certiprof®

ISO 22301 LEAD AUDITOR/ INTERNAL AUDITOR

PROFESSIONAL CERTIFICATION

I22301IA-LA™ Versión 092020

ISO 22301
INTERNAL AUDITOR / LEAD AUDITOR
(I22301IA/LA)

I22301IA-LA™ Versión 092020

¿Quién es Certiprof®?

Certiprof® es una entidad certificadora fundada en los Estados Unidos en 2015, ubicada actualmente en Sunrise, Florida.

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **Nuestros Lifelong Learners (LLL)** se identifican como Aprendices Continuos, lo que demuestra su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digital en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen.
- Las universidades, centros de formación, y facilitadores en todo el mundo forman parte de nuestra red de aliados **CPLS (Certified Partner For Learning Solutions).**
- **Los autores (co-creadores)** son expertos de la industria o practicantes que, con su conocimiento, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria.
- **Personal Interno:** Nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos está a cargo de superar obstáculos, encontrar soluciones y entregar resultados excepcionales.

Nuestras Afiliaciones

Memberships

Digital badges issued by

IT Certification Council – ITCC

Certiprof® es un miembro activo de ITCC.

Una de las ventajas de hacer parte del ITCC es como líderes del sector colaboran entre sí en un formato abierto para explorar maneras nuevas o diferentes formas de hacer negocios que inspiran y fomentan la innovación, estableciendo y compartiendo buenas prácticas que nos permiten extender ese conocimiento a nuestra comunidad.

Certiprof ha contribuido a la elaboración de documentos blancos en el Career Path Ways Taskforce, un grupo de trabajo que se implementó internamente para ofrecer a los estudiantes la oportunidad de saber qué camino tomar después de una certificación.

Algunos de los miembros del ITCC

- **IBM**
- **CISCO**
- **ADOBE**
- **AWS**
- **SAP**
- **GOOGLE**
- **ISACA**

Agile Alliance

Certiprof® es un miembro corporativo de Agile Alliance.

Al unirnos al programa corporativo Agile Alliance, continuamos empoderando a las personas ayudándolas a alcanzar su potencial a través de la educación. Cada día, brindamos más herramientas y recursos que permiten a nuestros socios formar profesionales que buscan mejorar su desarrollo profesional y sus habilidades.

https://www.agilealliance.org/organizations/certiprof/

Credly

Esta alianza permite que las personas y empresas certificadas con Certiprof® cuenten con una distinción a nivel mundial a través de un distintivo digital.

Credly es el emisor de insignias más importante del mundo y empresas líderes en tecnología como IBM, Microsoft, PMI,Nokia, la Universidad de Stanford, entre otras, emiten sus insignias con Credly.

Empresas que emiten insignias de validación de conocimiento con Credly:

- **IBM**
- **Microsoft**
- **PMI**
- **Universidad de Stanford**
- **Certiprof**

Insignias Digitales

Insignias Digitales:
¿Qué Son?

Según el estudio del IT Certification Council (ITCC), años atrás, la gente sabía muy poco sobre las insignias digitales. Hoy, grandes empresas e instituciones educativas de todo el mundo expiden insignias.

Las insignias digitales contienen metadatos detallados sobre quién las ha obtenido, las competencias requeridas y la organización que las ha expedido. Algunas insignias incluso están vinculadas a las actividades necesarias para obtenerlas.

Para las empresas e instituciones educativas, las insignias y la información que proporcionan son tan importantes que muchas decisiones, como las de contratación o admisión, se basan en los datos que aportan.

¿Por qué son importantes?

- **Facilidad de Compartir y Verificar Logros:**

  Las insignias digitales permiten a los profesionales mostrar y verificar sus logros de manera instantánea y global. Según un informe de Credly, **los perfiles de LinkedIn con insignias digitales reciben un 40% más de atención por parte de reclutadores y empleadores.**

- **Visibilidad en Plataformas Digitales:**

  En una encuesta realizada por Pearson y Credly, el **85%** de los usuarios que obtuvieron insignias digitales **las compartieron en LinkedIn,** y el **75%** reportó que esto mejoró su **credibilidad profesional en sus redes.** Además, el **76%** de los empleadores encuestados afirmó que las insignias digitales les ayudan a identificar rápidamente habilidades específicas.

¿Por qué son importantes?

- **Impacto en la Contratación:**

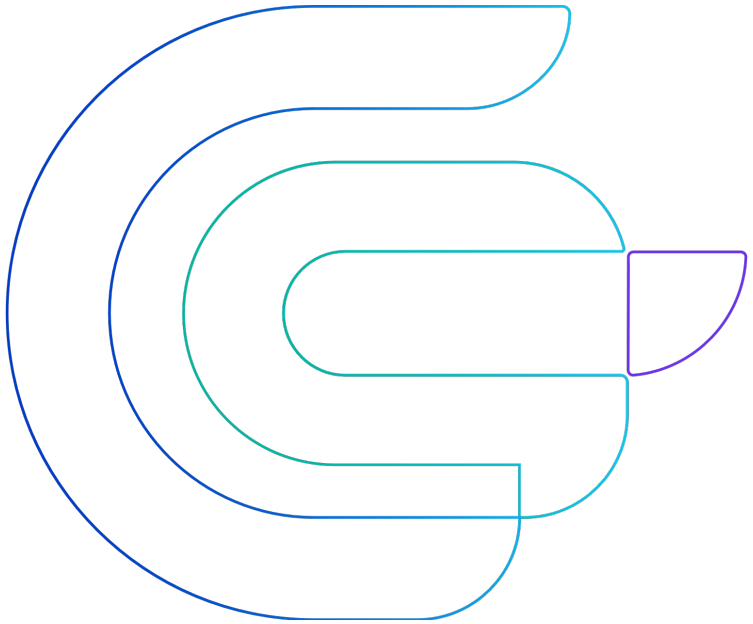
  Un estudio de la **Asociación Internacional de Gestión de Proyectos (PMI)** encontró que los candidatos que muestran insignias digitales de gestión de proyectos tienen **un 60%** más de probabilidades de ser contratados en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

¿Por qué son importantes?

- **Empoderamiento de la Marca Personal:**

La visibilidad y verificación instantánea proporcionada por las insignias digitales permiten a los profesionales no solo demostrar sus habilidades, sino también construir una marca personal fuerte. Según un estudio de LinkedIn, los profesionales que utilizan insignias digitales tienen un 24% más de probabilidades de avanzar en sus carreras.

La certificación y las insignias digitales no son solo una validación del conocimiento, sino también una herramienta poderosa para la mejora continua y la empleabilidad. En un mundo donde el aprendizaje permanente se ha convertido en la norma, estas credenciales son clave para el desarrollo profesional y la competitividad en el mercado laboral global.



No todas las insignias son iguales, y en **Certiprof,** estamos comprometidos con ofrecerte más que un simple reconocimiento digital. Al obtener una insignia emitida por certiprof, estarás recibiendo una validación de tu conocimiento respaldada por una de las entidades líderes en certificación profesional a nivel mundial.

Da el siguiente paso y obtén la insignia que te abrirá puertas y te posicionará como un experto en tu campo.

¿Por qué es importante obtener su certificado?

- **Prueba de experiencia:** Su certificado es un reconocimiento formal de las habilidades y conocimientos que ha adquirido. Sirve como prueba verificable de sus cualificaciones y demuestra su compromiso con la excelencia en su campo.

- **Credibilidad y reconocimiento:** En el competitivo mercado laboral actual, las empresas y los compañeros valoran las credenciales que le distinguen de los demás. Un certificado de una institución reconocida, como Certiprof, proporciona credibilidad instantánea e impulsa su reputación profesional.

- **Avance profesional:** Tener tu certificado puede abrirte las puertas a nuevas oportunidades. Ya se trate de un ascenso, un aumento de sueldo o un nuevo puesto de trabajo, las certificaciones son un factor diferenciador clave que los empleadores tienen en cuenta a la hora de evaluar a los candidatos.

¿Por qué es importante obtener su certificado?

- **Oportunidades de establecer contactos:** Poseer un certificado le conecta con una red de profesionales certificados. Muchas organizaciones cuentan con grupos de antiguos alumnos o de trabajo en red en los que puede compartir experiencias, intercambiar ideas y ampliar su círculo profesional.

- **Logro personal:** Obtener una certificación es un logro importante, y su certificado es un recordatorio tangible del trabajo duro, la dedicación y el progreso que ha realizado. Es algo de lo que puede sentirse orgulloso y mostrar a los demás.

Insignia

Earn this Badge

CertiProf ISO/IEC 22301 Internal Auditor - I22301A™

Issued by Certiprof

Holders of this certification have demonstrated an understanding of the principles, concepts and requirements of ISO/IEC 22301. They have demonstrated skills and ability to conduct audits and the structure and requirements for implementing a BCMS.

Learn more

Certification | Paid

Skills

Auditing | BCMS | Business Continuity Management (BCM) | Compliance | ISO 22301

https://www.credly.com/org/certiprof/badge/certiprof-iso-iec-22301-internal-auditor-i22301a

Insignia

Certiprof ISO 22301 Lead Auditor - I22301LA™

Issued by Certiprof

Holders of this certification have demonstrated an understanding of the principles, concepts and requirements of ISO/IEC 22301. They know the fundamental requirements for the implementation of a BCMS and the great importance of maintaining continuous process improvement by enhancing the organization's risk management framework, thus strengthening its ability to continue operating in times of crisis.

Learn more

Earn this Badge

Certification $ Paid

Skills

Auditing | BCMS | Business Continuity Management (BCM) | Compliance | Continual Improvement | Frameworks | ISO 22301 | Risk Management

https://www.credly.com/org/certiprof-iso-22301-lead-auditor-i22301la

Aprendizaje Permanente

- Certiprof ha creado una insignia especial para reconocer a los aprendices constantes.
- Para el 2024, se han emitido más de 1,000,000 de estas insignias en más de 11 idiomas.

Propósito y Filosofía

- Esta insignia está destinada a personas que creen firmemente en que la educación puede cambiar vidas y transformar el mundo.
- La filosofía detrás de la insignia es promover el compromiso con el aprendizaje continuo a lo largo de la vida.

Acceso y Obtención de la Insignia

- La insignia de Lifelong Learning se entrega sin costo a aquellos que se identifican con este enfoque de aprendizaje.
- Cualquier persona que se considere un aprendiz constante puede reclamar su insignia visitando:

https://certiprof.com/pages/certiprof-lifelong-learning

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#I22301IA-LA #certiprof

certiprof®

Agenda

Agenda

Fundamentos de la Norma ISO 22301

- Introducción a la norma.
- Términos y definiciones.
- Entendimiento de numerales de la Norma.
- Identificación de requisitos.
- Conclusiones.

Módulo de Auditor ISO 19011

- Conceptos claves de auditoría.
- Proceso de auditoría.
- Componentes de la auditoría.
- Preparación general para rol de auditor.
- Conclusiones.

**La agenda es una recomendación general, cada entrenador puede desarrollar el material bajo su experiencia.*

1. Introducción y Antecedentes

Introducción

- ISO 22301.
- Beneficios de un SGCN.
- Historia de la Norma.
- Estado actual.

Introducción

La norma especifica la estructura y los requisitos para la implantación y el mantenimiento de un Sistema de Gestión de Continuidad del Negocio (SGCN) que desarrolla la continuidad del negocio de manera apropiada a la magnitud y tipo de impacto que la organización puede o no aceptar luego de un incidente disruptivo.

Los resultados de mantener un SGCN están determinados por los requisitos legales, regulatorios, organizacionales e industriales, los productos o servicios ofrecidos, los procesos empleados, el tamaño, la estructura y los requisitos de las partes interesadas de la organización.

Introducción

Un SGCN destaca la importancia de:

- Comprender las necesidades de la organización y la necesidad de establecer la política y los objetivos de la gestión de la continuidad del negocio.
- La operación y el mantenimiento de los procesos, las capacidades y las estructuras de respuesta para asegurar que la organización sobrevivirá a los incidentes disruptivos.
- Realizar el seguimiento y la revisión del desempeño y la eficacia del SGCN, y la mejora continua basada en mediciones cualitativas y cuantitativas.

Beneficios de SGCN

El propósito de un SGCN es preparar para, proveer y mantener controles y las capacidades para gestionar la habilidad global de una organización para continuar operando durante los incidentes disruptivos.

a) Desde una perspectiva de negocio:
   - Apoyando a sus objetivos estratégicos.
   - Creando una ventaja competitiva.
   - Protegiendo y fortaleciendo su reputación y credibilidad.
   - Contribuyendo a la resiliencia de la organización.

Beneficios de SGCN

b) Desde una perspectiva financiera:
   - Reduciendo la exposición legal y financiera.
   - Reduciendo los costos directos e indirectos de los incidentes disruptivos.

c) Desde la perspectiva de las partes interesadas:
   - Protegiendo la vida, la propiedad y el medioambiente.
   - Considerando las expectativas de las partes interesadas.
   - Proporcionando confianza en la capacidad de la organización de ser exitosa.

d) Desde la perspectiva de los procesos internos:
   - Mejorando su capacidad de mantenerse eficaces durante los incidentes disruptivos.
   - Demostrando proactividad en el control de los riesgos de forma eficaz y eficiente.
   - Abordando las vulnerabilidades operacionales.

Historia de la Norma

Principales Cambios Realizados en la Norma ISO 22301

Los cambios principales en comparación con la edición previa son los siguientes:

- Se han aplicado los requisitos de ISO para estándares de sistemas de gestión, que han evolucionado desde 2012.
- Los requisitos se han clarificado, no se han agregado requisitos nuevos.
- Los requisitos específicos de la disciplina de continuidad del negocio están ahora casi por completo dentro del capítulo 8.
- El requisito 8 se ha reestructurado para proporcionar una comprensión más clara de los requisitos clave.
- Se han modificado varios términos específicos de la disciplina de continuidad del negocio para mejorar la claridad y reflejar el pensamiento actual.

2. Términos y Definiciones (Ver anexo)

3. Estructura de la Norma

Estructura de ISO 22301

Introducción.

1. Objeto.
2. Referencias normativas.
3. Términos y definiciones.
4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Apoyo.
8. Operación.
9. Evaluación del desempeño.
10. Mejora.

Bibliografía.

Introducción

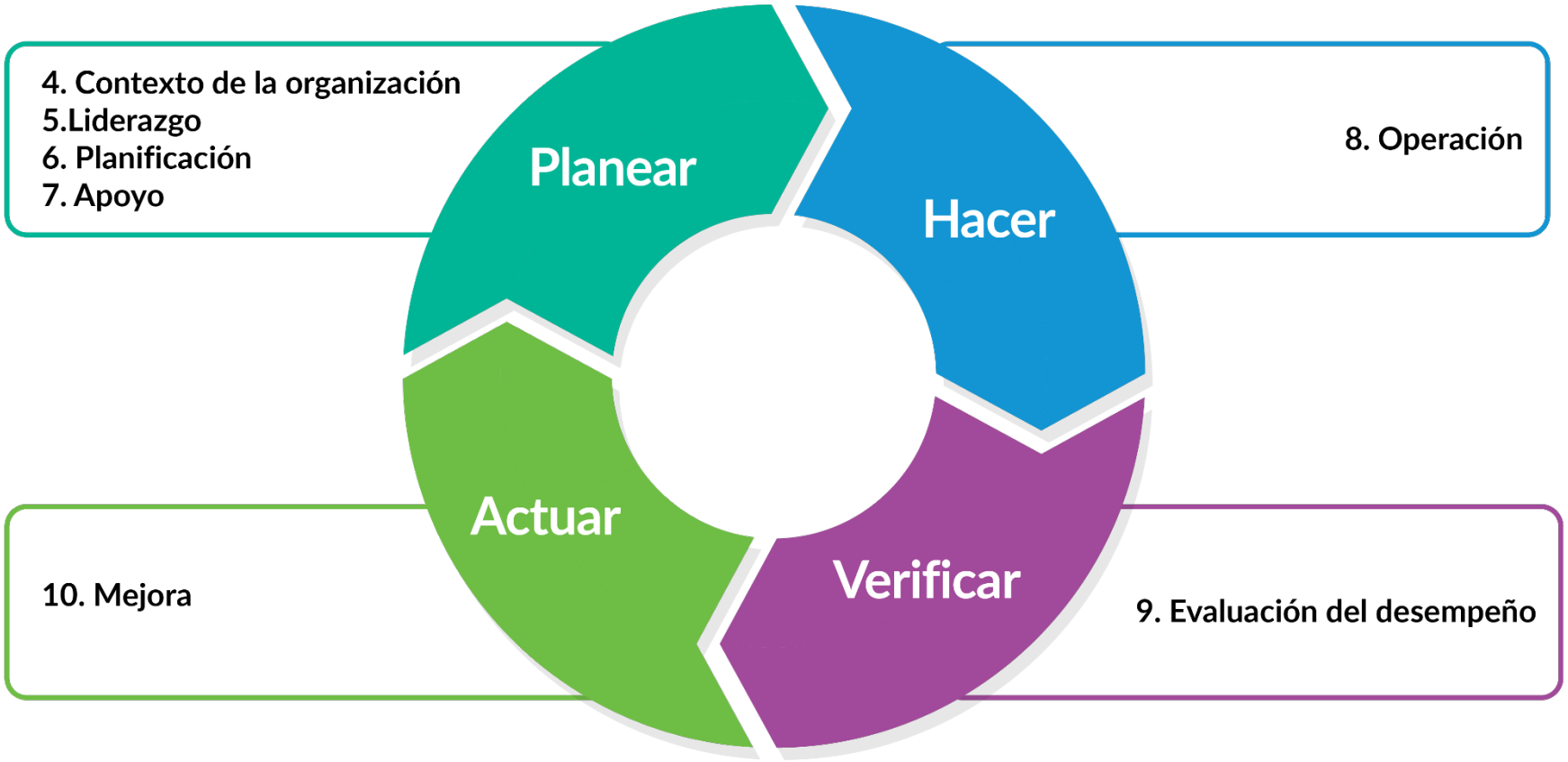
La norma ISO 22301 cumple con los requisitos de las normas de sistemas de gestión de ISO. Estos requisitos incluyen una estructura de alto nivel, texto básico idéntico y términos comunes con definiciones centrales, diseñados para beneficiar a los usuarios que implementan múltiples normas del sistema de gestión ISO.

La norma ISO 22301 contiene requisitos que una organización puede utilizar para implementar un SGCN y evaluar la conformidad.

Estructura de la ISO 22301

4 Contexto de la organización	5 Liderazgo	6 Planificación	7 Apoyo	8 Operación	9 Evaluación del desempeño	10 Mejora
• 4.1 Comprensión de la organización y su contexto • 4.2 Comprensión de las necesidades y expectativas de las partes interesadas • 4.3.2 Alcance del SGCN • 4.4 Sistema de gestión de la continuidad del negocio	• 5.1 Liderazgo y compromiso • 5.2 Política • 5.3 Roles, responsabilidades y autoridades	• 6.1 Acciones para abordar riesgos y oportunidades • 6.3 Planificación de los cambios del SGCN • 6.2 Objetivos de la continuidad del negocio y planificación para lograrlos	• 7.1 Recursos • 7.4 Comunicación • 7.3 Conciencia • 7.2 Competencia • 7.4 Comunicación • 7.5 Información documentada	• 8.1 Planificación operacional y control • 8.2 Análisis de impacto en el negocio y evaluación de riesgos • 8.3 Estrategias de continuidad del negocio y soluciones • 8.4 Planes y procedimientos de continuidad del negocio • 8.5 Programa de ejercicios • 8.6 Evaluación de la documentación y capacidades de continuidad del negocio	• 9.1 Seguimiento, medición, análisis y evaluación • 9.2 Auditoría interna • 9.3 Revisión por la dirección	• 10.1 No conformidad y acción correctiva • 10.2 Mejora continua

Ciclo PHVA Y SGCN



Estructura de ISO 22301

1. Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio – Requisitos.

