Centro de Especializaciones Noeder

Diplomado

IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

CICLO INTENSIVO

MÓDULO V

FORMACIÓN DE AUDITOR INTERNO ISO 27001 E ISO 22301 (PARTE I)

Mg. Ing. Julio Pereyra Rosales

1. ALCANCE DE LOS SISTEMAS DE GESTIÓN

La normas 22301:2019 / ISO 27001:2022 en el apartado **9.2 Auditoría Interna** , se establece:

La organización debe realizar auditorias internas a intervalos planificados, para determinar si:

Ha sido apropiadamente implementado y mantenido.

Cumplen los requisitos especificados, incluyendo los requisitos de la norma internacional, la legislación pertinente y/o regulaciones vigentes.

- La norma ISO19011:2018, es nuestra base de auditorías de todo sistema de gestión.
- Se debería definir un procedimiento documentado, en donde se establezcan los criterios, alcance, la frecuencia y los métodos de la auditoria

2. TÉRMINOS Y DEFINICIONES DE AUDITORÍA

Internas

Externas

Primera parte	Segunda parte	Tercera parte
• Auditores de la propia organización evalúan su propio sistema de gestión.	• Auditoría en la que un cliente audita a un proveedor ó proveedor potencial para dictaminar la capacidad de cumplir las condiciones contractuales.	• Auditorías realizadas por organizaciones auditoras independientes, tales como autoridades reglamentarias o aquellas que proporcionan la certificación.

