

# MN<sub>E</sub>MO

The cover features a complex geometric design. A large white triangle points downwards from the top left. The background is composed of various shades of green and grey. On the right side, there is a faded image of a cityscape with buildings and trees. Overlaid on the left and bottom are stylized illustrations of interlocking gears and technical lines, including circles and arrows, suggesting a mechanical or engineering theme.

## Módulo 9

Auditoría de un sistema  
de gestión de seguridad  
de la información

## Contenido

Introducción a la Auditoría .....	6
Conceptos básicos.....	6
Concepto de Seguridad de la Información.....	6
Concepto de Auditoría de Seguridad de la Información.....	7
Objetivos generales de una Auditoría de Seguridad de la Información.....	7
Fundamentos de la auditoría .....	8
Buenas Prácticas de Auditoría de los sistemas de Gestión (ISO 19011:2018 / 27007:2022) .....	8
¿Qué es ISO 19011:2018? .....	8
¿Qué es ISO/IEC 27007:2022? .....	9
Requisitos del SGSI .....	10
¿Qué tipos de auditoría pueden realizarse? .....	10
Auditoría interna .....	10
Auditoría externa .....	11
¿Qué es ISO/IEC 27006:2020? .....	12
Fases fundamentales de Auditoría y Certificación.....	13

Fase 1 de la auditoría .....	13
Fase 2 de la auditoría.....	14
¿Próximos pasos tras la auditoría? .....	14
¿Qué es una No Conformidad? .....	15
¿Qué es una No Conformidad mayor? .....	15
Gestión de No Conformidades .....	16
Control interno de la auditoría .....	17
Objetivos.....	17
Elementos a tener en cuenta en el control interno.....	18
Auditoría de seguridad .....	20
Tipos.....	20
Auditoría de primera parte.....	20
Auditoría de segunda parte .....	21
Auditoría de tercera parte .....	21
Evidencias.....	22
Concepto .....	22
Características.....	22

Tipos.....	22
Cuestionarios.....	24
Entrevistas .....	24
Checklists (Listas de Verificación) .....	24
Trazas y/o Huellas.....	24
Fases de metodología de auditoría de un SGSI .....	25
Aceptación de auditores .....	25
Recabar datos Iniciales del entorno a auditar. ....	25
Planificar y elaborar el Plan de Auditoría.....	27
Beneficios.....	32
Inconvenientes.....	32
Realizar las Actividades de Auditoría. ....	32
Ejecución – Reunión inicial .....	32
Ejecución - Realizar la auditoría .....	33
Ejecución - Control de la auditoría.....	33
Ejecución - Establecimiento de hechos.....	33
Ejecución - Mantenga informado al auditado.....	34

Ejecución - Reunión de revisión diaria .....	34
Realizar el Informe Final. ....	34
Realización del informe .....	35
Tipos de Informes finales .....	36
Redacción del Informe.....	37
Roles en la auditoría.....	38
Responsabilidades del auditor jefe.....	38
Tareas del auditor .....	39
Habilidades y comportamientos de un auditor eficaz.....	39



## Introducción a la Auditoría

¿Para qué se realizan las Auditorías de Seguridad?

Una auditoría de Seguridad (SGSI) se realiza para dar soporte al control y seguridad de la tecnología de información utilizada en la empresa, aplicando un enfoque de control orientado a los procesos de la misma.

## Conceptos básicos

### Concepto de Seguridad de la Información

Según ISO 27001: 2022 la seguridad de la información se caracteriza aquí como la preservación de:

- Su confidencialidad, asegurando que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Adicionalmente se podrían abarcar otras dimensiones como la responsabilidad, fiabilidad, no repudio o autenticidad.

La información es un activo que como otros activos importantes tiene un valor y requiere en consecuencia una protección adecuada.

Un activo de información puede estar:

- Impreso o escrito en papel.
- Almacenado electrónicamente.

- Transmitido por correo o medios electrónicos.
- Mostrado en proyecciones.
- Hablado en conversación.

Debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparte o almacene. Dependiendo del tipo de activo de Información, las medidas de protección a aplicar serán distintas.

### Concepto de Auditoría de Seguridad de la Información

La auditoría de un Sistema de Gestión de Seguridad de la Información es un proceso de revisión de cumplimiento de los requisitos de la norma ISO /IEC 27001:2022.

El proceso de auditoría debe estar normalizado, por lo que es recomendable que esté alineado con las guías ISO 19011:2018 e ISO/IEC 27006:2021.

La norma ISO 19011 consiste en un conjunto de Directrices para la auditoría de los sistemas de gestión (ya sean de seguridad o de otra temática).

Por otro lado, la norma ISO/IEC 27006:2021, corresponde con los requisitos para entidades de auditoría y certificación de los SGSIs, por lo que será de obligatorio cumplimiento para todas las entidades de certificación que auditan nuestro sistema.

### Objetivos generales de una Auditoría de Seguridad de la Información

- Asegurar la integridad, confidencialidad y disponibilidad de la información.
- Minimizar existencias de riesgos en el uso de Tecnología de información
- Verificar si todas las amenazas y todos los activos han sido tenidos en cuenta.
- Asegurar que todas las partes interesadas se han tenido en cuenta.
- Evaluar la Seguridad, privacidad y disponibilidad en el ambiente informático, así como también la seguridad del personal, de los datos, el hardware, el software y las instalaciones.



- Determinar el grado de conformidad del sistema de gestión, o partes del mismo, con los criterios de auditoría (conforme a la norma ISO/IEC 27001:2022, y conforme a la política de Seguridad y Procedimientos).
- Evaluar la capacidad del sistema de gestión de asegurar el cumplimiento de requisitos legales, regulatorios y contractuales.
- Evaluar la efectividad del Sistema de Gestión implantado a la hora de lograr sus objetivos especificados.
- Identificar áreas de mejora potencial del Sistema de Gestión.
- Verificar que los Procesos de la organización corresponden a la realidad y existen.
- En segundas y posteriores auditorías verificar si las NC (en caso de haberlas) de la auditoría que le precede se han corregido y las observaciones tenidas en cuenta. Es decir, si se han corregido los fallos encontrados con anterioridad.
- En definitiva, verificar que se trabaja conforme se dice en políticas, procedimientos, etc.

