembre de 2010); [27033-4](https://www.iso.org/obp/ui/#!iso:std:51583:en), aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (Publicada el 21 de Febrero de 2014); [27033-5](https://www.iso.org/obp/ui/#!iso:std:51584:en), aseguramiento de comunicaciones mediante VPNs (Publicada el 29 de Julio de 2013); [27033-6](https://www.iso.org/obp/ui/#!iso:std:51585:en), securización de redes IP wireless (Publicada en Junio de 2016).

[ISO/IEC 27034](https://www.iso.org/obp/ui/#!iso:std:44378:en)

Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 7 partes: [27034-1](https://www.iso.org/obp/ui/#!iso:std:44378:en), conceptos generales (Publicada el 21 de Noviembre de 2011); [27034-2](https://www.iso.org/obp/ui/#iso:std:iso-iec:27034:-2:ed-1:v1:en), marco normativo de la organización (Publicada el 15 de Agosto de 2015); [27034-3](https://www.iso.org/obp/ui/#iso:std:iso-iec:27034:-3:ed-1:v1:en), proceso de gestión de seguridad en aplicaciones (publicada en Mayo 2018); 27034-4, validación de la seguridad en aplicaciones (en fase de desarrollo); [27034-5](https://www.iso.org/obp/ui/#iso:std:iso-iec:27034:-5:ed-1:v1:en), estructura de datos y protocolos y controles de seguridad de aplicaciones (Publicada el 09 de Octubre de 2017); [27034-6](https://www.iso.org/obp/ui/#!iso:std:60804:en), guía de seguridad para aplicaciones de uso específico (Publicada en Octubre de 2016); [27034-7](https://www.iso.org/obp/ui/#iso:std:iso-iec:27034:-7:ed-1:v1:en), marco predictivo de en la seguridad (publicada en Mayo 2018).

[ISO/IEC 27035](https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:ed-1:v1:en)

Publicada el 17 de Agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información. Consta de 3 partes: [27035-1](https://www.iso.org/obp/ui/#!iso:std:60803:en), Principios en la gestión de incidentes (Publicada en Noviembre de 2016); [27035-2](https://www.iso.org/obp/ui/#!iso:std:62071:en), guías para la elaboración de un plan de respuesta a incidentes (Publicada en Noviembre de 2016); [27035-3](https://webstore.iec.ch/publication/67659?utm_source=Webstore+Just+Published&utm_campaign=d3c9e81cfe-JUST+PUBLISHED+by+the+IEC+-+Edition++2020-09&utm_medium=email&utm_term=0_61d266ee9e-d3c9e81cfe-51605729), guía de operaciones en la respuesta a incidentes (Publicada en Septiembre de 2020).

[ISO/IEC 27036](https://www.iso.org/obp/ui/#iso:std:iso-iec:27036:-1:ed-2:v1:en)

Guía en cuatro partes de seguridad en las relaciones con proveedores: [27036-1](https://www.iso.org/obp/ui/#iso:std:iso-iec:27036:-1:ed-2:v1:en), visión general y conceptos (Publicada inicialmente el 24 de Marzo de 2014 y revisada el 09 de Septiembre del 2021); [27036-2](https://www.iso.org/obp/ui/#!iso:std:59680:en), requisitos comunes (Publicada el 27 de Febrero de 2014); [27036-3](https://www.iso.org/obp/ui/#!iso:std:59688:en), seguridad en la cadena de suministro TIC (Publicada el 08 de Noviembre de 2013); [27036-4](https://www.iso.org/obp/ui/#!iso:std:59689:en), guía de seguridad para entornos de servicios Cloud (Publicada en Octubre de 2016).

[ISO/IEC 27037](https://www.iso.org/obp/ui/#!iso:std:44381:en)

Publicada el 15 de Octubre de 2012. Es una guía que propociona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositvos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

[ISO/IEC 27038](https://www.iso.org/obp/ui/#iso:std:iso-iec:27038:ed-1:v1:en)

Publicada el 13 de Marzo de 2014. Es una guía de especificación para seguridad en la redacción digital.

[ISO/IEC 27039](https://www.iso.org/obp/ui/#!iso:std:56889:en)

Publicada el 11 de Febrero de 2015. Es una guía para la selección, despliege y operativa de sistemas de detección y prevención de intrusión (IDS/IPS). Existe una [corrección al contenido inicial](https://www.iso.org/obp/ui/#!iso:std:51585:en) de 28 de Abril de 2016.

40

[ISO/IEC 27040](https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-1:v1:en)

Publicada el 05 de Enero de 2015, es una guía para la seguridad en medios de almacenamiento.

[ISO/IEC 27041](https://www.iso.org/obp/ui/#iso:std:iso-iec:27041:ed-1:v1:en)

Publicada el 19 de Junio de 2015, es una guía para la garantizar la la idoneidad y adecuación de los métodos de investigación.

[ISO/IEC 27042](https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en)

Publicada el 19 de Junio de 2015. Es una guía con directrices para el análisis e interpretación de las evidencias digitales.

[ISO/IEC 27043](https://www.iso.org/obp/ui/#iso:std:iso-iec:27043:ed-1:v1:en)

Publicada el 04 de Marzo de 2015. Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

[ISO/IEC 27045](https://www.iso.org/standard/63929.html)

En fase de desarrollo, el proyecto se inició en 2018 y cubrirá procesos de seguridad y privacidad en sistemas de big data.