2. TÉRMINOS Y DEFINICIONES DE AUDITORÍA

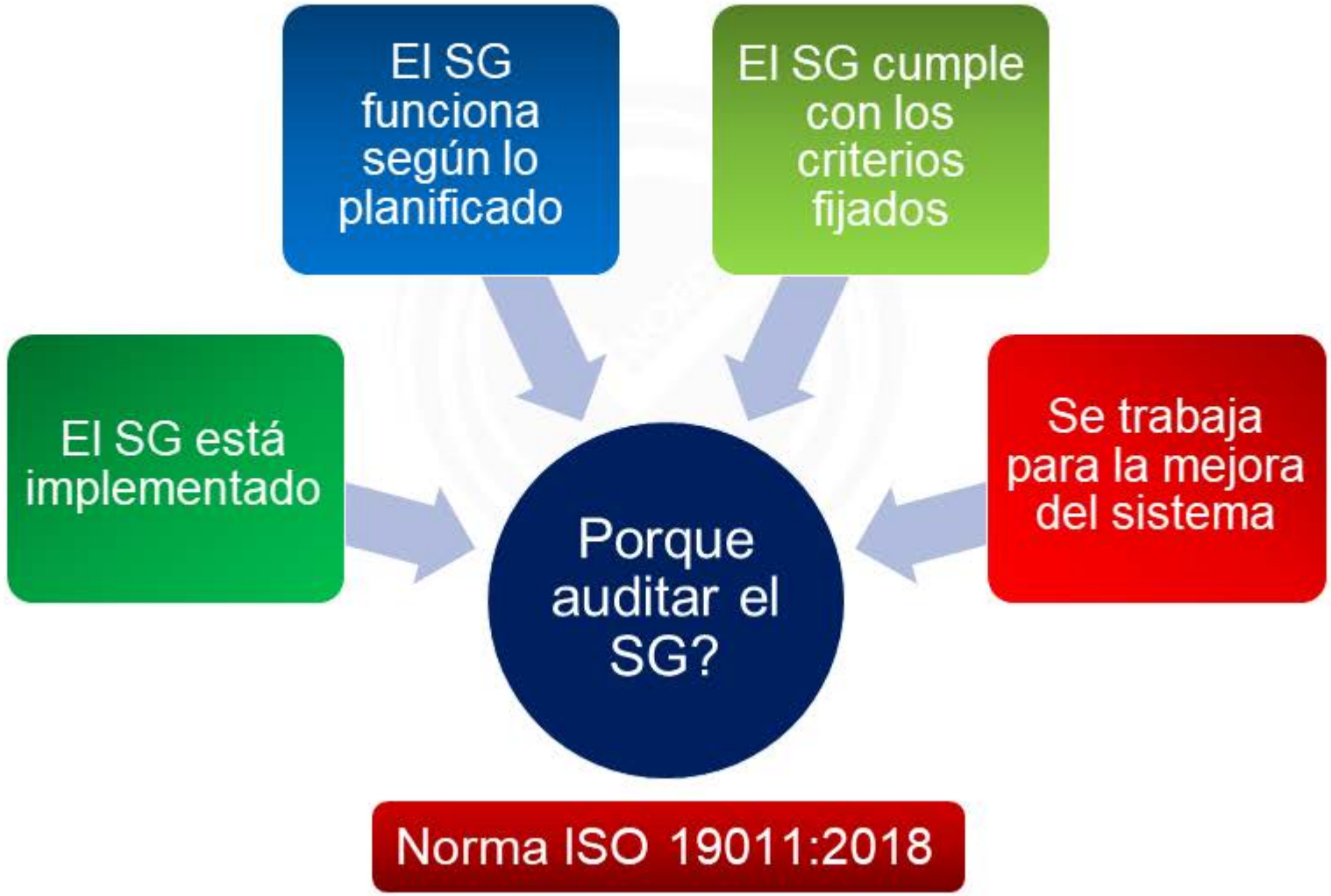
Combinadas

- Cuando se auditan juntos, por ejemplo, un sistema de gestión de la calidad, SGCN y un sistema de gestión ambiental.

Conjuntas

- Cuando dos o más organizaciones cooperan para auditar a un único auditado.

3. OBJETIVO DE LA AUDITORÍA



4. BENEFICIOS DE LAS AUDITORIAS DE SISTEMAS DE GESTIÓN

- Verificar el cumplimiento de requisitos.
- Comprobar que información documentada es aplicable y aplicada.
- Determinar oportunidades de mejora.
- Detectar necesidades de capacitación.
- Analizar la eficacia de las comunicaciones.
- Identificar causas de no conformidades.
- Proveer información para la mejora continua.

5. PRINCIPIOS DE AUDITORÍA

Integridad

- Realizar la auditoría de forma ética, con honestidad y responsabilidad.
- Sólo realizar actividades de auditoría si es competente para hacerlo.
- Realizar la auditoría de manera imparcial.
- Ser sensible a cualquier influencia que pueda ejercer sobre su juicio mientras lleva a cabo una auditoría.

Presentación Razonable

- Los hallazgos de la auditoría, las conclusiones de auditoría y los informes de auditoría deberían reflejar de manera veraz y precisa las actividades de auditoría.
- La comunicación es veraz, precisa, objetiva, oportuna, clara y completa.

5. PRINCIPIOS DE AUDITORÍA

Los auditores deben tener el debido cuidado de acuerdo con la importancia de la tarea que realizan y la confianza depositada en ellos por el cliente de auditoría y otras partes interesadas.

Los auditores ejercen discreción en el uso y la protección de la información adquirida en el desempeño de sus funciones.

5. PRINCIPIOS DE AUDITORÍA

Independencia

Los auditores debe ser independiente de la actividad auditada siempre que sea posible y, en todos los casos, deberían actuar de forma tal que no estén sujetos a prejuicios ni a conflictos de intereses.

Enfoque en el Riesgo

El enfoque basado en el riesgo influye sustancialmente en la planificación, conducción y presentación de informes de las auditorías para garantizar que las auditorías se centren en asuntos que son importantes para el cliente de auditoría y para lograr los objetivos del programa de auditoría.

5. PRINCIPIOS DE AUDITORÍA

Enfoque basado en evidencia.

- La evidencia de auditoría es verificable.
- En general, se basa en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un tiempo finito y con recursos limitados.
- Se debería aplicar un uso apropiado del muestreo, ya que está estrechamente relacionado con la confianza que se puede depositar en las conclusiones de la auditoría.

6. GESTIÓN DEL RIESGO

- Auditor no competente.
- No se cumpla con el programa de auditoría.
- El personal auditado no se presenta a tiempo en la auditoría.
- No existe una clara determinación de los objetivos de la auditoría.
- Demora en la entrega de los informes de auditoría.
- El personal designado (trabajo remoto / teletrabajo) se encuentran expuestos a riesgo operativos no identificados y vulnerables.

