THE BRIDGE

CYBER SECURITY

Auditorias

Algunos conceptos

- **Auditoria:** Es un proceso exhaustivo que evalúa la seguridad de los sistemas de información y las infraestructuras tecnológicas de una organización. Su objetivo es identificar vulnerabilidades, asegurar el cumplimiento de normativas y estándares de seguridad, y recomendar mejoras para proteger los datos y sistemas contra amenazas cibernéticas.

- Un **hallazgo de auditoría** es el resultado de la evaluación de la evidencia recopilada durante una auditoría, comparada con los criterios establecidos. Estos hallazgos pueden ser positivos, indicando conformidad con las normas y estándares, o negativos, señalando desviaciones o áreas de mejora. Se clasifican generalmente en:

    - **Conformidad**
    - **No conformidad.**
    - **Observaciones**.
    - **Oportunidades de mejora.**
    - **Puntos fuertes.**

Tipos de Auditorias

En función del sujeto »

Según quien sea el organismo que las realiza, encontramos dos tipos de auditorías:

Auditoría interna »

Auditoría externa »

Además, en función del sujeto, hay otros dos tipos de auditoría:

- **Auditoría combinada**
  Es aquella en la que se audita conjuntamente a un único auditado en dos o más sistemas de gestión de distintas disciplinas integrados en un único sistema.

- **Auditoría conjunta**
  Es aquella llevada a cabo por dos o más organizaciones auditoras a un único auditado.

En función del objeto »

Tipos de Auditoria

En función del sujeto »

En función del objeto »

Si tenemos en cuenta el objeto de la auditoría, es decir, lo que va a ser auditado, podemos clasificar las auditorías en cuatro grupos:

- **Auditoría del sistema de gestión** »
- **Auditoría de proceso** »
- **Auditoría de producto** »
- **Auditoría de proveedores** »

Pasos para la Auditoria

Programación

La frecuencia con la que se realizarán las auditorías se establecerá en función del estado e importancia de los procesos y las áreas a auditar.

Auditores

La selección de auditores debe asegurar la objetividad e imparcialidad de la auditoría. Los auditores no deben auditar su propio trabajo.

Resultados

Se deben registrar y comunicar al personal que tenga responsabilidad en el área auditada.

Acciones correctivas

Cuando en la auditoría aparecen no conformidades, el personal responsable de las áreas auditadas tomará acciones correctivas lo antes posible.

Seguimiento de la Auditoría

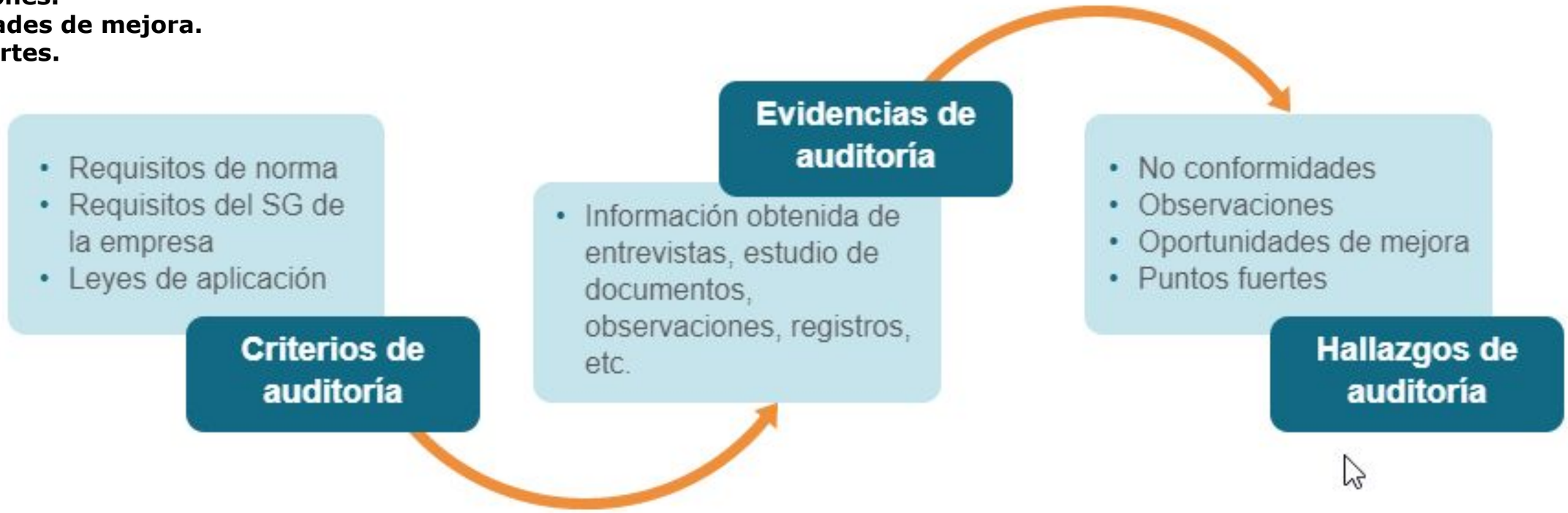
Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el informe de los resultados de la verificación.