Esta norma especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para protegerse contra, reducir la probabilidad de ocurrencia, prepararse para, responder a y recuperarse de incidentes disruptivos que puedan surgir.

Estructura de ISO 22301

Esta Norma Internacional es aplicable a todos los tipos y tamaños de organizaciones que:

a) Deseen implementar, mantener y mejorar un SGCN.

b) Busquen asegurar la conformidad con la política de continuidad de negocio establecida.

c) Necesiten poder continuar con la entrega de sus productos o servicios durante un incidente disruptivo con una capacidad aceptable predefinida.

d) Busquen fortalecer su resiliencia mediante la aplicación eficaz del SGCN.

Este documento puede ser utilizado para evaluar la capacidad de una organización para satisfacer sus necesidades y sus obligaciones de continuidad.

Estructura de ISO 22301

- **2. Referencias normativas.**

Proporciona detalles sobre las normas de referencia o publicaciones relevantes en relación a la norma concreta.

Como es la ISO 22300, Seguridad y resiliencia. Vocabulario

- **3. Términos y definiciones.**

Detalla términos y definiciones aplicables a la norma específica, además de cualquier otro término y definición relacionado con la norma.

Estructura de ISO 22301

- **4. Contexto de la organización.**
- **4.1 Comprensión de la organización y de su contexto.**
- **4.2 Compresión de las necesidades y expectativas de las partes interesadas.**
- **4.3 Determinación del alcance del SGCN.**
- **4.4 Sistema de gestión de la continuidad del negocio.**

4. Contexto de la Organización

4.1 Comprensión de la Organización y de su Contexto

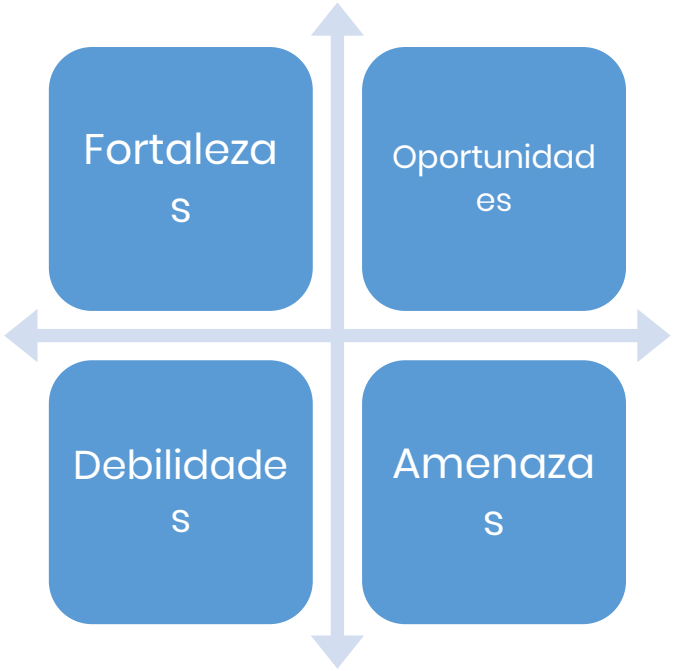
La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad de lograr los resultados deseados de su SGCN.

NOTA: Estas cuestiones pueden estar afectadas por los objetivos generales de la organización, sus productos y servicios y el tipo y nivel de riesgo que puede o no aceptar.

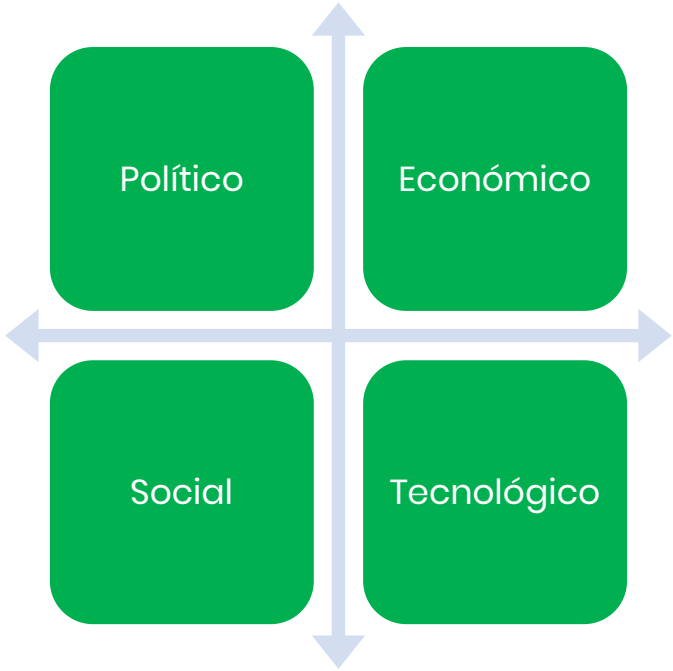
4.1 Comprensión de la Organización y de su Contexto

Para determinar el contexto podemos utilizar alguna de estas herramientas:

Análisis FODA



Análisis PSET



4.2 Compresión de las Necesidades y Expectativas de las Partes Interesadas

4.2.1 Generalidades

Al establecer su SGCN, la organización debe determinar:

a) Las partes interesadas que son pertinentes para el SGCN.

b) Los requisitos pertinentes de esas partes interesadas.

Ejemplo de partes interesadas:

- Accionistas.
- Gerencia.
- Personal Interno.
- Contratistas.
- Proveedores.
- Clientes.
- Entidades Reguladoras.
- Gobierno.
- Competidores.
- Grupos de Interés.

4.2 Compresión de las Necesidades y Expectativas de las Partes Interesadas

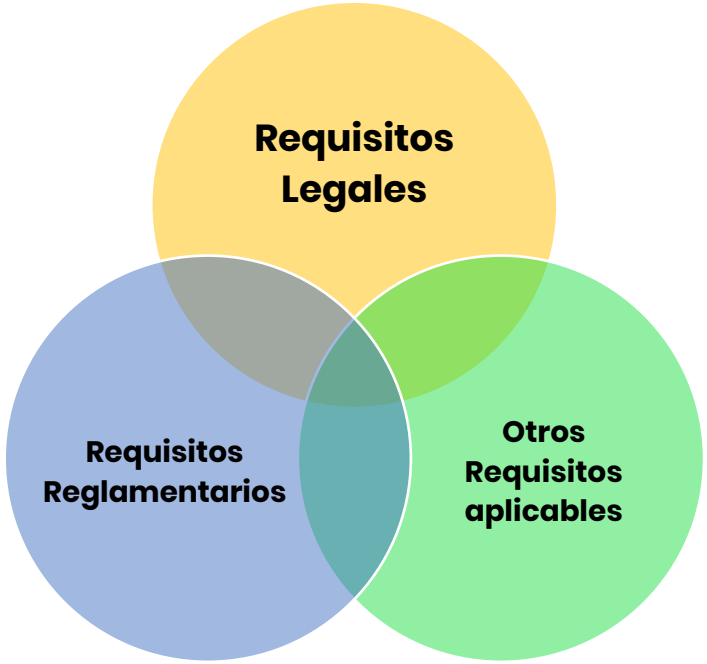
4.2.2 Los requisitos legales y reglamentarios

La organización debe:

a) Implementar y mantener un proceso para identificar, tener acceso a y evaluar los requisitos legales y reglamentarios relacionados con la continuidad de sus productos, servicios, actividades y recursos.

b) Asegurarse de que estos requisitos legales, reglamentarios y otros aplicables se tengan en cuenta en la implementación y el mantenimiento de su SGCN.

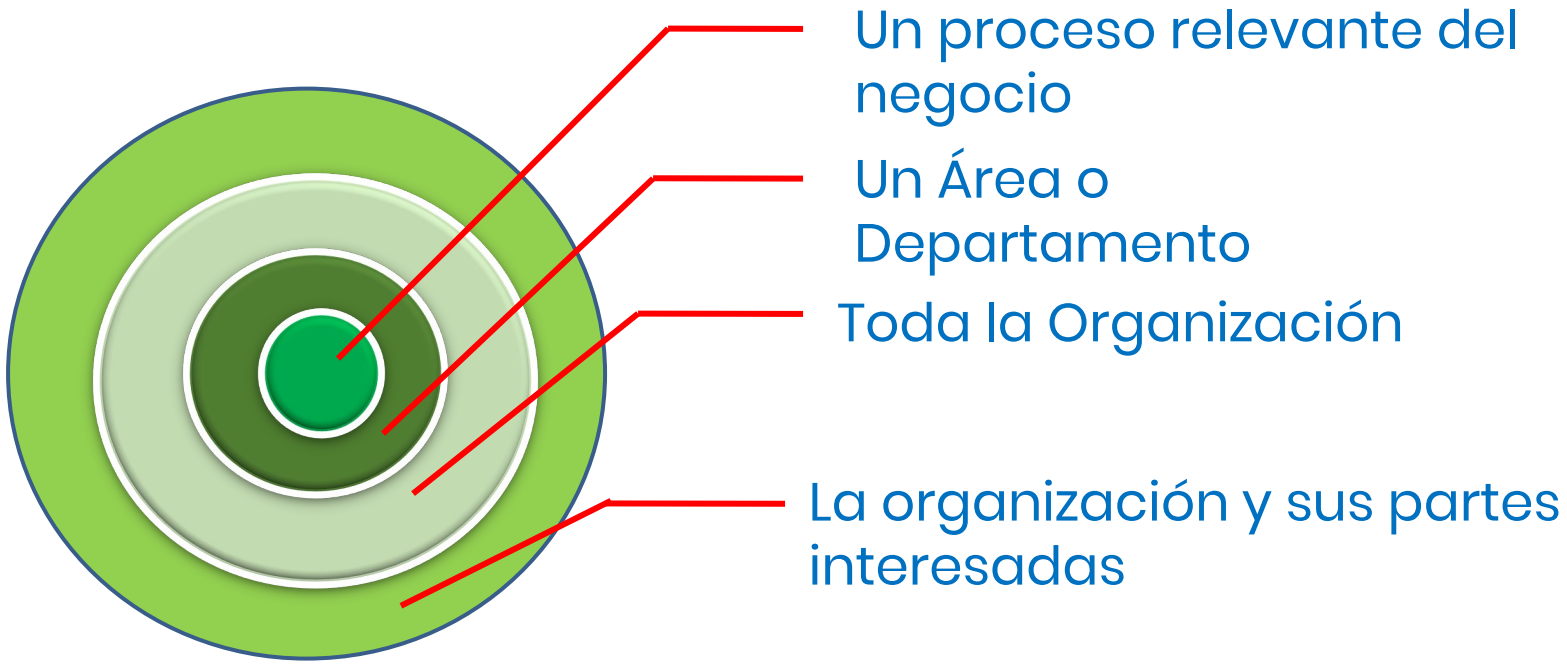
c) Documentar esta información y mantenerla actualizada.



Taller Sobre Requisitos 4.1 y 4.2

4.3 Determinación del Alcance del SGCN

La organización debe determinar los límites y la aplicabilidad del SGCN para establecer su alcance.



4.3 Determinación del Alcance del SGCN

4.3.1 Generalidades

La organización debe determinar los límites y la aplicabilidad del SGCN para establecer su alcance.

Al determinar el alcance, la organización debe considerar:

a) Las cuestiones internas y externas indicados en el apartado 4.1.
b) Los requisitos indicados en el apartado 4.2.
c) La misión, los objetivos y las obligaciones internas y externas.

El alcance debe estar disponible como información documentada.

4.3 Determinación del Alcance del SGCN

4.3.2 Alcance del SGCN

La organización debe:

a) Establecer las partes de la organización a ser incluidas en el SGCN, teniendo en cuenta sus localizaciones, tamaño, naturaleza y complejidad.

b) Identificar los productos y servicios a ser incluidos en el SGCN.

Al definir el alcance, la organización debe documentar y explicar las exclusiones.

Las exclusiones deben ser explicadas. Las mismas no deben afectar la capacidad y la responsabilidad de la organización de proveer continuidad del negocio y de las operaciones que cumplan con los requisitos del SGCN, según lo determinado por el análisis de impacto en el negocio o la evaluación de riesgos y los requisitos legales o reglamentarios.

4.4 Sistema de Gestión de la Continuidad del Negocio

Sistema de Gestión de la Continuidad del Negocio

La organización debe establecer, implementar, mantener y mejorar continuamente un SGCN, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

5. Liderazgo

Liderazgo

- 5. Liderazgo.
  - 5.1 Liderazgo y compromiso.
  - 5.2 Política.
  - 5.3 Roles, responsabilidades y autoridades.

5.1 Liderazgo y Compromiso

La alta dirección debe demostrar su liderazgo y compromiso con respecto al SGCN:

a) Asegurándose de que se establezcan la política y los objetivos para el SGCN, y que éstos son compatibles con la dirección estratégica de la organización.
b) Asegurándose de la integración de los requisitos del SGCN con los procesos de negocio de la organización.
c) Garantizar que los recursos necesarios para el SGCN estén disponibles.
d) Comunicar la importancia de una efectiva continuidad del negocio y la conforme con los requisitos del SGCN.
e) Garantizar que el SGCN logre los resultados previstos.
f) Dirigiendo y apoyando a las personas para contribuir a la eficacia del SGCN.

5.1 Liderazgo y Compromiso

g) Promoviendo la mejora continua.

h) Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo y compromiso en la forma en la que aplique a sus áreas de responsabilidad.

NOTA: este documento puede ser interpretado en términos generales en el sentido de aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.2 Política

5.2.1 Establecer la política de continuidad del negocio

La alta dirección debe establecer una política de continuidad del negocio que:

a) Sea apropiada al propósito de la organización.
b) Proporcione un marco de referencia para establecer los objetivos de continuidad del negocio.
c) Incluya un compromiso para satisfacer los requisitos aplicables.
d) Incluya un compromiso de mejora continua del SGCN.

5.2 Política

5.2.2 Comunicación de la política

La política de continuidad del negocio debe:

a) Estar disponible como información documentada.
b) Ser comunicada dentro de la organización.
c) Estar disponible para las partes interesadas, según corresponda.

5.3 Roles, Responsabilidades y Autoridades

La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles pertinentes se asignen y se comuniquen dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Asegurar que el SGCN cumpla con los requisitos de este documento.
b) Informar sobre el desempeño del SGCN a la alta dirección.

6. Planificación

Planificación

- 6. Planificación.
  - 6.1 Acciones para tratar riesgos y oportunidades.
  - 6.2 Objetivos de la continuidad del negocio y planificación para lograrlos.
  - 6.3 Planificación de los cambios del SGCN.

6.1 Acciones para Abordar Riesgos y Oportunidades

6.1.1 Determinación de riesgos y oportunidades

Al planificar el SGCN, la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario abordar con el fin de:

a) Asegurar que el SGCN puede lograr los resultados deseados.
b) Prevenir o reducir efectos no deseados.
c) Lograr la mejora continua.

6.1 Acciones para Abordar Riesgos y Oportunidades

6.1.2 Abordar riesgos y oportunidades

La organización debe planificar:

a) Las acciones para abordar estos riesgos y oportunidades.
b) Cómo integrar e implementar las acciones en sus procesos del SGCN (Véase 8.1).
c) Evaluar la eficacia de estas acciones (Véase 9.1).

NOTA: Los riesgos y oportunidades se relacionan con la eficacia del sistema de gestión. Los riesgos relacionados con los incidentes disruptivos del negocio son abordados en 8.2.

6.2 Objetivos de la Continuidad del Negocio y Planificación para Lograrlos

6.2.1 Establecimiento de los objetivos de continuidad del negocio

La organización debe establecer los objetivos de la continuidad del negocio para las funciones y niveles pertinentes.

Los objetivos de la continuidad del negocio deben:

a) Ser coherentes con la política de continuidad del negocio.
b) Ser medibles (si es posible).
c) Tener en cuenta los requisitos aplicables (véase 4.1 y 4.2).

6.2 Objetivos de la Continuidad del Negocio y Planificación para Lograrlos

d) Ser objeto de seguimiento.
e) Comunicarse.
f) Actualizarse, según corresponda.

La organización debe mantener información documentada sobre los objetivos de continuidad del negocio.

6.2 Objetivos de la Continuidad del Negocio y Planificación para Lograrlos

6.2.2 Determinación de los objetivos de continuidad del negocio

Al planificar cómo lograr sus objetivos de continuidad del negocio, la organización debe determinar:

a) Qué se va a hacer.
b) Qué recursos se requerirán.
c) Quién será responsable.
d) Cuándo se finalizará.
e) Cómo se evaluarán los resultados.

6.3 Planificación de los Cambios del SGCN

Cuando la organización determine la necesidad de cambios en el SGCN , incluyendo los identificados en el Capítulo 10, estos cambios se deben llevar a cabo de manera planificada.

La organización debe considerar:

a) El propósito de los cambios y sus consecuencias potenciales.
b) La integridad del SGCN.
c) La disponibilidad de recursos.
d) La asignación o reasignación de responsabilidades y autoridades.

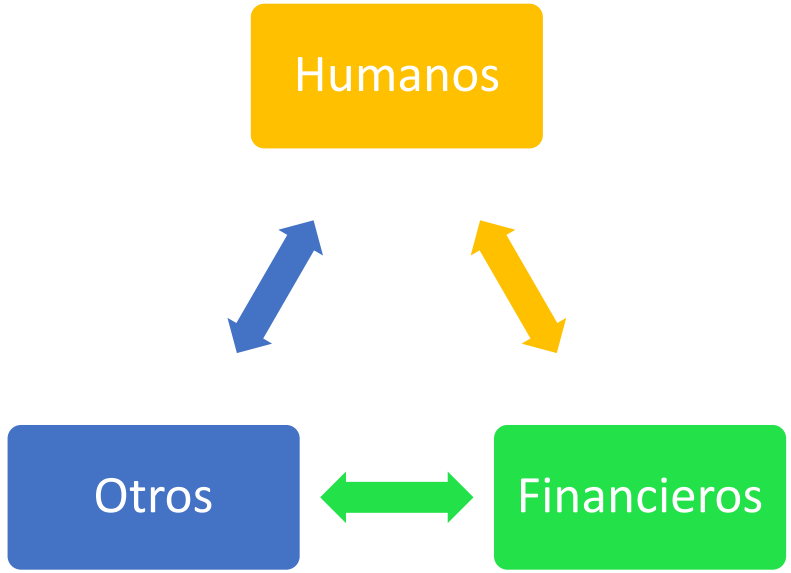
7. Apoyo (Soporte)

Apoyo

7. Apoyo.
    - 7.1 Recursos.
    - 7.2 Competencia.
    - 7.3 Conciencia.
    - 7.4 Comunicación.
    - 7.5 Información documentada.

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGCN.



7.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño de la continuidad del negocio.

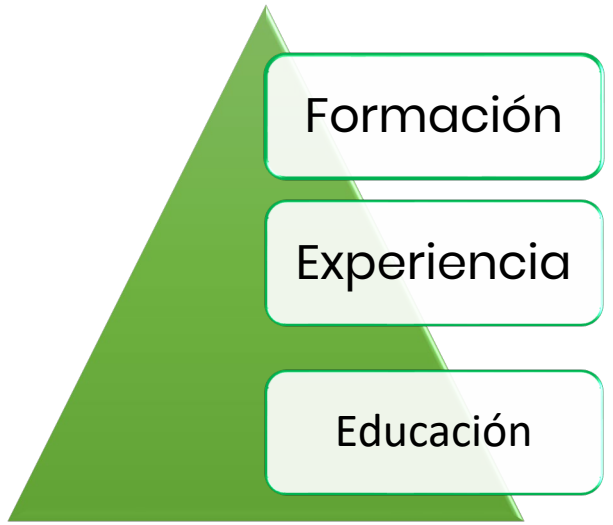
b) Asegurarse de que éstas personas sean competentes, basándose en la educación, formación o experiencia apropiadas.

7.2 Competencia

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas.

d) conservar la información documentada apropiada como evidencia de la competencia.

NOTA: Las acciones aplicables pueden incluir, por ejemplo, la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación o subcontratación de personas competentes.