7. PROGRAMA DE AUDITORÍA

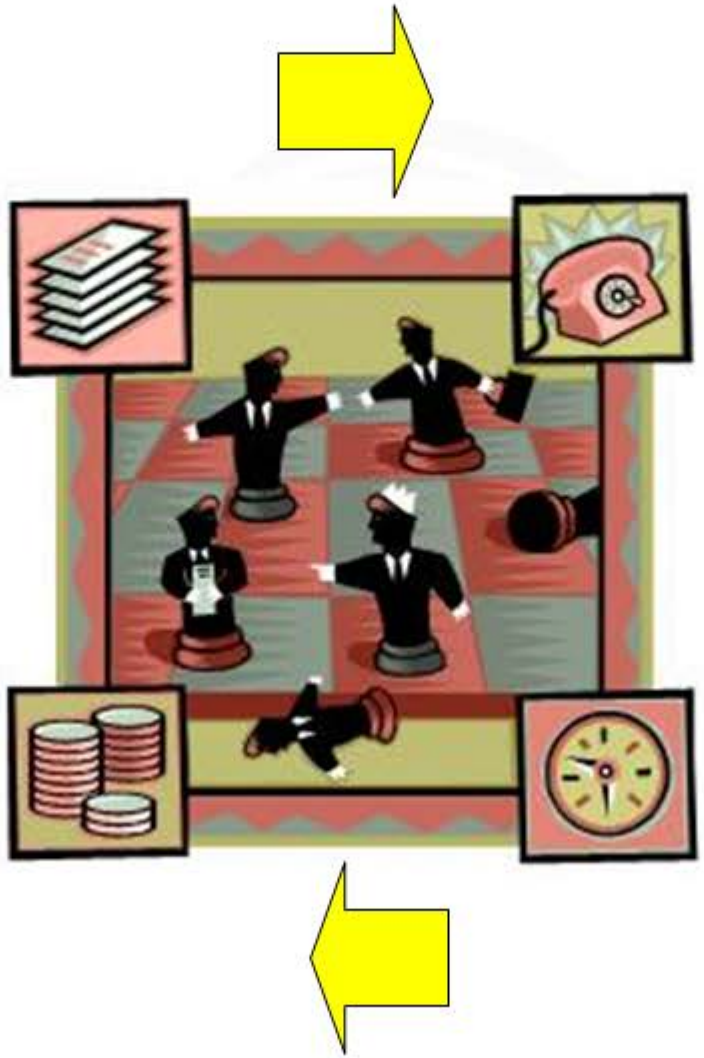
PLANEAR

Preparación de la auditoria:

Programa
Funciones
Competencias
Riesgos
Procedimiento
Recursos

HACER

Revisión Doc Plan
Doc. Trabajo
Eq. Auditor
Audit Campo
(Incl. Informe)



