unir LA UNIVERSIDAD EN INTERNET

Ser auditor ISO 27001, ¿cómo obtener la certificación de auditor?

Conviértete en auditor de la norma ISO 27001 y certifica a las empresas que han implantado un Sistema de Gestión de la Seguridad de la Información de manera óptima

La familia ISO/IEC 27000 está constituida por una serie de normas de seguridad de la información. De todas las normas estándares de esta familia (ISO/IEC 27000, 27001, 27002, etc.), la ISO 27001, publicada en 2022, es la única certificable por una entidad acreditadora y, además, está reconocida internacionalmente. Si estás interesado en **ser auditor ISO 27001** y quieres prepararte para obtener la certificación, en este post te damos las pautas a seguir.

El principal objetivo de la **norma ISO/IEC 27001** es **implantar la seguridad de la información**, su confidencialidad y disponibilidad, orientada a los procesos y objetivos de negocio de las organizaciones en base a un análisis de riesgos de TIC.

Las organizaciones que implantan un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la ISO/IEC 27001 pueden optar por certificar dicho sistema. Para ello, deberán superar una **auditoría de certificación conducida por un auditor externo** a la organización y perteneciente a una entidad auditora acreditada.

Los conocimientos necesarios para llegar a ser un auditor de esta norma se pueden adquirir a través de programas formales que incluyen el **curso de formación y el examen de certificación**, y que son impartidos por las entidades acreditadas para la realización de estas auditorías.

Objetivos

Los objetivos de estos programas formativos son:

- Comprender los conceptos generales y fundamentales de la gestión de la seguridad de la información en las organizaciones.
- Adquirir el conocimiento de las normas ISO/IEC 27001 y 27002 (guía de implementación de los controles de seguridad del anexo A de la 27001).
- Distinguir los distintos componentes de un SGSI.
- Conocer las ventajas de implementar un Sistema de Gestión de Seguridad de la Información.
- Comprobar amenazas de seguridad y gestionar riesgos.
- Adquirir los conocimientos necesarios para la realización (planificación y ejecución) de auditorías de SGSI.
- Conocer y entender el proceso de certificación.
- Dirigir y gestionar (liderar) un equipo de auditoría de SGSI.

- Comprender las distintas técnicas de entrevista, la realización de los informes de auditoría y adquirir la capacidad necesaria para comprobar la competencia del Sistema de Gestión de Seguridad de la Información.

Algunos de los **principales itinerarios formativos o programas** para adquirir los conocimientos y competencias necesarias para ser auditor de SGSI de conformidad con la norma ISO/IEC 27001 son:

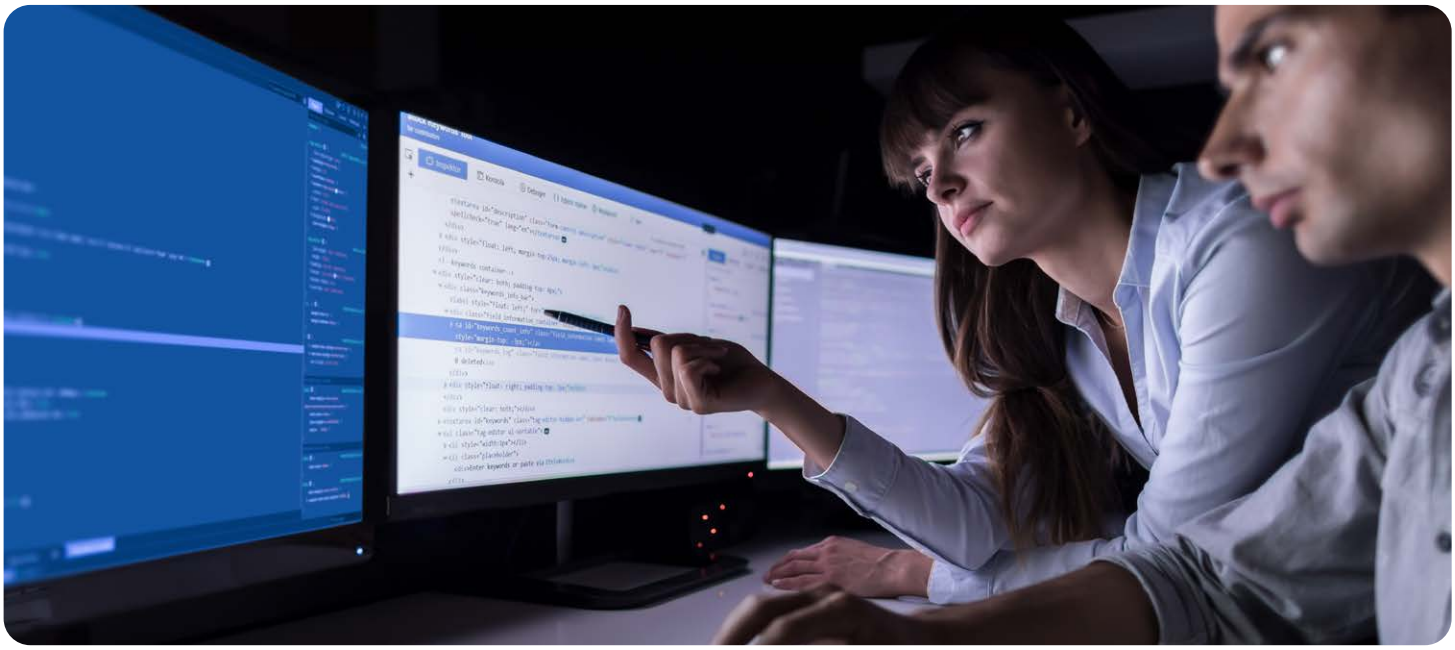
- Lead Auditor 27001 (Auditor líder o jefe) de AENOR.
- Auditor Jefe 27001 de BSI.

