27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Lista de documentación obligatoria requerida por ISO 27001 (Revisión 2013)

Advisera
Making certification simple.

Tabla de Contenidos

1. ¿Qué documentos y registros son necesarios?

La siguiente lista detalla la cantidad mínima de documentos y registros requeridos por la Revisión 2013 de la norma ISO/IEC 27001:

Documentos*	Capítulo de ISO 27001:2013
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2, 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d)
Plan de tratamiento del riesgo	6.1.3 e), 6.2, 8.3
Informe sobre evaluación y tratamiento de riesgos	8.2, 8.3
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para gestión de TI	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de la continuidad del negocio	A.17.1.2
Requisitos legales, normativos y contractuales	A.18.1.1

Registros*	Capítulo de ISO 27001:2013
Registros de capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de supervisión y medición	9.1
Programa de auditoría interna	9.2
Resultados de las auditorías internas	9.2
Resultados de la revisión por parte de la dirección	9.3
Resultados de acciones correctivas	10.1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	A.12.4.1, A.12.4.3

*Se pueden excluir los controles del Anexo A si una organización determina que no existen riesgos ni otros requisitos que podrían demandar la implementación de un control.

Esta no es, de ninguna forma, una lista definitiva de documentos y registros que se pueden utilizar durante la implementación de ISO 27001; la norma permite que se agregue cualquier otro documento que pueda mejorar el nivel de seguridad de la información.

2. Documentos no obligatorios de uso frecuente

Los siguientes son otros documentos que se utilizan habitualmente:

Documentos	Capítulo de ISO 27001:2013
Procedimiento para control de documentos	7.5
Controles para gestión de registros	7.5
Procedimiento para auditoría interna	9.2
Procedimiento para medidas correctivas	10.1
Política Trae tu propio dispositivo (BYOD)	A.6.2.1
Política sobre dispositivos móviles y tele-trabajo	A.6.2.1
Política de clasificación de la información	A.8.2.1, A.8.2.2, A.8.2.3
Política de claves	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
Política de eliminación y destrucción	A.8.3.2, A.11.2.7
Procedimiento para trabajo en áreas seguras	A.11.1.5
Política de pantalla y escritorio limpio	A.11.2.9
Política de gestión de cambio	A.12.1.2, A.14.2.4
Política de creación de copias de seguridad	A.12.3.1
Política de transferencia de la información	A.13.2.1, A.13.2.2, A.13.2.3
Análisis del impacto en el negocio	A.17.1.1
Plan de prueba y verificación	A.17.1.3
Plan de mantenimiento y revisión	A.17.1.3

3. Cómo estructurar los documentos y registros más comunes

Alcance del SGSI

Este documento es, habitualmente, bastante corto y se redacta al inicio de la implementación de ISO 27001. En general, se trata de un documento independiente, aunque puede ser unificado con una política de seguridad de la información.

Leer más en: Problemas para definir el alcance de la norma ISO 27001.

Políticas y objetivos de seguridad de la información

La política de seguridad de la información generalmente es un documento breve y de alto nivel que detalla el principal objetivo del SGSI. Los objetivos para el SGSI, en general, se presentan como un documento independiente, pero también pueden ser unificados en la política de seguridad de la información. Contrariamente a la revisión 2005 de ISO 27001, ya no se necesitan ambas políticas (Política del SGSI y Política de seguridad de la información); solo hace falta una política de seguridad de la información.

Leer más en: Política de Seguridad de la Información: ¿qué nivel de detalle debería tener?

Metodología e informes de evaluación y tratamiento de riesgos

La metodología de evaluación y tratamiento del riesgo es, habitualmente, un documento de 4 a 5 páginas y debe ser redactado antes que se realice la evaluación y el tratamiento de riesgos. El informe de evaluación y tratamiento de riesgos debe ser redactado una vez que se realizó la evaluación y el tratamiento de riesgos, y allí se resumen todos los resultados.

Leer más en: Evaluación y Tratamiento del Riesgo en ISO 27001 – 6 pasos básicos.

Declaración de aplicabilidad

La Declaración de aplicabilidad (o DdA) se redacta en base a los resultados del tratamiento del riesgo; es un documento clave dentro del SGSI porque describe no sólo qué controles del Anexo A son aplicables, sino también cómo se implementarán y su estado actual. También debería considerar a la Declaración de aplicabilidad como un documento que describe el perfil de seguridad de su empresa.

Leer más en: La importancia de la Declaración de aplicabilidad para la norma ISO 27001.

Plan de tratamiento del riesgo

Este es, básicamente, un plan de acción sobre cómo implementar los diversos controles definidos por la DdA. Este documento se desarrolla en función de la Declaración de aplicabilidad y se utiliza y actualiza activamente a lo largo de toda la implementación del SGSI. A veces se puede fusionar con el Plan del proyecto.