## Fundamentos de la auditoría


### Buenas Prácticas de Auditoría de los sistemas de Gestión (ISO 19011:2018 / 27007:2022)

#### *¿Qué es ISO 19011:2018?*

Norma Internacional que proporciona orientación sobre los principios de auditoría, la gestión de programas de auditoría, la realización de auditorías de sistemas de gestión (aplicando por lo tanto al SGSI).

Esta norma es aplicable a todas las organizaciones que tienen que realizar auditorías internas o externas de sistemas de gestión (calidad, ambiental, seguridad...) o que tengan que gestionar un programa de auditoría.

A continuación, se especificarán las buenas prácticas de Auditoría de ISO 19011 aplicadas a ISO/IEC 27001: 2022, a través de ISO 27007:2022.





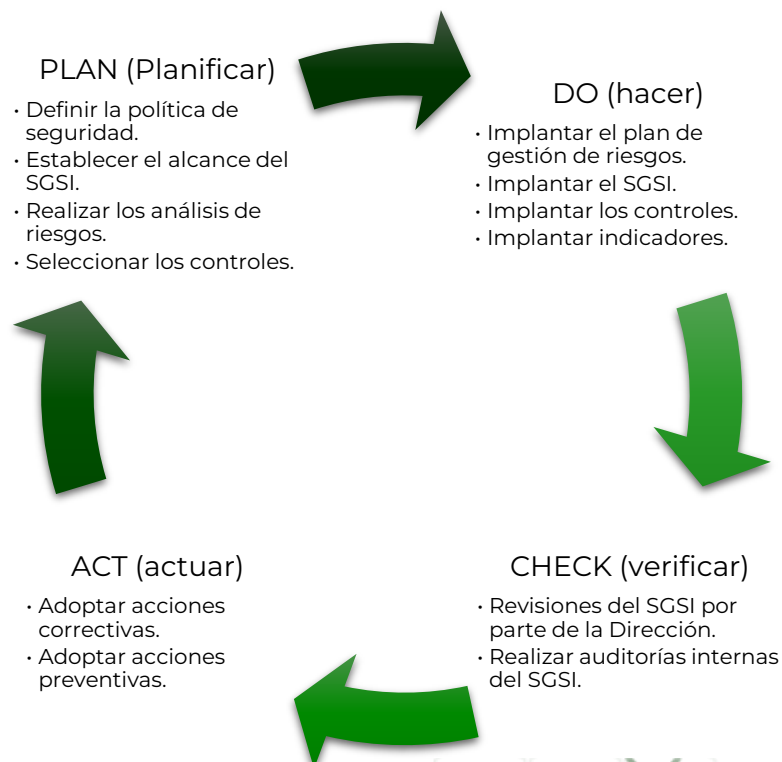
## ¿Qué es ISO/IEC 27007:2022?

ISO 27007:2022 (Normas de Auditoría).

“Directrices para la auditoría de los SGISs”.

- La norma ISO 27007:2022 ofrece orientación para auditar un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001:2022.
- Esta orientación específica del SGSI sirve para complementar la norma ISO 19011:2018.
- Manejar la orientación a los auditores en temas como: Establecimiento de los rastros de auditoría del SGSI, Auditoría de evidencia forense, Alcances del SGSI, Mediciones...

Plantea un círculo de actividades que tiene como objetivo la MEJORA CONTÍNUA.



### *Requisitos del SGSI*

- ISO/IEC 27001:2022.
- Requisitos legales, contractuales y de otras partes interesadas.
- Dominios de la norma/Documentos técnicos/ controles (Anexo A de 27001:2022).

Dominio 5: Controles Organizativos:  
Controles A5.1 a A5.37

Dominio 6: Controles  
de Personas:  
Controles A6.1 a A6.8

Dominio 7: Controles Físicos:  
Controles A7.1 a A7.14

Dominio 8: Controles Tecnológicos:  
Controles A8.1 a A8.34

¿Qué tipos de auditoría pueden realizarse?

### *Auditoría interna*

Podrán realizarlas:

- Personal interno de la empresa:

Aquella persona de la empresa capacitada para auditar el cumplimiento de la norma ISO/IEC 27001:2022.

Su misión es evaluar el sistema implantado en la propia empresa para mantenerlo, mejorarlo o, en su caso, preparar a la empresa para superar una auditoría de certificación.

- Personal externo a la empresa:

Aquella persona independiente contratada, normalmente a una empresa especializada en Auditorías o consultorías en ISO/IEC 27001:2022

Su misión es reflejar la situación de la empresa de una forma objetiva y, en su caso, preparar a la empresa para superar una auditoría de certificación.

### *Auditoría externa*

Podrán realizarla:

- Aquellas personas pertenecientes a una empresa autorizada a realizar auditorías de certificación. Por ejemplo, Organismos de certificación internacionales: BUREAU VERITAS, APPLUS, BSI, SGS, AENOR, etc.

La misión de esta auditoría es valorar si una organización, que ha solicitado el certificado, cumple o no con la norma de referencia para obtener un certificado oficial.

También se pueden contratar estas auditorías a modo de revisión. Es decir, una Auditoría externa no tiene por qué realizar necesariamente para obtener el certificado.

### ¿Qué acciones han de realizarse en una auditoría interna?

- Hacer el programa de auditoría.
- El Auditor Jefe debe elaborar y enviar el Programa de Auditoría.
- Reunión Inicial.

- El Auditor Jefe debe dirigir una reunión de inicio con todos los participantes, en la que se comentará el proceso de auditoría y se aclararán dudas.
- Auditoría documental (Fase I)
- Se revisará in-situ el cumplimiento documental con respecto a la norma (análisis de riesgos, gestión de riesgos, políticas, declaración de aplicabilidad...).
- Auditoría implantación (Fase II)
- Se revisará in-situ la implantación, controles, registros, objetivos, procedimientos...
- Elaborar y entregar informe. El informe de auditoría debe incluir como mínimo:
  - Fecha de realización
  - Auditores
  - Entrevistados
  - Alcance con sus detalles y norma de referencia Área o Dptos. auditados
  - Controles auditados
  - Conformidad del SGSI con la norma
  - No Conformidades
  - Cierre de la auditoría (reunión final)

El Auditor Jefe dirige una reunión en la que se presenta el informe de resultados de la auditoría.