7.3 Concienciación

Las personas que realizan trabajos bajo el control de la organización deben tomar conciencia de:

a) La política de continuidad del negocio.
b) Su contribución a la eficacia del SGCN, incluyendo los beneficios de una mejora en el desempeño de la gestión de continuidad del negocio.
c) Las implicaciones del incumplimiento de los requisitos del SGCN.
d) Su propio rol y responsabilidades antes, durante y después de los incidentes disruptivos.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGCN que incluyan:

a) Qué comunicar.
b) Cuándo comunicar.
c) A quién comunicar.
d) Cómo comunicar.
e) Quién comunica.

7.5 Información Documentada

7.5.1 Generalidades

El SGCN de la organización debe incluir:

a) La información documentada requerida por este documento.
b) La información documentada que la organización determine como necesaria para la eficacia del SGCN.

NOTA: la extensión de la información documentada para un SGCN puede variar de una organización a otra, debido a:

- El tamaño de la organización y su tipo de actividades, procesos, productos y servicios y recursos.
- La complejidad de los procesos y sus interacciones.
- Las competencias del personal.

7.5 Información Documentada

7.5.2 Elaboración y actualización

Al elaborar y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

a) Identificación y descripción (por ejemplo, título, fecha, autor o número de referencia).
b) Formato (el idioma, versión de software, gráficos), y los medios de soporte (por ejemplo, papel, electrónico).
c) La revisión y aprobación con respecto a la conveniencia y adecuación.

7.5 Información Documentada

7.5.3 Control de la información documentada

7.5.3.1 La información documentada requerida por el SGCN y por este documento se debe controlar para asegurar de que:

a) Esté disponible y sea idónea para su uso, donde y cuando se necesite.
b) Esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado o pérdida de la integridad).

7.5 Información Documentada

7.5.3.2 Para el control de la información documentada la organización debe abordar las siguientes actividades, según corresponda:

a) Distribución, acceso, recuperación y uso.
b) Almacenamiento y preservación, incluida la preservación de la legibilidad.
c) Control de cambios (por ejemplo, control de versión).
d) Retención y disposición.
e) La información documentada de origen externo, que la organización determina como necesaria para la planificación y la operación del SGCN, se debe identificar, según sea apropiado, y controlar.

NOTA: el acceso puede implicar una decisión en relación al permiso, solamente para consultar la información documentada, o al permiso y a la autoridad para consultar y modificar la información documentada.

8. Operación

Operación

- 8. Operación.
  - 8.1 Planificación operacional y control.
  - 8.2 Análisis de impacto en el negocio y evaluación de riesgos.
  - 8.3 Estrategias de continuidad del negocio y soluciones.
  - 8.4 Planes y procedimientos de continuidad del negocio.
  - 8.5 Programa de ejercicios.
  - 8.6 Evaluación de la documentación y capacidades de continuidad del negocio.

8.1 Planificación Operacional y Control

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en el apartado 6.1 mediante:

a) La determinación de los criterios para los procesos.
b) La implementación del control de los procesos de acuerdo con los criterios.
c) La conservación de la información documentada en la extensión necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no deseados, tomando acciones para mitigar cualquier efecto adverso, según sea necesario.

La organización debe asegurarse de que los procesos subcontratados son controlados.

8.2 Análisis de Impacto en el Negocio y Evaluación de Riesgos

8.2.1 Generalidades

La organización debe:

a) Implementar, y mantener un proceso sistemático para el análisis de impacto en el negocio y la evaluación de riesgos de incidentes disruptivos.
b) Revisar el análisis de impacto del negocio y la evaluación de riesgos a intervalos planificados y cuando existan cambios significativos, en la organización o su contexto en el que opera.

NOTA: la organización determina como se realiza el análisis de impacto en el negocio y la evaluación de riesgos.

8.2 Análisis de Impacto en el Negocio y Evaluación de Riesgos

8.2.2 Análisis del impacto en el negocio

La organización debe usar el proceso de análisis de impacto del negocio para determinar las prioridades y los requisitos de continuidad del negocio. El proceso debe:

a) Definir los tipos de impacto y los criterios pertinentes para el contexto de la organización.
b) La identificación de actividades que soportan el suministro de productos y servicios.
c) Usar los tipos de impactos y los criterios para evaluar los impactos con el transcurso del tiempo resultantes de la interrupción de estas actividades.
d) Identificar los plazos de tiempo en los cuales los impactos de no reanudar la actividades serían inaceptables para la organización.

NOTA 1: esto puede referirse como el **período máximo tolerable de interrupción MTPD** (por sus siglas en inglés, **maximum tolerable period of disruption).**

8.2 Análisis de Impacto en el Negocio y Evaluación de Riesgos

e) establecer períodos de tiempo prioritarios en el tiempo identificado en d) para reanudar las actividades interrumpidas a una capacidad mínima aceptable especificada.

NOTA 2: este período de tiempo puede ser denominado como **objetivo de tiempo de recuperación RTO** (por sus siglas en inglés, **Recovery Time Objective**).

f) Utilizar el análisis para identificar las actividades prioritarias.
g) Determinar los recursos que son necesarios para soportar las actividades prioritarias.
h) Determinar las dependencias, incluyendo socios y proveedores, y las interdependencias de las actividades prioritarias.

Taller 2: Análisis de Impacto en el Negocio (BIA)

8.2 Análisis de Impacto en el Negocio y Evaluación de Riesgos

8.2.3 Evaluación de riesgos

La organización debe implementar y mantener un proceso de evaluación de riesgos.

NOTA: En la norma ISO 31000 se aborda el proceso para la evaluación de riesgos.

La organización debe:

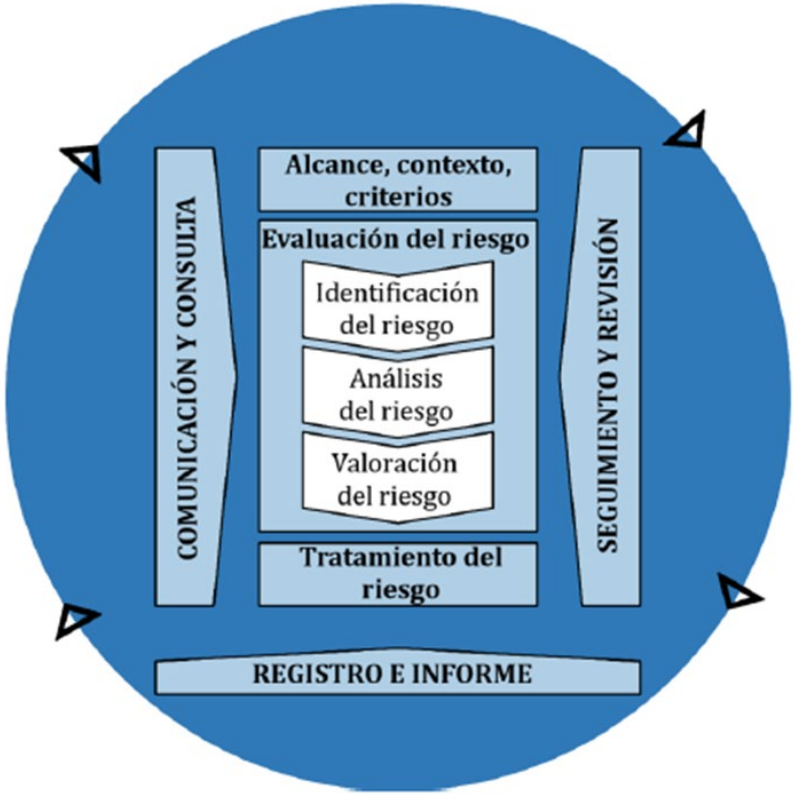
a) Identificar los riesgos de incidentes disruptivos para las actividades prioritarias de la organización y de sus recursos.
b) Analizar y valorar los riesgos identificados.
c) Determinar cuáles riesgos requieren tratamiento.

NOTA: los riesgos en este apartado son los relacionados con los incidentes disruptivos de las actividades del negocio. Los riesgos y oportunidades relacionados con la eficacia del sistema de gestión se abordan en 6.1.

8.2 Análisis de Impacto en el Negocio y Evaluación de Riesgos

8.2.3 Evaluación de riesgos

PROCESO DE GESTION DE RIESGOS SEGÚN ISO 31000

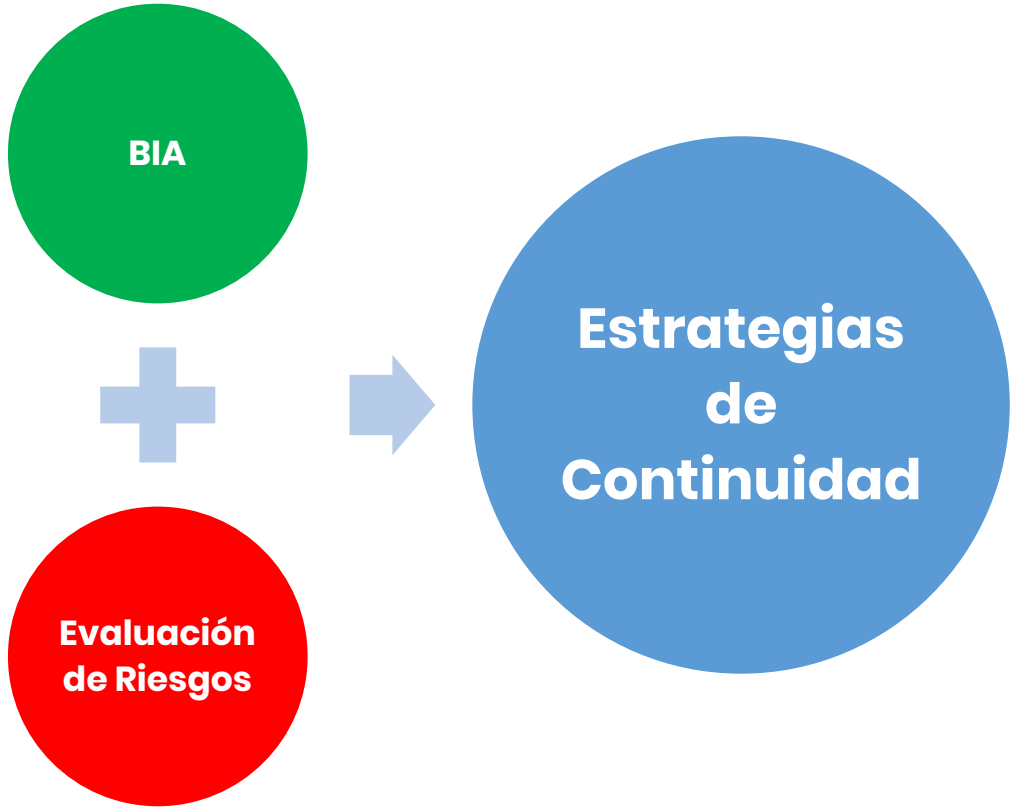


8.3 Estrategias de Continuidad del Negocio y Soluciones

8.3.1 Generalidades

Basándose en las salidas del análisis de impacto del negocio y la evaluación de riesgos, la organización debe identificar y seleccionar las estrategias de continuidad del negocio que considere las opciones para antes, durante y después de un incidente disruptivo.

Las estrategias de continuidad del negocio deben comprender una o más soluciones.



8.3 Estrategias de Continuidad del Negocio y Soluciones

8.3.2 Identificación de estrategias y soluciones

La identificación debe basarse en estrategias y soluciones que:

a) Cumplan con los requisitos de continuidad y recuperación de las actividades prioritarias en el marco de tiempo identificado y la capacidad acordada.
b) Protejan las actividades prioritarias de la organización.
c) Reduzcan la probabilidad de un incidente disruptivo.
d) Acorten los períodos de interrupción.
e) Limiten los impactos de los incidentes disruptivos en los productos y servicios de la organización.
f) Provean de la disponibilidad de los recursos adecuados.

8.3 Estrategias de Continuidad del Negocio y Soluciones

8.3.3 Selección de las estrategias y soluciones

La selección debe basarse en estrategias y soluciones que:

a) Cumplan con los requisitos de continuidad y recuperación de las actividades prioritarias en el marco de tiempo identificado y la capacidad acordada.
b) Consideren el tipo y nivel de riesgo que la organización puede o no aceptar.
c) Considere los costos y beneficios asociados.

8.3 Estrategias de Continuidad del Negocio y Soluciones

8.3.4 Requisitos de recursos

La organización debe determinar los requisitos de recursos para implementar las soluciones de continuidad de negocio seleccionadas. Los tipos de recursos considerados deben incluir, pero no limitarse a:

a) Las personas.
b) La información y los datos.
c) Infraestructura física como los edificios, el ambiente de trabajo y otras infraestructuras y servicios asociados.
d) Los equipos y los insumos.
e) Los sistemas de tecnología de la información y la comunicación (TIC).
f) El transporte y la logística.
g) Las finanzas.
h) Los socios y proveedores.

8.3.5 Implementación de la solución

La organización debe implementar y mantener las soluciones seleccionadas de continuidad del negocio para que puedan ser activadas cuando sea necesario.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.1 Generalidades

La organización debe implementar y mantener una estructura de respuesta que permitirá la advertencia y comunicación oportuna a las partes interesadas pertinentes. La organización debe proveer de los planes y procedimientos para gestionar la organización durante el incidente disruptivo.

Los planes y procedimientos deben ser utilizados cuando sea necesario activar las soluciones de continuidad del negocio.

NOTA: existen distintos tipos de procedimientos que constituyen los planes de continuidad de negocio.

8.4 Planes y Procedimientos de Continuidad del Negocio

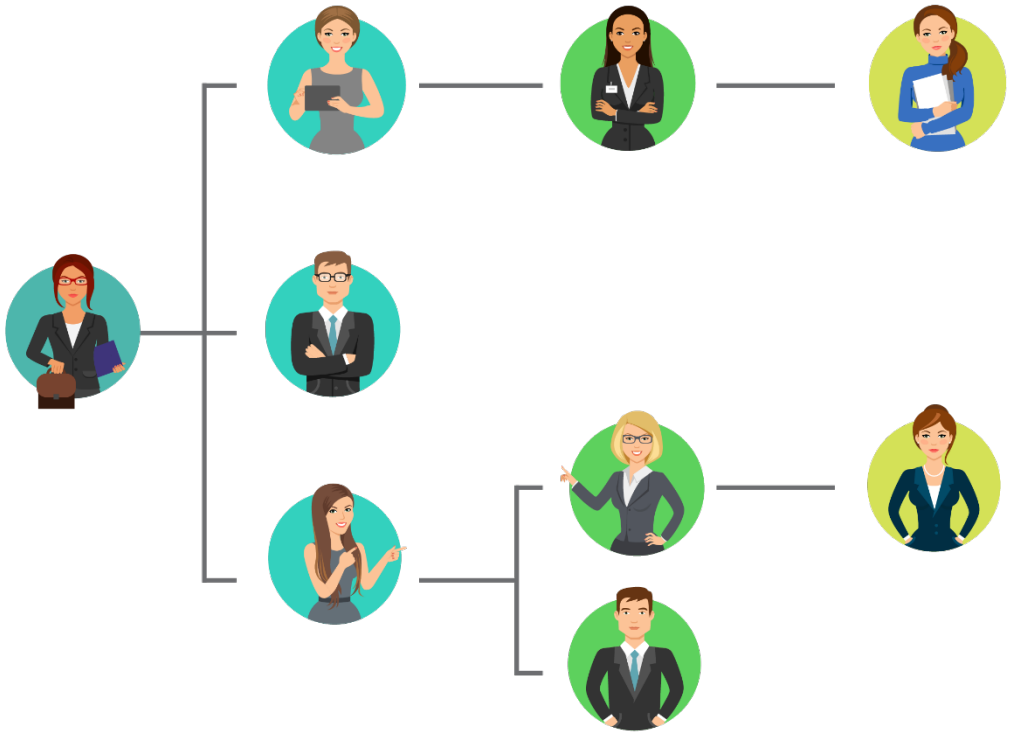
La organización debe identificar y documentar los planes y procedimientos de continuidad del negocio basándose en las salidas de las estrategias y soluciones seleccionadas.
Los procedimientos deben:

a) Ser específicos con respecto a las etapas inmediatas que deben tomarse durante un incidente disruptivo.
b) Ser flexibles para responder a los cambios en las condiciones internas y externas de un incidente disruptivo.
c) Enfocarse en el impacto de los incidentes que potencialmente podrían ser incidentes disruptivos.
d) Ser eficaces minimizando el impacto a través de la implementación de las soluciones apropiadas.
e) Asignar los roles y las responsabilidades para las tares durante los mismos.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.2 Estructura de respuesta

8.4.2.1 La organización debe implementar y mantener una estructura, identificando uno o más equipos responsables de dar respuesta a un incidente disruptivo.



8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.2.2 Los roles y responsabilidades de cada equipo y las relaciones entre los equipos deben ser establecidos claramente.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.2.3 En forma colectiva, los equipos deben ser competentes para:

a) Evaluar la naturaleza y el alcance de un incidente disruptivo y su impacto potencial.
b) Evaluar el impacto con límites predefinidos que justifican el inicio de una respuesta formal.
c) Activar una respuesta apropiada de continuidad del negocio.
d) Planificar las acciones que necesitan ser realizadas.
e) Establecer prioridades (utilizando la seguridad de la vida como primera prioridad).
f) Realizar seguimiento a los efectos del incidente disruptivo y la respuesta de la organización.
g) Activar las soluciones de continuidad del negocio.
h) Comunicarse con las partes interesadas pertinentes, las autoridades y los medios.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.2.4 Para cada equipo debe existir:

a) Personal identificado y sus suplentes con la responsabilidad necesaria, la autoridad y competencia para cumplir con el rol designado.
b) Procedimientos documentados para guiar sus acciones (ver 8.4.4), incluyendo aquellas para la activación, operación, coordinación y comunicación de la respuesta.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.3 Alertas y comunicación

La organización debe documentar y mantener procedimientos para:

a) la comunicación interna y externa con las partes interesadas pertinentes, incluyendo qué, cuando, a quién y cómo comunicar.

NOTA: la organización puede documentar y mantener procedimientos sobre cómo y bajo qué circunstancias la organización comunica a sus empleados y los contactos de emergencia.

8.4 Planes y Procedimientos de Continuidad del Negocio

b) Recibir, documentar y responder a las comunicaciones de las partes interesadas, incluyendo cualquier sistema de alerta de riesgo nacional o regional o equivalente.
c) Asegurar la disponibilidad de los medios de comunicación durante un incidente disruptivo.
d) Facilitar la comunicación estructurada con los servicios de respuesta de emergencia.
e) Suministrar detalles sobre la repuesta de la organización a los medios siguiendo un incidente, incluyendo una estrategia de comunicación.
f) Registrar los detalles sobre el incidente disruptivo, las acciones llevadas a cabo, y las decisiones tomadas.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.3.2 Cuando sea aplicable, también debe considerarse e implementarse lo siguiente:

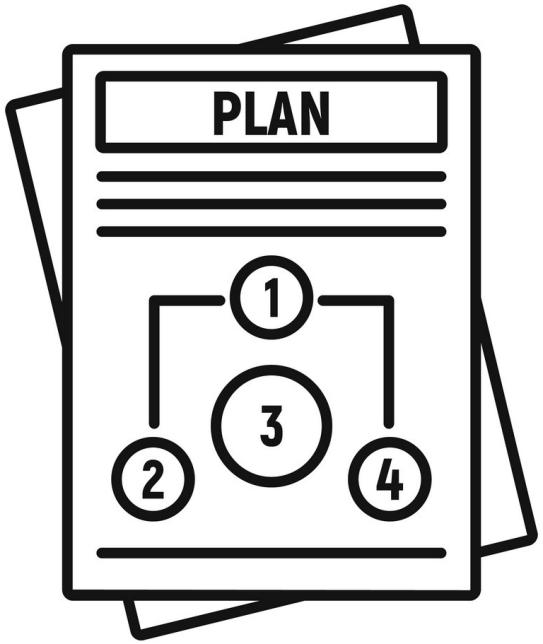
a) Alertar a las partes interesadas potencialmente afectadas por un incidente disruptivo real o inminente.
b) Asegurar la adecuada coordinación y comunicación entre las múltiples organizaciones de respuesta.