VERIFICAR

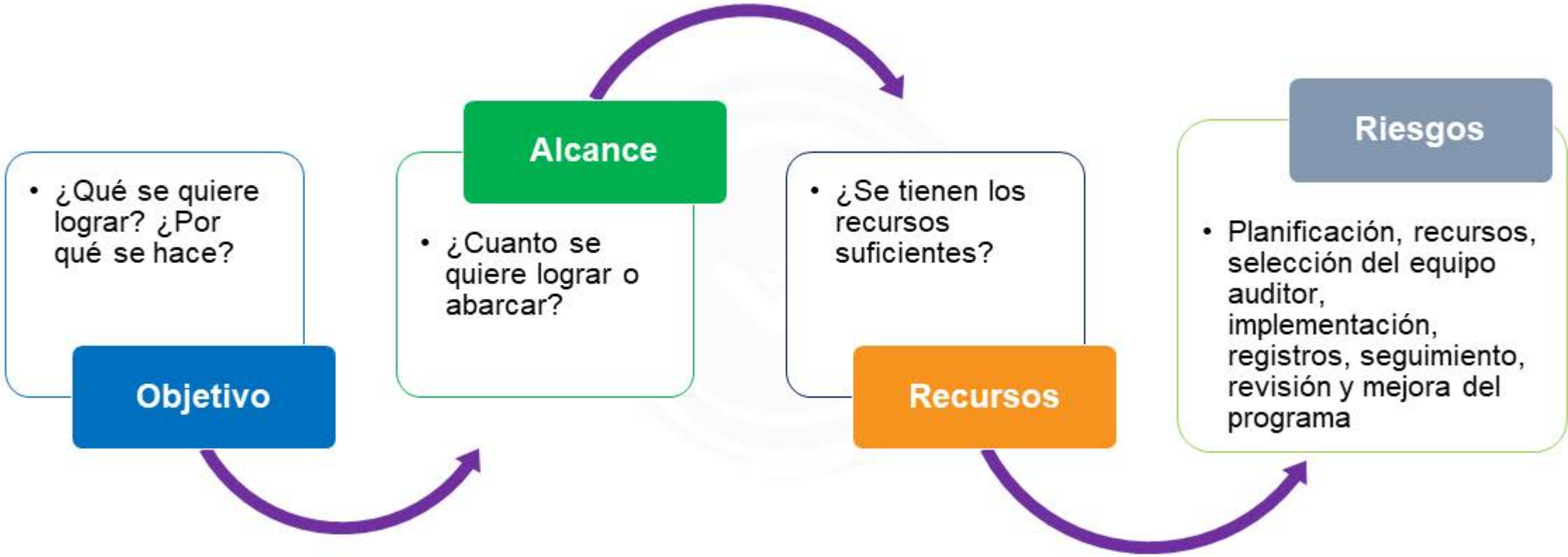
Seguimiento y revisión de resultados del Programa de auditoria

ACTUAR

Acciones de mejora del Programa

RESULTADOS

7. PROGRAMA DE AUDITORÍA



7. PROGRAMA DE AUDITORÍA

Actividades específicas de Auditoría

1. Inicio de la auditoría
2. Preparación de las actividades
3. Realización de las actividades de la auditoría
4. Preparación y distribución del informe de auditoría
5. Finalización de la auditoría
6. Actividades de seguimiento