¿Qué es ISO/IEC 27006:2020?

ISO/IEC 27006:2021: 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 SGSI) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2022 y los SGSI.

Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021-3:2019, cuando se aplican a entidades de certificación de ISO 27001:2022, pero no es una norma de acreditación por sí misma.

### Fases fundamentales de Auditoría y Certificación

- Fase 1:
  - Revisión Documental.
  - Plan De Auditoría.
  - Listas de verificación (checklists).
  - En función de los resultados, se puede determinar si se continúa o no con la auditoría.
- Fase 2:
  - Reunión de apertura.
  - Se toman los resultados obtenidos en la Fase 1.
  - Se realiza la Auditoría.
  - Se elabora un informe resumen /informe de No Conformidades.
  - Se realiza una reunión de cierre de la Auditoría.
  - Se debe elaborar un Plan de Acciones correctivas que solvante las No Conformidades detectadas.

#### *Fase 1 de la auditoría*

- No necesariamente tiene que ser in situ, puesto que se trata del análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2.
- Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.

### *Fase 2 de la auditoría*

- Se revisan in situ las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto.
- Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora.
- Se realiza una revisión de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés.
- Finaliza con una reunión de cierre en la que se presenta el informe de auditoría.

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses de operación, se puede pasar a la fase de auditoría y certificación, que se desarrolla de la siguiente forma:

- Solicitud de la auditoría por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.
- Respuesta en forma de oferta por parte de la entidad certificadora.
- Compromiso.
- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.

### *¿Próximos pasos tras la auditoría?*

Certificación: en el caso de que se descubran durante la auditoría no conformidades graves, la organización deberá implantar acciones correctivas si pretende obtener el certificado; una vez verificada dicha implantación o, directamente, en el caso de no haberse presentado no conformidades, el auditor podrá emitir un informe favorable y el SGSI de la organización será certificado según ISO 27001.

- Auditoría de seguimiento: semestralmente o, al menos, anualmente, debe realizarse una auditoría de mantenimiento; esta auditoría se centra, generalmente, en partes concretas del sistema, dada su menor duración, y tiene como objetivo comprobar el uso del SGSI y fomentar y verificar la mejora continua.
- Auditoría de re-certificación: cada tres años, es necesario superar una auditoría de certificación formal completa como la descrita.
- Auditoría Interna: al menos anualmente, y con objetivo de obtener un resultado favorable en la auditoría de seguimiento o re-certificación, se debe realizar una auditoría interna, llevada a cabo por personal interno, o bien por un tercero. La realización de estas auditorías es requisito de la norma ISO/IEC 27001:2022.

### *¿Qué es una No Conformidad?*

Una No Conformidad es un fallo o incumplimiento de algún requisito especificado.

### *¿Dónde se especifican los requisitos?*

- La norma ISO/IEC 27001:2022.
- La implantación de algún control aplicable del Anexo A de ISO/IEC 27001:2022
- La política de Seguridad de la Organización.
- Los procesos definidos en el alcance, o los procedimientos del SGSI existentes.
- La efectividad de los procesos y actividades desempeñados por la organización.
- Los requisitos legales, regulatorios o contractuales que aplican a la organización.

### *¿Qué es una No Conformidad mayor?*

Ocurre cuando el auditor detecta un fallo que no permite cumplir con uno o varios requisitos importantes de la ISO/IEC 27001:2022 o un dominio del Anexo A, afectando directamente a la efectividad del proceso sobre el que debería aplicarse el requisito o cuando la organización no corrige una NC menor resultante de auditorías anteriores. También aplicaría en el supuesto de existir dudas significativas sobre la capacidad del SGSI implantado de alcanzar los resultados estipulados.



### *Gestión de No Conformidades*

- Detección e identificación

Cualquier persona que intervenga en el sistema de gestión implantado (empleado y/o contratado) que detecte una No conformidad, deberá proceder a su identificación tan rápido como sea posible, para ello deberá notificar inmediatamente al Responsable del SGSI sobre dicha no conformidad, haciendo uso de cualquier medio: e-mail, teléfono, personalmente, etc., dejando éste en todo caso constancia del hecho mediante e-mail.

El Responsable del SGSI documenta el "Informe de no conformidad" en un documento diseñado para tal efecto, indicando al menos, su fecha de apertura, codificación, tipo de no conformidad (en función del origen), procesos afectados, controles implicados, una descripción y realizando un análisis de la causa raíz de la no conformidad (investigación para identificar el fallo raíz que ha ocasionado).

- Tratamiento

Tras la detección de una no conformidad y el análisis de su causa se pueden aplicar dos formas de tratamiento que dependerán de la complejidad y/o impacto del problema:

- a) La primera forma consiste en una solución inmediata a un problema puntual y no repetitivo detectado:

El responsable del tratamiento pone en marcha un tratamiento mediante la aplicación de una acción positiva inmediata. Dicha acción corregirá el fallo mostrado por la NC, pero no solucionará la causa raíz que dio origen a la misma.

- b) La segunda forma de tratamiento consiste en adoptar acciones necesarias para eliminar el problema y la posibilidad de que vuelva a ocurrir, estas acciones son denominadas "acciones correctivas".

En estos casos se deberá dejar reflejado en el Informe de no conformidad, el número de acción correctiva asociada (para facilitar su seguimiento en el registro de Acciones diseñado para tal efecto), indicando en su origen NC.

- Seguimiento y cierre

Tras el tratamiento y llegado el plazo máximo de ejecución establecido anteriormente, el Responsable del SGSI verificará que éste haya sido aplicado con eficacia y en el tiempo estipulado, para ello recogerá todas las evidencias posibles como pruebas de cumplimiento.

Además, cumplimentará el apartado correspondiente "seguimiento y cierre" del "informe de no conformidad", indicando el momento de cierre y la eficacia de la misma. Cuando la acción correctiva implantada de cómo resultado "no eficaz" se procederá a su cierre e inmediatamente se abrirá una nueva acción correctiva. En la acción correctiva ineficaz se indicará el número de la nueva acción asociada (para facilitar su seguimiento).