Los procedimientos de alerta y comunicación deben ser ejercitados como parte del programa de ejercicios indicado en 8.5.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.4 Planes de continuidad del negocio

8.4.4.1 la organización debe documentar y mantener planes y procedimientos de continuidad del negocio. Los planes de continuidad del negocio deben bridar orientación e información para apoyar a los equipos en la respuesta a un incidente disruptivo y dar apoyo a la organización con la respuesta y la recuperación.



8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.4.2 En su conjunto los planes de continuidad del negocio deben contener:

a) Los detalles de las acciones que los equipos realizaran para:
   1. Continuar y recuperar las actividades prioritarias en un período de tiempo predeterminado.
   2. Realizar el seguimiento del impacto del incidente disruptivo y la respuesta de la organización al mismo.

b) Una referencia a los límites predefinidos y los procesos para activar la respuesta.

c) Los procedimientos que permitan suministrar los productos y servicios a una capacidad acordada.

d) Los detalles para gestionar inmediatamente las consecuencias de un incidente disruptivo teniendo en cuenta:
   1. El bienestar de los individuos.
   2. La prevención de pérdidas mayores o la inviabilidad de actividades prioritarias.
   3. El impacto en el medioambiente.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.4.3 Cada plan debe incluir:

a) El propósito, alcance y objetivos.
b) Los roles y responsabilidades del equipo que implementará el plan.
c) Las acciones para implementar las soluciones.
d) La información de apoyo necesaria para activar (incluyendo los criterios de activación), operar, coordinar y comunicar las acciones del equipo.
e) Las interdependencias internas y externas.
f) Los recursos necesarios.
g) Los requisitos de informes.
h) Un proceso para retirarse del mercado.

Cada plan debe ser usado y estar disponible en el momento y lugar en que sea necesario.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.5 Recuperación

La organización debe tener procesos documentados para restaurar y volver a las actividades de negocios de las medidas temporales adoptadas durante y después de un incidente.

8.5 Programa de Ejercicios

La organización debe implementar y mantener un programa de ejercicios y prueba para validar en el tiempo la eficacia de sus estrategias y soluciones de continuidad del negocio. La organización debe llevar a cabo ejercicios y pruebas que:

a) Sean coherentes con los objetivos de continuidad del negocio.
b) Se basen en escenarios apropiados que están bien planificados con metas y objetivos claramente definidos.
c) Desarrollen equipo de trabajo, competencias, confianza y conocimiento para aquellos que tienen roles que desempeñar relacionados con los incidentes disruptivos.
d) Tomados en conjunto, a través del tiempo validen sus estrategias y soluciones de continuidad del negocio.
e) Realicen informes formales post-ejercicio que contengan resultados, recomendaciones y acciones para implementar mejoras.
f) Sean revisados en el contexto de promover la mejora continua.
g) Sean llevados a cabo a intervalos planificados y cuando hayan cambios significativos dentro de la organización o en el contexto en el que opera.

La organización debe actuar sobre los resultados de sus ejercicios y pruebas para implementar los cambios y mejoras.

8.6 Evaluación de la Documentación y Capacidades de Continuidad del Negocio

La organización debe:

a) Evaluar la adecuación y eficacia del análisis de impacto del negocio, la evaluación de riesgo, las estrategias, soluciones, los planes y procedimientos.
b) Llevar a cabo evaluaciones mediante revisiones, análisis, ejercicios, pruebas, informes posteriores a un incidente y evaluaciones de desempeño.
c) Realizar evaluaciones de la capacidad de continuidad del negocio de los socios y partes interesadas pertinentes.
d) Evaluar el cumplimiento con los requisitos legales y reglamentarios aplicables, las buenas prácticas industriales y la conformidad con sus propios políticas y objetivos de continuidad del negocio.
e) Actualizar la documentación y los procedimientos de forma oportuna.

Estas evaluaciones deben ser realizadas a intervalos planificados, después de un incidente o activación, y cuando ocurran cambios significativos.

9. Evaluación del Desempeño

Evaluación del Desempeño

- 9. Evaluación del desempeño.
  - 9.1 Seguimiento, medición, análisis y evaluación.
  - 9.2 Auditoria interna.
  - 9.3 Revisión por la dirección.

9.1 Seguimiento, Medición, Análisis y Evaluación

9.1.1 Generalidades

La organización debe determinar:

a) Qué necesita seguimiento y medición.
b) Los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos.
c) Cuándo y quiénes deben llevar a cabo el seguimiento y la medición.
d) Cuándo y quiénes se deben analizar y evaluar los resultados del seguimiento y la medición.

La organización debe conservar la información documentada apropiada como evidencia de los resultados.

La organización debe evaluar el desempeño y la eficacia del SGCN.

9.2 Auditoría Interna

9.2.1 Generalidades

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre como el SGCN.

a) Es conforme con:
   1. Los requisitos propios de la organización para su SGCN.
   2. Los requisitos de este documento.
b) Es eficazmente implementado y mantenido.

9.2 Auditoría Interna

9.2.2 Programas de auditorías

La organización debe:

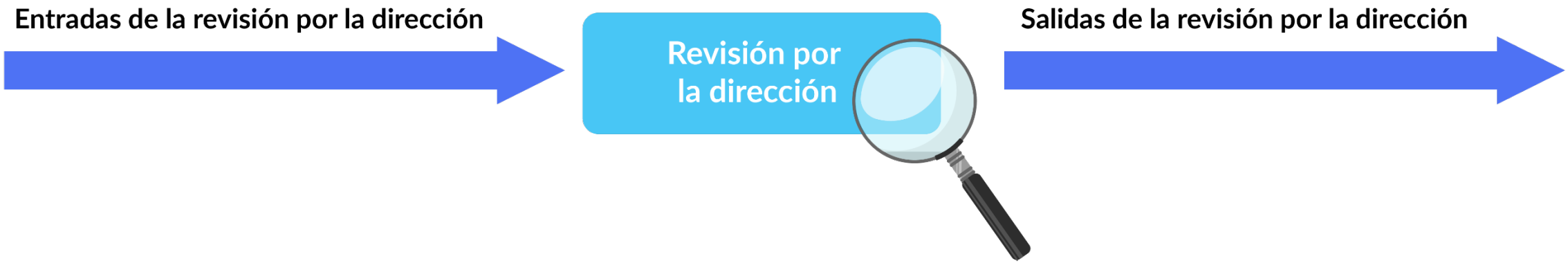
a) Planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, que deben tener en consideración la importancia de los procesos involucrados, los cambios que afecten a la organización y los resultados de las auditorías previas.
b) Definir los criterios de la auditoría y el alcance para cada auditoría.
c) Seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría.
d) Asegurarse de que los resultados de las auditorías se informen a los gerentes pertinentes.

9.2 Auditoría Interna

e) Conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías.
f) Asegurarse que se toman las acciones correctivas necesaria sin demora injustificada para eliminar las no conformidades y sus causas.
g) Asegurarse que las acciones de seguimiento de las auditorías incluyen la verificación de las acciones tomadas y el informe de los resultados de las verificaciones.

9.3 Revisión por la Dirección

La alta dirección debe revisar el SGCN de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia.



9.3 Revisión por la Dirección

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección debe incluir consideraciones sobre:

a) El estado de las acciones de las revisiones por la dirección previas.
b) Los cambios en las cuestiones externas e internas que sean pertinentes al SGCN.
c) La información sobre el desempeño del SGCN, incluidas las tendencias relativas a:
    1. Las no conformidades y acciones correctivas.
    2. Los resultados de seguimiento y medición.
    3. Los resultados de las auditorías.
d) La retroalimentación de las partes interesadas.
e) La necesidad de cambios en el SGCN, incluyendo la política y los objetivos.
f) Los procedimientos y recursos que pueden ser usados por la organización para mejorar el desempeño y la eficacia del SGCN.
g) Información sobre el análisis de impacto del negocio y la evaluación de riesgos.

9.3 Revisión por la Dirección

h) Las salidas de la evaluación de la documentación y capacidades relacionadas con la continuidad del negocio.
i) Los riesgos o cuestiones que no han sido abordados adecuadamente en una evaluación previa de riesgos.
j) Las lecciones aprendidas y las acciones que surgieron de los incidentes o incidentes disruptivos.
k) Las oportunidades de mejora continua.

9.3 Revisión por la Dirección

9.3.3 Resultados de la revisión por la dirección

9.3.3.1 las salidas de la revisión por la dirección deben incluir las decisiones y acciones relacionadas con las oportunidades de mejora; cualquier necesidad de cambio en el SGCN y las necesidades de cambio del SGCN para mejorar la eficacia y eficiencia, incluyendo lo siguiente:

a) Variaciones en el alcance del SGCN.
b) La actualización del análisis de impacto del negocio, de la evaluación de riesgos, , de las estrategias de continuidad de negocios, y las soluciones y los planes de continuidad del negocio.
c) La modificación de los procedimientos y controles para responder a las cuestiones internas o externos que puedan impactar en el SGCN.
d) Cómo se medirá la eficacia de los controles.

9.3 Revisión por la Dirección

9.3.3.2 la organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.

La organización debe:

a) Comunicar los resultados de la revisión de gestión a las partes interesadas pertinentes.
b) Tomar las acciones apropiadas relacionadas con esos resultados.

10. Mejora

Mejora

- 10. Mejora.
  - 10.1 No conformidad y acción correctiva.
  - 10.2 Mejora continua.

10.1 No Conformidad y Acción Correctiva

10.1.1 La organización debe determinar las oportunidades para mejora e implementar cualquier acción necesaria para lograr los resultados deseados de su SGCN.

10.1.2 Cuando ocurra una no conformidad, la organización debe:

a) Reaccionar ante la no conformidad y, cuando sea aplicable:
   1. Tomar acciones para controlarla y corregirla.
   2. Hacer frente a las consecuencias.

b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:
   1. La revisión de la no conformidad.
   2. La determinación de las causas de la no conformidad.
   3. La determinación de si existen no conformidades similares, o que potencialmente puedan ocurrir.

10.1 No Conformidad y Acción Correctiva

c) Implementar cualquier acción necesaria.
d) Revisar la eficacia de cualquier acción correctiva tomada.
e) Si fuera necesario, hacer cambios al SGCN.

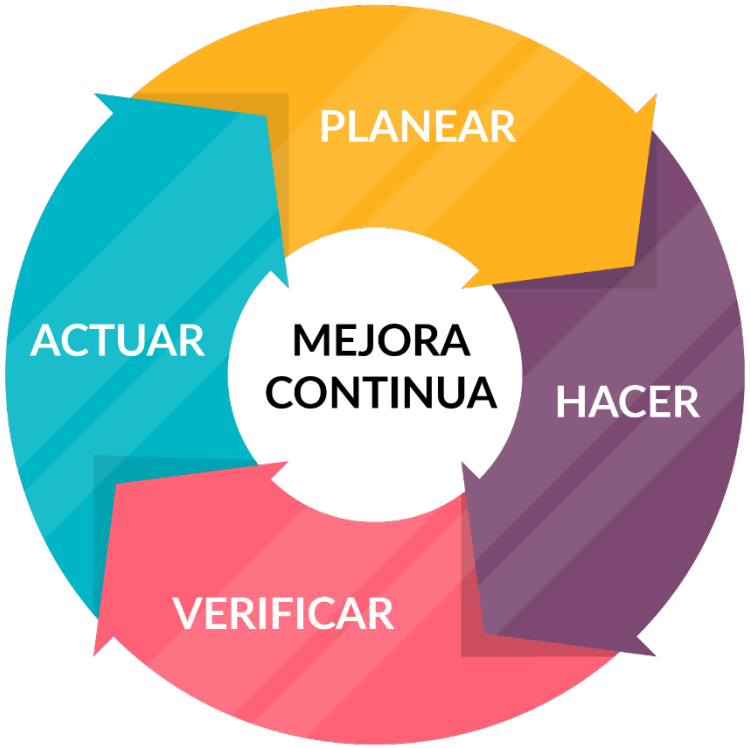
Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

10.1.3 La organización debe conservar la información documentada como evidencia de:

- La naturaleza de las no conformidades y de cualquier acción tomada posteriormente.
- Los resultados de cualquier acción correctiva.

10.2 Mejora Continua

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGCN basado en mediciones cualitativas y cuantitativas.



10.2 Mejora Continua

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGCN basado en mediciones cualitativas y cuantitativas.

La organización debe considerar los resultados del análisis y la evaluación, y las salidas de la revisión por la dirección, para determinar si hay necesidades u oportunidades relacionadas con la continuidad del negocio o con el SGCN, que deben considerarse como parte de la mejora continua.

NOTA: la organización puede usar los procesos del SGCN como el liderazgo, la planificación, y la evaluación de desempeño para lograr la mejora.

Anexo 1: Términos y Definiciones

3.1 Actividad

Conjunto de una o más tareas con una salida definida.

[Fuente: ISO 22300:2018, 3.1 modificado. La definición ha sido reemplazada y se eliminó el ejemplo]

3.2 Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

- **NOTA 1:** Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).

- **NOTA 2:** La auditoría interna la realiza la propia organización (3.1.14) o una parte externa en su nombre.

- **NOTA 3:** "Evidencia de la auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.

3.2 Auditoría

- **NOTA 4:** los elementos fundamentales de una auditoría incluyen la determinación de la conformidad de un objeto de acuerdo a un procedimiento llevado a cabo por personas que no son responsables por el objeto auditado.

- **NOTA 5:** una auditoría interna puede ser para la revisión por la dirección y otros propósitos internos y puede ser la base para la declaración de conformidad de una organización. La independencia puede ser demostrada mediante la no responsabilidad por la actividad que está siendo auditada. Las auditorías externas incluyen las de segunda y tercera parte. Las auditorías de segunda parte son realizadas por una parte que tiene un interés en la organización, como los clientes o por otras personas en su representación. Las auditorías de tercera parte son realizadas por organizaciones auditoras externas e independientes, como las que proveen la certificación o registro de conformidad o las agencias gubernamentales.

- **NOTA 6:** éste constituye uno de los términos comunes y las definiciones claves de la estructura de alto nivel de las normas de sistemas de gestión de ISO. La definición original fue modificada con la adición delas Notas a la entrada 4 y 5.

3.3 Continuidad del Negocio

Capacidad de la organización para continuar con la entrega de productos o servicios en un marco de tiempo aceptable a niveles predefinidos aceptables durante un incidente disruptivo.

[Fuente: ISO 22300:2018, 3.24 modificado- Esta definición ha sido reemplazada]

3.4 Plan de Continuidad del Negocio

Información documentada que guía a una organización para responder a un incidente disruptivo y recuperar, reanudar y restaurar la entrega de productos y servicios en forma coherente con sus objetivos de continuidad del negocio

[Fuente: ISO 22300:2018, 3.27 modificado- La definición ha sido reemplazada y la nota 1 a la entrada ha sido eliminada]

3.5 Análisis del Impacto en el Negocio

Proceso de análisis de impacto en el tiempo de un incidente disruptivo en la organización.

- **NOTA 1:** el resultado es una declaración y justificación de los requisitos (3.28) de continuidad del negocio (3.3).

[Fuente: ISO 22300:2018, 3.29 modificado. La definición ha sido reemplazada y la Nota 1 a la entrada ha sido añadida)]

3.6 Competencia

Capacidad de aplicar conocimientos y habilidades para alcanzar los resultados previstos.

- **NOTA 1**: Éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.7 Conformidad

Cumplimiento de un requisito.

- **Nota 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.8 Mejora Continua

Actividad recurrente para mejorar el desempeño.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.9 Acción Correctiva

Acción para eliminar las causas de una no conformidad y para prevenir la recurrencia.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.10 Incidente Disruptivo

Incidente anticipado o no anticipado, que causa una desviación no planificada y negativa de la entrega esperada de productos o servicios de acuerdo a los objetivos de una organización.

[Fuente: ISO 22300:2018, 3.70 modificado. La definición ha sido reemplazada.]

3.11 Información Documentada

Información que requiere ser controlada y mantenida por una organización (3.219 y el medio en que está contenida.

- **NOTA 1:** la información documentada puede estar en cualquier formato y medio y puede ser de cualquier fuente.
- **NOTA 2:** la información documentada se puede referir a:
  - El sistema de gestión, incluyendo los procesos relacionados.
  - La información creada para la operación de la organización (documentación).
  - La evidencia de los resultados logrados (registros).
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.12 Eficacia

Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.13 Impacto

Resultado de un incidente disruptivo afectando a los objetivos.

[Fuente: ISO 22300:2018, 3.107 modificado. La definición ha sido reemplazada.]

3.14 Incidente

Evento que puede ser o puede dar lugar a un incidente disruptivo, pérdida, emergencia o crisis.

[Fuente: ISO 22300:2018, 3.111 modificado. La definición ha sido reemplazada.]

3.15 Partes Interesadas

Persona u organización que puede afectar, ser afectada, o percibirse a sí misma como afectada por una decisión o actividad.

Ejemplo: Los clientes, propietarios, personal, proveedores, bancos, reguladores, uniones, socios y la sociedad que puede incluir competidores o grupos opositores de presión.

- **NOTA 1:** una parte interesada puede ser un tomador de decisiones.
- **NOTA 2:** se consideran partes interesadas las comunidades afectadas o las poblaciones locales.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO. Se ha modificado la definición original con el agregado de un ejemplo y las Notas 1 y 2 a la entrada.

3.16 Sistema de Gestión

Conjunto de elementos interrelacionados o que interactúan, de una organización para establecer políticas y objetivos y los procesos para alcanzar dichos objetivos.

- **NOTA 1:** un sistema de gestión puede abordar una o varias disciplinas.
- **NOTA 2:** los elementos del sistema incluyen la estructura de la organización, los roles y responsabilidades, la planificación, operación, etc.
- **NOTA 3:** el alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones a través de un grupo de organizaciones.
- **NOTA 4:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.17 Medición

Proceso para determinar un valor.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.18 Seguimiento

Determinar el estado de un sistema, un proceso o una actividad.

- **NOTA 1:** para determinar el estado puede haber una necesidad de comprobar, supervisar u observar críticamente.
- **NOTA 2:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.19 No Conformidad

Incumplimiento de un requisito.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.20 Objetivo

Resultado a ser logrado.

- **NOTA 1:** un objetivo puede ser estratégico, táctico u operacional.
- **NOTA 2:** los objetivos se pueden relacionar con diferentes disciplinas (tales como objetivos financieros, de la salud y la seguridad, y ambientales) y pueden aplicarse a diferentes niveles (tales como, estratégico, en toda la organización, proyecto, producto y proceso.
- **NOTA 3:** un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado deseado, un propósito, un criterio operacional, como una continuidad del negocio o por el uso de otras palabras de significado similar (por ejemplo, objetivo general , meta o aspiración).
- **NOTA 4:** en el contexto de las normas de sistemas de gestión de continuidad del negocio, los objetivos de continuidad del negocio son establecidos por la organización, en coherencia con la política (3.24) de continuidad del negocio, para lograr resultados específicos.
- **NOTA 5:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.21 Organización

Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

- **NOTA 1:** el concepto de organización incluye, pero no se limita a, compañía, corporación, firma, empresa, autoridad, asociación, empresa unipersonal, caridad o institución, o parte o combinación de los mismos, ya sean incorporadas o no, públicas o privadas.
- **NOTA 2:** para las organizaciones con más de un equipo de operación, una sola unidad operativa puede definirse como una organización.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO. La definición original fue modificada con el agregado de la Nota 2 a la entrada.

3.22 Subcontratar

Convenir un arreglo en el cual una organización externa realice parte de los procesos o funciones de una organización.

- **NOTA 1**: una organización externa está fuera del alcance del sistema de gestión aunque la función o el proceso externalizado estén dentro del alcance.
- **NOTA 2**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.23 Desempeño

Resultado medible.