También existe la posibilidad de ser **auditor interno de ISO 27001 de una organización**, una opción que brinda el **Máster en Ciberseguridad** de UNIR (además de la de ser auditor externo). Con una formación 100% online, este postgrado oficial te formará en seguridad defensiva (sistemas operativos, desarrollo de software, comunicaciones, etc.), seguridad ofensiva (análisis de vulnerabilidades, test de penetración, análisis de malware, etc.), delitos informáticos, criptografía y mecanismos de seguridad, entre otras cuestiones.

¿Qué contenidos se ven en los cursos para ser auditor?

Los contenidos impartidos en los cursos de preparación del examen de certificación incluyen:

- Conceptos básicos de la seguridad de la información y su gestión.
- La norma ISO/IEC 27002, que es una guía explicativa de implantación para cada control de seguridad de la norma 27001.
- Procesos para la definición de un SGSI según la norma ISO/IEC 27001.
- Cómo se define el alcance de un Sistema de Gestión de Seguridad de la Información.
- Cómo implantar un SGSI según la norma 27001.
- Factores de éxito en la gestión de la seguridad de la información.
- Definición y tipos de auditoría de un SGSI.
- Metodología (procesos y fases) de auditoría de un SGSI.
- Proceso de certificación de un Sistema de Gestión de Seguridad de la Información de conformidad con la norma ISO/IEC 27001.



unir LA UNIVERSIDAD EN INTERNET

¿Qué es la certificación ISO 27001 y para qué sirve?

Cuestiones como el acceso controlado a la información, su clasificación o seguridad física quedan garantizadas gracias a los Sistema de Gestión de Seguridad de la Información y la norma ISO 27001.

La ISO 27001 es una norma internacional de Seguridad de la Información que pretende **asegurar la confidencialidad, integridad y disponibilidad de la información** de una organización y de los sistemas y aplicaciones que la tratan. Este estándar ha sido desarrollado por la Organización Internacional de Normalización (*ISO: "International Organization for Standardization") y por la Comisión Electrotécnica Internacional (IEC: "International Electrotechnical Commission").*

La norma define de manera genérica, independientemente de los factores ambientales de organización (entorno, contexto, activos de las TIC, información, cultura organizacional, etc.) —tanto internos como externos a la misma— y de los activos de los procesos de la organización (políticas, procedimientos, procesos, etc.), cómo se planifica, implanta, verifica y controla un Sistema de Gestión de Seguridad de la Información, a partir de la realización de un análisis de riesgos y de la planificación e implantación de la respuesta a los mismos para su mitigación. Es decir, **cualquier empresa u organización puede desplegar un SGSI** siguiendo este estándar.

Recomendaciones para administrar la información

Pero, ¿qué es un SGSI? Es un enfoque sistemático o conjunto de políticas y procedimientos para administrar la información de una empresa u organismo cumpliendo una serie de requisitos. Así, hay que garantizar su **confidencialidad** (sólo las personas autorizadas pueden acceder a esta), su **integridad** (no ha sido manipulada de manera no autorizada) y su **disponibilidad** (la información puede ser accedida por las personas autorizadas cuando lo necesitan), mediante una gestión de los riesgos que considera a las personas, procesos y

sistemas de TIC (Tecnología de la Información y las Comunicaciones) relacionados con la misma. La norma está alineada con la **ISO 27002**, que define una serie de buenas prácticas de gestión de la seguridad de la información para todos los interesados y responsables de un SGSI.