## Control interno de la auditoría

### *Objetivos*

- Controlar que todas las actividades de los sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la organización.
- Asegurar que las medidas que se obtienen de los mecanismos implantados sean correctas y válidas.
- Verificar que las evidencias suministradas son veraces y ayudan a demostrar el cumplimiento de lo que se está auditando.
- Colaborar y apoyar el trabajo entre los miembros del equipo de auditoría.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

### *Elementos a tener en cuenta en el control interno*

- Ambiente de control
  - Integridad, Ética y Capacidad del personal de la empresa.
  - Factores de Evaluación:
    - Existencia e Implantación de una Política de Seguridad.
    - Existencia e implantación de Políticas de Seguridad para usuarios de los sistemas de Información.
    - Verificar si las metas de eficacia se han alcanzado y son realistas.
    - Descripción de los Puestos de Trabajo.
    - Análisis de conocimientos y Habilidades que se requieren.
  - Participación de la Alta Dirección (apoyo de la Dirección).
  - Responsabilidad de los empleados.
- Evaluación del Riesgo
  - Las organizaciones, cualquiera sea su tamaño, se enfrentan a diversos riesgos de origen interno y externo.
  - Podemos definir el riesgo como la probabilidad de que una amenaza cause un daño (impacto) en la organización.
  - La evaluación del riesgo es la identificación y análisis de dichos riesgos en lo que se refiere a la consecución de los objetivos, y constituye la base para determinar la forma de gestionar el riesgo. Existen 4 maneras de gestionar el riesgo:

- Asumir (de manera consciente y objetiva).
  - Reducir (aplicando controles).
  - Transferir: por ejemplo, mediante acuerdos con aseguradoras.
  - Evitar.
  - Debe ser un proceso continuo, una actividad básica de la organización, como la evaluación continua de la utilización de los sistemas de información o la mejora continua de los procesos.
  - Lo importante no es utilizar determinada metodología de evaluación del riesgo sino convertir la evaluación del riesgo en parte natural del proceso de planificación de la empresa.
- Actividades de control.
  - Las actividades de control deben estar integradas en el proceso de evaluación del riesgo. Una vez analizados los riesgos, la dirección desarrolla actividades de control, las que deben cumplirse correcta y oportunamente.
  - Dichas actividades garantizan que se adopten las medidas necesarias para hacer frente a los riesgos que amenazan la consecución de los objetivos. En algunos entornos, las actividades de control se clasifican en:
    - **Controles preventivos:** Tratar de evitar el hecho no deseado. Por ejemplo, implantar un software de seguridad que impida los accesos no autorizados al sistema.
    - **Controles de detección:** Cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, registro de intento de acceso no autorizado.
    - **Controles correctivos:** Vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de una BD a partir de copias de seguridad.

- Controles manuales o de usuario.
- Controles informáticos o de T.I.
- Controles de la dirección.

## Auditoría de seguridad

### Tipos

TIPOS	SEGURIDAD
De primera parte	<ul style="list-style-type: none"> <li>• Auditorías Internas.</li> <li>• Las realizadas por miembros de la propia empresa.</li> </ul>
De segunda parte	<ul style="list-style-type: none"> <li>• Auditorías externas de clientes.</li> <li>• Las realizadas por sucursales o clientes de la empresa.</li> </ul>
De tercera parte	<ul style="list-style-type: none"> <li>• Auditorías de certificación.</li> <li>• Las realizadas por organizaciones independientes.</li> </ul>

### Auditoría de primera parte

Es aquella realizada por una organización sobre sí misma, para determinar si sus sistemas y procedimientos están mejorando de forma consistente los productos y servicios ofrecidos a sus clientes y usuarios, y como vía para determinar la conformidad con sus procedimientos y la norma. Se le conoce también como Auditoría Interna, y la puede realizar personal interno de la organización, o un externo.

Razones para las auditorías de primera parte:

- Cumplimiento del marco normativo (norma, anexo, legislación aplicable, etc.).
- Mecanismo de control usado por la dirección.

- Para corregir no conformidades antes de que las entidades externas las detecten.
- Para mejorar sistemáticamente la organización.

### Auditoría de segunda parte

Una auditoría de segunda parte es aquella que se realiza a un proveedor potencial o actual; normalmente, para usar el resultado de la auditoría como parte de la decisión de compra. Pocas organizaciones, incluso en esta época de la Ilustración en seguridad de la información, deciden comprar de un proveedor sólo en base a una auditoría de seguridad de la información.

El cliente puede solicitar este tipo de auditoria por varios motivos:

- Auditoria de evaluación. Antes de comenzar una relación contractual con un suministrador, puede desear que se someta a una auditoría para hacer una evaluación del mismo.
- auditoría de seguimiento. Dentro de un marco contractual, el cliente puede desear evaluar de forma periódica a su suministrador.
- Dentro del marco contractual, puede desearse evaluar al suministrador después, por ejemplo, de la implantación de un plan de acciones correctoras emprendido ante los resultados de una auditoria anterior.

### Auditoría de tercera parte

- La entidad de certificación, de cara a tener auditada de forma independiente su profesionalidad e integridad, establece un programa, incluyendo política, organización y procedimientos y es auditada por una entidad de acreditación.
- Si la supera, obtiene una acreditación que se muestra no sólo en su propio certificado de acreditación sino en todos los certificados emitidos a sus clientes.

## Evidencias

### *Concepto*

La recopilación de material que ayude en la generación de una opinión lo más correcta posible es un paso clave en el proceso de la auditoría.

- El auditor debe conocer las diversas formas de evidencias y como puede ser recopilada y examinada para respaldar los hallazgos de la auditoría.
- Después de recopilar la suficiente evidencia, el siguiente paso es evaluar la información recopilada a fin de desarrollar opiniones y recomendaciones finales.

### *Características*

- Evidencia que existe.
- No influenciada por sentimientos o prejuicios.
- Puede ser declarada (manifestada).
- Puede ser documentada.
- Debe ser cuantitativa (contable).
- Debe ser cualitativa (medible).
- Debe ser verificable (es decir, documentada o basada en hechos observables).