- **NOTA 1:** el desempeño puede relacionarse con resultados cuantitativos o cualitativos.
- **NOTA 2**: el desempeño puede relacionarse con la gestión de actividades, procesos productos (incluidos los servicios), sistemas u organizaciones.
- **NOTA 3**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.24 Política

Intenciones y dirección de una organización como ha sido expresado formalmente por la alta dirección de la organización.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.25 Actividad Prioritaria

Actividad (3.1) a la que se le debe tratar con urgencia para evitar los impactos (3.13) no aceptables para el negocio durante un incidente disruptivo.

[Fuente: ISO 22300:2018, 3.176, modificada- La definición ha sido reemplazada y la Nota 1 a la entrada ha sido eliminada.]

3.26 Proceso

Conjunto de actividades (3.1) interrelacionadas o que interactúan, las cuales transforman elementos de entrada en salidas

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.27 Productos y Servicios

Salidas o resultados proporcionados por una organización a sus partes interesadas.

- **NOTA 1:** por ejemplo los artículos manufacturados, seguros de automóviles y enfermería comunitaria.

[Fuente: ISO 22300:2018, 3.181, modificada- La definición ha sido reemplazada.]

3.28 Requisito

Necesidad o expectativa establecida, generalmente implícita u obligatoria.

- **NOTA 1:** organización y las partes interesadas que la necesidad o expectativa bajo consideración esté implícita.
- **NOTA 2:** un requisito especificado es uno que está establecido, por ejemplo, en la información documentada.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.29 Recursos

Todos los activos, personas, habilidades, información, tecnología (incluidas la planta física y los equipos), las instalaciones, y los suministros e información (ya sea electrónica o no) que una organización tiene que tener disponibles para su uso, cuando sea necesario, con el fin de operar y cumplir con sus objetivos.

[Fuente: ISO 22300:2018, 3.193, modificada- La definición ha sido reemplazada.]

3.30 Riesgo

Efecto de la incertidumbre sobre los objetivos (3.20).

- **NOTA 1:** un efecto es una desviación de lo esperado: positivo o negativo.
- **NOTA 2:** la incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, entendimiento o conocimiento de un evento, su consecuencia o probabilidad.
- **NOTA 3:** el riesgo a menudo se caracteriza por la referencia a potenciales "eventos" (como se define en la Guía ISO 73) y "consecuencias" (como se define en la Guía ISO 73), o una combinación de estos.
- **NOTA 4:** el riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad de ocurrencia asociada (como se define en la Guía ISO 73).
- **NOTA 5:** esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO. La definición ha sido modificada para agregar "sobre los objetivos" para ser consistente con la norma ISO 31000.

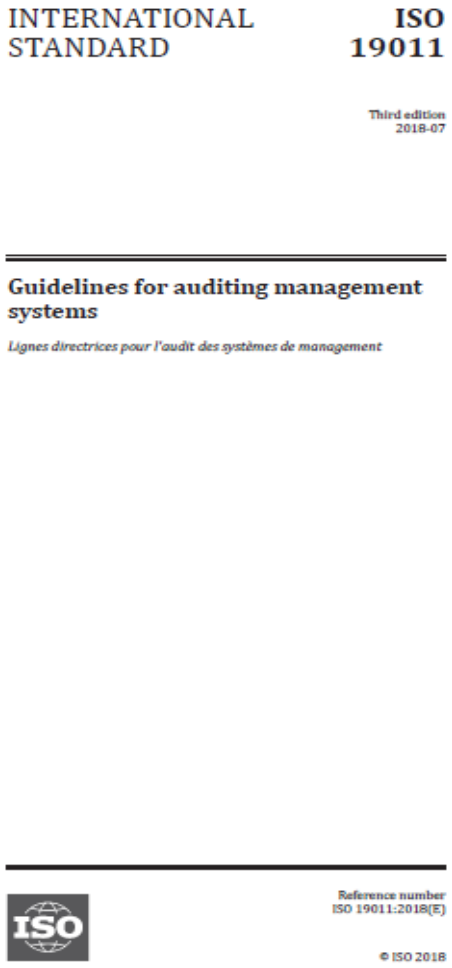
3.31 Alta Dirección

Persona o grupo de personas que dirigen y controlan una organización al más alto nivel.

- **NOTA 1:** la alta dirección tiene la facultad de delegar la autoridad y de proporcionar los recursos dentro de la organización.
- **NOTA 2:** si el alcance del sistema de gestión sólo cubre una parte de la organización, entonces, la alta dirección se orienta a los que dirigen y controlan esa parte de la organización.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

11. Módulo de Auditoría ISO 19011

ISO 19011:2018


INTERNATIONAL STANDARD

ISO 19011

Third edition
2018-07

Guidelines for auditing management systems

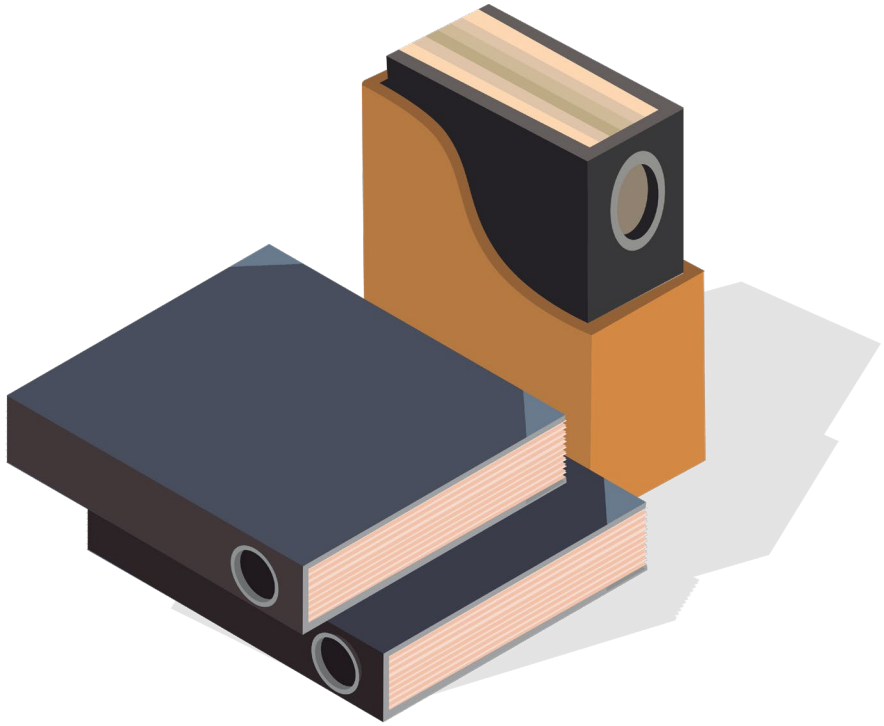
Lignes directrices pour l'audit des systèmes de management

Reference number
ISO 19011:2018(E)

© ISO 2018

Esta norma proporciona una guía para todos los tamaños y tipos de organizaciones y auditorías de diferentes alcances y escalas, incluidas aquellas realizadas por grandes equipos de auditoría, generalmente de organizaciones más grandes, y aquellas realizadas por auditores individuales, ya sea en organizaciones grandes o pequeñas. Esta orientación debería adaptarse según corresponda al alcance, la complejidad y la escala del programa de auditoría.

Estructura de la ISO 19011:2018



Prefacio.
Introducción.
1. Alcance.
2. Referencias normativas.
3. Términos y definiciones.
4. Principios de auditoría.
5. Administrar de un programa de auditoría.
6. Realización de una auditoría.
7. Competencia y evaluación de los auditores.

Anexo A.
Bibliografía.

Alcance ISO 19011:2018

Este documento proporciona orientación sobre auditoría a sistemas de gestión, incluidos los principios de auditoría, la gestión de un programa de auditoría y la realización de auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas involucradas en el proceso de auditoría.

Estas actividades incluyen las personas que administran el programa de auditoría, los auditores y los equipos de auditoría.

Es aplicable a todas las organizaciones que necesitan planificar y llevar cabo auditorías internas o externas de los sistemas de gestión o administrar un programa de auditoría.

La aplicación de este documento a otros tipos de auditorías es posible, siempre que se otorgue una consideración especial a la competencia específica necesaria.

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencia objetiva y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría.

NOTA 1: las auditorías internas, a veces llamadas auditorías de primera parte, son realizadas por, o en nombre de la organización misma.

NOTA 2: Las auditorías externas incluyen aquellas generalmente llamadas auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por las partes que tienen un interés en la organización, como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte son llevadas a cabo por organizaciones de auditoría independientes, como aquellas que proporcionan certificación / registro de conformidad o agencias gubernamentales.

Tipos de Auditoría

Tabla 1 - Diferentes tipos de auditorías

Auditoría de primera parte	Auditoría de segunda parte	Auditoría de tercera parte
Auditoría interna	Auditoría de proveedor externo	Auditoría de certificación y/o acreditación
	Otra auditoría de parte interesada externa	Auditoría legal, regulatoria y similar

Tipos de Auditoría

A) Auditorías internas: a veces llamadas auditorías de primera parte, son realizadas por, o en nombre de, la organización misma.

B) Auditorías externas: incluyen aquellas generalmente llamadas auditorías de segunda y tercera parte.

1. Auditorías de segunda parte se llevan a cabo por las partes que tienen un interés en la organización, como los clientes, o por otras personas en su nombre.

2. Auditorías de tercera parte son llevadas a cabo por organizaciones de auditoría independientes, como aquellas que proporcionan certificación / registro de conformidad o agencias gubernamentales.

Criterios de Auditoría

Conjunto de requisitos utilizados como referencia con respecto a los cuales se compara la evidencia objetiva.

NOTA 1: Si los criterios de auditoría son legales (incluidos los requisitos legales o reglamentarios), las palabras "cumplimiento" o "incumplimiento" a menudo se utilizan en una conclusión de auditoría

NOTA 2: Los requisitos pueden incluir políticas, procedimientos, instrucciones de trabajo, requisitos legales, obligaciones contractuales, etc..

Evidencia de la Auditoría

- La evidencia objetiva son los datos que respaldan la existencia o la verdad de algo.

- **NOTA 1:** La evidencia objetiva se puede obtener a través de observación, medición, prueba o por otros medios.

- **NOTA 2:** La evidencia objetiva para el propósito de la auditoría generalmente consiste en registros, declaraciones de hechos u otra información que son relevantes para los criterios de auditoría y verificables.

Resultados de la Auditoría

Los resultados de la evaluación de la evidencia de auditoría recopilada contra los criterios de auditoría.

Resultados de la Auditoría

- **NOTA 1:** los hallazgos de la auditoría indican conformidad o no conformidad.

- **NOTA 2:** los hallazgos de la auditoría pueden conducir a la identificación de riesgos, oportunidades de mejora o registro de buenas prácticas.

- **NOTA 3:** en inglés, si los criterios de auditoría se seleccionan de entre los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoría se denomina cumplimiento o incumplimiento.

Resultados de la Auditoría

- Hallazgo de cumplimiento.
- Requisitos (norma, legal, reglamentario, contractual).
- El elemento se ajusta a la exigencia.
- La implantación corresponde a la intención.
- La implantación es eficaz.

Mejores prácticas:

- Verificar los hechos verbales.
- Definir la naturaleza de la no conformidad con el auditado, detallando la evidencia de auditoría.
- Tomar notas y consultarlas posteriormente para realizar el reporte.
- Hacer un bosquejo del reporte de hallazgos durante la toma de información.
- Al finalizar cada jornada terminar en la revisión privada.

Conclusiones de la Auditoría

Resultado de una auditoría después de considerar los objetivos de auditoría y todos los resultados (hallazgos) de auditoría.

Cliente de la Auditoría

Organización o persona que solicita una auditoría.

•**NOTA 1:** en el caso de la auditoría interna, el cliente de auditoría también puede ser el auditado o la persona (s) que administra el programa de auditoría. Las solicitudes de auditoría externa pueden provenir de fuentes tales como reguladores, partes contratantes o clientes potenciales o existentes.

Auditado

Organización que está siendo auditada.

Auditor

Persona que lleva a cabo una auditoría.

Equipo Auditor

- Una o más personas que realizan una auditoría, apoyadas si es necesario por expertos técnicos.

- **NOTA 1:** Un auditor del equipo de auditoría es designado como el líder del equipo de auditoría.
- **NOTA 2:** El equipo de auditoría puede incluir auditores en capacitación.

Experto Técnico

- Persona que proporciona conocimientos o experiencia específicos al equipo de auditoría.

- **NOTA 1:** el conocimiento específico o experiencia se relaciona con la organización, la actividad, el proceso, el producto, el servicio, la disciplina que se auditará, el idioma o la cultura.
- **NOTA 2:** Un experto técnico del equipo de auditoría no actúa como auditor.

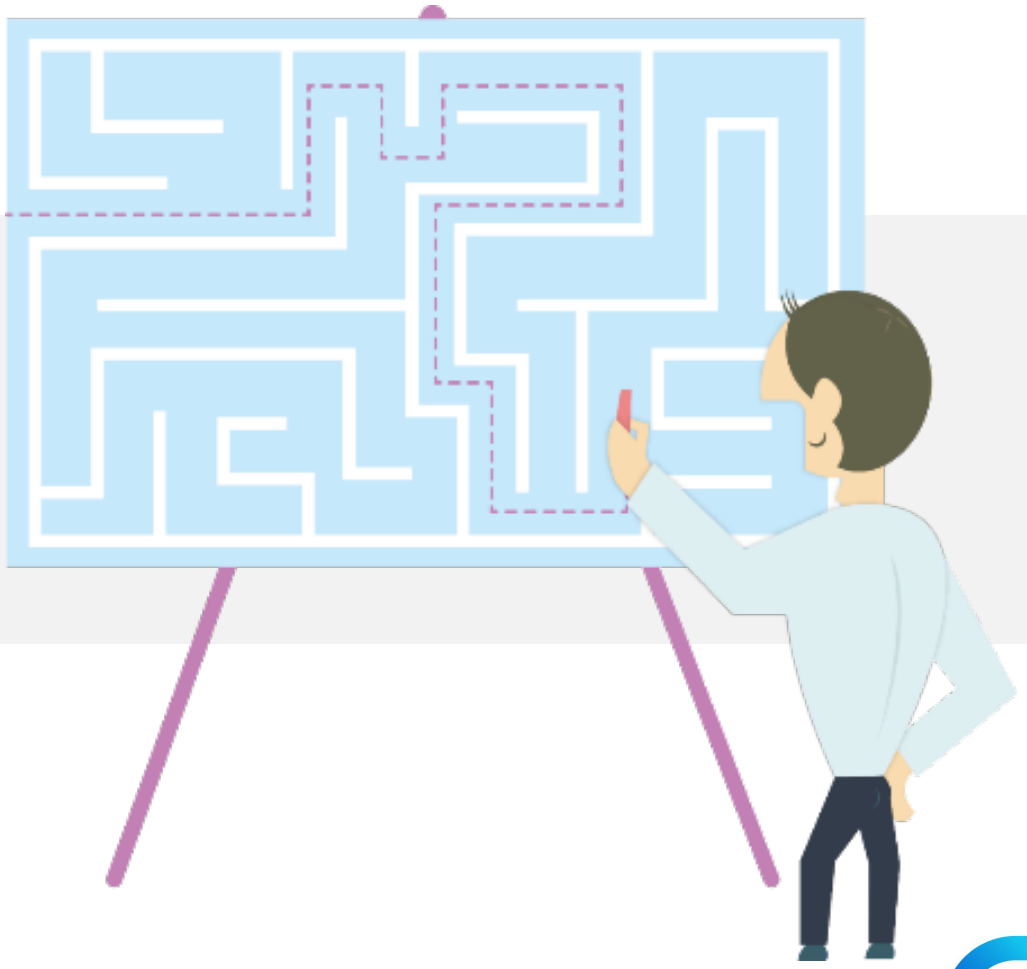
Observador

•Individuo que acompaña al equipo de auditoría pero que no actúa como auditor.

.

Guía

Persona designada por el auditado para asistir al equipo auditor.



Programa de Auditoría

- Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

Alcance de la Auditoría

•**Alcance de auditoría** se refiere al alcance y límites de una auditoría.

•El alcance de la auditoría generalmente incluye una descripción de las ubicaciones físicas y virtuales, funciones, unidades organizativas, actividades y procesos, así como el período de tiempo cubierto.

•Una ubicación virtual es cuando una organización realiza un trabajo o proporciona un servicio usando un entorno en línea que permite a las personas, independientemente de las ubicaciones físicas, ejecutar procesos.

Plan de Auditoría

Descripción de las actividades y de los detalles acordados de una auditoría.

Conformidad

Cumplimiento de un requisito.

No Conformidad

Incumplimiento de un requisito.

Pruebas de Auditoría

Registros, declaraciones de hechos u otra información, que sean relevantes para los criterios de auditoría y verificables.

Métodos de Auditoría

Alcance de la participación entre el auditor y el auditado	Ubicación del auditor	
	En el sitio	Remota
Interacción humana	Realización de entrevistas Completar listas de verificación y cuestionarios con participación del auditado Realización de una revisión de documentos con participación del auditado Muestreo	A través de comunicación interactiva significa: - realización de entrevistas; - observar el trabajo realizado con la guía remota; - completando listas de verificación y cuestionarios; - realización de revisión de documentos con participación de los propietarios.
Sin interacción humana	Realización de revisión de documentos (por ejemplo, registros, análisis de datos) Observando el trabajo realizado Llevando a cabo una visita in-situ Completando listas de verificación Muestreo (por ejemplo, productos)	Realización de revisión de documentos (por ejemplo, registros, análisis de datos) Observar el trabajo realizado a través de medios de vigilancia, teniendo en cuenta los requisitos sociales, estatutarios y normativos Análisis de datos
Las actividades de auditoría en el sitio se realizan en la ubicación del auditado. Las actividades de auditoría remota se realizan en cualquier lugar que no sea la ubicación del auditado, independientemente de la distancia. Las actividades de auditoría interactiva implican la interacción entre el personal del auditado y el equipo de auditoría. Las actividades de auditoría no interactivas no implican interacción humana con las personas que representan al auditado, pero sí implican la interacción con el equipo, las instalaciones y la documentación.		

Cláusula 4: Principios de Auditoría

1. Integridad: la base del profesionalismo.
2. Presentación justa: la obligación de informar veraz y exactamente.
3. Debido cuidado profesional: la aplicación de la diligencia y el juicio en la auditoría.
4. Confidencialidad: seguridad de la información.
5. Independencia: la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría.
6. Enfoque basado en la evidencia: el método racional para llegar a conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático.
7. Enfoque basado en el riesgo: un enfoque de auditoría que considera riesgos y oportunidades.

Cláusula 4: Principios de Auditoría

Integridad: la base del profesionalismo.

Los auditores y la(s) persona(s) que administran un programa de auditoría deberían:

a) Realizar su trabajo de forma ética, con honestidad y responsabilidad.
b) Solo realizar actividades de auditoría si es competente para hacerlo.
c) Realizar su trabajo de manera imparcial, es decir, seguir siendo justo e imparcial en todos sus tratos.
d) Ser sensible a cualquier influencia que pueda ejercer sobre su juicio mientras lleva a cabo una auditoría.

Cláusula 4: Principios de Auditoría

Presentación justa: la obligación de informar veraz y exactamente.

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. Se deberían informar los obstáculos significativos encontrados durante la auditoría y las opiniones divergentes no resueltas entre el equipo de auditoría y el auditado. La comunicación debería ser veraz, precisa, objetiva, oportuna, clara y completa.

Cláusula 4: Principios de Auditoría

Debido cuidado profesional: la aplicación de la diligencia y el juicio en la auditoría

Los auditores deberían 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. Un factor importante para llevar a cabo su trabajo con la debida atención profesional es tener la capacidad de emitir juicios razonados en todas las situaciones de auditoría.

Cláusula 4: Principios de Auditoría

Confidencialidad: seguridad de la información.