7. PROGRAMA DE AUDITORÍA

Actividades de Auditoría

Inicio de la auditoría

Responsabilidad del equipo auditor

Establecer los contactos iniciales con el auditado

Determinar la viabilidad de la auditoría

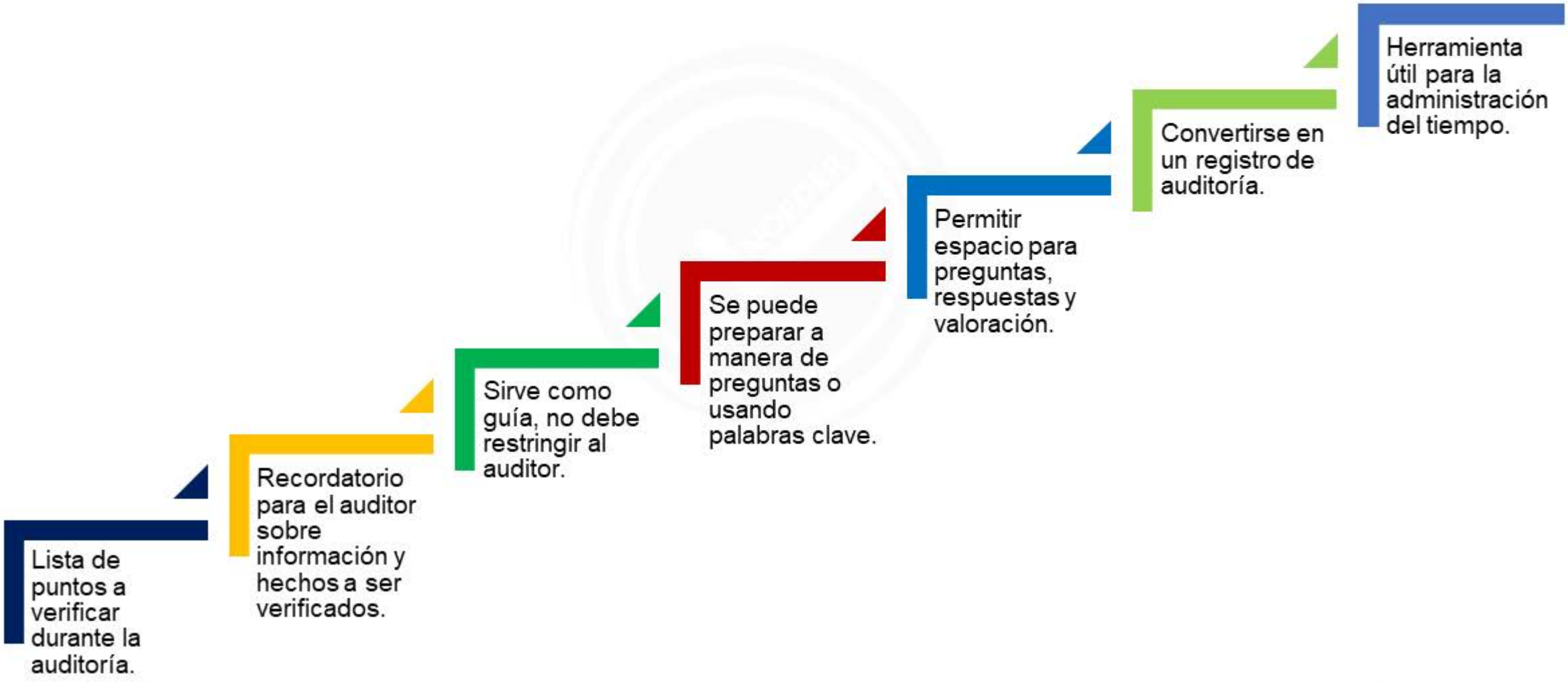
7. PROGRAMA DE AUDITORÍA

Plan de Auditoría

- Contenido recomendado por la ISO 19011
- Asignación de funciones entre los integrantes del equipo
- Envío previo para su revisión por el auditado
- Herramienta útil para la administración del tiempo

7. PROGRAMA DE AUDITORÍA

Lista de Verificación



8. EJECUCIÓN DE LA AUDITORÍA

1. Reunión de apertura
2. Revisión de la documentación durante la auditoría
3. Comunicación durante la auditoría
4. Funciones y responsabilidades de los guías y observadores
5. Recolección y verificación de la información
6. Generación de hallazgos de auditoría
7. Preparación de las conclusiones de la auditoría
8. Reunión de cierre

8. EJECUCIÓN DE LA AUDITORÍA

Cómo conducir la auditoría

Una guía para auditar:

Pregunte

Cuestionamientos para obtener información

Observe

Lo que se esta haciendo

Registre

Evidencia objetiva comparada con los criterios de auditoria

Verifique

La disponibilidad de información documentada, toma de conciencia del auditado, consistencia, eficacia

8. EJECUCIÓN DE LA AUDITORÍA

"Lenguajes" de una organización

Control de riesgos, desempeño y tecnología.

Medidas de control operacional, respuesta ante emergencias.

Desempeño y evaluación de cumplimiento.

Elaboración del producto o prestación del servicio, planificación y control operacional, organización técnica.

8. EJECUCIÓN DE LA AUDITORÍA

Tipo de preguntas

- Comenzar con preguntas abiertas
- Emplear preguntas cerradas ante la necesidad de confirmar datos
- No utilizar las preguntas inductivas
- Emplear preguntas con alternativas solo en caso de dilaciones, y siempre en base a información aportada por el entrevistado

9. DETECCIÓN DE HALLAZGOS

Definiciones

Evidencias	• Información verificable objetivamente que permita determinar si el sistema se ajusta a los criterios o valores previamente fijados.
Criterios de auditoría	• Políticas, prácticas, información documentada o requisitos frente a los cuales el auditor compara las evidencias recogidas.
Hallazgos	• Resultados de la evaluación de las evidencias de la auditoría frente a los criterios de la auditoría.

9. DETECCIÓN DE HALLAZGOS

9. DETECCIÓN DE HALLAZGOS

No Conformidad N° 1 - SGSI

1. Incumplimiento :
No se evidencia que la organización haya evaluado los riesgos de seguridad de la información a intervalos planificados.

2. Evidencia :
De acuerdo con el procedimiento PRO-SGSI-002 Evaluación de riesgos de seguridad de la información se ha identificado en el acápite N.º 2 inciso c, que la evaluacion de riesgos se realiza como mínimo una vez al año. De acuerdo a la revisión realizada, se consigna como última evaluación de riesgos en el mes de marzo 2023.