### *Tipos*

- Evidencia ocular
  - Comparación: es observar la similitud o diferencia existente entre dos o más elementos.
  - Observación: es el examen ocular para cerciorarse como se ejecutan las operaciones.
- Evidencia Oral



- Indagación: es el acto de obtener información verbal sobre un asunto mediante averiguaciones directas o conservaciones con los funcionarios de la empresa.
- Entrevistas: pueden ser efectuadas al personal de la empresa auditada o personas beneficiarias de los programas o proyectos.
- Encuestas: pueden ser útiles para recopilar información de un gran universo de datos o grupos de personas.
- Evidencia Escrita/Documentación
  - Analizar: consiste en la separación y evaluación crítica, objetiva y minuciosa de los elementos o partes que conforman una operación, actividad, o proceso, con el fin de establecer su naturaleza, su relación y conformidad con los criterios normativos y técnicos existentes.
  - Confirmación: es la técnica que permite comprobar la autenticidad de los registros y documentos analizados, a través de información directa y por escrito, otorgada por funcionarios que participan o realizan las operaciones sujetas a examen.
  - Rastreo: es utilizada para dar seguimiento y controlar una operación de manera progresiva, de un punto a otro de un proceso interno determinado o, de un proceso a otro realizado por una unidad operativa dada.
- Evidencia Física:
  - Es el examen físico y ocular de activos, obras, documentos y valores, con el objeto de establecer su existencia y autenticidad.
  - La evidencia de esa naturaleza puede presentarse en forma de fotografías, gráficas, mapas o muestra materiales.

## Cuestionarios

Conjunto de preguntas a las que el sujeto puede responder oralmente o por escrito, cuyo fin es poner en evidencia determinados aspectos.

VENTAJAS	DESVENTAJAS
Ahorra tiempo	Responde a objetivos descriptivos
Aporta información generalizada	Impide profundizar en las respuestas
Facilita la confidencialidad	Resulta difícil de realizar

## Entrevistas

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

## Checklists (Listas de Verificación)

El auditor deberá elaborar cuestionarios en función de los escenarios que tenga que auditar. El objetivo es disponer de una pequeña guía que ayude a tener claro lo que se necesita saber, y por qué.

## Trazas y/o Huellas

De cara a verificar las afirmaciones indicadas en un Documento, o que indica el personal entrevistado, se puede solicitar que se muestren los logs que demuestren que verdaderamente se registra aquello que se indica.

Ejemplo: Se registran los intentos de Acceso. Para verificarlo, se puede solicitar que se muestren los intentos de acceso de los últimos días.

## Fases de metodología de auditoría de un SGSI

### Aceptación de auditores

Comunicación con el auditor anterior; antes de aceptar el trabajo se puede requerir que el nuevo auditor se comuniquen, ya sea en forma oral o escrita con el auditor anterior.

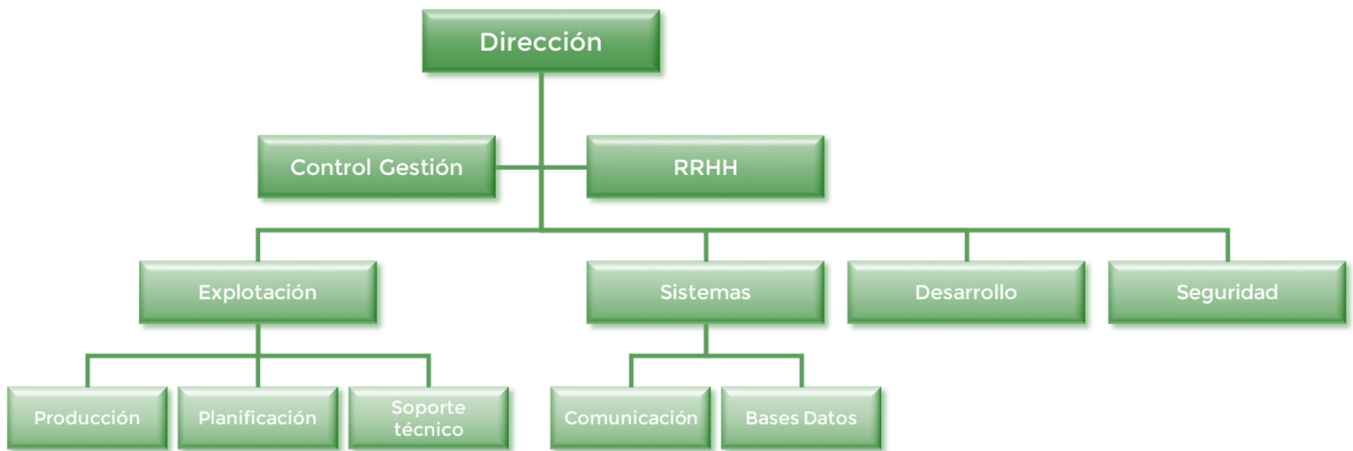
Selección del equipo auditor; esta selección debe asegurar la objetividad, capacitación e imparcialidad del proceso de la auditoría.

### Recabar datos Iniciales del entorno a auditar.

- Aclarar el alcance y el objetivo de auditoría.
- Comprender el negocio.
- Definir el flujo de procesos y sus interacciones.
- Acordar procedimientos a usar durante la auditoría.
- Resolver cualquier malentendido.
- Identificar necesidades especiales, conocimientos, ropa de protección o seguridad...
- Conocer la distribución física de la organización y sus centros de trabajo.

Tener conocimientos de:

- Organización
  - Organigrama: El organigrama expresa la estructura oficial de la organización.
  - Departamentos: Órganos que siguen inmediatamente a la Dirección.



- Ubicación geográfica
  - Situación Geográfica.
  - Diferentes CPDs, con responsables y mismos estándares de trabajo.
- Activos informáticos
  - Arquitectura y Configuración Hardware y Software.
  - Configuración de diferentes CPDs compatibles y que estén intercomunicados.
  - Inventario Hardware y Software.
  - CPUs, procesadores, PCs, periféricos, etc.
  - Software básico, software interno y software comprado.
  - Comunicaciones y Redes de Comunicación.
  - Líneas de Comunicación.
  - Acceso a red pública e intranet.
- Recursos humanos
  - La cantidad depende del alcance de la auditoría.
  - Determinación de incremento de carga del auditado y consenso en fechas y duración de actividades de auditoría.
  - ¿Cuántos puestos de trabajo hay?