Los auditores deberían ejercer discreción en el uso y la protección de la información adquirida en el desempeño de sus funciones. La información de auditoría no debería ser utilizada de manera inapropiada para beneficio personal por el auditor o el cliente de auditoría, o de una manera perjudicial para los intereses legítimos del auditado. Este concepto incluye el manejo adecuado de información sensible o confidencial.

Cláusula 4: Principios de Auditoría

Independencia: la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría.

Los auditores deberían ser independientes 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. Para las auditorías internas, los auditores deberían ser independientes de la función que se está auditando, si es posible. Los auditores deberían mantener la objetividad durante todo el proceso de auditoría para garantizar que los hallazgos y conclusiones de la auditoría se basen solo en la evidencia de auditoría.

Para las organizaciones pequeñas, puede que los auditores internos no sean totalmente independientes de la actividad que se audita, pero se deberían hacer todos los esfuerzos para eliminar el sesgo y alentar la objetividad.

Cláusula 4: Principios de Auditoría

Enfoque basado en la evidencia: el método racional para llegar a conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático.

La evidencia de auditoría debería ser verificable. En general, debería basarse 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.

Cláusula 4: Principios de Auditoría

Enfoque basado en el riesgo: un enfoque de auditoría que considera riesgos y oportunidades

El enfoque basado en el riesgo debería influir 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.

Cláusula 5: Programa de Auditoría

La 19011 lo define como arreglos para un conjunto de una o más auditorías planificadas para un marco de tiempo específico y dirigidas hacia un propósito específico.

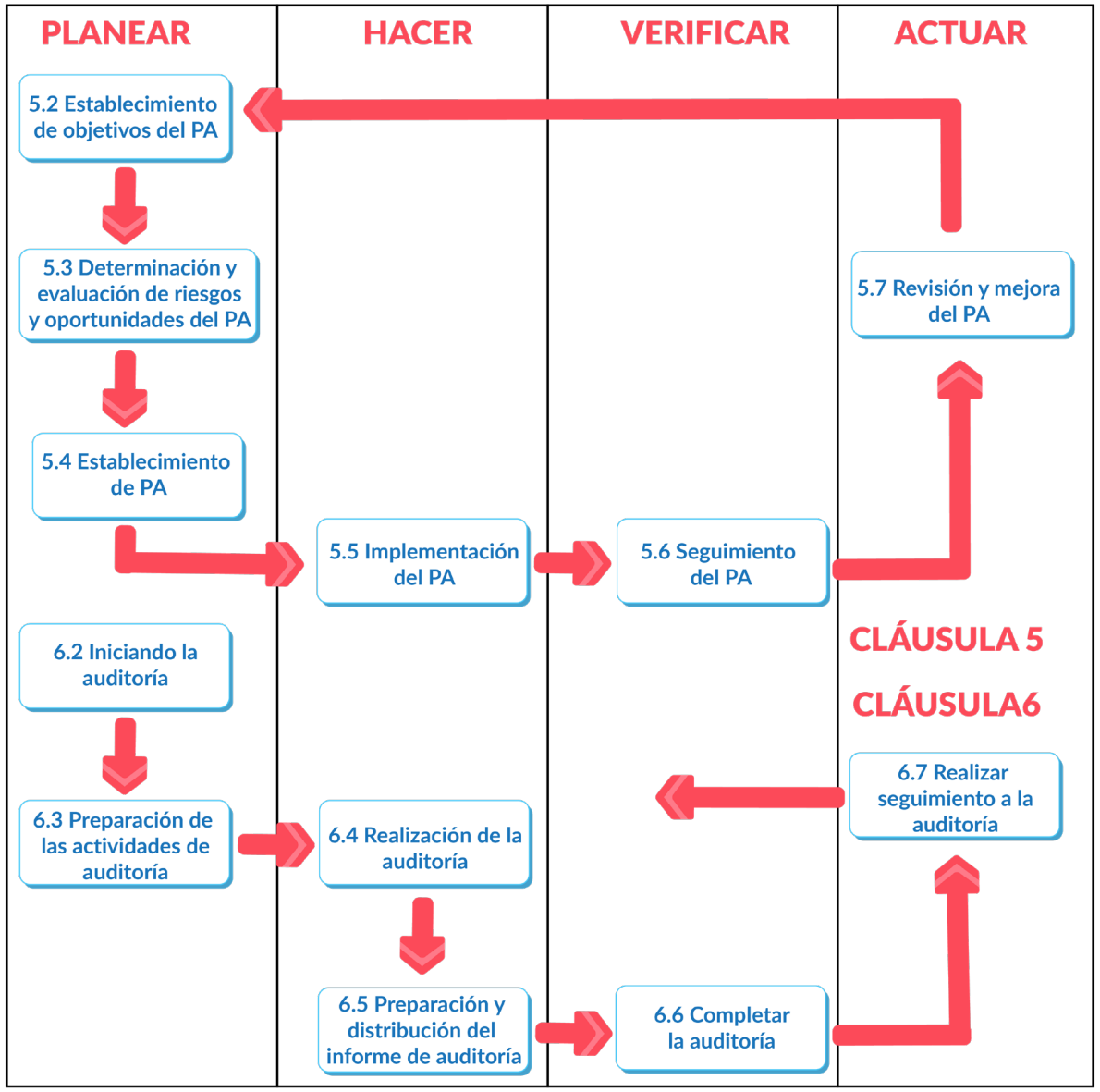
Un programa de auditoría puede incluir una o más auditorías, dependiendo del tamaño, la naturaleza y la complejidad de la organización que va a ser auditada.

El alcance de un programa de auditoría debería basarse en el tamaño y la naturaleza del auditado, así como en la naturaleza, funcionalidad, complejidad, el tipo de riesgos y oportunidades, y el nivel de madurez de los sistemas de gestión a ser auditados.

Para comprender el contexto del auditado, el programa de auditoría debería, del auditado; tener en cuenta:

- Objetivos organizacionales.
- Cuestiones externas e internas relevantes.
- Las necesidades y expectativas de las partes interesadas pertinentes.
- Requisitos de confidencialidad y seguridad de la información.

Flujo de procesos para gestionar un programa de auditoría (PA)



Cláusula 5: Programa de Auditoría

Nota 1: Esta figura ilustra la aplicación del ciclo Planear - Hacer - Verificar - Actuar, en este documento.

Nota 2: La numeración de cláusulas/subcláusulas se refiere a las cláusulas/subcláusuluas relevantes de este documento.

Figura 1: Flujo de proceso para la gestión de un programa de auditoría.

Cláusula 5: Programa de Auditoría

Auditorías	Enero	Febrero	Marzo	Abril	Mayo
Auditoría No. 1					
Auditoría No. 2					
Auditoría No. 3					
Auditoría No. 4					
Auditoría No. 5					

Cláusula 6: Actividades de la Auditoría

Esta cláusula proporciona orientación sobre la planificación y la forma de llevar a cabo las actividades de auditoría como parte de un programa de auditoría.

01

6.2 Inicio de la Auditoría
6.2.1 Generalidades.
6.2.2 Establecer contacto con el auditado.
6.2.3 Determinación de la viabilidad de la auditoría.

02

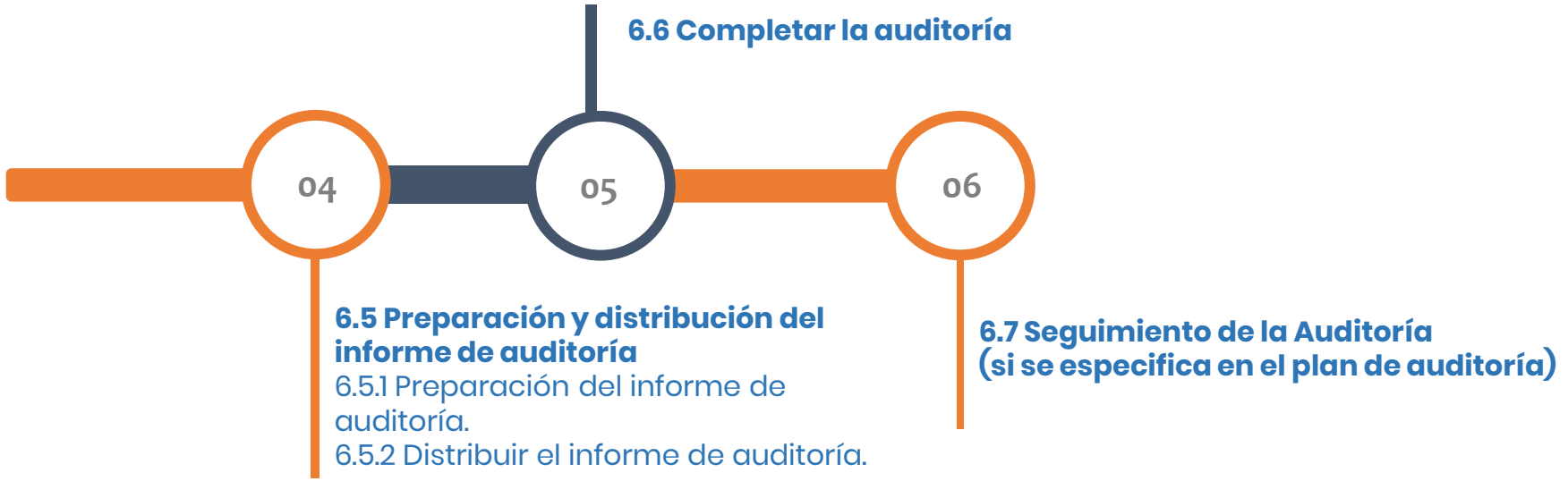
6.3 Preparación de actividades de auditoría
6.3.1 Realizar revisión de información documentada.
6.3.2 Planificación de auditoría.
6.3.3 Asignación de trabajo al equipo de auditoría.
6.3.4 Preparación de información documentada para auditoría.

03

6.4 Realización de actividades de auditoría
6.4.1 Generalidades.
6.4.2 Asignación de roles y responsabilidades de guías y observadores.
6.4.3 Realización de la reunión de apertura.
6.4.4 Comunicación durante la auditoría.
6.4.5 Disponibilidad y acceso a la información de auditoría.
6.4.6 Revisión de información documentada durante la realización de la auditoría.
6.4.7 Recopilación y verificación de información.
6.4.8 Generación de hallazgos de auditoría.
6.4.9 Determinación de conclusiones de auditoría.
6.4.10. Realización de la reunión de cierre.

Cláusula 6: Actividades de la Auditoría

Esta cláusula proporciona orientación sobre la planificación y la forma de llevar a cabo las actividades de auditoría como parte de un programa de auditoría.



Cláusula 7: Competencia y Evaluación de los Auditores

Esta cláusula trata las competencias de los auditores al realizar una auditoría. Los auditores deben:

Poseer cualidades personales, tales como diplomacia, sinceridad, percepción, persistencia, etc. para que la auditoría se realice en forma profesional y correcta a la vez.

Poseer conocimientos genéricos y habilidades tales como:

- Aplicar principios, procedimientos y técnicas de auditoría.
- Planificar y organizar el trabajo en forma eficaz.
- Conocer los códigos, leyes y normativas locales, regionales y nacionales.

Cláusula 7: Competencia y Evaluación de los Auditores

Poseer un adecuado nivel de educación, experiencia laboral, capacitación como auditor y experiencia en auditorías.

Mantener y mejorar en forma continua sus habilidades y competencias.

Métodos para Evaluar a los Auditores

Método de evaluación	Objetivos	Ejemplos
Revisión de registros	Verificar los antecedentes del auditor	Análisis de registros de educación, capacitación, empleo, credenciales profesionales y experiencia en auditoría
Retroalimentación	Obtener/proporcionar información sobre cómo se percibe el desempeño del auditor	Encuestas, cuestionarios, referencias personales, testimonios, reclamos, evaluación de desempeño, revisión por pares
Entrevista	Evaluar el comportamiento profesional deseado y las habilidades de comunicación. Verificar la información y probar el conocimiento, y Adquirir información adicional	Entrevistas personales
Observación	Evaluar el comportamiento profesional deseado y la capacidad de aplicar los conocimientos y las habilidades	Role playing, auditorías atestiguadas, desempeño en el trabajo.
Pruebas	Evaluar el comportamiento deseado, el conocimiento, las habilidades y su aplicación	Exámenes orales y escritos, pruebas psicométricas
Revisión posterior a la auditoría	Proporcionar información sobre el desempeño del auditor durante las actividades de auditoría, identificar fortalezas y oportunidades de mejora	Revisión del informe de auditoría, entrevistas con el líder del equipo de auditoría, el equipo de auditoría y, si corresponde, retroalimentación del auditado

Cláusula 7: Atributos Personales

a) **Ético,** es decir, justo, veraz, sincero, honesto y discreto.
b) **De mente abierta**, es decir, dispuesto a considerar ideas o puntos de vista alternativos.
c) **Diplomático**, es decir, discreto al tratar con individuos.
d) **Observador**, es decir, observando activamente el entorno físico y las actividades.
e) **Perceptivo**, es decir, consciente de y capaz de comprender situaciones.
f) **Versátil**, es decir, capaz de adaptarse fácilmente a diferentes situaciones.
g) **Tenaz**, es decir persistente y enfocado en alcanzar objetivos.
h) **Decisivo,** es decir, capaz de llegar a conclusiones oportunas basadas en el razonamiento lógico y el análisis.
i) **Autosuficiente,** es decir, capaz de actuar y funcionar independientemente mientras interactúa efectivamente con otros.

Cláusula 7: Atributos Personales

j) **Capaz de actuar con fortaleza,** es decir, capaz de actuar de manera responsable y ética, aunque estas acciones no siempre sean populares y en ocasiones pueden dar lugar a desacuerdos o confrontaciones.
k) **Abierto a la mejora,** es decir, dispuesto a aprender de las situaciones.
l) **Culturalmente sensible,** es decir, atento y respetuoso con la cultura del auditado.
m) **Colaborador,** es decir, interacción efectiva con otros, incluidos los miembros del equipo de auditoría y el personal del auditado.

Cláusula 7: Conocimientos Genéricos y Habilidades

Los auditores deberían tener conocimiento y habilidades en las áreas que se detallan a continuación.

a) Principios, procesos y métodos de auditoría: el conocimiento y las habilidades en esta área le permiten al auditor asegurar que las auditorías se realicen de manera consistente y sistemática.

Un auditor debería ser capaz de:

- Comprender los tipos de riesgos y oportunidades asociados con la auditoría y los principios del enfoque de auditoría basado en el riesgo.
- Planificar y organizar el trabajo de manera efectiva.
- Realizar la auditoría dentro del cronograma acordado.
- Priorizar y enfocarse en asuntos importantes.

Cláusula 7: Conocimientos Genéricos y Habilidades

- Comunicarse de manera efectiva, oralmente y por escrito (ya sea personalmente o mediante el uso de intérpretes).
- Recopilar información mediante entrevistas efectivas, escuchar, observar y revisar información documentada, incluidos registros y datos.
- Comprender la idoneidad y las consecuencias del uso de técnicas de muestreo para la auditoría.
- Entender y considerar las opiniones de los expertos técnicos.
- Auditar un proceso de principio a fin, incluidas las interrelaciones con otros procesos y diferentes funciones, según corresponda.
- Verificar la relevancia y exactitud de la información recopilada.
- Confirmar la suficiencia e idoneidad de la evidencia de auditoría para respaldar los hallazgos y conclusiones de la auditoría.
- Evaluar aquellos factores que pueden afectar la confiabilidad de los hallazgos y conclusiones de la auditoría.
- Documentar las actividades de auditoría y los hallazgos de auditoría, y preparar informes.
- Mantener la confidencialidad y seguridad de la información.

Cláusula 7: Conocimientos Genéricos y Habilidades

b) Normas del sistema de gestión y otras referencias: el conocimiento y las habilidades en esta área le permiten al auditor comprender el alcance de la auditoría y aplicar criterios de auditoría, y deberían cubrir lo siguiente:

- Normas del sistema de gestión u otros documentos normativos u orientativos/de apoyo utilizados para establecer criterios o métodos de auditoría.
- La aplicación de los estándares del sistema de gestión por el auditado y otras organizaciones.
- Relaciones e interacciones entre los procesos del sistema de gestión.
- Comprender la importancia y la prioridad de múltiples estándares o referencias.
- Aplicación de estándares o referencias a diferentes situaciones de auditoría.

Cláusula 7: Conocimientos Genéricos y Habilidades

c) La organización y su contexto: el conocimiento y las habilidades en esta área le permiten al auditor comprender la estructura, el propósito y las prácticas de gestión del auditado y debería cubrir lo siguiente:

- Necesidades y expectativas de las partes interesadas relevantes que impactan en el sistema de gestión.
- Tipo de organización, gobierno, tamaño, estructura, funciones y relaciones.
- Conceptos generales de negocios y gestión, procesos y terminología relacionada, incluida la planificación, presupuestación y gestión de personas.
- Aspectos culturales y sociales del auditado.

Cláusula 7: Conocimientos Genéricos y Habilidades

d) Requisitos reglamentarios y legales aplicables y otros requisitos: el conocimiento y las habilidades en esta área le permiten al auditor conocer y trabajar dentro de los requisitos de la organización. Los conocimientos y habilidades específicos de la jurisdicción o de las actividades, procesos, productos y servicios del auditado deberían cubrir lo siguiente:

- Requisitos legales y reglamentarios, así como sus agencias de gobierno.
- Terminología jurídica básica.
- Contratación y responsabilidad.

NOTA: la conciencia de los requisitos legales y reglamentarios no implica pericia legal y una auditoría del sistema de gestión no debería tratarse como una auditoría de cumplimiento legal.

Establecimiento de Objetivos del Programa de Auditoría

El cliente de auditoría debería asegurarse de que los objetivos del programa de auditoría se establezcan para dirigir la planificación y la realización de auditorías, y debería garantizar que el programa de auditoría se implemente de manera efectiva.

Los objetivos del programa de auditoría deberían ser coherentes con la orientación estratégica y los objetivos y la política del sistema de gestión de soporte del cliente de auditoría.

Establecimiento de Objetivos del Programa de Auditoría

Estos objetivos pueden basarse en la consideración de lo siguiente:

a) Las necesidades y expectativas de las partes interesadas pertinentes, tanto externas como internas.
b) Características y requisitos de procesos, productos, servicios y proyectos, y cualquier cambio en ellos.
c) Requisitos del sistema de gestión.
d) Necesidad de evaluación de proveedores externos.
e) El nivel de rendimiento y el nivel de madurez del sistema o sistemas de gestión del auditado, como se refleja en los indicadores de rendimiento relevantes (por ejemplo, KPI's), la ocurrencia de no conformidades, incidentes o quejas de las partes interesadas.
f) Identificó riesgos y oportunidades para el auditado.
g) Resultados de auditorías anteriores.

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

Existen riesgos y oportunidades relacionados con el contexto del auditado que pueden asociarse con un programa de auditoría y pueden afectar el logro de sus objetivos.

La persona responsable del programa de auditoría **debería considerar los riesgos** durante el desarrollo del programa:

a) **Planificación**, por ejemplo; no establecer los objetivos de auditoría relevantes y determinar el alcance, el número, la duración, las ubicaciones y el cronograma de las auditorías.

b) **Recursos,** por ejemplo; permitir tiempo, equipo y/o capacitación insuficientes para desarrollar el programa de auditoría o realizar una auditoría.

c) **Selección del equipo de auditoría,** por ejemplo; competencia global insuficiente para realizar auditorías de manera efectiva.

d) **Comunicación,** por ejemplo; procesos/canales de comunicación externos/internos ineficaces.

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

e) **Implementación**, por ejemplo; coordinación ineficaz de las auditorías dentro del programa de auditoría, o no considerar la seguridad y confidencialidad de la información.

f) **Control de la información documentada**, por ejemplo; la determinación ineficaz de la información documentada necesaria requerida por los auditores y las partes interesadas pertinentes; la falta de protección adecuada de los registros de auditoría para demostrar la eficacia del programa de auditoría.

g) **Supervisar, revisar y mejorar el programa de auditoría**, por ejemplo; seguimiento ineficaz de los resultados del programa de auditoría.

h) **Disponibilidad y cooperación del auditado** y disponibilidad de evidencia para ser muestreada.