Evidencia

- Durante la auditoria el auditor obtiene una serie de evidencias.

- Estas se evalúan frente a los criterios de autoría para determinar los hallazgos, clasificar cuales representan un incumplimiento de los requisitos específicos y son, por lo tanto, no conformidades, llegando así a la conclusión de la auditoria
  - **Criterios de auditoría**
  - **Evidencias de auditoría**
  - **Hallazgos de auditoría**

- Son los resultados de la evaluación de las evidencias frente a los criterios de auditoría. Los hallazgos pueden incluir:
  - **No conformidades.**
  - **Observaciones.**
  - **Oportunidades de mejora.**
  - **Puntos fuertes.**



Programar una auditoria

- El **programar una auditoría** implica una serie de pasos estructurados para asegurar que el proceso sea eficiente y efectivo. Aquí te detallo los pasos esenciales:
  - **Definir los objetivos de la auditoría**.
  - **Alcance.**
  - **La frecuencia**
    - Cambios importantes en la gestión
    - Organización
    - Políticas
    - Técnicas
    - Tecnologías
    - Cambios en el propio sistema
    - Resultados de auditorías anteriores.
    - Etc.
  - **Responsabilidades**.

Preparación de la auditoria

- Antes de su ejecución, cada auditoría incluida en el programa debe prepararse, desarrollando las siguientes actividades:
  - **La planificación:** Antes de realizar una auditoría, es crucial desarrollar un plan detallado que guíe todo el proceso. Este plan debe incluir los objetivos, el alcance, los criterios de auditoría, y los recursos necesarios.
  - **El estudio de la documentación:** Es fundamental revisar la documentación relevante, como manuales y procedimientos, para entender el sistema de gestión de la empresa y los procesos que serán auditados.
- Estas actividades anteriores a la realización de una auditoría son determinantes para el éxito de la misma.
- La planificación comienza con la elaboración de un plan de auditoría, que guiará el desarrollo de la auditoría.
- En esta etapa previa, también es útil que el auditor identifique la documentación relacionada, como manuales y procedimientos.
- De esta forma, el auditor obtiene información sobre el sistema de gestión de la empresa y los procesos a auditar.

Definición de los objetivos

- Los objetivos de la auditoría deben ser coherentes con el objetivo global del programa de auditoría y con el alcance describe la extensión y límites de la auditoría: actividades, procesos, ubicación, etc.

- Definición de la norma **ISO 19011**

  - **Alcance de la auditoría**

    - Extensión y límites de una auditoría

    - Esta incluye generalmente una descripción del tiempo físico y virtuales; funciones, unidades organizativas, actividades y procesos, así como los periodos de tiempo cubierto.