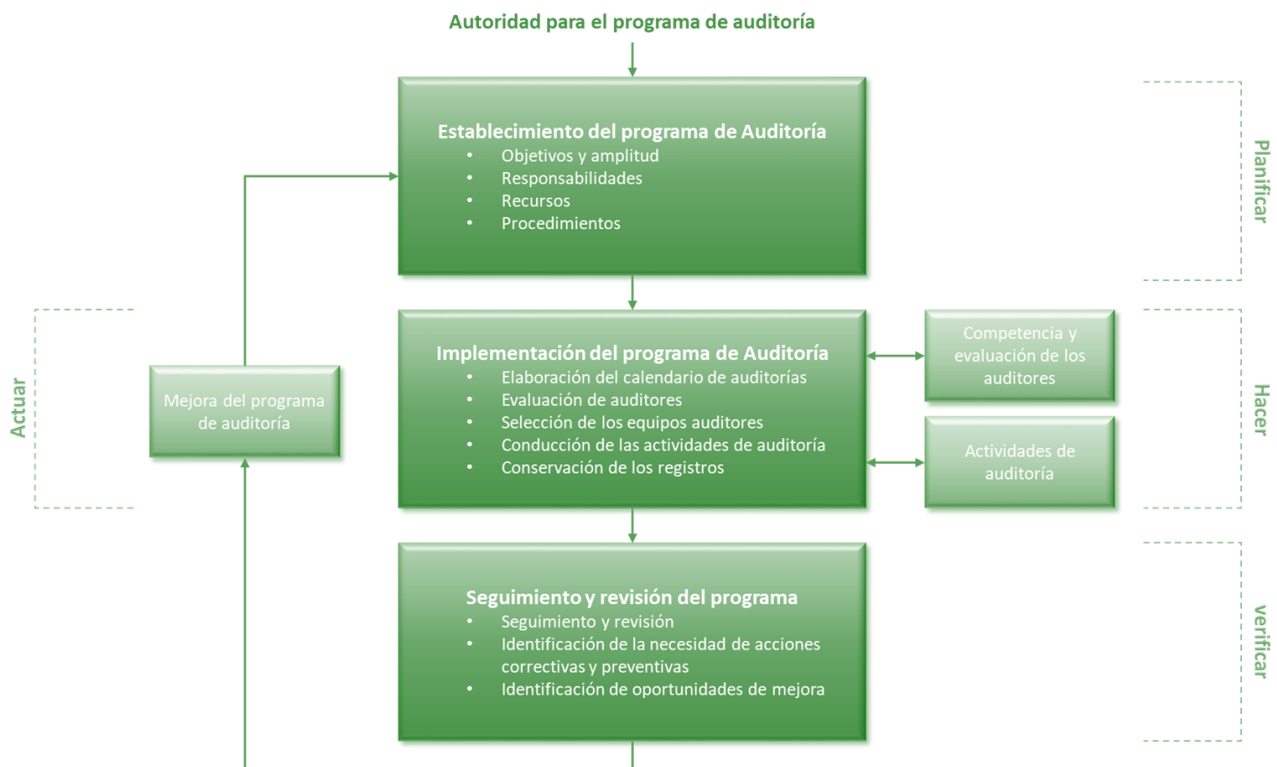
- Cada puesto de trabajo ha de tener un nombre distinto. Si hay varios nombres con una misma función, existen Diferencias de estructura.
- Número de Personas por Puesto de Trabajo.
- Distribución de recursos ineficiente.
- Necesidad de reorganización.

### Planificar y elaborar el Plan de Auditoría.

Un programa de auditoría puede incluir una o más auditorías, dependiendo del tamaño, la naturaleza y la complejidad de la organización que va a ser auditada. Estas auditorías pueden tener diversos objetivos y pueden incluir auditorías combinadas o conjuntas.

Un programa de auditoría también incluye todas las actividades necesarias para planificar y organizar el tipo y número de auditorías, y para proporcionar los recursos para llevarlas a cabo de forma eficaz y eficiente dentro de los plazos establecidos.

Una organización puede establecer más de un programa de auditoría.



Conforme al diagrama, para elaborar un plan de auditoría básico; se deben fijar:

- Calendario: Fechas y lugares en donde se realizará la auditoría.
- Objetivos y alcance.
- Las normas, los requisitos legales, reglamentarios y contractuales, y otros criterios de auditoría.
- Miembros del equipo auditor.
- Medios y recursos necesarios para la ejecución.
- Horario de la auditoría.
- Personas responsables de cada área.

La amplitud de un programa de auditoría puede variar y estará influenciada por el tamaño, la naturaleza y la complejidad de la organización que se audite, así como por lo siguiente:

- El alcance, el objetivo y la duración de cada auditoría que se realice.
- La frecuencia de las auditorías que se realicen.

- El número, la importancia, la complejidad, la similitud y la ubicación de las actividades que se auditen.
- Las normas, los requisitos legales, reglamentarios y contractuales, y otros criterios de auditoría.
- La necesidad de acreditación o de certificación /registro.
- Las conclusiones de las auditorías previas o los resultados de una revisión de un programa de auditoría previo.
- Cualquier aspecto idiomático, cultural y social.
- Las inquietudes de las partes interesadas.
- Los cambios significativos en la organización o en sus operaciones.

La responsabilidad de la gestión de un programa de auditoría debería asignarse a una o más personas con conocimientos generales de los principios de la auditoría, de la competencia de los auditores y de la aplicación de técnicas de auditoría.

Estas personas deberían tener habilidades para la gestión, así como conocimientos técnicos y del negocio, pertinentes para las actividades que van a auditarse.

Aquellos a los que se ha asignado la responsabilidad de gestionar el programa de auditoría deberían:

- Establecer los objetivos y la amplitud del programa de auditoría.
- Establecer las responsabilidades y los procedimientos, y asegurarse de que se proporcionan recursos.
- Asegurarse de la implementación del programa de auditoría.
- Asegurarse de que se mantienen los registros pertinentes del programa de auditoría.
- Realizar el seguimiento, revisar y mejorar el programa de auditoría.

Cuando se identifiquen los recursos para el programa de auditoría, deberían considerarse:

- Los recursos financieros necesarios para desarrollar, implementar, dirigir y mejorar las actividades de la auditoría.