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

Las oportunidades para mejorar el programa de auditoría pueden incluir:

a) Permitir múltiples auditorías en una sola visita.
b) Minimizar el tiempo y las distancias que viajan al sitio.
c) Hacer coincidir el nivel de competencia del equipo de auditoría con el nivel de competencia necesario para alcanzar los objetivos de la auditoría.
d) Alinear las fechas de auditoría con la disponibilidad del personal clave del auditado.

Establecimiento del Programa de Auditoría

Roles y responsabilidades de las personas que gestionan el programa de auditoría

a) Establecer la extensión del programa de auditoría de acuerdo con los objetivos relevantes y cualquier restricción conocida.

b) Determinar los problemas externos e internos, y los riesgos y oportunidades que pueden afectar el programa de auditoría, e implementar acciones para abordarlos, integrando estas acciones en todas las actividades de auditoría relevantes, según corresponda.

c) Garantizar la selección de los equipos de auditoría y la competencia general para las actividades de auditoría mediante la asignación de funciones, responsabilidades y autoridades, y el apoyo al liderazgo, según corresponda.

Establecimiento del Programa de Auditoría

d) Establecer todos los procesos relevantes, incluidos los procesos para:

- La coordinación y programación de todas las auditorías dentro del programa de auditoría.
- El establecimiento de objetivos de auditoría, alcance(s) y criterios de las auditorías, determinación de los métodos de auditoría y selección del equipo de auditoría.
- Evaluación de auditores.
- El establecimiento de procesos de comunicación externa e interna, según corresponda.
- La resolución de disputas y el manejo de quejas.
- Seguimiento de auditoría si corresponde.
- Informar al cliente de auditoría y a las partes interesadas pertinentes, según corresponda.

Establecimiento del Programa de Auditoría

e) Determinar y garantizar la provisión de todos los recursos necesarios.
f) Garantizar que se prepare y mantenga la información documentada apropiada, incluidos los registros del programa de auditoría.
g) Monitorear, revisar y mejorar el programa de auditoría.
h) Comunicar el programa de auditoría al cliente de auditoría y, según corresponda, a las partes interesadas pertinentes.

Las personas que gestionan el programa de auditoría deberían solicitar su aprobación al cliente de auditoría.

Competencia del(los) Individuo(s) que Gestiona(n) el Programa de Auditoría

La(s) persona(s) que gestiona(n) el programa de auditoría deberían tener la competencia necesaria para gestionar el programa, sus riesgos y oportunidades asociados y los problemas externos e internos de manera efectiva y eficiente, incluido el conocimiento de:

a) Principios de auditoría, métodos y procesos.

b) Normas del sistema de gestión, otras normas pertinentes y documentos de referencia / orientación.

c) Información sobre el auditado y su contexto (por ejemplo, asuntos externos/internos, partes interesadas relevantes y sus necesidades y expectativas, actividades comerciales, productos, servicios y procesos del auditado.

d) Requisitos legales y reglamentarios aplicables y otros requisitos relevantes para las actividades comerciales del auditado.

Establecer el Alcance del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían determinar el alcance del programa de auditoría. Esto puede variar según la información proporcionada por el auditado con respecto a su contexto.

Otros factores que impactan en el alcance del programa de auditoría:

a) El objetivo, el alcance y la duración de cada auditoría y la cantidad de auditorías que se llevarán a cabo, el método de notificación y, si corresponde, el seguimiento de la auditoría.
b) Las normas del sistema de gestión u otros criterios aplicables.
c) El número, la importancia, la complejidad, la similitud y la ubicación de las actividades a auditar.

Establecer el Alcance del Programa de Auditoría

d) Aquellos factores que influyen en la efectividad del sistema de gestión.
e) Los criterios de auditoría aplicables, tales como los arreglos planificados para las normas del sistema de gestión pertinentes, los requisitos legales y reglamentarios, y otros requisitos con los que la organización está comprometida.
f) Resultados de auditorías internas o externas previas y revisiones de la dirección, si corresponde.
g) Resultados de una revisión previa del programa de auditoría.
h) Problemas lingüísticos, culturales y sociales.
i) Las preocupaciones de las partes interesadas, tales como las quejas de los clientes, el incumplimiento de los requisitos legales y reglamentarios y otros requisitos con los que la organización se compromete, o los problemas de la cadena de suministro.

Establecer el Alcance del Programa de Auditoría

j) Cambios significativos en el contexto del auditado o sus operaciones y riesgos y oportunidades relacionados;

k) Disponibilidad de tecnologías de información y comunicación para respaldar las actividades de auditoría, en particular el uso de métodos de auditoría remota.

l) La ocurrencia de eventos internos y externos, tales como no conformidades de productos o servicios, fugas de seguridad de la información, incidentes de salud y seguridad, actos delictivos o incidentes ambientales.

m) Riesgos y oportunidades comerciales, incluidas las acciones para abordarlos.

Determinar los Recursos del Programa de Auditoría

Al determinar los recursos para el programa de auditoría, las personas que gestionan el programa de auditoría deberían considerar:

a) Los recursos financieros y de tiempo necesarios para desarrollar, implementar, administrar y mejorar las actividades de auditoría.
b) Métodos de auditoría.
c) La disponibilidad individual y general de auditores y expertos técnicos que posean las competencias apropiadas para los objetivos particulares del programa de auditoría.
d) La extensión del programa de auditoría y los riesgos y oportunidades del programa de auditoría.
e) Tiempo de viaje y costo, alojamiento y otras necesidades de auditoría.

Determinar los Recursos del Programa de Auditoría

f) El impacto de las diferentes zonas horarias.
g) La disponibilidad de tecnologías de información y comunicación (por ejemplo, los recursos técnicos necesarios para establecer una auditoría remota utilizando tecnologías que admiten la colaboración remota).
h) La disponibilidad de cualquier herramienta, tecnología y equipo requerido.
i) La disponibilidad de la información documentada necesaria, según se determine durante el establecimiento del programa de auditoría.
j) Los requisitos relacionados con la instalación, incluidos los espacios de seguridad y el equipo (por ejemplo, equipo de protección personal entre otras).

Implementación del Programa de Auditoría

a) Comunicar las partes pertinentes del programa de auditoría, incluidos los riesgos y oportunidades, a las partes interesadas pertinentes e informarles periódicamente de su progreso, utilizando los canales de comunicación externos e internos establecidos.
b) Definir objetivos, alcance y criterios para cada auditoría individual.
c) Seleccionar métodos de auditoría.
d) Coordinar y programar auditorías y otras actividades relevantes para el programa de auditoría.
e) Garantizar que los equipos de auditoría tengan la competencia necesaria.

Implementación del Programa de Auditoría

f) Proporcionar los recursos individuales y globales necesarios a los equipos de auditoría.
g) Garantizar la realización de auditorías de acuerdo con el programa de auditoría, gestionando todos los riesgos, oportunidades y problemas operativos (es decir, eventos inesperados), tal como surgen durante el despliegue del programa.
h) Garantizar que la información documentada relevante con respecto a las actividades de auditoría se gestiona y mantiene de forma adecuada.
i) Definir e implementar los controles operativos necesarios para la supervisión del programa de auditoría.
j) Revisar el programa de auditoría para identificar oportunidades para su mejora.

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual

Cada auditoría individual debería basarse en objetivos de auditoría definidos, alcance y criterios. Estos deberían ser consistentes con los objetivos generales del programa de auditoría.

Los objetivos de la auditoría definen que se va a lograr con la auditoría individual y pueden incluir lo siguiente:

a) Determinación del grado de conformidad del sistema de gestión a ser auditado, o partes de él, con los criterios de auditoría.

b) Evaluación de la capacidad del sistema de gestión para ayudar a la organización a cumplir los requisitos legales y reglamentarios pertinentes y otros requisitos con los que la organización está comprometida.

c) Evaluación de la efectividad del sistema de gestión para alcanzar los resultados esperados.

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual

d) Identificación de oportunidades para la mejora potencial del sistema de gestión.

e) Evaluación de la idoneidad y adecuación del sistema de gestión con respecto al contexto y la dirección estratégica del auditado.

f) Evaluación de la capacidad del sistema de gestión para establecer y alcanzar objetivos y abordar de manera efectiva los riesgos y oportunidades, en un contexto cambiante, incluida la implementación de las acciones relacionadas.

El alcance de la auditoría debería ser coherente con el programa de auditoría y los objetivos de auditoría.

Selección y Determinación de Métodos de Auditoría

El(los) individuo(s) que gestiona(n) el programa de auditoría debería(n) seleccionar y determinar los métodos para llevar a cabo eficazmente y de manera eficiente una auditoría, dependiendo de los objetivos de auditoría definidos, el alcance y criterios.

Las auditorías pueden realizarse en el sitio, de forma remota o como una combinación. El uso de estos métodos debería estar adecuadamente equilibrado, en función de, entre otros, la consideración de los riesgos y oportunidades asociados.

Si un auditado opera dos o más sistemas de gestión de diferentes disciplinas, se pueden incluir auditorías combinadas en el programa de auditoría.

Selección de los Miembros del Equipo de Auditoría

El(los) individuo(s) que gestiona(n) el programa de auditoría debería(n) nombrar a los miembros del equipo de auditoría, incluyendo el líder del equipo y cualquier expertos técnicos necesarios para la auditoría específica.

Se debería seleccionar un equipo de auditoría, teniendo en cuenta la competencia necesaria para alcanzar los objetivos de la auditoría individual dentro del alcance definido. Si solo hay un auditor, el auditor debería realizar todas las tareas aplicables de un líder del equipo de auditoría.

Asignación de Responsabilidades al Líder del Equipo Auditor para una Auditoría Individual

Las personas que gestionan el programa de auditoría deberían asignar la responsabilidad de llevar a cabo la auditoría individual a un líder del equipo de auditoría.

La asignación debería hacerse con suficiente tiempo antes de la fecha programada de la auditoría, a fin de garantizar la planificación efectiva de la auditoría.

Para que la auditoría se lleve a cabo eficazmente, se deberá proporcionar al auditor líder información sobre:

a) Objetivos de auditoría.
b) Criterios de auditoría y cualquier información documentada relevante.
c) Alcance de la auditoría, incluida la identificación de la organización y sus funciones y procesos a auditar.

Asignación de Responsabilidades al Líder del Equipo Auditor para una Auditoría Individual

d) Procesos de auditoría y métodos asociados.
e) Composición del equipo de auditoría.
f) Los datos de contacto del auditado, las ubicaciones, el marco temporal y la duración de las actividades de auditoría que se llevarán a cabo.
g) Los recursos necesarios para llevar a cabo la auditoría.
h) Información necesaria para evaluar y abordar los riesgos y oportunidades identificados para el logro de los objetivos de la auditoría.
i) Información que respalda al(los) líder(es) del equipo de auditoría en sus interacciones con el auditado para la efectividad del programa de auditoría.

Gestión de los Resultados del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían garantizar que se realicen las siguientes actividades:

a) Evaluación del logro de los objetivos para cada auditoría dentro del programa de auditoría.
b) Revisión y aprobación de informes de auditoría sobre el cumplimiento del alcance y los objetivos de la auditoría.
c) Revisión de la efectividad de las acciones tomadas para abordar los hallazgos de auditoría.
d) Distribución de informes de auditoría a las partes interesadas pertinentes.
e) Determinación de la necesidad de cualquier auditoría de seguimiento.

La persona que administra el programa de auditoría debería considerar, cuando corresponda:

- Comunicar los resultados de auditoría y las mejores prácticas a otras áreas de la organización, y las implicaciones para otros procesos.

Administrar y Mantener los Registros del Programa de Auditoría

Las personas que administran el programa de auditoría deberían garantizar que los registros de auditoría se generen, administren y mantengan para demostrar la implementación del programa de auditoría.

Los registros pueden incluir lo siguiente:

a) Registros relacionados con el programa de auditoría, tales como:

- Calendario de auditorías.
- Objetivos y alcance del programa de auditoría.
- Aquellos que abordan los riesgos y oportunidades del programa de auditoría, y los problemas externos e internos relevantes.
- Revisiones de la efectividad del programa de auditoría.

Administrar y Mantener los Registros del Programa de Auditoría

b) Registros relacionados con cada auditoría, tales como:

- Planes de auditoría e informes de auditoría.
- Evidencia de auditoría objetiva y hallazgos.
- Informes de no conformidad.
- Correcciones e informes de acciones correctivas.
- Informes de seguimiento de auditoría.

c) Registros relacionados con el equipo de auditoría que cubren temas tales como:

- Evaluación de competencia y desempeño de los miembros del equipo de auditoría.
- Criterios para la selección de equipos de auditoría y miembros del equipo y formación de equipos de auditoría.
- Mantenimiento y mejora de la competencia.

Administrar y Mantener los Registros del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían garantizar la evaluación de:

a) Si se están cumpliendo los cronogramas y si se están logrando los objetivos del programa de auditoría.

b) El desempeño de los miembros del equipo de auditoría, incluido el líder del equipo de auditoría y los expertos técnicos.

c) La capacidad de los equipos de auditoría para implementar el plan de auditoría.

d) Retroalimentación de clientes de auditoría, auditados, auditores, expertos técnicos y otras partes relevantes.

e) Suficiencia y adecuación de la información documentada en todo el proceso de auditoría.

Revisión y Mejora del Programa de Auditoría

Las personas que gestionan el programa de auditoría y el cliente de auditoría deberían revisar el programa de auditoría para evaluar si se han alcanzado sus objetivos.

La revisión del programa de auditoría debería considerar lo siguiente:

a) Resultados y tendencias del seguimiento del programa de auditoría.

b) Conformidad con los procesos del programa de auditoría e información documentada relevante.

c) La evolución de las necesidades y expectativas de las partes interesadas pertinentes.

Revisión y Mejora del Programa de Auditoría

d) Registros del programa de auditoría.

e) Métodos de auditoría alternativos o nuevos.

f) Métodos alternativos o nuevos para evaluar a los auditores.

g) Efectividad de las acciones para abordar los riesgos y oportunidades, y problemas internos y externos asociados con el programa de auditoría.

h) Cuestiones de confidencialidad y seguridad de la información relacionadas con el programa de auditoría.

Establecer Contacto con el Auditado

Es responsabilidad del auditor líder

Propósito

a) Confirmar los canales de comunicación con los representantes del auditado.
b) Confirmar la autoridad para realizar la auditoría.
c) Proporcionar información relevante sobre los objetivos, el alcance, los criterios, los métodos y la composición del equipo de auditoría, incluidos los expertos técnicos.
d) Solicitar acceso a información relevante para fines de planificación, incluida información sobre los riesgos y oportunidades que la organización ha identificado y cómo se abordan.
e) Determinar los requisitos legales y reglamentarios aplicables y otros requisitos relevantes para las actividades, procesos, productos y servicios del auditado.

Establecer Contacto con el Auditado

f) Confirmar el acuerdo con el auditado sobre el alcance de la divulgación y el tratamiento de la información confidencial.
g) Hacer arreglos para la auditoría incluyendo el cronograma.
h) Determinar los arreglos específicos de ubicación para el acceso, la salud y la seguridad, la confidencialidad u otros.
i) Acordar la asistencia de los observadores y la necesidad de guías o intérpretes para el equipo de auditoría.
j) Determinar cualquier área de interés, preocupación o riesgo para el auditado en relación con la auditoría específica.
k) Resolver problemas relacionados con la composición del equipo de auditoría con el auditado o el cliente de auditoría.

Determinación de la Viabilidad de la Auditoría

La determinación de la viabilidad debería tener en cuenta factores como la disponibilidad de lo siguiente:

a) Información suficiente y apropiada para planificar y llevar a cabo la auditoría.
b) Cooperación adecuada del auditado.
c) Tiempo y recursos adecuados para realizar la auditoría.

Realizar Revisión de Información Documentada

Debería revisarse la documentación para:

- Recopilar información para comprender las operaciones del auditado y preparar las actividades de auditoría y los documentos de trabajo de auditoría aplicables (ver 6.3.4), por ejemplo; en procesos y funciones.
- Establecer una visión general del alcance de la información documentada para determinar la posible conformidad con los criterios de auditoría y detectar posibles áreas de preocupación, como deficiencias, omisiones o conflictos.

La información documentada debería incluir, pero no limitarse a:

- Documentos y registros del sistema de gestión.
- Informes de auditoría anteriores.

La revisión debería tener en cuenta el contexto de la organización del auditado, incluidos su tamaño, naturaleza y complejidad, y sus riesgos y oportunidades relacionados. También debería tener en cuenta el alcance, los criterios y los objetivos de la auditoría.

Planificación de Auditoría

Enfoque basado en el riesgo para la planificación

El líder del equipo de auditoría debería adoptar un enfoque basado en el riesgo para planificar la auditoría con base en la información del programa de auditoría y la información documentada proporcionada por el auditado.

Al planificar la auditoría, el líder del equipo auditor debería considerar lo siguiente:

a) La composición del equipo de auditoría y su competencia general.
b) Las técnicas de muestreo apropiadas.
c) Oportunidades para mejorar la efectividad y eficiencia de las actividades de auditoría.
d) Los riesgos para lograr los objetivos de auditoría creados por una planificación de auditoría ineficaz.
e) Los riesgos para el auditado creados al realizar la auditoría.

Planificación de Auditoría

Detalles de planificación de auditoría

La planificación de la auditoría debería abordar o hacer referencia a lo siguiente:

a) Los objetivos de la auditoría.
b) El alcance de la auditoría, incluida la identificación de la organización y sus funciones, así como los procesos a auditar.
c) Los criterios de auditoría y cualquier información documentada de referencia.
d) Las ubicaciones (físicas y virtuales), las fechas, el tiempo previsto y la duración de las actividades de auditoría que se llevarán a cabo, incluidas las reuniones con la administración del auditado.

Planificación de Auditoría

Detalles de planificación de auditoría

e) La necesidad de que el equipo de auditoría se familiarice con las instalaciones y los procesos del auditado (por ejemplo, realizando un recorrido por la(s) ubicación(es) física(s), o revisando la tecnología de información y comunicación).
f) Los métodos de auditoría que se utilizarán, incluido el grado en que el muestreo de auditoría es necesario para obtener suficiente evidencia de auditoría.
g) Las funciones y responsabilidades de los miembros del equipo de auditoría, así como guías y observadores o intérpretes.
h) La asignación de recursos apropiados en base a la consideración de los riesgos y oportunidades relacionados con las actividades que se auditarán.

Planificación de Auditoría

Detalles de planificación de auditoría

La planificación de la auditoría debería tener en cuenta, según corresponda:

- Identificación del(los) representante(s) del auditado para la auditoría.
- El lenguaje de trabajo y de informes de la auditoría cuando esto es diferente del lenguaje del auditor o el auditado o ambos.
- Los temas del informe de auditoría.
- Arreglos de logística y comunicaciones, incluidos arreglos específicos para las ubicaciones que se auditarán.
- Cualquier acción específica que se tome para abordar los riesgos para alcanzar los objetivos de auditoría y las oportunidades que surjan.

Planificación de Auditoría

Detalles de planificación de auditoría

La planificación de la auditoría debería tener en cuenta, según corresponda:

- Cuestiones relacionadas con la confidencialidad y la seguridad de la información.
- Cualquier acción de seguimiento de una auditoría anterior u otra(s) fuente(es), por ejemplo.
- Lecciones aprendidas, revisiones de proyectos.
- Cualquier actividad de seguimiento de la auditoría planificada.
- Coordinación con otras actividades de auditoría, en caso de una auditoría conjunta.

Preparación del Plan de Auditoría

El plan de auditoría debería incluir:

1. Los objetivos de la auditoría.
2. El alcance de la auditoría.
3. Los criterios de la auditoría.
4. Ubicación, las fechas, el horario y la duración incluyendo las reuniones con la dirección del auditado.
5. Las funciones y responsabilidades de los miembros del equipo auditor, así como los guías y observadores.
6. La asignación de los recursos necesarios.
7. La identificación del representante del auditado.
8. El idioma.