    - Una utilización virtuosa en línea que permite a las personas trabajar juntas o proporcionar un servicio utilizando un entorno en línea donde se organizan las realizas, independientemente de las ubicaciones físicas, ejecutar procesos.

Selección del Equipo Auditor

- La selección de los auditores debe realizarse teniendo en cuenta la competencia necesaria en la materia o en el proceso a auditar.
- La selección adecuada de los auditores es crucial para el éxito de la auditoría.
- Un auditor competente y objetivo puede identificar áreas de mejora y asegurar que la organización cumpla con las normativas y estándares aplicables.
- Además, un auditor independiente garantiza que los resultados de la auditoría sean confiables y creíbles.
- En el caso de que se forme un equipo auditor, deberá nombrarse al auditor líder o líder del equipo auditor, que se responsabilizará del proceso de auditoría y de las comunicaciones, tanto con el cliente como con el auditado.
- El auditor líder también se encarga de las comunicaciones con el cliente (la organización que solicita la auditoría) y con el auditado (la entidad o área que está siendo auditada).
- Esto incluye la presentación de los hallazgos y la discusión de las acciones correctivas necesarias.
- Si se designa un solo auditor, éste asumirá todas las responsabilidades.

Contacto Inicial con el Auditado

- El contacto inicial con el auditado es una etapa crucial en el proceso de auditoría. Este contacto se realiza antes de comenzar la auditoría propiamente dicha y tiene varios propósitos importantes:
  - **Establecer comunicaciones.**
  - **Confirmar la autoridad.**
  - **Proporcionar información.**
  - **Acceso a documentos**.
  - **Requisitos legales y contractuales.**
  - **Confidencialidad**.
  - **Preparativos logísticos.**
  - **Requisitos específicos.**
  - **Observadores y guías**.
  - **Áreas de interés**.

Plan de Auditoria

- **Objetivos y Alcance**: Definen qué se espera lograr con la auditoría, como evaluar la conformidad con normas específicas o mejorar procesos.
- **Criterios**: Son los estándares, políticas, procedimientos y requisitos contra los cuales se evaluarán las evidencias durante la auditoría.
- **Áreas de la organización**: Especifica las partes de la organización que serán revisadas, como departamentos, unidades de negocio o procesos.
- **Representante del auditado y personal**: Identifica a las personas clave dentro de la organización auditada que serán responsables de proporcionar información y colaborar durante la auditoría.
- **Documentos de referencia:** Incluye todos los documentos que se utilizarán como referencia durante la auditoría, como normas ISO, manuales de procedimientos y políticas internas.
- **Identificación de los miembros del equipo auditor: D**etalla quiénes son los auditores, sus roles específicos y las responsabilidades.
- **Idioma:** El idioma en el que se llevará a cabo la auditoría, lo cual es importante en organizaciones multinacionales o con equipos diversos.
- **Fechas y lugares:** Indica cuándo y dónde se realizarán las actividades de auditoría, permitiendo una planificación adecuada.
- **Horario y duración:** Proporciona un cronograma detallado de las actividades de auditoría, incluyendo la duración estimada de cada una.
- **Recursos**: Enumera los recursos logísticos necesarios para llevar a cabo la auditoría, como salas de reuniones, equipos y transporte.
- **Calendario de las reuniones**: Planifica las reuniones con la dirección de la organización auditada para discutir los hallazgos y las recomendaciones.
- **Requisitos de confidencialidad**: Establece cómo se manejará la información confidencial durante y después de la auditoría para proteger la privacidad y los datos sensibles.
- **Lista de distribución del informe**: Define quiénes recibirán el informe final de la auditoría y cuándo se espera que se emita.

Preparación de la auditoria

- **Revisión Documental**
  - Auditorías internas
    - Los documentos aplicables según el alcance de la auditoría (manual, procedimientos, instrucciones, etc.).
    - Informes de auditorías anteriores.

  - Auditorías externas
    - Datos referentes a la estructura y organización de la empresa.
    - Número de empleados.
    - Documentos generales del sistema.
    - Número y ubicación de los emplazamientos.
    - Legislación aplicable al sector de actividad.
    - Normas de referencia.