- Las técnicas de auditoría.
- Los procesos para alcanzar y mantener la competencia de los auditores, y para mejorar su desempeño.
- La disponibilidad de auditores y expertos técnicos que tengan la competencia apropiada para los objetivos particulares del programa de auditoría.
- La amplitud del programa de auditoría.
- El tiempo de viaje, alojamiento y otras necesidades de la auditoría.

Deberían establecerse los objetivos de un programa de auditoría para dirigir la planificación y realización de las auditorías.

Estos objetivos pueden basarse considerando:

- Prioridades de la dirección.
- Propósitos comerciales.
- Requisitos del sistema de gestión.
- Requisitos legales, reglamentarios y contractuales.
- Necesidad de evaluar a los proveedores.
- Requisitos del cliente.
- Necesidades de otras partes interesadas.
- Riesgos para la organización. Personas responsables de cada área.

Ejemplos de objetivos de un programa de auditoría: Se proponen los 4 ejemplos siguientes:

- Cumplir los requisitos para la certificación de conformidad con una norma de sistema de gestión.
- Verificar la conformidad con los requisitos contractuales.
- Obtener y mantener la confianza en la capacidad de un proveedor.
- Contribuir a la mejora del sistema de gestión.

## Preparación de CHECKLISTS:

- Pueden ser una ayuda importante para asegurar la profundidad y continuidad de la auditoría.
- Deberían ser representativas del área auditada.
- Deberían ser preparadas de forma que indiquen el flujo de operación y de proceso.
- No deberían llevar a respuestas de sólo "sí" o "no".
- Deberían prepararse como un memorándum o cuaderno de notas.

Desarrollar listas de verificación: esta etapa permite obtener los últimos datos importantes para la ejecución de la auditoría, como, por ejemplo, ¿qué quiero mirar?, ¿qué estoy buscando?, ¿con quién debo hablar?, ¿qué deseo preguntarle?

Preguntas	Información requerida	Resultado
¿Qué?	Normas, políticas y procedimientos aplicados a sistemas y controles claves.	Conocimiento de la empresa.
¿Por qué?	Objetivos, metas y planificación estratégica.	Líneas de responsabilidad funcional.
¿Cómo?	Objetivos metas y planificación estratégica.	Líneas de responsabilidad funcional.
¿Quién?	División de funciones y responsabilidad.	Empresa.
¿Dónde?	Observaciones del medio ambiente.	Factores internos y externos.
¿Cuándo?	Fechas y eventos importantes, variación de tiempo y vida útil.	Situaciones importantes.

### *Beneficios*

- Mantienen claros los objetivos de la auditoría.
- Sirven como evidencia de la planificación de la auditoría.
- Ayudan a mantener el ritmo y continuidad de la auditoría.
- Mantienen la imparcialidad del auditor.
- Ayudan a guiar al auditor, de tal forma que se analicen todos los puntos importantes.

### *Inconvenientes*

- Tienden a perder valor si se convierten en:
  - Listas de punteo o de verificación tipo Check list.
  - Una lista de pasos a seguir, de forma limitada, y que no permitan profundizar en las cuestiones importantes.
  - Cuestionarios (con opciones de respuesta solamente sí/no).

## Realizar las Actividades de Auditoría.

### Ejecución – Reunión inicial

- Presentaciones – tomar nota de los asistentes.
- Establecer el tono de la auditoría.
- Confirmar el propósito y alcance de la auditoría.
- Revisar y confirmar el plan de auditoría.
- Asignar guías para el equipo auditor.
- Comunicar la metodología de auditoría.
- Confirmar:
  - Método de realización de informes.
  - La auditoría está basada en métodos de muestreo.
  - Confidencialidad.

- Hora de reunión final (o de cierre).
- Aspectos logísticos.
- Establecer cualquier restricción.
- Aclaraciones.

## Ejecución - Realizar la auditoría

- Visitar las áreas implicadas.
- Deberá existir un guía o persona designada que acompañe al auditor durante la visita..
- El auditor especificará todo lo que necesita ver en cada área
- Se investigará con la profundidad que se considere necesaria intentando respetar los tiempos definidos en el Plan de Auditoría.
- Si no se encuentran problemas, se seguirá adelante con otra área (no hay que auditar hasta encontrar un problema).

## Ejecución - Control de la auditoría

- La lista de verificación (checklist) es una herramienta, y no una norma.
- Si aparecen pistas potenciales de auditoría, decida si:
  - Descartarlas.
  - Anotarlas para más adelante.
  - Seguir las inmediatamente.
    - Pueden afectar al tamaño de la muestra.
    - Pueden afectar al plan de auditoría.

## Ejecución - Establecimiento de hechos

- Verificar los hallazgos.
- Establecer y acordar los hechos.
- Comentar y aclarar cualquier preocupación.
- Establecer por qué es, o no, una no conformidad.

- Obtener un acuerdo sobre lo que se está tratando.

### Ejecución - Mantenga informado al auditado

Para una auditoría resulte útil y se realice con profesionalidad:

- Es necesario revisar el progreso de la auditoría de forma regular para tener claros los hallazgos e información obtenida hasta el momento, y que podría ser de gran utilidad para el resto de la auditoría.
- El auditado debe estar informado, y debe entender los hechos que se desarrollen a lo largo de la auditoría, con el objetivo de evitar rumores sobre el trabajo del auditor.
- Deberá existir entendimiento entre auditor y auditado, y mantener un trato cordial durante la auditoría.

### Ejecución - Reunión de revisión diaria

Se recomienda realizar una reunión al final de cada día de la auditoría. Dicha reunión no debería durar más de 20 minutos, y en ella se deberán tratar los siguientes puntos:

- Resumen y revisión de No Conformidades encontradas.
- Clarificar cualquier duda, problema o malentendido que le haya podido surgir al auditado durante la auditoría.
- Informar sobre progreso de la auditoría, indicando lo que se ha visto y lo que queda por ver.

### Realizar el Informe Final.

El líder del equipo auditor debería ser responsable de la preparación y del contenido del informe de la auditoría.