Leer más en: Risk Treatment Plan and risk treatment process – What's the difference?

Funciones y responsabilidades de seguridad

El mejor método es describir estas funciones y responsabilidades en todas las políticas y procedimientos de la forma más precisa posible. Evite expresiones como "debería hacerlo"; en cambio, utilice algo como "el Jefe de seguridad realizará xyz todos los lunes a las zxy horas". Algunas empresas prefieren detallar las funciones y responsabilidades de seguridad en sus descripciones del trabajo; sin embargo, esto puede generar mucho papelerío.

Las funciones y responsabilidades de seguridad para terceros se definen a través de contratos.

Leer más en: What is the job of Chief Information Security Officer (CISO) in ISO 27001?

Inventario de activos

Si no contaba con un inventario de este tipo antes del proyecto ISO 27001, la mejor forma de hacerlo es directamente a partir del resultado de la evaluación de riesgos ya que allí, de todos modos, se tienen que identificar todos los activos y sus propietarios; entonces, simplemente puede copiar el resultado desde ese instrumento.

Leer más en: How to handle Asset register (Asset inventory) according to ISO 27001.

Uso aceptable de los activos

Habitualmente, este documento se confecciona bajo la forma de una política y puede cubrir un amplio rango de temas porque la norma no define muy bien este control. Probablemente, la mejor forma de encararlo es la siguiente: (1) déjelo para el final de la implementación de su SGSI y (2) todas las áreas y controles que no haya cubierto con otros documentos y que involucran a todos los empleados, inclúyalos en esta política.

Política de control de acceso

En este documento usted puede cubrir sólo la parte comercial de la aprobación de acceso a determinada información y sistemas, o también puede incluir el aspecto técnico del control de acceso. Además, puede optar por definir reglas para acceso lógico únicamente o también para acceso físico. Debería redactar este documento solamente después de finalizado su proceso de evaluación y tratamiento de riesgos.

Procedimientos operativos para gestión de TI

Puede crear este procedimiento como un único documento o como una serie de políticas y procedimientos; si se trata de una empresa pequeña, debería tener menor cantidad de documentos. Normalmente, aquí puede abarcar todas las áreas de las secciones A.12 y A.13: gestión de cambios, servicios de terceros, copias de seguridad, seguridad de red, códigos maliciosos, eliminación y destrucción, transferencia de información, supervisión del sistema, etc. Este documento se debería redactar solamente una vez que finalice su proceso de evaluación y tratamiento de riesgos.

Leer más sobre gestión de TI aquí: ITIL & ISO 20000 Blog.

Principios de ingeniería para sistema seguro

Este es un nuevo control en ISO 27001:2013 y requiere que se documenten los principios de ingeniería de seguridad bajo la forma de un procedimiento o norma y que se defina cómo incorporar técnicas de seguridad en todas las capas de arquitectura: negocio, datos, aplicaciones y tecnología. Estos principios pueden incluir validación de datos de entrada, depuración, técnicas para autenticación, controles de sesión segura, etc.

Política de seguridad para proveedores

Este también es un control nuevo en ISO 27001:2013, y una política de este tipo puede abarcar un amplio rango de controles: cómo se realiza la selección de potenciales contratistas, cómo se ejecuta la evaluación de riesgos de un proveedor, qué cláusulas incluir en el contrato, cómo supervisar el cumplimiento de cláusulas contractuales de seguridad, cómo modificar el contrato, cómo cerrar el acceso una vez cancelado el contrato, etc.

Leer más en: 6-step process for handling supplier security according to ISO 27001.

Procedimiento para gestión de incidentes

Este es un procedimiento importante que define cómo se informan, clasifican y manejan las debilidades, eventos e incidentes de seguridad. Este procedimiento también define cómo aprender de los incidentes de seguridad de la información para que se puedan evitar en el futuro. Un procedimiento de esta clase también puede invocar al plan de continuidad del negocio si un incidente ha ocasionado una interrupción prolongada.

Procedimientos de la continuidad del negocio

Generalmente se trata de planes de continuidad del negocio, planes de respuesta ante incidentes, planes de recuperación para el sector comercial de la organización y planes de recuperación ante desastres (planes de recuperación para infraestructura de TI). Estos procedimientos se describen con mayor detalle en la norma ISO 22301, la principal norma internacional para continuidad del negocio.

Para conocer más, haga clic aquí: Business continuity plan: How to structure it according to ISO 22301.

Requisitos legales, normativos y contractuales

Este listado debe confeccionarse en la etapa más temprana posible del proyecto porque muchos documentos tendrán que ser desarrollados de acuerdo a estos datos. Este listado debe incluir no sólo las responsabilidades para el cumplimiento de determinados requerimientos, sino también los plazos.

Registros de capacitación, habilidades, experiencia y calificaciones

Es el departamento de recursos humanos el que generalmente se encarga de llevar estos registros. Si usted no tiene un sector de este tipo, cualquier persona que habitualmente se encargue de los registros

de los empleados debería ser quien realice este trabajo. Básicamente, sería suficiente una carpeta en la que se encuentren todos los documentos.

Leer más en: How to perform training & awareness for ISO 27001 and ISO 22301.

Resultados de supervisión y medición

La forma más sencilla de describir cómo se miden los controles es a través de políticas y procedimientos que definan a cada control. En general, esta descripción puede ser realizada al final de cada documento, y cada descripción tiene que definir los tipos de ICD (indicadores clave de desempeño) que es necesario medir para cada control o grupo de controles.

Una vez que se estableció este método de control, usted debe realizar la medición en función de dicho método. Es importante reportar los resultados de esta medición en forma regular a las personas que están a cargo su evaluación.

Leer más aquí: ISO 27001 control objectives – Why are they important?

Programa de auditoría interna

El programa de auditoría interna no es más que un plan anual para realizar las auditorías; para las empresas más pequeñas, puede tratarse solamente de una auditoría, mientras que para las organizaciones más grandes puede ser una serie de, por ejemplo, 20 auditorías internas. Este programa debe definir quién realizará las auditorías, los métodos que se utilizarán, los criterios que se aplicarán, etc.

Leer más en: How to make an Internal Audit checklist for ISO 27001 / ISO 22301.

Resultados de las auditorías internas

Un auditor interno debe generar un informe de auditoría, que incluye los resultados de la auditoría (observaciones y medidas correctivas). Este informe debe ser confeccionado dentro de un par de días luego de realizada la auditoría interna. En algunos casos, el auditor interno tendrá que verificar si todas las medidas correctivas se aplicaron según lo esperado.

Resultados de la revisión por parte de la dirección

Estos registros se presentan, normalmente, bajo la forma de actas de reunión y deben incluir todo el material tratado durante la reunión de la dirección, como también todas las decisiones que se tomaron. Estas actas pueden ser en papel o en formato digital.

Leer más en: Why is management review important for ISO 27001 and ISO 22301?

Resultados de acciones correctivas

Generalmente, estos son incluidos en los formularios para medidas correctivas (FMC). Sin embargo, es mucho mejor agregar estos registros en alguna aplicación que ya esté en uso en la organización; por ejemplo, la Mesa de ayuda, porque las medidas correctivas no son más que listas de actividades a realizar con responsabilidades, tareas y plazos bien definidos.

Leer más en: Practical use of corrective actions for ISO 27001 and ISO 22301.

Registros sobre actividades de los usuarios, excepciones y eventos de seguridad

Habitualmente se llevan de dos formas: (1) en formato digital, generados en forma automática o semiautomática como registros de diversas TI y de otros sistemas, y (2) en papel, donde cada registro se hace manualmente.

Procedimiento para control de documentos

En general, este es un procedimiento independiente, de 2 o 3 páginas de extensión. Si usted ya implementó alguna otra norma como ISO 9001, ISO 14001, ISO 22301 o similar, puede utilizar el mismo procedimiento para todos estos sistemas de gestión. A veces es mejor redactar este procedimiento como el primer documento de un proyecto.

Leer más aquí: Gestión de documentación en las normas ISO 27001 y BS 25999-2.

Controles para gestión de registros

La forma más sencilla es redactar el control de registros en cada política o procedimiento (u otro documento) que requiera la generación de un registro. Estos controles, normalmente son incluidos

hacia el final de cada documento y se confeccionan bajo el formato de una tabla que detalla dónde se archiva el registro, quién tiene acceso, cómo se protege, por cuánto tiempo se archiva, etc.

Procedimiento para auditoría interna

Habitualmente este es un procedimiento independiente que puede tener entre 2 y 3 páginas y que tiene que ser redactado antes que comience la auditoría interna. En cuanto al procedimiento para control de documentos, un procedimiento para auditoría interna puede ser utilizado para cualquier sistema de gestión.

Leer más aquí: Dilemas con los auditores internos de las normas ISO 27001 y BS 25999-2.

Procedimiento para medidas correctivas

Este procedimiento no debería exceder las 2 o 3 páginas y puede ser confeccionado al final del proyecto de implementación, aunque es mejor hacerlo antes para que los empleados puedan familiarizarse con él.

4. Plantillas de documentación de muestra

Aquí usted puede descargar una muestra gratis del Paquete de documentos sobre ISO 27001 e ISO 22301: en esta muestra gratis podrá ver la Tabla de contenidos de cada una de las políticas y procedimientos mencionados, como también algunas partes de cada documento.

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORAR **ADVISERA**

EU GDPR Academy · 27001 Academy · 9001 Academy · 14001 Academy · 45001 Academy · 13485 Academy · 9100 Academy

16949 Academy · 17025 Academy · 20000 Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.