- **Lista de comparación o checklist**

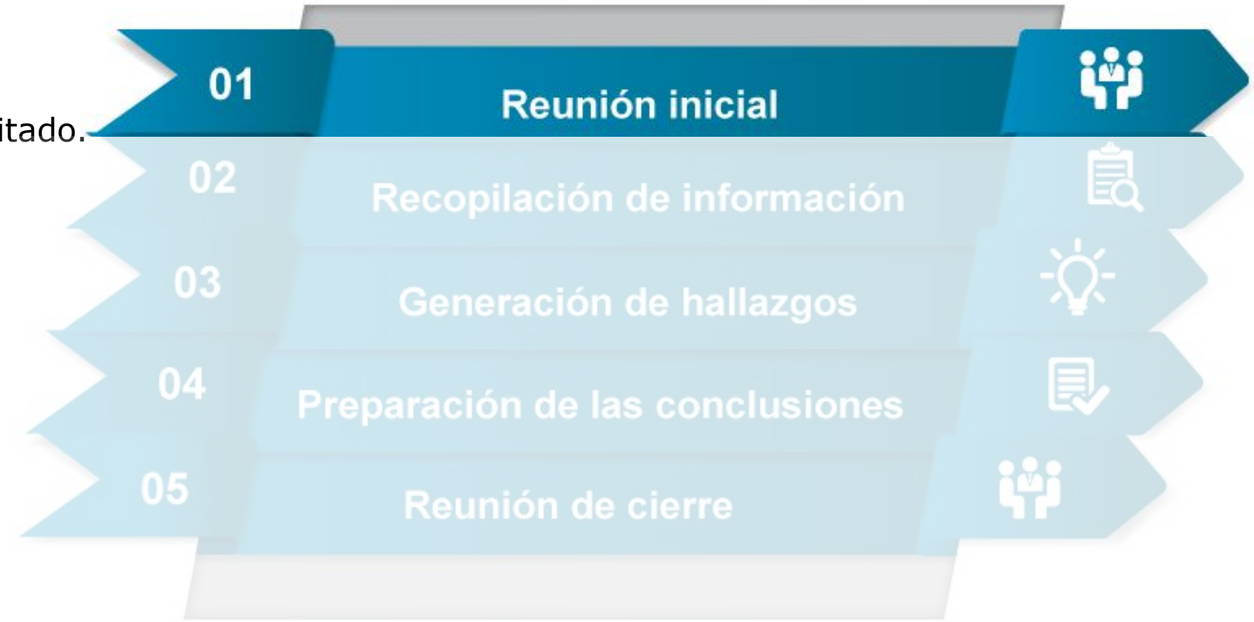
  - Si las listas de comprobación no se preparan de forma personalizada, su uso presenta un inconveniente importante; si el auditor se ciñe excesivamente al contenido de la lista y no hace otras preguntas en el transcurso de la auditoría, puede perder la oportunidad de obtener más información.

  - Cuando no se conoce bien la empresa, las listas de chequeo suelen prepararse con una visión parcial proporcionada por los documentos de referencia revisados previamente y su utilidad es limitada.

  - En estos casos, es habitual obtener información adicional durante el desarrollo de la auditoría.