[ISO/IEC 27050](https://www.iso.org/obp/ui/#!iso:std:63081:en)

Norma desarrollada en tres partes sobre la información almacenada en dispositivos electrónicos en relación a su identificación, preservación, recolección, procesamiento, revisión, análisis y producción: [27050-1](https://www.iso.org/obp/ui/#!iso:std:63081:en), conceptos generales (Publicada en Noviembre de 2016 y con [descarga gratuita](https://standards.iso.org/ittf/PubliclyAvailableStandards/c063081_ISO_IEC_27050-1_2016.zip)); [27050-2](https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-2:ed-1:v1:en), Guía para el gobierno y gestión (publicada en Octubre de 2018); [27050-3](https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-3:ed-1:v1:en), código de buenas prácticas (publicada en Octubre de 2017 y en fase avanzada de revisión). Existe la posible extensión a una cuarta parte con orientaciones sobre la tecnología eDiscovery, es decir, las herramientas y sistemas forenses que respaldan la recopilación, el almacenamiento, la recopilación, la búsqueda, el análisis y la producción de ESI (Electronically Stored Information), además de los procesos relacionados.

[ISO/IEC 27070](https://www.iso.org/standard/56571.html)

En fase de desarrollo, establecerá requisitos de seguridad para establecer raíces virtualizadas de confianza en la nube, es decir, para la provisión de entornos informáticos confiables en la nube, donde las máquinas virtuales se crean dinámicamente para proporcionar servicios en la nube.

[ISO/IEC 27071](https://www.iso.org/standard/56572.html)

En fase de desarrollo, recomendará controles de seguridad para establecer conexiones confiables entre dispositivos y servicios en la nube.

[ISO/IEC 27099](https://www.iso.org/standard/56590.html)

En fase de desarrollo, identificará los requisitos de gestión de seguridad de la información para los proveedores de servicios de confianza de PKI.

[ISO/IEC 27100](https://www.iso.org/standard/72434.html)

Publicada el 22 de Diciembre de 2020. Este documento proporciona una descripción de la ciberseguridad y los conceptos relevantes, incluida la forma en que se relaciona y se diferencia de la seguridad de la información. Adicionalmente, establece el contexto de la ciberseguridad cubriendo parte de los términos y definiciones aplicables a la ciberseguridad sin excluir definiciones procedentes de otros estándares o nuevos términos de uso relacionados.

[ISO/IEC 27102](https://www.iso.org/obp/ui/#iso:std:iso-iec:27102:ed-1:v1:en)

Publicada el 13 de Agosto de 2019. Este documento proporciona pautas en el momento de considerar la contratar un ciberseguro como una opción de tratamiento de riesgos para gestionar el impacto de un ciberincidente dentro del marco de gestión de riesgos de seguridad de la información de la organización.

[ISO/IEC TR 27103](https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27103:ed-1:v1:en)

Publicada el 22 de Febrero de 2018. Norma desarrollada Primera edición para proporcionar orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.

[ISO/IEC TS 27110](https://www.iso.org/standard/72435.html)

Publicada el 16 de Febrero de 2021. La audiencia de este documento son los creadores de marcos de ciberseguridad con el objetivo de este documento es garantizar que se utilice un conjunto mínimo de conceptos para definir los marcos de ciberseguridad ayudando a aliviar la carga de los creadores de marcos de ciberseguridad y de los usuarios de estos marcos. Los principios de este documento son la flexibilidad (para permitir la existencia de múltiples tipos de marcos de ciberseguridad), la compatibilidad (para permitir la alineación de múltiples marcos de ciberseguridad) y la interoperabilidad (para permitir que los usos múltiples de un marco de ciberseguridad sean válidos).

[ISO/IEC TR 27550](https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27550:ed-1:v1:en)

Publicada por primera vez en Septiembre de 2019, cubre aspectos de privacidad en ingeniería de sistemas TIC (Tecnologías de la Información y Comunicaciones).

[ISO/IEC 27551](https://www.iso.org/standard/72018.html)

En fase de desarrollo, especificará los requisitos para la autenticación de entidad no enlazable basada en atributos.

[ISO/IEC 27553](https://www.iso.org/standard/71671.html)

En fase de desarrollo, especificará los requisitos para la autenticación biométrica en dispositivos móviles.

[ISO/IEC AWI 27554](https://www.iso.org/standard/71672.html)

En fase de desarrollo, asesorará sobre el uso de ISO 31000 para evaluar el riesgo relacionado con la gestión de identidad.

[ISO/IEC 27555](https://www.iso.org/obp/ui/#iso:std:iso-iec:27555:ed-1:v1:en)

Publicada inicialmente el 08 de Octubre del 2021 este documento proporciona un marco para desarrollar y establecer políticas y procedimientos para la eliminación de PII que pueden ser implementados por una organización en sus procesos funcionales y aplicaciones TIC. Este marco permite la eliminación coherente de PII en toda una organización.

[ISO/IEC AWI 27556](https://www.iso.org/standard/71674.html)

En fase de desarrollo, generará un marco centrado en el usuario para manejar la PII en función de las preferencias de privacidad.

[ISO/IEC TS 27570](https://www.iso.org/standard/71678.html)

Publicada por primera vez el 28 de Enero de 2021 este documento ofrece orientación sobre la privacidad de los ciudadanos como punto de atención principal en el desarrollo de ecosistemas para las denominadas ciudades inteligentes (smart cities). Este documento es aplicable a todo tipo y tamaño de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro que brindan servicios en entornos de ciudades inteligentes.

[ISO/IEC 27701](https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en)

Publicada por primera vez en Agosto de 2019 este documento especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de información de privacidad (PIMS) a modo de extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad dentro del contexto de la organización. Especifica los requisitos relacionados con PIMS y proporciona orientación para los controladores y procesadores de PII que tienen la responsabilidad y la responsabilidad del procesamiento de PII.

[ISO 27799](https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en)

Publicada el 12 de Junio de 2008 dispone de una segunda revisión actualizada desde Julio 2016. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.