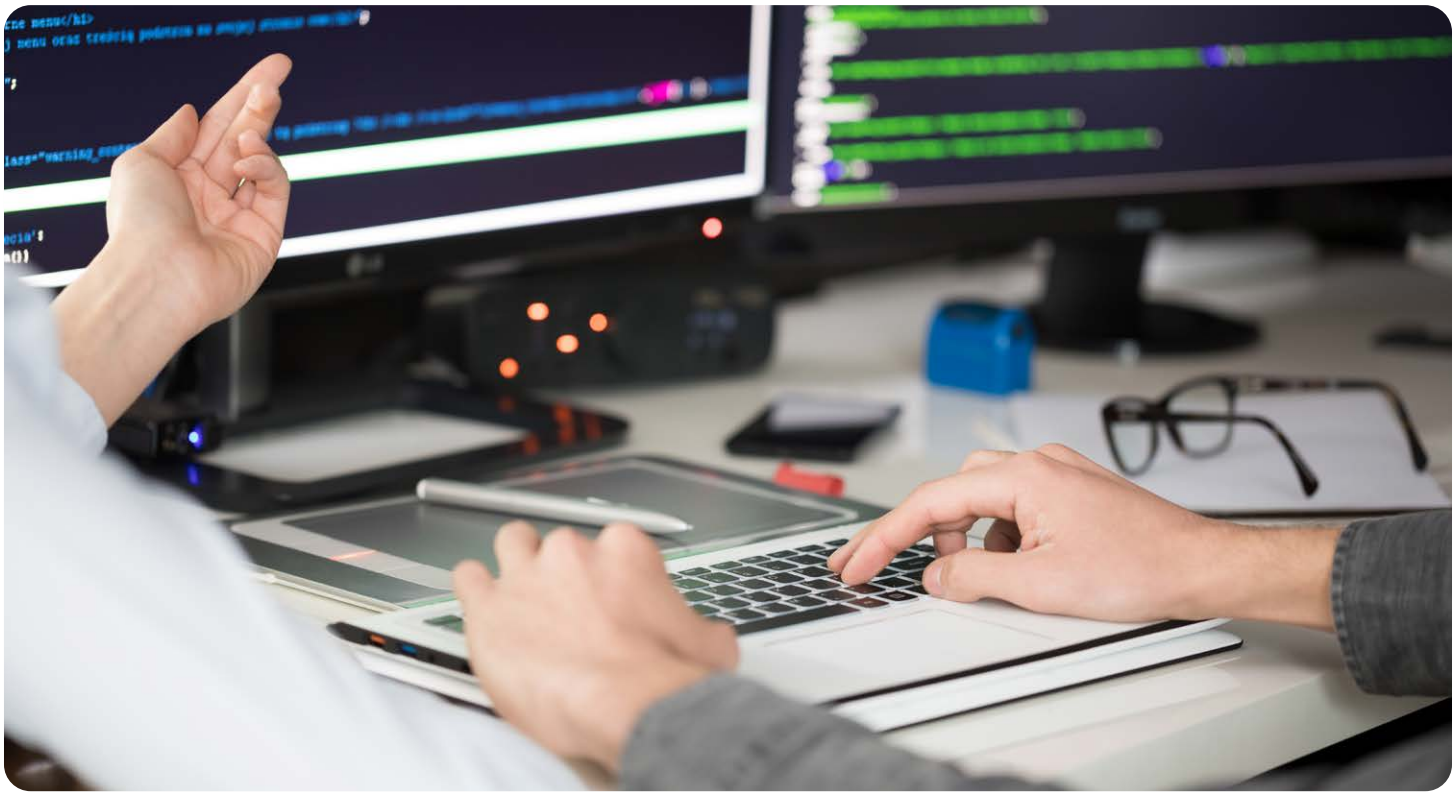
Gestión de la calidad PDCA

La ISO 27001 se basa en la teoría de gestión de la calidad PDCA (también conocida como ciclo de Deming), como se podrá observar en la estructura de esta.

- **Planificar ("Plan")**: etapa inicial de diseño del SGSI en la que se realiza la identificación inicial de los riesgos asociados con la Seguridad de la información. Esta cuestión se complementa con un análisis cualitativo y cuantitativo (si es necesario) de los riesgos identificados y la planificación de la respuesta y los controles necesarios para la mitigación de estos.
- **Hacer ("Do"):** implantación y operación del Sistema de Gestión de Seguridad de la Información definido y desarrollado.
- **Verificar ("Check"):** revisar y evaluar su eficacia y eficiencia. Si el desempeño no es el esperado analizar las causas y determinar las mejoras.
- **Actuar ("Act"):** mejora continua del SGSI.