El informe de la auditoría debería proporcionar un registro completo de la auditoría, preciso, conciso y claro, y debería incluir, o hacer referencia a lo siguiente:



- Los objetivos de la auditoría.
- El alcance de la auditoría, particularmente la identificación de las unidades de la organización y de las unidades funcionales o los procesos auditados y el intervalo de tiempo cubierto.
- La identificación del cliente de la auditoría.
- La identificación del líder del equipo auditor y de los miembros del equipo auditor.
- Las fechas y los lugares donde se realizaron las actividades de auditoría in situ.
- Los criterios de auditoría.
- Los hallazgos de la auditoría.
- Las conclusiones de la auditoría.
- Estas conclusiones deberán incluir las No Conformidades detectadas durante la auditoría. Se especificará la Descripción de la No Conformidad, la evidencia o evidencias, y la referencia al punto incumplido de la Norma.

### Realización del informe

- Estilo y Contenido: Objetivo, claro, conciso, constructivo y oportuno.
  - Apropiado a los destinatarios.
  - Identificar organización auditada.
  - Incluye título, firma y fecha.
- Objetivos (lo que trata de cumplir la auditoría).
- Alcance: naturaleza, tiempo y extensión del trabajo de auditoría.
  - Área funcional.
  - Período de auditoría.
  - Sistemas de información, aplicaciones o entornos auditados.
- Realización del Informe (continuación):
  - Restricción sobre su distribución.
  - Hallazgos significativos de la auditoría (causas y riesgos).
  - Conclusión: evaluación del auditor sobre el área auditada.
  - No Conformidades.

- Presentación: lógica y organizada.
- Redacción de los Incumplimientos / No Conformidades:
  - Requisito
    - Cite el requisito (la parte relevante del mismo).
  - Fuente del requisito
    - Normativa que se incumple.
  - Referencia al punto de la norma incumplido.
    - Hallazgo (cómo no se cumple el requisito).
    - Formulación ("refleja" el requisito).
  - Evidencia para hacerlo verificable
    - Identifique todas las evidencias objetivas de forma que sean trazables.
- Resumen en 3 o 4 folios del contenido del informe final.
- Incluye fecha, naturaleza, objetivos y alcance de la auditoría.
- Proporciona una conclusión general, concretando las áreas de gran debilidad.
- Presentar las debilidades en orden de importancia.

### Tipos de Informes finales

- Favorable sin No Conformidades: trabajo realizado.
  - Sin limitaciones de alcance y sin incertidumbre.
  - De acuerdo con la norma ISO/IEC 27001:2022, el cumplimiento legal y profesional.
- Favorable con No Conformidades.

El informe deberá contener las No Conformidades estructuras de una forma clara y exacta.



Para ello, se establece que al menos se deberá incluir la siguiente información por cada No Conformidad detectada:

Se citará el requisito exacto de la norma ISO/IEC 27001:2022 que se incumple.

Se especificará la fuente del requisito, detallando el número de cláusula ISO 27001:2022, o referencia o sección de la documentación del SGSI.

También, se especificará el hallazgo, describiendo el porqué del incumplimiento del requisito.

Por último, si aplica, se especificarán las evidencias que demuestran el incumplimiento.

- Desfavorable
  - Identificación de irregularidades.
  - Incumplimiento de la norma ISO/IEC 27001:2022, el cumplimiento legal y profesional que afecte a significativamente a los objetivos estipulados.
- Denegada
  - Limitaciones al alcance.
  - Incertidumbres significativas.
  - Irregularidades.
  - Incumplimiento de norma ISO/IEC 27001:2022, cumplimiento legal y profesional.

## Redacción del Informe

- Párrafos
  - Un solo asunto por párrafo.
  - 8 o 10 líneas por párrafo.

- Frases
  - Una sola idea por frase.
  - No más de 3 líneas.
- Otros consejos
  - Lenguaje sobrio y normal.
  - Voz activa, nunca pasiva.
  - Omitir palabras innecesarias (con referencia a, consecuentemente con, etc.).
  - Evitar redundancias.
  - No utilizar adverbios y adjetivos simultáneamente.

## Roles en la auditoría

Puesta en común: ¿cuáles son las funciones y responsabilidades de los participantes en la auditoría?

- Obligatorios:
  - Auditor Jefe

En determinadas circunstancias, el Auditor Jefe puede ir en compañía de otros auditores que le ayuden a desempeñar su labor, por lo que también se podrá tener en cuenta la figura de: Auditor(es)

- Auditado

En algunos casos, puede haber participantes en formación:

- Observadores.
- Auditores en formación.

## Responsabilidades del auditor jefe

- Planificará y gestionará todas las fases de las auditorías.

- Utilizará eficazmente los recursos durante la auditoría.
- Será el representante del equipo auditor en las comunicaciones con el cliente (auditado).
- Gestionará y dirigirá a los miembros del equipo auditor, en el caso de disponer de auditores a su cargo.
- Proporcionará orientación a los auditores en formación.
- Obtendrá las conclusiones de la auditoría.
- Prevendrá y resolverá posibles conflictos.
- Realizará el informe de la auditoría.

#### Tareas del auditor

- Apoyará al auditor jefe en sus decisiones.
- Preparará listas de verificación (checklists) que estime oportunas, conforme a los elementos a auditar.
- Asistirá la reunión de inicio.
- Llevará a cabo las tareas que le asigne el Auditor jefe.
- Al igual que el Auditor Jefe, intentará respetar a los tiempos del plan de auditoría.
- Documentará todos los hallazgos encontrados durante la auditoría.
- Mantendrá informado al auditado.
- Ayudará al auditor jefe con el informe de auditoría.
- Mantendrá la confidencialidad en todo momento.

#### Habilidades y comportamientos de un auditor eficaz

Un auditor debe ser:

- Ético, es decir, imparcial, sincero, honesto y discreto.
- De mentalidad abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos.
- Diplomático, es decir, con tacto en las relaciones con las personas.
- Observador, es decir, activamente consciente del entorno físico y las actividades.
- Perceptivo, es decir, instintivamente consciente y capaz de entender las situaciones.

- Versátil, es decir, se adapta fácilmente a diferentes situaciones.
- Tenaz, es decir, persistente, orientado hacia el logro de los objetivos.
- Decidido, es decir, alcanza conclusiones oportunas basadas en el análisis y razonamiento lógicos.
- Seguro de sí mismo, es decir, actúa y funciona de forma independiente a la vez que se relaciona eficazmente con otros.