El plan de auditoría puede ser revisado y aceptado por el cliente de la auditoría y debería presentarse al auditado.

Taller 3: Elaborar Plan de Auditoría

Taller 4: Matriz de Plan de Auditoría

Asignación de Tareas al Equipo Auditor

El líder del equipo auditor, consultando con el equipo auditor, asigna a cada miembro del equipo responsabilidad para:

- Auditar procesos.
- Actividades.
- Funciones.
- Lugares específicos.

Las asignaciones deberían considerar la necesidad de:

- Independencia y competencia de los auditores.
- El uso eficaz de los recursos.
- Diferentes funciones y responsabilidades de los auditores, auditores en formación y expertos técnicos.

Funciones y Responsabilidades de Guías y Observadores

Los guías y observadores pueden acompañar al equipo de auditoría con las aprobaciones del líder del equipo de auditoría, el cliente de auditoría y/o el auditado, de ser necesario.

No deberían influir ni interferir en la realización de la auditoría. Si esto no puede garantizarse, el líder del equipo auditor debería tener el derecho de negar la presencia de observadores durante ciertas actividades de auditoría.

Funciones y Responsabilidades de Guías y Observadores

Para los Guías sus responsabilidades deberían incluir lo siguiente:

a) Ayudar a los auditores a identificar a los individuos para que participen en las entrevistas y confirmen los horarios y las ubicaciones.
b) Organizar el acceso a ubicaciones específicas del auditado.
c) Garantizar que los miembros del equipo de auditoría y los observadores conozcan y respeten las normas relativas a los acuerdos específicos de localización para el acceso, la salud y la seguridad, el medio ambiente, la seguridad, la confidencialidad y otros asuntos, y que se aborden los riesgos.
d) Ser testigo de la auditoría en nombre del auditado, cuando corresponda.
e) Proporcionar aclaraciones o ayudar a recopilar información, cuando sea necesario.

Preparación de los Documentos de Trabajo

Los miembros del equipo auditor deben recopilar y revisar la información pertinente a las tareas asignadas y preparar los documentos de trabajo, según sea necesario, para referencia y registro de evidencias de la auditoría.

Posibles Ventajas de las Listas de Verificación

a) Aseguran que nada importante se pase por alto.
b) Ayudan a brindar continuidad a la auditoría.
c) Ayudan a planificar una auditoría eficaz.
d) Ayudan a identificar los aspectos más críticos del sistema.
e) Ayudan a controlar la profundidad, continuidad y ritmo de la auditoría.
f) Registran los hallazgos positivos y negativos.
g) Pueden proporcionar un registro de oportunidades de mejora.
h) Las listas de verificación previamente confeccionadas pueden inhibir a los auditores.
i) Los auditores pueden pasar por alto cuestiones importantes por no estar incluidas en las listas de verificación.

Uso de las Listas de Verificación

a) Considerar las listas de verificación como un ayuda memoria.
b) Evitar sentirse inhibidos por ellas.
c) Escribir prolijamente: la lista de verificación es parte del informe de auditoría.
d) Registrar conclusiones finales.
e) Registrar oportunidades de mejora.
f) Registrar identidades específicas de las muestras examinadas.

Taller 5: Elaborar una Lista de Verificación para Auditar las Clausulas Señaladas por el Instructor

Reunión de Apertura

PROPÓSITO:

a) Confirmar el acuerdo de todos los participantes (por ejemplo, auditado, equipo de auditoría) con el plan de auditoría.

b) Presentar al equipo de auditoría y sus roles.

c) Garantizar que se puedan realizar todas las actividades de auditoría planificadas.

Reunión de Apertura

PUNTOS A CONSIDERAR:

- Los objetivos, el alcance y los criterios de la auditoría.
- El plan de auditoría y otros arreglos relevantes con el auditado, como la fecha y hora de la reunión de cierre, cualquier reunión interina entre el equipo de auditoría y la administración del auditado, y cualquier cambio necesario.
- Canales de comunicación formales entre el equipo de auditoría y el auditado.
- El idioma que se utilizará durante la auditoría.
- El auditado debería mantenerse informado del progreso de la auditoría durante la auditoría.
- La disponibilidad de los recursos y las instalaciones que necesita el equipo de auditoría.
- Cuestiones relacionadas con la confidencialidad y la seguridad de la información.
- Acceso relevante, salud y seguridad, seguridad, emergencia y otros arreglos para el equipo de auditoría.
- Actividades en el sitio que pueden afectar la realización de la auditoría.

Reunión de Apertura

PUNTOS A CONSIDERAR:

La presentación de información sobre los siguientes elementos se debería considerar, según corresponda:

- El método de informar los hallazgos de la auditoría, incluidos los criterios para la calificación, si corresponde.
- Condiciones bajo las cuales puede darse por terminada la auditoría.
- Cómo tratar con posibles hallazgos durante la auditoría.
- Cualquier sistema de retroalimentación del auditado sobre los hallazgos o conclusiones de la auditoría, incluidas las quejas o apelaciones.

Revisión de la Documentación en la Auditoría

La información documentada relevante del auditado debería ser revisada para:

- Determinar la conformidad del sistema, en la medida documentada, con los criterios de auditoría.
- Recopilar información para apoyar las actividades de auditoría.

La revisión se puede combinar con las otras actividades de auditoría y puede continuar a lo largo de la auditoría, siempre que esto no sea perjudicial para la efectividad de la realización de la auditoría.

Si no se puede proporcionar la información documentada adecuada dentro del marco de tiempo dado en el plan de auditoría, el líder del equipo de auditoría debería informar tanto a la(s) persona(s) que gestionan el programa de auditoría como al auditado. Dependiendo de los objetivos y el alcance de la auditoría, se debería tomar una decisión sobre si la auditoría debería continuar o suspenderse hasta que se resuelvan los problemas de información documentada.

Comunicación Durante la Auditoría

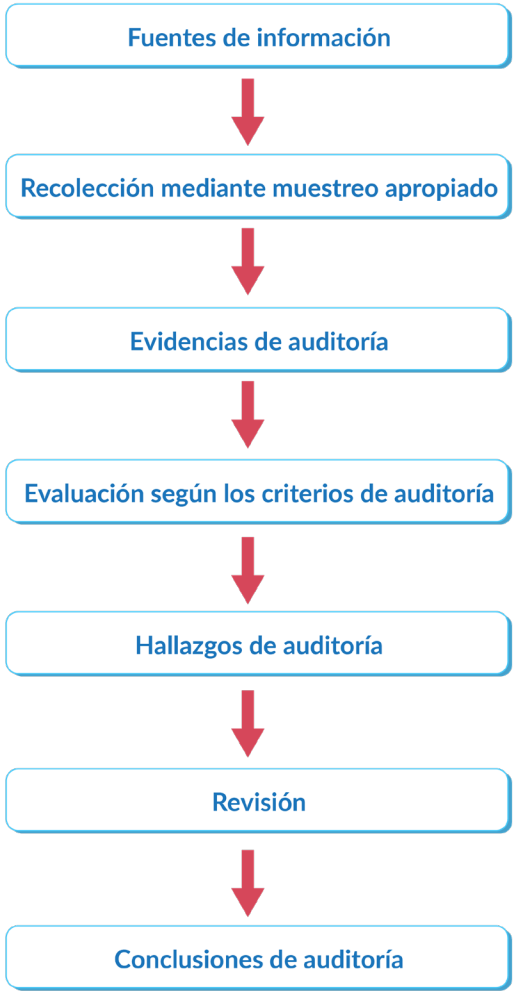
Durante la auditoría, puede ser necesario hacer arreglos formales para la comunicación dentro del equipo de auditoría, así como con el auditado, el cliente de auditoría y potencialmente con partes interesadas externas (por ejemplo, reguladores), especialmente cuando los requisitos legales y reglamentarios requieren la notificación obligatoria de incumplimiento.

- El equipo de auditoría debería consultar periódicamente para intercambiar información, evaluar el progreso de la auditoría y reasignar el trabajo entre los miembros del equipo de auditoría, según sea necesario.
- Durante la auditoría, el líder del equipo de auditoría debe comunicar periódicamente el avance de la auditoría y cualquier inquietud al auditado.
- Cuando los objetivos de la auditoría no sean alcanzables el líder del equipo auditor debería informar de las razones a las partes interesadas para tomar acciones apropiadas.
- Las acciones pueden incluir la reconfirmación o la modificación del plan, cambios en los objetivos, alcance o la interrupción de la auditoría.
- Los cambios deberían revisarse y aprobarse tanto por el gestor del programa de auditoría como por el auditado.

Métodos para Recopilar Información

- Entrevistas.
- Observación de actividades o lugares de trabajo.
- Revisión de documentos, incluyendo registros.
- Registros, tales como reportes de ocurrencias de eventos de seguridad, de mediciones de la eficacia de los controles, actas de reunión, informes de auditoría.
- Resúmenes de datos, análisis e indicadores de desempeño de incidentes de seguridad.
- Informes de otras fuentes, por ejemplo, datos de entidades reguladoras.

Métodos para Recopilar Información



Visión general de un proceso típico, desde la recopilación de información hasta llegar a conclusiones de auditoría.

La Entrevista

a) Las entrevistas deben realizarse con personas de niveles apropiados y funciones que realizan actividades o tareas dentro del alcance de la auditoría.
b) Las entrevistas deben realizarse durante el horario laboral normal y donde sea práctico, en lugar de trabajo normal de la persona que se está entrevistado.
c) Se debe tratar que la persona que se entrevista esté cómoda antes y durante la entrevista.
d) Se debe explicar la razón para la entrevista y cualquier nota que se tome.
e) Se deben resumir y revisar los resultados de la entrevista con la persona entrevistada.
f) Se debe agradecer a las personas entrevistadas por su participación y cooperación.

Preguntas Claves del Auditor

Tipo de Preguntas

- ¿Realizaron auditorías internas?
- ¿Existe una política del Sistema de Gestión?
- ¿El Sistema de Gestión ha sido comunicado?
- ¿Es usted parte del grupo auditor interno?
- ¿El proceso se ejecuta como está documentado?
- ¿En dónde registra la información?
- ¿Cuál procedimiento?
- ¿Conoce la política?
- ¿Cumple la legislación?

Ejecutando la Auditoría

- Haga un muestreo de actividades, no se centre en una.
- Busque evidencia observando lo que ocurre y revisando registros.
- Haga anotaciones completas.
- Escuche las explicaciones del auditado.
- Anote y confirme los hallazgos u observaciones. Si tiene dudas sobre el cumplimiento de un requisito podría hacer algunas preguntas abiertas adicionales.
- Siempre escriba los detalles de lo observado o evidenciado, por ejemplo, debería anotar el procedimiento auditado, los identificadores de los registros, numero de órdenes, identificación de lotes, códigos de documentos etc.
- Auditoría abierta y amigable resultará en un acuerdo de que el problema existe.
- Verifique si la No Conformidad es o no puntual.

Realización de Entrevistas

- Sea amigable.
- Haga sentir cómodo al auditado.
- Explicar las razones de la entrevista y de las notas tomadas.
- Iniciar con una descripción de las actividades.
- No realizar preguntas inductivas (Evita preguntas cuya respuesta sea SI o NO).
- Agradecer a los auditados.

¿Cómo entorpecer la Auditoría (Auditado)?

- Perdida de tiempo.
- Manejar al auditor.
- Situaciones inesperadas.
- Probar el carácter del auditor.
- Respuestas limitadas.
- Engañar al auditor.

Administración del Tiempo

- Realizar primero las actividades más complejas o difíciles.
- Asignar trabajo a los otros auditores.
- Adquirir el hábito de hacerlo de inmediato.
- Conocer curva de cansancio del auditado y auditor.
- Establecer limite de tiempo y cumplirlo.
- Ser creativo.

Manejo de Situaciones Difíciles

- A la reunión de apertura no se presenta el responsable del proceso o actividad auditada.
- En la auditoría se tenía previsto visitar dos instalaciones y no hay disponibles vehículos, ni acompañantes.
- El auditado desvía la pregunta del auditor. Ejemplo: pregunta por la forma como se controlan los documentos y el auditado explica la forma como se controlan los registros, dado que los documentos son un tipo de registro.
- El auditado suministra poca información. Ejemplo: se solicita información sobre los resultados de enero a mayo y solo presenta los resultados del último mes.
- El auditado reformula las preguntas del auditor.
- El auditado cuestiona las preguntas del auditor. Ejemplo: lo que usted pregunta no tiene sentido.
- En la reunión de apertura no hay acuerdo con el objeto y alcance de la auditoría.

Resultados de la Auditoría

Hallazgo

- Resultados de la evaluación de la evidencia objetiva recopilada frente al conjunto de políticas, procedimientos o requisitos utilizados como referencia.

- Es registrado en la lista de verificación como respuesta a los cuestionamientos que han sido preparados.

Tipos de Hallazgos

- **No conformidad**

Incumplimiento de un requisito especificado.

- **Observación**

Situación que potencialmente puede afectar el sistema de gestión.

Incumplimientos más Comunes

- Documentación no encontrada.
- Competencias de recurso humano no evaluada.
- Controles implementados inadecuados.
- No conformidades por auditorías internas sin cierre eficaz.
- Acciones correctivas sin revisión de la dirección.
- Deficiencia en metodología de análisis de riesgo.
- Incumplimiento de procedimientos.

Redacción de las No Conformidades

- **La Evidencia**

Lista de hallazgos, respaldados con evidencias objetivas o atestiguadas por el auditado.

- **La Referencia**

Al requisito de la norma y/o manual de calidad o procedimiento. Un requisito a la vez, el que más aplica.

- **La Conclusión**

Genérica, breve, precisa y aceptada por el auditado.

Redacción de las No Conformidades

No Conformidad: Incumplimiento a un requisito de la Norma auditada.

Observación: Hallazgo detectado en Auditoría que podría generar una no conformidad si no es tratado.

Oportunidad de Mejora: Son situaciones que no representan incumplimiento, pero pueden ser revisadas por la organización, cuando lo estime conveniente para mejorar la eficacia del proceso.

Fórmula de Redacción de No Conformidades

Reporte debe contener como mínimo:

- Una visión general del hallazgo.
- Descripción completa y precisa de lo observado.
- Ejemplos de la evidencia de auditoría.
- Referencia a la cláusula del estándar/documento de la organización.
- Explicación de los requisitos de la cláusula/documento.
- Las discrepancias deben atribuirse solamente a una cláusula de la norma, la más aplicable.
- En ocasiones, la única referencia es la documentación de la organización.

Conclusiones de Auditoría

El equipo auditor debe reunirse antes de la “reunión de cierre” para:

- Revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma.
- Acordar conclusiones de auditoría.
- Preparar recomendaciones, si así lo especifica el plan de auditoría.

Las conclusiones de auditoría pueden tratar aspectos como:

- Evaluación del grado de cumplimiento con el criterio de auditoría.
- Eficacia de la implementación, mantenimiento y mejoras del sistema de gestión.
- Capacidad del proceso de revisión por la dirección para asegurar la adecuación, eficacia y mejora sostenida del SGSI.

Informe de Auditoría

Debería contener:

- Objetivos de la auditoría.
- Alcance de la auditoría, particularmente la definición de las unidades de la organización o de los procesos auditados y el período de la auditoría.
- Documentación de la persona de contacto.
- Documentación del auditor líder y otros auditores.
- Fechas y ubicaciones donde se desarrollaron las actividades de la auditoría.
- Criterio de auditoría.
- Declaraciones de auditoría.
- Conclusiones de la auditoría.

Reunión de Cierre

Es facilitada por el auditor líder.

Según corresponda, lo siguiente debería explicarse al auditado en la reunión de clausura:

a) Informar que la evidencia de auditoría recopilada se basó en una muestra de la información disponible y no es necesariamente representativa de la eficacia general de los procesos del auditado.
b) El método de informar.
c) Cómo debería abordarse la conclusión de la auditoría en función del proceso acordado.
d) Posibles consecuencias de no abordar adecuadamente los hallazgos de la auditoría.
e) Presentación de los hallazgos y conclusiones de auditoría de tal manera que la gerencia del auditado los comprenda y los reconozca.
f) Cualquier actividad posterior a la auditoría relacionada (por ejemplo, implementación y revisión de acciones correctivas, tratamiento de quejas de auditoría, proceso de apelación).

Preparación y Distribución del Informe de Auditoría

El líder del equipo auditor debería informar las conclusiones de la auditoría de acuerdo con el programa de auditoría.

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

a) Objetivos de auditoría.
b) Alcance de la auditoría, particularmente identificación de la organización (el auditado) y las funciones o procesos auditados.
c) Identificación del cliente de auditoría.
d) Identificación del equipo de auditoría y los participantes del auditado en la auditoría.

Preparación y Distribución del Informe de Auditoría

e) Fechas y lugares donde se llevaron a cabo las actividades de auditoría.
f) Criterios de auditoría.
g) Hallazgos de auditoría y evidencia relacionada.
h) Conclusiones de auditoría.
i) Una declaración sobre el grado en que se han cumplido los criterios de auditoría.
j) Cualquier opinión divergente no resuelta entre el equipo de auditoría y el auditado.
k) Las auditorías por naturaleza son un ejercicio de muestreo; como tal, existe el riesgo de que la evidencia de auditoría examinada no sea representativa.

Preparación y Distribución del Informe de Auditoría

El informe de auditoría debería emitirse dentro del tiempo acordado. Si se retrasa, los motivos deberían comunicarse al auditado y a la(s) persona(s) que gestionan el programa de auditoría.

El informe de auditoría debería estar fechado, revisado y aceptado, según corresponda, de conformidad con el programa de auditoría.

El informe de auditoría debería distribuirse a las partes interesadas pertinentes definidas en el programa de auditoría o el plan de auditoría.

Al distribuir el informe de auditoría, se deberían considerar medidas apropiadas para garantizar la confidencialidad.

Preparación y Distribución del Informe de Auditoría

La auditoría se completa cuando se han llevado a cabo todas las actividades de auditoría planificadas, o según se acuerde con el cliente de auditoría (por ejemplo, puede haber una situación inesperada que impida completar la auditoría de acuerdo con el plan de auditoría).

La información documentada relativa a la auditoría debería conservarse o eliminarse por acuerdo entre las personas participantes y de acuerdo con el programa de auditoría y los requisitos aplicables.

A menos que lo exija la ley, el equipo de auditoría y las personas que gestionan el programa de auditoría no deberían divulgar ninguna información obtenida durante la auditoría, o el informe de auditoría, a ninguna otra parte sin la aprobación explícita del cliente de auditoría y, cuando corresponda, la aprobación del auditado.

Las lecciones aprendidas de la auditoría pueden identificar riesgos y oportunidades para el programa de auditoría y el auditado.

Realización de Seguimiento de Auditoría

El resultado de la auditoría puede, dependiendo de los objetivos de la auditoría, indicar la necesidad de correcciones o de acciones correctivas u oportunidades de mejora. Tales acciones generalmente son decididas y llevadas a cabo por el auditado dentro de un plazo acordado. Según corresponda, el auditado debería mantener informadas a las personas que gestionan el programa de auditoría y/o al equipo de auditoría sobre el estado de estas acciones.

La finalización y efectividad de estas acciones debería ser verificada. Esta verificación puede ser parte de una auditoría posterior. Los resultados se deberían informar a la persona que gestiona el programa de auditoría y se informa al cliente de auditoría para su revisión por la dirección.

Las Auditorías de Seguimiento

Responsabilidades del auditor:

- Acordar la fecha de la auditoría de seguimiento.
- Desarrollar la auditoría de seguimiento de acuerdo con las acciones correctivas y preventivas.
- Presentar e informar los resultados de la auditoría de seguimiento.
- Evaluar la eficacia de las acciones correctivas implantadas.

Taller 6: Según el Formato, Realizar el Informe de Auditoría

¡Síguenos, ponte en contacto!

www.certiprof.com