Realización de la Auditoria

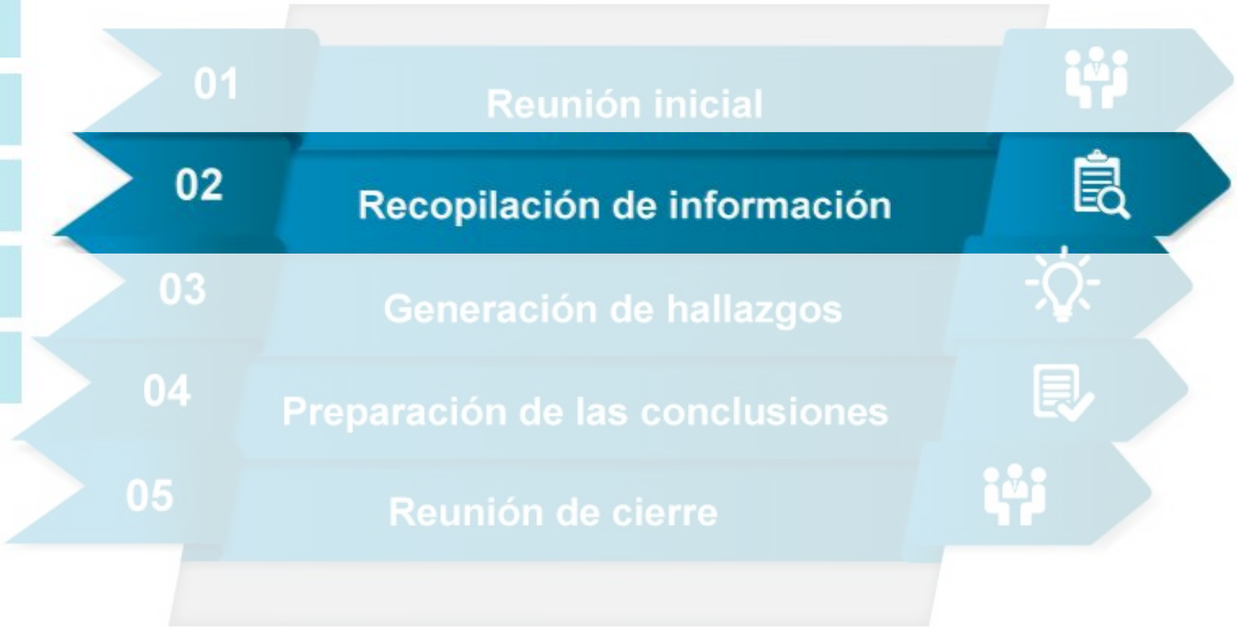
- El orden del día para una reunión inicial puede ser el siguiente:
  - El auditor líder presenta a su equipo.
  - Las personas de la empresa que asisten a la reunión se presentan y pueden presentar la empresa.
  - Se recuerda el objeto y el alcance de la auditoría. Por ejemplo, en una auditoría de certificación, se establece que el propósito es confirmar la capacidad de la empresa para satisfacer los requisitos de la norma de referencia, dentro del alcance acordado previamente.
  - Se confirma que el plan de auditoría es adecuado y se puede cumplir.
  - Se designa a las personas de la empresa que van a acompañar al equipo auditor.
  - Disponibilidad de los recursos requeridos (salas, facilidades, equipos de seguridad, ropa de protección, etc.).
  - Resumen de los métodos y procedimientos que se van a utilizar.
  - Establece la forma de comunicación entre el equipo auditor y el auditado.
  - Confirma la fecha y hora para la reunión final y cualquier reunión
  - Se asegura la confidencialidad de todos los datos.
  - La empresa pregunta a los auditores para resolver dudas.
  - Se cierra la reunión para comenzar la auditoría.



Realización de la Auditoria

Para obtener la información, el auditor puede utilizar diferentes métodos de "rastreo".

De lo general a lo particular	De procedimiento a registro específico
De lo particular a lo general	De registro a procedimiento
Seguimiento horizontal	Requisitos que tienen aplicación en todo el ámbito del sistema
Seguimiento vertical	Requisitos cuya aplicación se lleva a cabo en un proceso específico
Seguimiento cronológico	Requisitos cuya aplicación se lleva a cabo secuencialmente dentro de las actividades de gestión
Documentales	Documentos, registros
Físicas	Material, mercancía, equipo
Testimoniales	Declaraciones
Circunstanciales	Situaciones surgidas en el transcurso de la auditoría

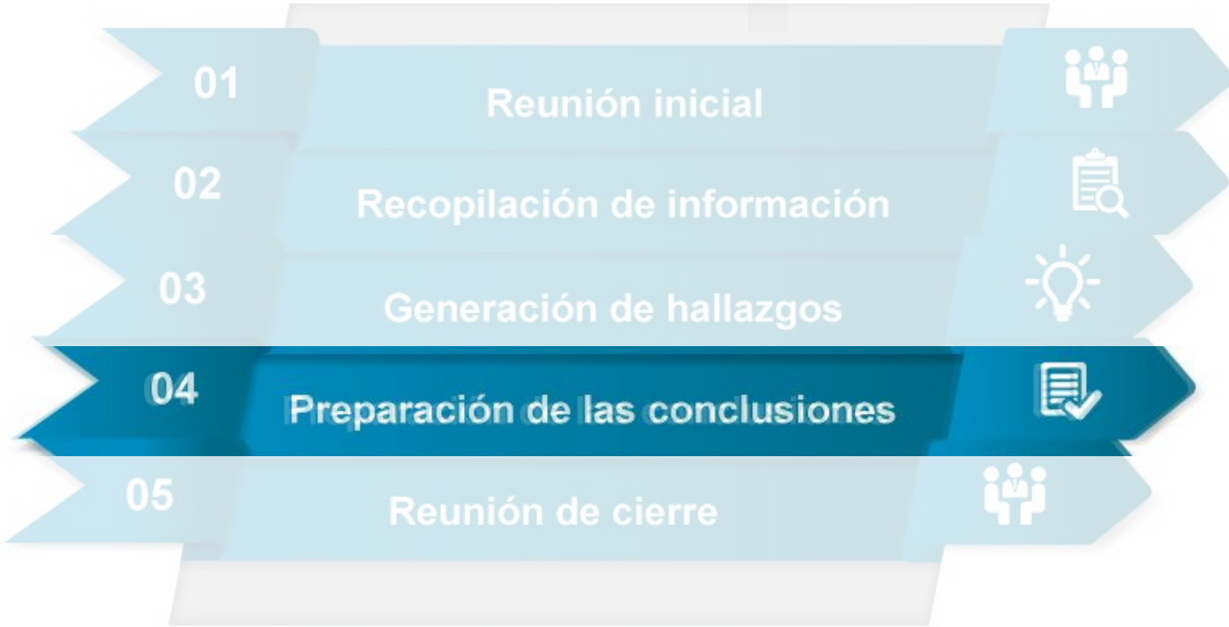


Realización de la Auditoria

- El resultado de la evaluación de las evidencias frente a los criterios de auditoria genera los **hallazgos**
- Como resultado de esta evaluación, el auditor
  - Emite un juicio positivo si todas las comprobaciones son positivas
  - Puede emitir un juicio positivo si una sola de las comprobaciones son negativas
  - Emite juicio negativo en todos los otros casos
  - Puede repetir el muestreo en casos particulares
- Los **hallazgos** de la auditoria pueden indicar tanto **conformidad** como **no conformidad** con los criterios de auditoria.
- Si así se especifica, los hallazgos pueden también identificar **oportunidades de mejora**.