3. Requisito : 8.2 Evaluación de los riesgos de la seguridad de la información (ISO 27001:2022)

9. DETECCIÓN DE HALLAZGOS

No Conformidad N° 2 - SGCN

1. Incumplimiento :
No se ha seleccionado las estrategias para la continuidad del negocio en base a la evaluación de riesgos.

2. Evidencia :
De acuerdo con el REG-SGCN-001 Evaluación de Riesgos del Negocio se ha identificado:

Proceso: Almacén
- Riesgo : No contar el stock disponible
- Estrategias: Inventarios semanales, análisis de stock, procedimiento de almacenamiento y distribución, adquisicion de nuevos equipos de transporte
- Selección de estrategias: No se evidencia los criterios de selección de dichas estrategias.

Proceso: Operaciones
- Riesgo : Generación de mermas en planta.
- Estrategias: Análisis y balance de materia prima, control de materias primeras, rediseño del flujo de proceso, mantenimiento predictivo de maquinaria.
- Selección de estrategias: No se evidencia los criterios de selección de dichas estrategias.

Proceso :Recursos Humanos
- Riesgo : No seleccionar oportunamente a postulantes para puestos clave.
- Estrategias: Contratación de headhunter especializado, procedimiento de reclutamiento y selección, plataforma digital de trackeo de perfiles de postulantes
- Selección de estrategias: No se evidencia los criterios de selección de dichas estrategias.

3. REQUISITO : 8.3.1. Generalidades (ISO 22301:2019) (OTROS)

9. DETECCIÓN DE HALLAZGOS

Oportunidad de mejora

Oportunidad de mejora N° 1 (proceso : SGCN / SGSI) :
Revisar la conveniencia de actualizar las metas porcentuales, que permanentemente se están cumpliendo, asociadas a los indicadores de gestión del SGCN / SGSI.

Oportunidad de mejora N° 2 (proceso : Gestión de riesgos) :
Revisar la conveniencia de implementar un sistema de información , que reduzca los tiempos de consolidación de datos en el proceso de detección de riesgos.

Oportunidad de mejora N° 3 (proceso : Gestión Legal):
Revisar la conveniencia de determinar el tiempo de comunicación de normas legales relacionados al SGCN / SGSI.

10. ERRORES DE DOCUMENTACIÓN

EVITE CITAR:

- **Algunos** ….. Equipos están con certificado de calibración
- **Muchos** …… Registros no tienen los resultados de …
- **Pocos …….** Auditores no tienen la independencia
- **Casi todos ….** Los contratos están vencidos
- **Varios ….** Reclamos muestran despachos tardíos
- **Ciertos …** Operarios desconocen donde están los instructivos

11. REUNIÓN DE CIERRE

Propósito: Presentar resultados mas relevantes y aclarar dudas.

Contenido:

- Agradecer al auditado y su organización por su cooperación.
- Resumir brevemente el alcance de la auditoría.
- Aclarar el objetivo y la razón de la auditoría.
- Nueva presentación del equipo de auditores.
- Aclarar que se reportan las no conformidades y no todo lo que está conforme.

12. INFORME DE AUDITORÍA

Índice

1. Objetivo y alcance de auditoria.
2. Cliente de auditoria.
3. Equipo de auditoría y auditados.
4. Fecha y lugares de las actividades.
5. Criterios de auditoria.
6. Hallazgo de auditoria y evidencias.
7. Conclusiones de la auditoria.
8. Declaración del grado de cumplimiento de los criterios.
9. Opiniones divergentes no resueltas.
10. Riesgo que la evidencia no sea representative.

13. COMPETENCIAS DEL AUDITOR

1. ETICO
2. MENTE ABIERTA
3. DIPLOMÁTICO
4. PERCEPTIVO
5. OBSERVADOR
6. VERSÁTIL

7. TENAZ
8. DECIDIDO
9. SEGURO DE SI MISMO
10. CON VALOR MORAL
11. ABIERTO A LA MEJORA
12. CULTURA ABIERTA

13. COLABORADOR

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón