\*\* VERSIÓN DE MUESTRA GRATIS \*\*

Gracias por descargar la vista previa gratuita del Paquete de documentos de ISO 27001.

**Apéndice 3 – Lista de verificación de** **auditoría interna para ISO 27001 e ISO 22301**

# Lista de verificación de auditoría interna para ISO 27001

|  |  |  |  |
| --- | --- | --- | --- |
| **Capítulo** | **Requerimiento de la norma** | **…** | **…** |
| 4.2 | ¿La organización determinó las partes interesadas? |  |  |
| 4.2 | ¿Existe la lista de todos los requerimientos para las partes interesadas? |  |  |
| 4.3 | ¿Está documentado el alcance con límites e interfaces claramente definidos? |  |  |
| 5.1 | ¿Los objetivos generales del SGSI son compatibles con la dirección estratégica? |  |  |
| 5.1 | ¿La dirección asegura que el SGSI cumple sus objetivos? |  |  |
| 5.2 | ¿Existe la Política de seguridad de la información con objetivos o marco para establecer los objetivos? |  |  |
| 5.2 | ¿Se comunica la Política de seguridad de la información dentro de la organización? |  |  |
| 5.3 | ¿Las roles y responsabilidades para seguridad de la información están asignados y comunicados? |  |  |
| 6.1.2 | ¿Está documentado el proceso de evaluación de riesgos, incluidos los criterios de aceptabilidad de riesgos y de evaluación de riesgos? |  |  |
| 6.1.2, 8.2 | ¿Están definidos los riesgos, sus propietarios, probabilidad, consecuencias y nivel de riesgo? ¿Estos resultados están documentados? |  |  |
| 6.1.3 | ¿Está documentado el proceso de tratamiento del riesgo, incluidas las opciones para tratamiento de los riesgos? |  |  |
| 6.1.3, 8.3 | ¿Todos los riesgos no aceptables son tratados utilizando las opciones y controles del Anexo A? ¿Estos resultados están documentados? |  |  |
| 6.1.3 | ¿La Declaración de aplicabilidad está confeccionada con justificaciones y estados para cada control? |  |  |
| 6.1.3, 8.3 | ¿Existe el Plan de tratamiento de riesgos aprobado por los propietarios de los riesgos? |  |  |
| 6.2 | ¿El Plan de tratamiento de riesgos define quién es responsable de la implementación de qué control, con qué recursos, con qué plazos y cuál es el método de evaluación? |  |  |
| 7.1 | ¿Se proporcionan los recursos adecuados para todos los elementos del SGSI? |  |  |
| 7.2 | ¿Están definidas las competencias requeridas, las capacitaciones realizadas y se llevan registros de competencias? |  |  |
| 7.3 | ¿El personal es consciente de la Política de seguridad de la información, de su rol y de las consecuencias por el no cumplimiento de las normas? |  |  |
| 7.4 | ¿Existe el proceso para la comunicación relacionada con seguridad de la información, incluidas las responsabilidades y qué hay que comunicar? |  |  |
| 7.5 | ¿Existe el proceso para gestión de documentos y registros, incluidos quiénes revisan y aprueban documentos, dónde y cómo se publican, archivan y protegen? |  |  |
| 7.5 | ¿Se controlan los documentos de origen externo? |  |  |
| 8.1 | ¿Se identifican y controlan los procesos externalizados? |  |  |
| 9.1 | ¿Está definido qué debe ser medido, con qué método, quién es responsable, quién analizará y evaluará los resultados? |  |  |
| 9.1 | ¿Están documentados los resultados de la medición y son reportados a las personas responsables? |  |  |
| 9.2 | ¿Existe el programa de auditoria que define los tiempos, responsabilidades, informes, criterios y alcance de la auditoría? |  |  |
| 9.2 | ¿Las auditorías internas se realizan de acuerdo al programa de auditoría, los resultados son informados a través del Informe de auditoría interna y se elevan las acciones correctivas correspondientes? |  |  |
| 9.3 | ¿Se realiza periódicamente la revisión por parte de la dirección y sus resultados son documentados en actas de la reunión? |  |  |
| 9.3 | ¿La dirección tuvo decisión sobre todos los temas críticos importantes para el éxito del SGSI? |  |  |
| 10.1 | ¿La organización reacciona ante cada no-conformidad? |  |  |
| 10.1 | ¿La organización considera eliminar las causas de la no-conformidad y, cuando corresponde, toma acciones correctivas? |  |  |
| 10.1 | ¿Se registran todas las no-conformidades, junto con las acciones correctivas? |  |  |
| A.5.1 | ¿Todas las políticas de seguridad de la información necesarias son aprobadas por la dirección y luego publicadas? |  |  |
| A.5.1 | ¿Todas las políticas de seguridad de la información son revisadas y actualizadas? |  |  |
| A.5.2 | ¿Están claramente definidas todas las responsabilidades concernientes a la seguridad de la información a través de uno o varios documentos? |  |  |
| A.5.3 | ¿Están definidos los deberes y responsabilidades de forma tal que se evite un conflicto de intereses, particularmente con la información y los sistemas que involucran altos riesgos? |  |  |
| A.5.4 | ¿La dirección exige activamente que todos los empleados y contratistas cumplan con las reglas de seguridad de la información? |  |  |
| A.5.5 | ¿Está claramente definido quién debe ponerse en contacto con qué autoridades? |  |  |
| A.5.6 | ¿Está claramente definido quién debe ponerse en contacto con qué grupos de interés especiales o asociaciones profesionales? |  |  |
| A.5.7 | ¿Se recopilan y analizan las amenazas a la seguridad de la información para generar inteligencia sobre amenazas? |  |  |

...

\*\* FIN DE MUESTRA GRATIS \*\*

Si ha decidido que el Paquete de documentos de ISO 27001 es la mejor elección para su compañía, consulte la siguiente tabla para elegir el paquete de documentos con el nivel de soporte experto adecuado.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Paquete de documentos con apoyo de un experto** | **Paquete de documentos con ampliación de soporte** | **Paquete de documentos superior** |
|  | **US $897** | **US $1397** | **US $2397** |
| **45 plantillas de documentos que cumplen con ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Acceso a tutoriales en video (en inglés)** | **🗸** | **🗸** | **🗸** |
| **Plantillas de documentos actualizadas a la versión ISO 27001:2022** | **🗸** | **🗸** | **🗸** |
| **Herramienta de Análisis de Brecha en ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Soporte mediante correo electrónico** | 10 preguntas por mes | Ilimitado | Ilimitado |
| **Asistencia personalizada con un experto en ISO 27001** | 1 hora | 5 horas | 15 horas |
| **Revisión de expertos (documentos completos)** | 1 documento | 5 documentos | 15 documentos |
| **Formación en concienciación sobre seguridad (en inglés)** | **X** | 20 usuarios | 50 usuarios |
| **Revisión previa a la auditoría** | **X** | **🗸** | **🗸** |
|  | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718229&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-expert-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718230&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-extended-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718232&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-power-support&utm_content=lang-es) |
|  | (haga clic en el siguiente enlace presionando CTRL+clic) | | |