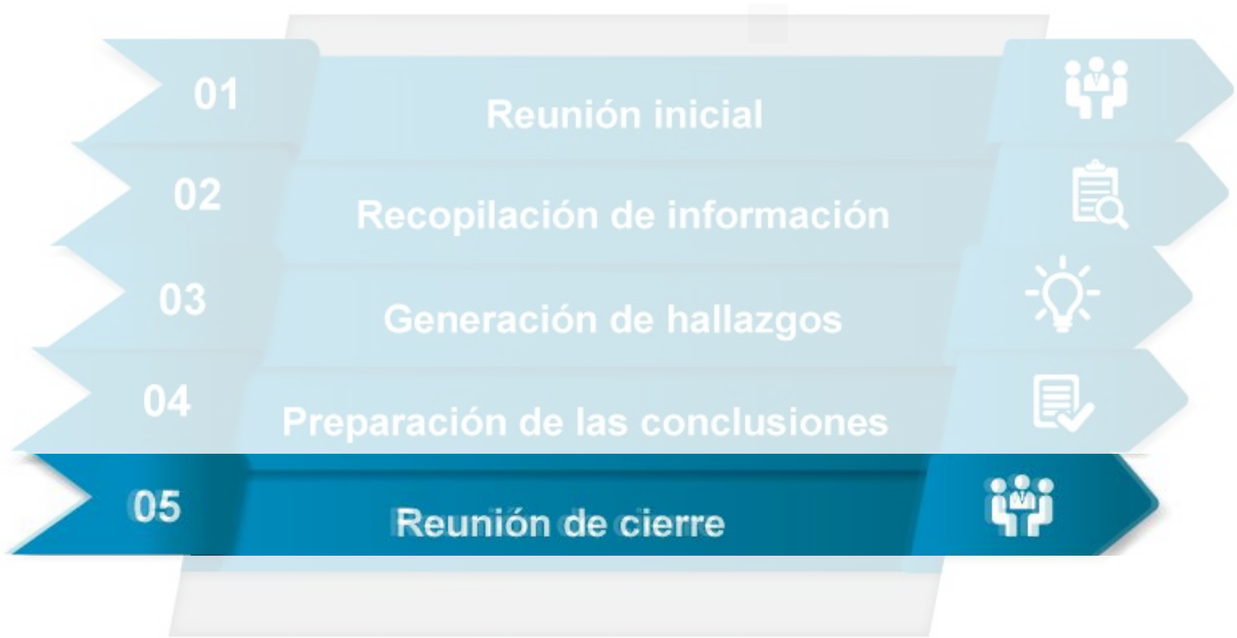
Realización de la Auditoria

- Seguir el plan de auditoría, desviándose únicamente por razones justificadas aceptables, anotando todo lo que se observe durante la auditoría, números de referencia, fechas, equipos, etc.
- Escribir detalles específicos que puedan comprobar tanto deficiencias como situaciones aceptables.
- Verificar la información obtenida a través de las entrevistas con otras fuentes independientes como la observación física y medición y los registros del auditado.
- Ante un **incumplimiento**, no darlo por cierto o efectivo al momento analizando otras muestras.
- Comprobar con normas comparativas detectadas en auditorías anteriores.
- Las conclusiones deben presentarse de forma que sean comprendidas por el auditado.
- Los auditados, en esta reunión, pueden expresar sus discrepancias, presentar otras pruebas, etc.
- El equipo auditor debe tratar de alcanzar el consenso.
- Teniendo en cuenta que la mayor parte de las no conformidades se han puesto de manifiesto durante el transcurso de la auditoría, el acuerdo debería obtenerse pronto.
- Si no fuera así, se tomará nota de las diferencias.



Realización de la Auditoria

- El informe puede contener, según los casos, los siguientes elementos:
  - Objetivo y alcance de la auditoría.
  - Detalle del plan de la auditoría, identificación de los miembros del equipo auditor y de los representantes del auditado, fechas de la auditoría e identificación de procesos o unidades específicas auditadas.
  - Identificación de los criterios frente a los cuales se ha realizado la auditoría (norma, manual, etc.).
  - Resumen de la auditoría.
  - Relación de las no conformidades detectadas.
  - Apreciación del equipo auditor sobre el grado de conformidad del sistema de gestión de la calidad del auditado.
  - Opiniones divergentes entre auditor y auditado que no hayan podido resolverse.
  - Recomendaciones para la mejora.
  - Seguimiento acordado.
  - Declaraciones de confidencialidad.
  - Plazo y lista de distribución del informe de auditoría.
- Se presenta el Informe con los acuerdos y hallazgos al auditado.
- La auditoría se da por finalizada con la aceptación de ambas partes.