Estructura del estándar

1. **Objeto y campo de aplicación:** objetivos y uso de la norma en el contexto de las diferentes organizaciones.
2. Referencias normativas del estándar.
3. Términos y definiciones utilizados en el desarrollo de la norma.



4. **Contexto de la organización:** requisitos y expectativas de los interesados tanto a nivel interno como externo y que influirán en el SGSI y determinación del alcance de este.

5. **Liderazgo:** importancia de la implicación de la gerencia con el sistema, mediante el establecimiento de políticas, integrando el SGSI en los procesos de la organización, y asegurando los recursos necesarios.

6. **Planificación:** es imprescindibles detectar, analizar y valorar los riesgos de seguridad de la información tomando como referencia los umbrales aceptables de riesgo de la organización (apetito al riesgo), así como planificar estrategias de respuesta (mitigación).

7. **Soporte:** recursos necesarios para la capacitación y concienciación del personal, además de la importancia de la comunicación y la propia información.

8. **Operación:** cómo operar el sistema e implantar la respuesta a los riesgos.

9. **Evaluación de desempeño:** pautas para la monitorización, seguimiento y control del SGSI y la evaluación de su eficiencia y eficacia.

10. **Mejora:** se centra en cómo abordar las no conformidades con la norma, las acciones correctivas que hay que implementar y la mejora periódica del Sistema de Gestión de Seguridad de la Información.

11. Anexo A: definición de los controles para mejorar la seguridad de la información.

Sin duda, **la ISO 27001 es fundamental para gestionar la seguridad de la información** en organismos y empresas independientemente de su tamaño, objetivos o estructura.

Beneficios de la implantación de la Norma ISO 27001

Estas son algunas de las **ventajas de implementar la norma ISO 27001:**

1. Permite el **equilibrio y la coordinación** de los procesos de seguridad.

2. **Minimiza riesgos y aumenta el nivel de seguridad** en la información que se maneja gracias a las metodologías que proporciona.

3. Facilita un **plan de acción** para responder a cualquier riesgo o amenaza que se materialice.

4. Prioriza el cumplimiento de los **requerimientos legales.**

5. Contar con esta certificación supone un **valor añadido** para la empresa.

6. **Reduce costes** al aumentar la eficiencia.

7. Contribuye a crear un **ambiente de confianza** entre todas las partes implicadas en la organización (trabajadores, usuarios o clientes y proveedores).

8. Activa un **sistema de alertas** al detectar una actividad sospechosa.

9. Mantiene un **seguimiento constante** de los controles de seguridad.

10. Es una herramienta de gran utilidad en la **planificación de los procesos.**

11. Aporta un plus a la **imagen corporativa.**

LA UNIVERSIDAD EN INTERNET

Claves para la implantación de la norma en una compañía

La implantación de la norma ISO 27001 debe realizarse prestando atención a las siguientes claves:

- **Fijar objetivos.** Hay que establecer cuáles son los objetivos de la empresa con respecto al Plan de Seguridad y definir en qué áreas va a implantarse, cuál será la metodología en la evaluación de riesgos y qué requisitos legales debe cumplir.
- **Reconocer riesgos.** Definidas las metas hay que identificar cuáles son los posibles riesgos a los que tendrá que enfrentarse la empresa y cuáles sus puntos más vulnerables. Es importante también fijar quién se encargará de gestionarlos.
- **Analizar esos riesgos.** Debe calcularse cuál será el impacto y la frecuencia de los riesgos, determinando cuáles pueden ser eliminados y cuáles no y cómo se van a gestionar.
- **Redactar la Declaración de Aplicabilidad.** Con los objetivos de control definidos hay que elegir cuáles van a aplicarse y cómo, justificando cada punto. Todo esto debe recogerse en un documento: la Declaración de Aplicabilidad.
- **Poner en marcha el Sistema de Gestión de Seguridad de la Información** (SGSI).
- **Formación.** Para que los procesos de control sean eficaces es necesario que el personal cuente con los conocimientos necesarios sobre las nuevas tecnologías y los protocolos que van a implementarse.
- **Monitoreo.** Todos los procesos deben ser sometidos a una auditoría para comprobar su funcionamiento y que realmente se están logrando los objetivos fijados.

¿Quién se encarga de la implantación?

Los Sistema de Gestión de Seguridad de la Información son una herramienta que permite reducir riesgos para el negocio, por lo tanto debe ser la **Dirección de la empresa** quien asuma la responsabilidad de la implantación de la ISO 27001.

Su aplicación implica un proceso de concienciación del personal, de cambios de mentalidad y de modelos de actuación, algo que solamente puede indicar la Dirección. Para ello es importante contar con profesionales formados en seguridad informática, una formación que aporta titulaciones como el **Máster en Ciberseguridad** de UNIR.