Plan de Actuación Correctiva (PAC)

- Una vez finalizada la auditoría, la organización auditada analizará las conclusiones de la auditoría para definir y llevar a cabo las acciones oportunas en el plazo acordado.
- Estas acciones deberán planificarse, estableciendo responsables, plazos y recursos para su implantación.
- Asimismo, se verificará si las acciones se completan y si son eficaces.

1 CORRECCIÓN DE LA NO CONFORMIDAD

En caso de que sea posible reparar o corregir la no conformidad el cliente indicará la acción que va a llevar a cabo. Si no fuese posible establecer acción alguna para corregir la no conformidad se indicará como no aplicable (N/A). Para corregir una no conformidad no es necesario conocer la causa de la misma.

Este apartado no siempre deberá estar cumplimentado:

Ejemplo: *Un registro de autocontrol correspondiente al periodo reflejado en la no conformidad, ya no tiene sentido rellenarlo.*

Sin embargo se cumplimentará cuando pueda solucionarse el problema: *Si se ha detectado uno o varios documentos no controlados, pueden ser sometidos a control, por ejemplo, codificándolos, revisándolos y aprobándolos.*

2 CAUSA DE LA NO CONFORMIDAD

Se indicará el resultado de la investigación de los motivos (causas) que provocaron la no conformidad. La investigación debe ser tal que permita identificar la causa o causas raíz que ha provocado dicha situación.

Una herramienta sencilla para profundizar en la causa de una no conformidad es la técnica conocida como el por qué del por qué.

Ejemplo: *¿Por qué no se han registrado los autocontroles?*

Porque el operario no había recibido la formación necesaria (falta de conocimiento)

¿Por qué el operario no había recibido la formación necesaria?.

Porque cuando se dio la formación correspondiente a la cumplimentación del nuevo formato de registro de autocontrol, el operario estaba de baja.

Como el siguiente ¿por qué? nos daría información sobre la causa de la baja del operario, que no tiene porqué tener relación con la causa de la no conformidad, podemos terminar en este punto con la secuencia de los "¿por qué ...?". Si no fuese así, deberíamos continuar dicha secuencia.

3 MAGNITUD DE LA NO CONFORMIDAD

Para poder dimensionar adecuadamente la acción correctiva, conviene conocer si la no conformidad es ocasional o repetitiva así como la amplitud o envergadura de la misma.

En el ejemplo anterior, *la magnitud podría ser considera como repetitiva, ya que el mismo caso podría darse con empleados de vacaciones, de viaje...*

4 ACCIÓN CORRECTIVA

Se indicará la acción o acciones que se van a emprender para **eliminar la causa y, de este modo, evitar que el problema vuelva a ocurrir.** Una vez conocidas la causa y la magnitud de la no conformidad puede establecerse una acción correctiva proporcional al problema detectado.

Continuando con el ejemplo, *una acción apropiada podría ser: "Una vez realizada una acción formativa, el responsable de la formación comparará la lista de los asistentes con la de los convocados y en caso de que alguna persona no haya recibido la formación, se programará de nuevo la acción formativa". Se revisará el procedimiento de formación para incluir esta circunstancia.*

5 FECHA Y RESPONSABLE DE LA IMPLANTACIÓN

Se indicará bien el plazo o periodo de implantación, así como el responsable.

Fecha de implantación 10 de septiembre
Propietario del proceso de gestión de RRHH G. García

6 EVIDENCIAS DOCUMENTALES Y/O REGISTROS

Se indicarán los documentos y/o registros que se hayan generado como consecuencia de las acciones correctivas establecidas.

7 REVISIÓN / VALORACIÓN DE LAS ACCIONES CORRECTIVAS IMPLANTADAS

Una vez implantadas las acciones correctivas, la organización llevará a cabo una revisión de las mismas para valorar los resultados, dejando constancia de la fecha, responsable y conclusiones.

El responsable correspondiente analizará si las acciones correctivas implantadas han eliminado la causa o causas origen de la no conformidad y si se evita su repetición. Se dejará constancia de las conclusiones a las que se ha llegado así como el responsable que la ha realizado y fecha.


THE
BRIDGE